



Technical Study on Smart Borders

Final Report

Written by PwC
October - 2014



EUROPEAN COMMISSION

Directorate-General for Home Affairs
Directorate C— Schengen
Unit C.3 — Transeuropean Networks for Freedom and Security and Relations with eu-LISA

Contact: Marc SULON

E-mail: HOME-SMART-BORDERS@ec.europa.eu

*European Commission
B-1049 Brussels*

Technical Study on Smart Borders

Final Report

***Europe Direct is a service to help you find answers
to your questions about the European Union.***

Freephone number (*):

00 800 6 7 8 9 10 11

(* The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2014

ISBN

doi:

© European Union, 2014

Reproduction is authorised provided the source is acknowledged.

Revisions

Date	Release	Notes
15/04/2014	v.3.0 Snapshot report	The very first version of the report.
30/04/2014	v.5.1	Enhanced version of Snapshot report.
15/05/2014	v.8.0 Inception report	The first version of Inception report.
05/06/2014	v.9.0 Inception report	The second version of Inception report.
10/06/2014	Chapters 3 and 4	Enhanced version of chapters 3 and 4 to MS review.
16/06/2014	v.9.5 Snapshot report	The main amendments of this version are provided in the processes, architecture and statistics chapters. The assessments of legislative proposal compliance have been added to the processes, biometrics and data chapters.
20/06/2014	v.10.0 Inception report	The third (final) version of Inception report. This version contains the results of investigations on the Thematic Files 1, 2, 3, 4, 9, 10, 11, 12 and 14, and addresses the comments received on the previous versions (8.0 and 9.0).
30/06/2014	v.11.0 Draft final report	The first version of Draft final report. It addresses all the Thematic Files.
15/07/2014	v.12.2 Draft final report	The second version of Draft final report which addresses the comments received on the version 11.0.
17/07/2014	v.12.3 Draft final report	The update of v.12.2.
12/08/2014	v.13.0 Draft final report	The third version of Draft final report which addresses the comments received on the version 12.3.
15/08/2014	v.14.0 Final report	The first version of Final report.
15/09/2014	v.15.0 Final report	The second version of Final report.
19/09/2014	v.16.0 Final report	The update of v.15.0
10/10/2014	v.17.0 Final report	The third version of the Final report.

Table of Contents

Executive Summary	Error! Bookmark not defined.
1. Introduction	13
1.1 Objective	26
1.2 Scope	27
2. Methodological approach	29
2.1. Overall approach	29
2.2. Analysis criteria	30
2.3. Options analysis	31
2.4. Basic assumptions	32
2.5. Relevant sources of law	36
3. EES and RTP - Border Control Processes	38
3.1. Context	39
3.1.1. Border processes today	40
3.2. The EES process (TF4.1, TF6.1, TF6.2 and TF8.1)	41
3.2.1. Overview of EES	42
3.2.2. Process description	43
3.3. The RTP process (TF4.1, TF7.1, TF7.2, TF8.2)	57
3.3.1. Overview of RTP	57
3.3.2. Process description for application/enrolment process	59
3.3.3. Process description at entry and exit	66
3.3.4. Consultation of the RTP database (TF 7.3)	70
3.3.5. Alternative options to the token (TF10)	71
3.3.6. Identification of the possible interactions between EES and RTP (TF7.4)	74
3.3.7. Consulting the EES in the VIS application process	75
3.4. Impact of EES and RTP	75
3.4.1. Impact on Border Crossing Points crossing time, security and complexity (TF5)	76
3.4.2. Impact on average border crossing time for TCNs and general impact on queues at entry and exit (TF 5.3 and TF 5.4)	85
3.4.3. Impact on the resources of Border Crossing Points (TF 5.5)	88
3.4.4. Impact in relation to Local Border Traffic (TF 4.4)	89
3.4.5. Impact in relation to residence permits in EES and RTP (TF4.3)	93
3.4.6. Variations for air, land and sea borders (TF4.2/TF8.3)	95
3.5. Process accelerators	106

<u>3.5.1. Decreasing the average crossing time (TF9.1)</u>	106
<u>3.5.2. Organisation of Border Crossing Points (TF9.2)</u>	113
<u>3.5.3. Minimising the number of documents used (TF9.3)</u>	115
<u>3.5.4. Process automation (TF8.4)</u>	116
<u>3.5.5. Using iris as an accelerator</u>	117
<u>3.5.6. Process Accelerators – summary</u>	118
<hr/>	
<u>3.6. The RTP process – alternative proposal</u>	119
<u>3.6.1. Overview of the RTP (alternative)</u>	119
<u>3.6.2. Consequences for the report</u>	122
<hr/>	
<u>3.7. Smart borders: EES and RTP summary of options</u>	123
<u>3.7.1. EES</u>	124
<u>3.7.2. RTP (entry –exit)</u>	137
<u>3.7.3. Main general recommendations for successful implementation of EES and RTP (processes)</u>	139
<hr/>	
<u>3.8. Compliance with the EES legislative proposal and with other legal instruments</u>	141
<u>3.9. Compliance with the RTP legislative proposal and with other legal instruments</u>	146
<hr/>	
<u>4. Use of biometric characteristics</u>	149
<hr/>	
<u>4.1. Objectives, approach and structure of this chapter</u>	149
<u>4.1.1. Objectives</u>	149
<u>4.1.2. Approach</u>	149
<u>4.1.3. Structure</u>	150
<hr/>	
<u>4.2. Context</u>	150
<u>4.2.1. Biometric characteristics related to the EES and RTP</u>	150
<u>4.2.2. Sources used for the TF analysis</u>	153
<hr/>	
<u>4.3. TF analysis</u>	154
<u>4.3.1. Evaluation factors that contribute to the TF analysis</u>	154
<u>4.3.2. Observations related to these factors</u>	156
<hr/>	
<u>4.4. Biometric characteristics in the EES (TF1)</u>	159
<u>4.4.1. Number of fingerprints to be used (TF1.1)</u>	159
<u>4.4.2. EES and RTP biometric options capturing fingerprints (TF1.2)</u>	163
<u>4.4.3. Synergies with other systems (VIS, RTP) (TF1.3)</u>	166
<u>4.4.4. Impact of the use of the biometric identifier on the border control process as well as on enrolment time (incl. degraded mode) (TF1.4)</u>	167
<u>4.4.5. Use of facial recognition in combination with the use of fingerprints (TF1.5)</u>	169
<u>4.4.6. Facial image/fingerprints possibly captured from the travel document (TF1.6)</u>	170
<hr/>	
<u>4.5. Biometric characteristics in RTP (TF2)</u>	172
<u>4.5.1. Biometric identifier(s) to be used for RTP (TF2.1)</u>	172
<u>4.5.2. Impact of the use of biometric identifier(s) on the border control process (TF2.2)</u>	176
<u>4.5.3. How and when to capture them? (TF2.3)</u>	176
<u>4.5.4. Synergies with other systems recording biometrics, Visa information System (VIS) and EES (TF2.4)</u>	176
<u>4.5.5. Impact of the use of biometric identifiers on the border control process including the degraded mode (TF2.5)</u>	177

4.6. Transition period (TF3)	178
4.6.1. Broad analysis of possible options	178
4.6.2. Advantages and disadvantages of an alphanumeric-only EES transition period (TF3.1)	182
4.6.3. Consequences of having an EES transition process without biometric identifiers (TF3.2)	183
4.6.4. Advantages and disadvantages of a phased approach (TF3.3)	184
4.7. Data protection considerations	185
4.7.1. Extension of the use of biometric characteristics for identification purposes to all TCNs	185
4.7.2. Main options analysed	186
4.7.3. Use of fingerprints only, for both EES and RTP	191
4.7.4. Use of facial images only	191
4.7.5. Combined use of fingerprints and facial images, for both EES and RTP	192
4.8. Impact of the different options on legislative proposals and relevant legislation in force	193
5. Data	196
5.1. Context	196
5.2. Minimum dataset required to fulfil the EES and RTP objectives (TF11.1)	196
5.2.1. Dataset foreseen by the EES legislative proposal	198
5.2.2. Proposal of a data model for EES and RTP	198
5.2.3. EES minimum dataset	200
5.2.4. Analysis of the candidate data sources for EES	204
5.2.5. Dataset outlined in the RTP legislative proposal	206
5.2.6. EES and RTP data management	207
5.2.7. Identification of the biometric identifier(s)	211
5.3. Retention period (TF12)	214
5.3.1. RTP and EES data retention as per the legislative proposals	214
5.3.2. Alternative options in case of EES and RTP as separate systems	218
5.3.3. Considerations regarding data retention in the case of a single system	224
5.3.4. Considerations regarding coherence with VIS data retention	226
5.4. Law Enforcement Access (TF13)	228
5.4.1. Analysis of statistics concerning LEA to VIS (TF 13.1)	228
5.4.2. Definition of the data required for LEA to the EES (TF 13.3)	230
5.4.3. Technical consequences of LEA (TF 13.2, 13.5)	234
5.4.4. Impact of LEA on the border control process (TF 13.4)	237
5.5. Output of EES and RTP systems (TF14)	237
5.5.1. EES/RTP System outputs – information to be provided to the border guards	238
5.5.2. EES/RTP System outputs – information to be provided to the travellers	238
5.5.3. EES and RTP system(s) outputs – information to be provided to the carriers	243

5.6. Data protection considerations on the options brought forward by the Study	245
5.6.1. Minimum dataset	245
5.6.2. Further processing of data	246
5.6.3. Balance between system integration and data protection	246
5.6.4. Law enforcement access	247
5.7. Impact on legislative proposals and relevant legislation in force	247
5.8. Summary	250
<hr/>	
6. Architecture	254
<hr/>	
6.1. Context	255
6.1.1. Expectations, needs and capabilities	255
6.1.2. Link to the EES and RTP processes	257
6.1.3. Broader issues to be taken into account	265
6.1.4. High-level requirements	265
6.1.5. Architecture building blocks	267
<hr/>	
6.2. General architecture	270
6.3. EES and RTP: single or separate systems (TF11.2, TF15)	273
6.3.1. <i>Comparison of EES and RTP data sets (TF11.2)</i>	273
6.3.2. <i>Option 1: two separate systems (TF15.1.1)</i>	276
6.3.3. <i>Option 2: a single system (TF15.1.2)</i>	279
6.3.4. <i>Comparison of the two options (TF15.2)</i>	282
<hr/>	
6.4. EES, RTP and VIS: independent or integrated (TF 16)	282
6.4.1. <i>Comparison and synergies of EES, RTP and VIS (TF16.1, TF16.2)</i>	282
6.4.2. <i>Option 1: EES and RTP independent from VIS</i>	284
6.4.3. <i>Option 2: EES and RTP integrated with VIS</i>	287
6.4.4. <i>Option 3: Progressive approach: re-using VIS artefacts allowing further synergies</i>	292
6.4.5. <i>Common SOA-based BMS (TF16.4)</i>	295
6.4.6. <i>Comparison of the options</i>	297
<hr/>	
6.5. Interaction with other IT systems (TF17)	297
6.5.1. <i>Other IT systems used for the Border Control Processes (TF17.1)</i>	297
6.5.2. <i>Potential interaction and dependencies between the systems (TF17.2, TF17.3)</i>	299
6.5.4. <i>Consultation mechanism between authorities (TF17.4)</i>	305
<hr/>	
6.6. Re-use and integration of existing national systems (TF18)	305
6.6.2. <i>Possibilities to re-use or integrate the existing systems with EES and RTP (TF18.1, TF18.3)</i>	306
6.6.3. <i>Data aggregation (TF18.4)</i>	307
6.6.4. <i>Definition of the common interface (TF18.2)</i>	308
<hr/>	
7. Statistics and forecasts	322
<hr/>	
7.1. Statistics on visas issued	323
7.2. Data collection from the MS in 2014	324
7.2.1. Overview of data collection exercise	324
7.2.2. Outcome of the one-week data collection	325

7.3. Extrapolations and forecasts	329
7.3.1. Extrapolation from one-week values to yearly values	329
7.3.2. Estimation of growth rate for the forecasts	331
7.3.3. Outcome and summary of key forecasts for 2020/2025	333
7.3.4. Estimation of the number of individual files	335
7.3.5. RTP demand estimation	338
<hr/>	
8. Conclusions	341
<hr/>	
8.1. Introduction	341
8.2. EES TOMs A, B and C	348
8.2.1. Overview	349
8.2.2. Estimated durations, security and complexity by each TOMs	350
8.2.3. Evaluation of the TOMs for the EES (A, B and C)	355
<hr/>	
8.3. RTP TOMs M and N	358
8.3.1. Overview	358
8.3.2. Simulations results related to RTP	360
8.3.3. Summary of the TOMs for the RTP (M and N)	360
<hr/>	
9. Options for the Pilot	363
Appendix A. - List of abbreviations	369
Appendix B. - Glossary	372
Appendix C. - Reference documents	375
Appendix D. - Biometrics overview	378
<hr/>	
D.1. Introduction to biometrics	378
D.2. Introduction to electronic passports	381
D.3. Security features to protect biometric data in e-Passports	381
D.3.1. Summary of e-passport logical security mechanisms	381
D.3.2. Logical security mechanisms of e-passports	384
<hr/>	
D.4. Security analysis	389
D.4.1. Security	390
<hr/>	
D.5. Role of biometrics in existing systems	397
D.6. NIST biometric evaluations	398
D.6.1. Fingerprint	398
D.6.2. Face	398
D.6.3. Iris	398
D.6.4. Multiple Biometrics	398
<hr/>	
D.7. Further references	399
<hr/>	
Appendix E. - Case Law	400

Appendix F. - Exceptions	402
F.1. Handling exceptions at entry and exit	402
F.1.1. EES Check	402
F.1.2. EES Entry-exit	404
F.2. Handling exceptions – RTP enrolment	406
F.2.1. RTP entry-exit	408
Appendix G. - Assessment tables for the technical options for the Pilot	410
Technical options for the use of data and biometrics	410
Appendix H. - Overview of the relevant existing systems	412
H.1.1. Visa Information System (VIS)	412
H.1.2. Schengen Information System (SIS II)	414
H.1.3. National border control initiatives	415
Appendix I. - Thematic Files	417
Appendix J. - Simulations border control processes	421
J.1. Simulation of air borders	423
J.1.2. Summary of the results – air borders	427
J.2. Simulation of land borders	432
J.2.2. Summary of the results – land borders	432
J.2.3. Summary of the results – RTP	436
Appendix K. - Topics for further studies	440

Executive Summary

The “**Smart Borders Package**” was proposed by the Commission in February 2013. It follows the European Commission (EC) Communication of February 2008 suggesting the establishment of an Entry/Exit System (EES) and a Registered Traveller Programme (RTP). The Smart Borders Package is constituted of three legislative proposals. It aims to improve the management of the external borders of the Schengen Member States (MS), fight against irregular immigration and provide information on overstayers, as well as facilitate border crossings for pre-vetted frequent third country national (TCN) travellers.

During the first examination of the Smart Borders Package, which was completed in February 2014, the Council and the European Parliament (EP) voiced technical, operational and cost concerns, mainly related to the **overall feasibility of the proposed new systems** and of some of their features. Concerns related especially to the impact on the actual border control process, the RTP token, the data retention period in the EES, the choice of biometric identifiers, the extent to which national Entry/Exit Systems could be integrated and/or reused, the need for enhanced synergies and/or interoperability with existing border control systems, and the possibility for law enforcement authorities to access the EES.

In order to further assess the technical, organisational and financial impacts of the various possible ways to address these issues, the Commission subsequently initiated – with the support of both co-legislators – a **proof of concept** exercise aimed at identifying options for implementing the Smart Borders package. This exercise consists of two stages:

1. A Commission-led **Technical Study** (this report) aimed at **identifying** and **assessing** the most suitable and promising **options and solutions**. Based on this Study, the options and solutions to be tested through a pilot project should be identified by the end of 2014.
2. A Pilot project to be entrusted to the Agency for the Operational Management of large-scale IT Systems in the area of Freedom, Security and Justice (eu-LISA), aimed at verifying the feasibility of the options identified in the Technical Study and validating the selected concepts for both automated and manual border controls.

This Study addressed a series of questions raised in 20 Thematic Files (TFs) that were jointly **agreed between the EC’s Directorate General for Home Affairs (DG HOME), the MS and EP representatives** in February 2014. These questions focused on six domains:

- | | | |
|---------------|-----------------------------|-------------------------|
| 1. Statistics | 3. Border control processes | 5. Architecture |
| 2. Biometrics | 4. Data | 6. Costs ¹ . |

The Study’s methodological approach was primarily based on stakeholders’ consultations through workshops, phone interviews and feedback from MS on the draft deliverables. The stakeholders consulted included MS, the EP, the European Data Protection Supervisor (EDPS), DG HOME, DG Justice (DG JUST), DG Taxation and Customs Union (DG TAXUD), eu-LISA, Frontex and representatives from industry.

The Study also built upon extensive desk research, literature review and various on-site visits. In addition, a specific data collection survey was carried out at the external borders of the Schengen Area by the MS at the end of May 2014. This survey allowed collecting up-to-date quantitative data concerning border crossings, including their number and type (air, land and sea), and the

¹ The cost analyses are presented in separate report.

categories of travellers (i.e. EU/EEA/CH - abbreviated as EU-citizens, third country nationals either visa-exempt (TCN**VE**) or visa holders (TCN**VH**)).

The Study explored numerous options in relation to biometrics, border control processes, data, architecture and costs, to cover all aspects of the 20 TFs and **find the optimal design for the EES and RTP**. In order to present feasible combinations of the activities (e.g. enrolment for EES individual file, EES biometric verification, identification) and the choices to be made to effectively operate the EES and RTP, the concept of potential **Target Operating Model (TOM)** was introduced. Each TOM is unique and corresponds to a possible hypothetical scenario (assembly of system components into a consistent set) for the implementation of the future systems.

An overview of each domain addressed in the TFs is provided below. A summary of the suggested TOMs and options for the Pilot are presented at the end of this Executive Summary.

Biometrics

The Study analysed in detail the use of biometric characteristics as a means to **enhance** and strengthen **identity checks** at external borders, and the overall **security of border controls**. The advantages, drawbacks and specificities derived from the use of biometric characteristics for the EES and RTP were looked at.

The Study evaluated the number of fingerprints (FPs) to be used, the different options to capture FPs and possible **synergies with other systems**. In addition, it explored the use of facial image (FI) recognition either as standalone biometric or in combination with FPs. The use of iris was also considered.

Concerning the number of FPs to be used **for verification and identification**, the Study observed that 1 FP alone can be used for verification. A higher number of FPs enrolled leads to a better performance in terms of accuracy (for both identification and verification) and processing time. Yet, it may lead to problems at certain borders. In particular, taking into account the difficulty of capturing more than 4 FPs at land borders where limitations in enrolment quality and time may rise regarding the travellers in vehicle and use of hand-held equipment². The Study considers the use of 4 FPs for EES and RTP as an approach that will facilitate synergies with the Visa Information System (VIS). The Study also suggests adding the enrolment of 4 and 8 fingerprints to the Pilot as one of the test cases involving ABC gates, hand-held equipment and self-service kiosks.

The Study also highlighted that if FI would be used in **combination with FPs**, then it has a **beneficial impact** on both **verification** and **identification** in terms of **speed** and **security** leading to **lower false rejection rate and reduction** in number of **FPs** enrolled.

Concerning the introduction of **FI** as a biometric characteristic, the Study concludes that the use of FI alone is an option to be considered for EES and RTP.

The inclusion of FI as a biometric identifier should also be seen in the light of the current ABC gates that mostly handle FI recognition.

While the FI can be taken from the electronic machine readable travel document (e-MRTD³) relatively easily, the FPs are impossible to access as long as there is no efficient and constraining mechanism for distributing the secret cryptographic keys used (so-called Extended Access Control for Terminal Access) at an international level (To this end, a shared certificate masterlist at European or Schengen level for exchange of certificates for cryptographic processing is recommended). For this reason and also because the inclusion of only two FPs in the electronic passport is optional, the Study suggests not relying solely on FPs taken from the e-MRTD.

For the RTP, the Study assessed the possible use of FI only to facilitate border crossings for frequent travellers. Three possible options were investigated:

1. use of **FI only**;

² In any case, all FP-capturing devices should satisfy international security standards (FBI, LivDet and ISO 15408) for anti-spoofing purposes.

³, i.e. 'chip passport' or 'electronic passport'

2. use of **FI** combined with a reduced number of **FPs** (the same or a subset of EES and/or VIS);
3. use of **no biometric data** at all.

Finally, the Study explored different options for introducing a **transitional period** for the use of biometrics in the EES as foreseen in the 2013 legislative proposal. Two main options were assessed:

- No use of biometric data in the EES during the transitional period. The system would rely instead on the alphanumeric data of the travel documents, and the use of biometric characteristics would only be introduced after the transition period. A variant would consist in using the photo in the e-MRTD during the transition period.
- Inclusion of biometric characteristics in the EES from the start by MS that are ready, with the other MS joining progressively so as to reach full implementation by a target date. This phased approach was used for the VIS.

The choice of one or the other option depends on whether the equipment installed at the border crossing points to perform FP verifications of visas (which become mandatory from 10 October 2014) will also be capable of enrolling 4 FPs. If the answer is positive, then the EES and RTP could be implemented without changes of FP scanners at the borders. In the opposite case, this implementation would become more time-consuming and costly. To clarify the situation, the pilot project should include actions aimed at assessing various possibilities for enrolling or verifying FPs.

For instance, an option is the mandatory enrolment of fingerprints following a given period. An alternative would be to make the most of using the photo in the e-MRTD and/or managing verification of the identity without biometrics for a certain period.

Border Control Processes – impact, alternatives and accelerators

The Study identified and assessed potential future border crossing processes for the EES and RTP, including a number of feasible options. The analysis focused on:

1. Estimating the **duration impact** of the new or modified activities of entries and exits for the various categories of travellers due to the implementation of EES and RTP mainly by:
 - minimising the data needed for EES first entry registration;
 - maximising the use of VIS data and biometrics (for TCNVHs) for both the EES and the RTP;
 - facilitating border control operations by maximising the use of e-MRTDs (as they are a reliable source of information);
 - analysing whether to include local border traffic permit holders and residence permit holders into the EES and RTP.
2. Proposing an **alternative application process** for the RTP that could limit the additional resources needed at MS level for dealing with RTP applications;
3. Highlighting **process accelerators** to speed up border crossing times.

Duration impact on border control processes

The Study outlined in detail the future processes for the border crossing of TCNs at entry (first and subsequent) and at exit by TCNVH, TCNVE and registered traveller.

The main variables impacting the border crossing time are the **data and biometrics** used in each step of the border control process, so, the data used throughout the processes are studied.

The **photo** stored in **e-MRTDs** is of high quality and the Study suggests using it as much as possible. The Machine Readable Zone (MRZ) and the visa number were found to be a sufficient set

of alphanumeric data for the purpose of the **EES individual file**, and do not make the border control process longer. The unique key composed by the issuing country together with the document number is sufficient to retrieve the EES individual file.

For the entry/exit records, additional optional data could be useful for immigration control and law enforcement purposes, however, this would add to the duration of the border crossing as these data would have to be collected manually.

For reasons of travellers' convenience and to ensure synergies with the VIS, the Study recommends that biometric characteristics be **captured only once**. Hence, for TCNVHs it is recommended to rely on the VIS biometrics as regards the EES and RTP. For TCNVEs, biometric characteristics used for the RTP should mirror the ones stored in the EES. This synergy is important as the first time enrolment of FPs would be limited to TCNVEs since TCNVHs would not need to enrol FPs a second time after having done so to obtain their visa.

Use of a the e-MRTD as a token for the RTP

In order to speed up border crossing times, **travellers with RTP status** could use ABC gates, where possible, and be verified using a live photo checked against the e-MRTD or fingerprints/photo checked against the central system.

To this end, the Study analysed the pros and cons of using a separate token to prove RT status or, as an alternative, **the use of the e-MRTD as a token**. The Study concluded that a separate token would provide no added value and would add operational complexity, whereas using the e-MRTD would be less costly and less complex to implement and maintain, while providing the necessary security level and not impacting the border crossing time.

The use of MRTDs as tokens by registered travellers was also examined, and the Study came to the conclusion that the MRTD would not work well in any existing or planned ABC gates since these normally require an e-MRTD for security reason. RTs with an MRTD would therefore only be able to use manual gates. However, using MRTDs at manual gates would not make it possible to reach the same security level in document check and bearer authentication as with e-MRTDs. Moreover, the use of EU/EEA/CH lanes by RTs with MRTDs could possibly adversely impact the duration for EU citizens by slowing down the crossings at this lane, because of the manual (ocular) inspection needed.

Variations between air, land and sea borders

General conditions are not the same today at air, sea and land borders and they also differ at each specific Schengen border crossing point. For instance, RTP travellers would be able to use ABC gates mainly at air borders, and the facial image can only be taken from an **e-MRTD** to verify or enrol the traveller where e-MRTD readers are in use.

The assessment of the duration impact was supported by the simulation of **real data** from border crossing points processing tools developed by Frontex. The simulations of an average and a large air border allowed demonstrating that an added duration below 60 seconds at first entry would have very limited impact on service level and average dwelling time, and that an added duration below 30 seconds would have practically no impact. With an additional 60 seconds, the service level would still not be impacted but there would progressively be a slow increase of dwelling time and workload.

The simulation of a land border demonstrated the impact to be more important. To limit adverse effects on service level and dwelling time, the added duration should preferably remain below 60 seconds per vehicle. To have minimal adverse effects the limit to the added duration should be set at 30 seconds per vehicle.

The Study also looked into the practical terms and constraints of enrolling biometrics at various borders. While enrolling 8 or 10 fingerprints seems challenging at all types of border crossings and in various types of conditions, state-of-the-art mobile technology is already available today, which enables the enrolment of a minimum of 4 fingerprints using handheld equipment.

Local border traffic permit holders and residence permit holders

In addition, the Study looked at the opportunity of including in the scope of EES or RTP local border traffic (LBT) permit holders (who currently account for up to 10 million border crossings per year at land borders, i.e. +/- 3% of the total) and residence permit holders (currently around 6 million EU and national long-term residence permit holders cross the border every year in total, i.e. +/- 2% of the total). Three options were assessed:

- unchanged procedure for LBT and residence permit holders;

- registration of LBT and residence permit holders in the EES;
- registration of LBT and residence permit holders in the RTP.

The Study concluded that the added value of including LBT and residence permit holders within the EES would not outweigh the disadvantages, such as longer duration of border crossing or mandatory registration of EU family members in the EES. Therefore, it recommends **not to register** LBT and residence permit holders in the EES.

Their enrolment in the RTP, on the other hand, was deemed to be a viable option. Their registration would be made on the same basis as for any other TCN. A same person could then have both a LBT permit to facilitate travel in a border area and an RT status to facilitate checks at any other Schengen border crossing. The registration of residence permit holders in the RTP was considered as possible provided a specific enrolment process is defined and their entries and exits are not recorded in EES.

Alternative application process for the RTP

The Study presents an alternative proposal for the RTP process, where registration in the EES would be a prerequisite to apply for RTP status. The application for RTP member status could then be simplified and made online, which would reduce the workload at consular posts, common application centres and external crossing points. The system would thus not store its own set of biometric data, but would rely on EES and VIS biometrics. The Target Operating Model (TOM) N represents this alternative process for the RTP, which should be further analysed if considered a feasible option.

Use of process accelerators to speed up border crossing times

Several innovative approaches were analysed and assessed with a view to accelerate the border control process. They include gathering information from transport companies before arrival (e.g. Advance Passenger Information- API), enabling traveller self pre-registration before the border check, extending the EES data retention period to decrease the number of registrations of the individual file in the EES, minimising the number of documents used (e.g. maximise the use of the e-MRTD), as well organisational measures (e.g. separate TCNVE and TCNVH lanes, use of ABC gates for TCNs at exit).

Pre-border registration/checks could have a very positive impact on border crossing times, mainly at international airports and large land border crossings (rail or road) or ferry/cruise ship terminals. It would also make it possible to release a share of the border guards from manual processing. If such pre-border registration/checks were to be implemented, however, actions such as supervision of the self-registration kiosks would be required, which could be implemented for all TCNs (and not only RTs).

Another potential accelerator would be to minimise the number of documents used, in particular by removing the need for a separate token for the RTP and relying only on the e-MRTD as the token (as described at the beginning of this section).

Data – 26 items as minimum dataset for EES and RTP

A direct consequence of the introduction of EES and RTP will be that the manual stamping of the TCN passports will disappear and will be replaced by the creation of Entry/Exit records in the systems. This new situation will impact amongst others:

- the work of the border guard who will not have any more the possibility to see the stamps corresponding to Schengen border crossings that occurred in the past,
- the TCN travellers as they will not have any more the possibility to calculate the maximum number of day for authorised stay in the Schengen area,
- the carriers that will not have any more the possibility to check on the passport if a visa was already used.

The Study identified the **minimum and sufficient dataset** required to satisfy EES and RTP processes requirements while complying with data protection legislation. With regard to the retention period, the Study assessed different options against the main purposes of the system.

The chapter also investigated the technical consequences of giving law enforcement authorities access to EES. Finally, the chapter looked into the output information that EES and RTP should provide to travellers, border guards and carriers.

While the EES legislative proposal suggests storing a set of 36 data items, the Study identified that the EES **minimum dataset** considered necessary to fulfil the objective of the EES while maximising automation is composed of **26 data** items. The collection of additional data than the minimum dataset would go against the data minimisation and proportionality principles, would not add value for first line checks and would slow down border crossing times. With regard to the RTP dataset, the Study concluded that the dataset as per the legislative proposal is sufficient to meet RTP objectives.

The Study has not identified any disadvantages derived from the data retention period as set up by the current RTP legislative proposal, i.e. the maximum of five years starting from the expiry date of granted or extended access to the RTP. Therefore no alternative options have been investigated.

In contrast to RTP, the current data retention rules established by the EES legislative proposal present a series of disadvantages with regard to the border crossing process. Therefore the Study has investigated alternative options to overcome certain drawbacks such as the need to repeat biometrics enrolment procedure and loss of time for border guards among others. The Study suggests for the case of two separate systems the following options:

- to maintain the retention period as proposed in the EES proposal but for RTs align the EES data retention period of the individual file with the length of the RTP status;
- a uniform 5-year retention period;
- a maximum of 366 days after the last exit record, if there is no entry record within 365 days following that last exit record.

For the case of one single EES/RTP system, the data retention options would need to be further examined depending on the final technical choices made.

Summarising the assessment of the options, the longer the data retention period, the smaller the number of enrolment procedures per TCN. As a consequence, requiring TCNs to enrol fewer times – compared to what would result if the current legislative proposal were maintained – would shorten the overall border crossing time. At the same time, a longer data retention period coincides with the expectations of law enforcement authorities. However, personal data shall not be kept for longer than is necessary for the purpose for which they were collected. Thus, the decision on the data retention option should be based on the right balance between data protection considerations and the purposes of EES.

The Study also explores the additional requirements necessary in case it would be decided to provide **law enforcement access** (LEA) to the EES while taking into account data protection principles. Indeed, if the option to provide access to law enforcement authorities is positively considered, the Study recommends ensuring that data are handled only by the designated competent authorities to the extent necessary for the performance of their task, based on the “need to know” principle.

Regarding the **information to be provided to travellers** at the borders, the Study examines many options. However, the preferred option is a systematic display at ABC gates of at least the maximum number of days for authorised stay in the Schengen Area combined with at least one other option such as on demand print. Regarding information to be provided to travellers on demand within and outside borders, the Study recommends the use of the existing automatic calculator, which has been developed for the general public and for the Member States authorities.

Finally, analysis of the options regarding **information to be provided to the carriers** revealed that they could be relieved from their obligation to verify whether the single-entry visa or multiple entry visa has already been used by the travellers. This option would reduce the number of actors accessing the personal data of travellers. Alternatively, a restricted and secured access to the personal data of travellers could be provided to the carriers to enable them to fulfil their current obligations. One more option would be to extend their obligations to check entry requirements by including checks on the remaining authorised days of stay, taking into account the overall duration of the stay and the return date. The Study does not take any stand on one preferred option;

however, it indicates that the latter alternative has the greatest legal implications both in terms of impact on the legislative proposal and on data protection compliance.

Architecture – integration options

The Study examined the main architectural options for the EES and RTP, and their potential impacts on related systems such as the VIS, Biometric Matching System (BMS), national entry and exit systems and existing border management systems. The Study also assessed the option of developing a National Uniform Interface (NUI) providing national end-user systems with the uniform services needed to easily integrate the use of the EES and RTP in their business processes.

The study assessed the pros and cons of two main possible architecture options – developing the EES and RTP as two separate systems (option A) or as a single system (option B). It appears that **option A would reduce the complexity of the systems’ development and implementation. However,** it would generate a significant risk of functionality and data overlap. This could lead to a much bigger development effort and a duplication of hardware and software, negatively impacting investment and maintenance costs.

Option B is in line with the process and minimal dataset approach for both the EES and RTP. While infrastructure and development costs would be lower, there would be a risk of added complexity in **the systems’ development and implementation, which should be managed carefully. The Study** considers this option as the most suitable one.

Concerning synergies between the new systems and the VIS, three options were analysed: (i) EES and RTP independent from the VIS, (ii) EES and RTP integrated with the VIS, (iii) EES and RTP independent from the VIS but reusing some VIS artefacts. The first option would make the testing phase and entry into operation easier, but duplication of capabilities and data flows would be unavoidable. The second option would be less cost-effective and would require the VIS legal basis to be amended. The evolution of a complex existing system, already operational across 30 countries, with high requirements of availability, would lead to a more complex testing phase and entry into operation compared to the development of stand-alone new systems. Having in mind the lessons learned from the SIS II implementation, the impact of this second option on MS systems and organisation could be important and should be analysed extensively.

The third option would mitigate the complexity risk but would still have an impact at national level and would probably lead to a more difficult testing phase and entry into operation than the first option.

The Study also assessed the option of creating a new RTP and EES – BMS and the option of further developing a common SOA-based BMS that would be accessed by the RTP, EES and VIS. A less complex architecture could be envisioned for developing a new RTP and EES – BMS, but there would be a negative impact on costs and a significant functionality overlap between the new BMS and the VIS-BMS. Reusing the technology and expertise gained from the VIS-BMS and further developing a common SOA-based BMS would help achieve significant cost savings.

With respect to ease of use and data sharing, a practical balance needs to be found. As a result, regardless of the option chosen, the Study recommends including additional safeguards and mitigating measures to reduce the impact on personal data protection such as differentiated access rights to read and query the data stored.

Finally, the Study investigated the services that a National Uniform Interface (NUI) would offer to the MS and the way in which it would ease the integration of the new systems in their business processes. The NUI would be developed by eu-LISA and maintained centrally. It would include all message handling services that are common to all MS. As such, it would reduce the development effort of MS and the effort of integrating the national domain. It would also provide means for integrating existing MS systems performing similar functions as the EES, where they exist.

Target operating models (TOM) – key component combinations

The various analyses lead the Study to envisage the future target operating models (TOMs) of the EES and RTP. These TOMs consist in a unique set of components assembled to effectively operate a future system. In this perspective, five different TOM alternatives were identified, three for the EES and two for the RTP. The five TOMs were elaborated considering that the EES and RTP would

be built up into one central system not integrated with the VIS. The biometric information would however be processed by the same AFIS as for the VIS if fingerprints are used.

The TOMs are articulated on the basis of the process steps and their sub-processes to combine different biometric and data components (e.g. number of fingerprints enrolled, optional vs. systematic identification).

In addition to the unique set of components, TOMs are comprised of generic features (e.g. for the EES: data retention, minimal dataset, LEA, LBT residence permits, transition period, use of self-service kiosks; and for the RTP: data retention, minimal dataset, e-MRTD as RTP token), a choice of system architecture (one or two systems, national uniform interface), and the use of process accelerators and additional cross-cutting items (e.g. management of LBT and residence permits, transition period, law enforcement access, use of self-service kiosks).

An overview of the EES TOMs is presented below:

Border check	TOM A Using only FI and no systematic 1:N identification	TOM B Using FI, 4 FPs and systematic 1:N identification at first entry	TOM C Using FI, 8 FPs and systematic 1:N identification at first entry
Document authenticity and validity	MRTD/e-MRTD: Physical/optical document safeguards e-MRTD: Passive and Active Authentication		
Bearer verification at each border crossing	VEs: MRTD: visual check of picture vs bearer e-MRTD manual lane: FI from e-MRTD vs bearer e-MRTD in ABC: FI from e-MRTD against live photo VHs: bearer verification considered to be part of the VIS framework		
Biometric enrolment at first entry ⁴	VEs/VHs: FI from e-MRTD ⁵ stored in EES VHs: no FP enrolment (10 FP's are stored in VIS)		
	VEs: No FPs are stored	VEs: 4 FPs are stored in EES	VEs: 8 FPs are stored in EES
Biometric verification at subsequent entries/exits (holder vs. travel document and holder vs. database)	VEs: verification of FI from e-MRTD against photo in EES VHs: live FP (1,2 or 4) against VIS	VEs: live FP (1,2, or 4) against EES VHs: live FP (1,2, or 4) against VIS Verification of FI in ABC-gates using FI	
Biometric identification at first entry ⁶	VEs: Discretionary 1:few using FI and alphanumerical data VHs: Systematic identification was done at the moment of the visa application	VEs: Systematic 1:N identification using FPs VHs: Systematic identification was done at the moment of the visa application	
Entry/Exit record creation	Data recording of border crossing, e.g. day, time, BCP		

⁴ EES search is made using issuing country and document number but an individual file in EES is not found.

⁵ If the e-MRTD is not available, then a live picture or the scan of the travel document could be used instead.

⁶ At first entry or in case a new passport is used, to avoid duplicates and to increase security.

With regard to TOM M and TOM N of the RTP, they would not vary at entry and exit regarding process steps, yet the source of biometrics verification would be different. Namely, **TOM M** would rely on fingerprints and photo being part of the registration in the RTP application process (VE), while **TOM N** would rely on the existing biometrics of the EES (VE). No enrolment of biometrics would be made in the RTP application process. Identifications and verifications in the border control process would be made using the EES.

Options		TOM M	TOM N
• RTP enrolment procedure based on EES data.		No	Yes
• EES individual file created at the end of the application process		✓	EES file is a pre-requisite
• 1:N identification using FPs against the RTP (in the RTP application process – to prevent RTP shopping)	• VEs:	✓	
	• VHs:	Not necessary – person already identified within the VIS	Not necessary – person already identified within the VIS
• Number of FPs enrolled for RTP application	• VEs:	Same as for the EES (i.e. for TOM B, 4)	0 FPs, relies on the EES for the biometric verification
	• VHs:	0 FPs, the VIS FP verification is trusted.	0 FPs, the VIS FP verification is trusted.
• Verification using photo (ABC) ⁷ , FPs (ABC or manual)		✓	✓ (EES process used)

Each TOM alternative was assessed against the following main criteria: security (compliance with the Schengen Borders Code and related best practices), duration of the border crossing for travellers, and complexity of system implementation.

The main cost items impacted by the choice of TOMs are (i) network, (ii) hardware and (iii) software. TOMs C and M were taken as the baselines for the calculation of costs, as they are the closest to the legal proposals, as well as the most expensive options. The main conclusion was that TOM A is always the cheapest alternative (approximately -5% to -10%) regardless of the EES scenario. As regards RTP, TOM N does not have a significant impact on the cost to be borne at central level but it could impact national budgets.

Options for the Pilot – live tests

The Pilot's objective is to test the potential options in operational and relevant environments in order to contribute to the preparation of the development and full implementation of EES and RTP in the Schengen Area. The Pilot would not cover a full end-to-end test of EES and RTP due to time and budget constraints. Hence, the objective would be to test significant parts or components.

Built on the conducted analysis, the options for the Pilot were selected based on the following criteria:

1. Additional evidence is needed to verify the expected impact;
2. Need to test possible process changes;
3. Requirements for specific technical solutions and need to test related constraints or possibilities;
4. Results from TOMs analysis indicating the options that add duration and/or complexity.

⁷ Applicable only for VE, unless the VIS regulation is revised, as it currently mandate the verification through FPs.

The different sets of options to be considered for the Pilot are as follows:

Border control processes and use of biometrics

- Biometrics: impact of the enrolment of FI or of different numbers of FP,
- Technology: feasibility and process impact of the usage of different types of devices for the biometric devices, use innovative or developing technology (e.g. enrolment of specific **number of fingerprints using “touchless sensors” or enrolment/verification** of fingerprints and facial image with handheld equipment at various types of borders or enrolment of iris); capturing a photo (FI) from the e-MRTD or taking a live photo and verifying it against another source;
- VIS: searching VIS based on travel document number, without using the visa-sticker number;

Process accelerators

- Self-service kiosks: the usefulness, usability and security in relation to using self-service kiosks for registering, checking and enrolling biometrics;
- Pre-border checks: the feasibility of introducing pre-border checks in the waiting areas of land borders.

For the Pilot execution phase, the necessary budget in terms of equipment and integration has **been estimated to amount around €0.5 m. Others costs, estimated to amount approximately to €1.9 m**, such as equipment leasing costs, meetings costs, travelling costs and contractor costs, must be taken into account as well. The evaluation of the costs for the pilot concludes that the **proposed set of pilot options fit within the € 3.0 m budget.**

Statistics – 76 million TCN travellers with 302 border crossings in 2025

An effort was made to identify the number of people whose border crossings will be managed using EES and/or RTP.

The Study is based on a time-line that foresees the start of operations for the EES and RTP on **01/01/2020. In order to ensure that the systems’ capacity is sufficient for the first years of operations, it builds on sizing estimates for the period up to 2025.**

Volumes of border crossings were measured during a seven-day period from 18 until 26 May 2014 by all current Schengen MS and four EU MS that do not yet fully implement the Schengen acquis (Bulgaria, Croatia, Cyprus and Romania). The results obtained were extrapolated for one year, and towards 2020 and 2025 for the current Schengen MS. Based on consultation with various stakeholders, an annual growth rate of 4.2% was used to estimate figures for 2020 until 2025.

The total number of border crossings in 2025 is estimated at 887 million. The diagram below presents the projected number of entry and exit border crossings for Schengen countries in 2025 per type of passenger across the various types of borders.

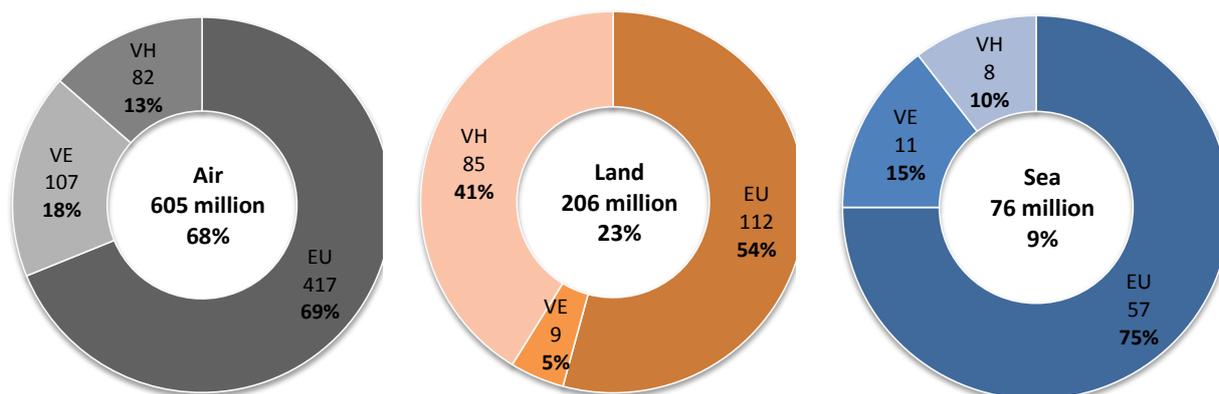


Figure 1 Breakdown of the projected number of entry and exit border crossings for **Schengen countries in 2025** per type of passenger across the various types of borders (figures in millions)

Key lessons from the analysis are as follows:

- As is already the case, **air borders** will account for the majority of border crossings by 2025, followed by land borders and then sea borders.
- For each border type, "EU" (EU/EEA/CH) citizens – who are not directly impacted by the Smart Borders package - will account for the largest share of border crossings.
- The total number of border crossings by TCN**VE** is estimated at 127 million in 2025, occurring predominantly at air borders (107 million).
- The total number of border crossings by TCN**VH** is estimated at 175 million⁸ in 2025, occurring for an almost equal share at land borders (85 million) and at air borders (82 million).

These numbers have been estimated based on the fact that one traveller generates two border crossings per visit and on an estimate of the number of return visits for TCNVE and TCNVH, as presented in the following table:

Table 1 Summary of estimations for the size of the individual file database (in millions)

		2014	2020	2025
VE	Border crossings (entry + exit)	81	104	127
	Number of travellers	30	39	47
VH	Border crossings (entry + exit)	110	141	175
	Number of travellers	19	24	29
Border crossings total		191	145	302
Travellers total		49	63	76

The number of RTP users was estimated based on the assumption that the following TCNs will be most likely to enrol:

- TCNVEs who perform return visits and cross air borders, for whom the use of Automated Border Gates provides tangible benefits;
- TCNVHs having Multiple Entry Visas (MEVs);

⁸ Based on 2014 situation of countries requiring a visa to enter the Schengen area.

- Holders of Residence permits and cards if a provision is made for this population to apply for RTP enrolment (to allow these travellers to use the ABC gates).

Based on those assumptions, the Study estimated that up to **9.2 million TCNs** (representing 12% of the number of travellers) may apply for **RTP membership by 2025**⁹.

These estimates are instrumental in defining the type and magnitude of requirements for implementing the EES and RTP, in terms of processes, data and architecture.

Conclusions

The study explored and analysed the various options, impacts, accelerators, constraints and related costs of the future EES and RTP systems from different angles: biometrics (identifiers), border processes (impacts, alternatives and accelerators), data (minimum number of data to enable the systems to operate) and architecture (leveraging on the current systems landscape, best practices and potential risks).

It brings a comprehensive overview of the various and tangible scenario to operate those systems in the most effective and efficient way (TOMs). The analysis provides also the impact on the legal basis and data protection concerns.

The chapter concerning the costs will be published in a separated document.

In combination with the Pilot phase to be run next to this technical study, it will provide the decision makers with evidenced based information allowing to support their decisions.

⁹ The number of individual files stored within the central database was estimated according to different data retention scenario, using the estimated number of travellers per year and the estimated number of returning travellers. These estimations are based on the data collected from the MS for border crossings, the likelihood that a traveller has to return to the country, and the number of visas issued, single and multi-entry, per year.

• **Introduction**

In February 2008, the European Commission (EC) suggested the establishment of an **Entry/Exit System (EES)** as a sensible next step in border management in the European Union (EU). This proposal was endorsed by the Stockholm Programme agreed by the European Council a year later. After conducting an initial feasibility study (2008) and a cost assessment (2010), in February 2013, the EC presented the three following proposals as the Smart Borders Package:

1. A proposal for a Regulation establishing an **EES** to register entry and exit data of third-country Nationals (TCN) crossing the external borders of the Member States (MSs) of the EU¹⁰;
2. A proposal for a Regulation establishing a **Registered Traveller Programme (RTP)**¹¹;
3. A proposal for a Regulation amending Regulation (EC) No 562/2006 establishing a **Community Code** on the rules governing the movement of persons across borders (**Schengen Borders Code**) as regards the use of the EES and RTP¹².

The **aim of the Smart Borders Package is to improve the management of the Member States' external borders, fight irregular immigration and provide information on overstayers (EES). It is also to allow for facilitated border crossings for pre-vetted frequent third country travellers (RTP) in order to reduce the time spent at the border crossing points, facilitate travel and cross-border contact and contribute to the protection of borders. Indeed, the foreseen facilitation should result in releasing human resources needed at the external borders for thorough checking where appropriate and/or carrying out other relevant tasks).**

According to the Smart Borders Package legislative proposals, the above-mentioned objectives will be pursued by means of, *inter alia*, the establishment of building two large-scale IT systems: the EES and the RTP central systems that will:

As regards the EES:

- **Calculate and monitor the calculation of the authorised stay** of TCNs admitted for a short stay;
- **Assist in the identification** of any person who may not, or may no longer, fulfil the conditions for entry to, or stay on the territory of the Member States;
- **Enable authorities of the Member States to identify overstayers and take appropriate measures;**
- **Gather statistics on the entries and exits of TCNs for the purpose of** analysis;
- In addition, the EES legislative proposal provides for an evaluation of **the possible access to the system for law enforcement purposes** after a period of two years.

¹⁰ COM(2013) 95 Final.

¹¹ COM(2013) 97 Final.

¹² COM(2013) 96 Final.

As regards the RTP:

- **Facilitate border crossings** for pre-screened and pre-vetted frequent third country travellers by allowing them to use the ABC gates or the lanes reserved for EU/EEA/CH citizens.

After the presentation of the three legislative proposals, negotiations with the Member States and the European Parliament raised a certain number of technical, cost-related and operational questions. These encompass inter alia:

- The overall feasibility of both IT systems, the practicability of certain technical features such as the token in the RTP and the biometric identifiers considered;
- The extent to which EES and/or RTP systems could be integrated;
- The need for enhanced synergies and /or interoperability with existing systems used during border controls.

The magnitude of the corresponding investment calls for the demonstration that the solution's underlying architecture and processes are technically feasible, operationally sound and cost-effective.

The Commission has hence to conduct a proof of concept with involvement of volunteer Member States and eu-LISA (the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice). The proof of concept will be divided into two phases: the present study of the technical options for the systems and a pilot.

The Commission will present its recommendations to the Council and the EP and in order to determine the choices to be the subject of the pilot project by the end of 2014.

1.1 Objective

The objective of the study is to analyse in-depth a set of key issues that have emerged during the discussions with the co-legislators and that are deemed to require further investigation. These issues have been further defined in so-called Thematic Files included in the scope defined on 7 February 2014 (see next section).

These analyses will explore the **various technical options** available and recommend **options for the Smart Borders Pilot** to be implemented by eu-LISA. They will provide evidence-based recommendations on what is potentially to be included in or excluded from this future Pilot.

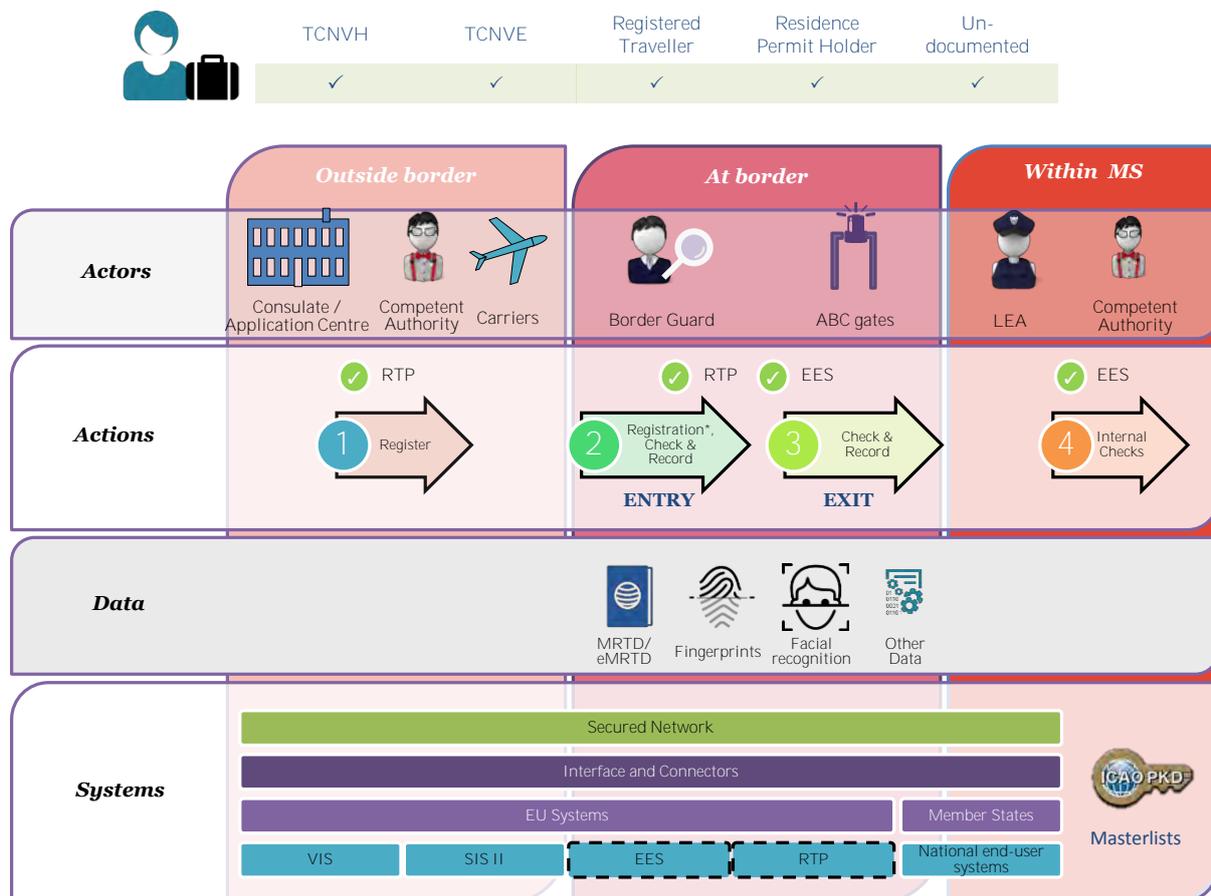
1.2 Scope

The **scope of this Study** is based on the outcome of the **workshop called "Meeting of 7 February 2014 to establish the objectives of the study to identify option for the pilot of the Entry Exit and the Registered Traveller Programme"** organised by the Commission (DG Home Affairs) with the participation of Member States and EP representatives. The participants in this workshop jointly agreed on **20 Thematic Files (TFs)**.

The 20 TFs are organised under the following six domains:

1. Border Control Processes;
2. Biometrics;
3. Architecture;
4. Data;
5. Statistics;
6. Costs (handled separately and to be reported in September 2014).

The following graph provides an overview of the actors, actions (border crossing processes), data and systems involved in the EES and RTP.



* Registration at the first entry in the EES. The registration in the RTP is also possible at some BCP.

Figure 1 Overview of actors, actions, data and systems involved in the EES and RTP

The Smart Borders Package focuses on Third-Country Nationals (TCNs), be they visa-exempt (TCNVEs) or visa-holders (TCNVHs), and introduces the concept of Registered Travellers (RTs), who can be visa-exempt (VE) as well as visa-holders (VHs).

In addition, the analysis also covers third country nationals who have the right of free movement (as defined in the Schengen Borders Code (Article 2(5)); they include TCNs who are family members of EU citizens holding a residence card or residence permit.

As regards border checks, the Study addresses **first-line border checks** for TCNs, inland checks for immigration (i.e. to identify "undocumented" persons who may not or no longer fulfil conditions of entry to or stay in the territory of the MS) and data access by law enforcement authorities (LEA). The first-line border checks for TCNs will consider the need to differentiate between a first entry into the Schengen area, a subsequent entry within the data retention period, and a subsequent entry beyond such period. The Study also includes RTP registration and check.

The Study addresses the differences for **air, land and sea borders**. Two situations have been analysed for each type of border: **manual controls** (controls performed by a border guard who interacts with various systems) and **automated controls** (travellers interact with the system under border guard supervision).

Out of scope

- The Study defines the future operation of the EES and RTP but does not systematically address issues related to an **implementation plan**, although within the cost analysis a gradual sizing of system over the time has been taken into account. The only issue regarding the roll-out timeline addressed in this Study is the deferred or gradual use of biometrics at border checks for the EES;
- The Study does not address the issues occurring upon the launch of the EES and RTP. As an example, when the EES is launched, there will be exits of travellers for which no entry was recorded, as their entry may have occurred before EES went live. Specific measures will be **necessary to handle these situations as compared to ones applicable in "continuous operations"**. The Study addresses however the question of a transition period for the introduction of biometrics.
- While the Study identifies the need to perform e-MRTD authentications (PA/AA), the usage and possible creation and management of a Schengen Masterlist of CSCA certificates is out of scope.

• **Methodological approach**

– **Overall approach**

The methodological approach to this fact-based analysis is based on the six phases shown in the graph below:

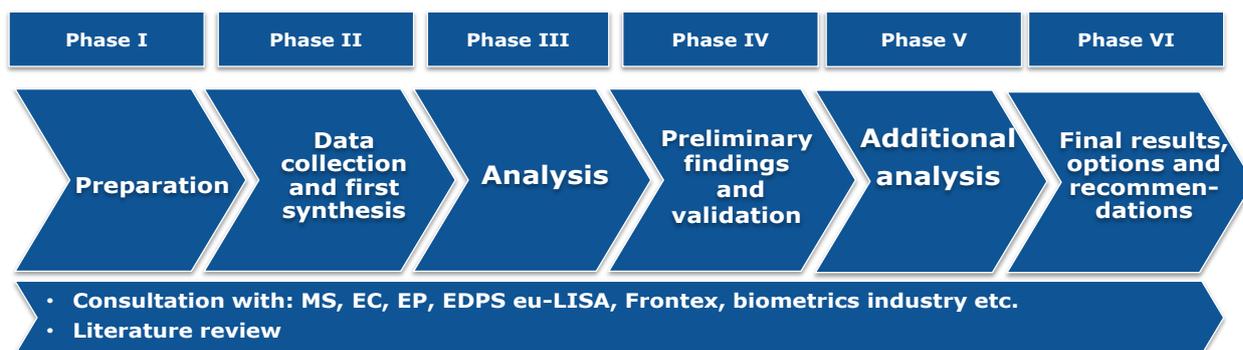


Figure 2 Methodology overview

The pillars of the work are the following:

- Discussions, workshops, on-site visits and interviews with DG Home Affairs, MS experts, eu-LISA, EP representatives, EDPS, Frontex and biometrics industry. Regular talks and workshops are held to ensure that all options are debated and discussed concretely and extensively;
- Literature review: read and review all documents available, which are relevant to the Study's scope;
- Analysis: perform evidence-based analysis and detailed review of the impact of various options; compare proposed options with existing legislative proposals, relevant current legislation as well as relevant case law.

The technical options for a Pilot will include "Privacy by Design" as an underlying principle throughout the whole life cycle of the data process. To ensure that the identified options fulfil the necessary privacy and data protection requirements, this Study aims to develop a solution that takes into consideration the principles of data protection by design and by default as provided for in Article 23 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)¹³. More generally it takes into account the seven Foundational Principles of Privacy by Design¹⁴:

1. **Proactive not Reactive; Preventative not Remedial:** anticipate data protection risks and include mitigating actions and safeguards to prevent violation of data protection and privacy rights;

¹³ COM(2012) 11 final.

¹⁴ <http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/>

2. **Privacy as the default setting:** introduce requirements that will be incorporated into processes and technologies including data minimisation, purpose specification and limitation, barriers to data linkages and differentiated access;
3. **Privacy embedded into the design:** embed privacy in the design and architecture of the IT systems;
 -
4. **Full functionality:** positive sum not zero sum – ensure that both security and data protection requirements are met;
5. **End-to-end security:** comprise data protection and privacy safeguards throughout the entire data lifecycle, from collection to deletion;
6. **Visibility and transparency:** include independent verification mechanisms to ensure the lawful processing of personal data;
7. **Respect for the user:** make sure that appropriate information is provided to the user.

– **Analysis criteria**

The objective of the analysis, considering the timeline and materials available, is to focus on what matters the most. To achieve this in a consistent and comprehensive manner, a list of high-level evaluation criteria has been defined. For each TF, the objective would be to identify the main criteria that are fundamental or of the utmost importance. Cost and data protection have been identified as cross-cutting criteria that need to be taken into account throughout the analysis.

The list of analysis criteria is the following:

Table 2 Analysis criteria for TF 1-18

	Analysis criterion	Definition
1	Cost	High level assessment based on the cost effectiveness taking into consideration both investment or operational costs such as software, hardware, communication, network, HR and maintenance alongside long term returns on any investments made. <i>* Detailed cost assessment is provided in the separate report addressing TF 19, "Cost analysis of the Various Options".</i>
2	Data protection	Assessment based on privacy and data protection principles and regulations. These principles aim to ensure: <ul style="list-style-type: none"> • The minimisation of access to data based on the need to know principle: the proportionality between the amount of information collected and retained and the objective of the system; • The safekeeping of the data collected and differential access control; • The minimisation of negative outcomes in the event of data breach; • The monitoring of activities performed on data with the most appropriate granularity (keeping of records).
3	Duration of the border crossing (D)	Assessment based on the impact on the time it takes travellers to cross borders, including check and waiting times. This is a crucial performance indicator for Border Control Processes.
4	Leveraging existing	Assessment based on the possibility of reusing and achieving

	Analysis criterion	Definition
	systems	synergies with existing IT systems, such as for instance national entry-exit systems, national ABC gates, VIS and SIS II.
5	Implementation complexity (C)	Assessment based on the difficulties that can be foreseen during implementation. Solutions that are too cumbersome to implement could lead to issues, delays and cost overruns.
6	Impact on relevant legislative proposals as well as current legislation in force	Assessment based on the impact that an option would have on the current Smart Borders Package legislative proposals, other relevant legislative proposals as well as on relevant legislation in force such as the one related to the Schengen Borders Code, VIS and SIS II.
7	Impact on Infrastructures	Assessment based on infrastructural constraints. Existing infrastructure and space are important aspects that can make it impossible to implement some solutions at certain Border Crossing Points.
8	Quality of data	Assessment based on the overall solution reliability for the EES and the RTP that have an impact on the quality of data captured in the system. This criterion is of particular importance when evaluating the possible source of data and the options for the capture of biometric identifiers.
9	Usability of the system	Assessment based on the ease of use of the system or the option proposed for all end-users including border guards, competent authorities and travellers. While some solutions might be technically valid and characterised by excellent performance, they might fail to achieve their objectives if not practical in real circumstances for the end-users.
10	Security (S)	Compliance with the Schengen Borders Code and related best practices, and added value of the biometric functionality (including biometric reliability) to support the Border Control Processes.

The options analysed in the Study that deviate from the current legislative proposal are highlighted and argued.

– **Options analysis**

The answers to the TFs provide the basis for identifying various potential technical options that are then described and assessed based on the chosen analysis criteria. These assessments are used to define the Target Operating Model (TOM) and its alternatives (*see chapter 8*). The TOM includes the necessary activities in the new EES and RTP.

The assessment (scoring) of each option against the chosen criteria is made in comparison with the “as-is” situation. A five-level scoring scale is used as described in the table below.

Table 3 Definition of the scoring scale for options assessment

Scoring	Definition
- -	High negative impact on the Border Control Processes, in relation to the specific criteria
-	Limited negative impact on the Border Control Processes, in relation to the specific criteria
N	Neutral impact on the Border Control Processes, in relation to the specific criteria
+	Limited positive impact on the Border Control Processes in relation to the specific criteria
++	High positive impact on the Border Control Processes, in relation to the specific criteria

– **Basic assumptions**

The following main assumptions have been identified for the Study:

- The objectives and scope of legislative proposals comprising the Smart Borders Package will not be changed. The Smart borders proposal will not be changed as regards its objectives and scope meaning that the entry and exit of TCN's needs to be recorded, the need for stamping passports removed, and a facilitation programme for registered travellers introduced while not reducing security. The analysis is aimed to provide answers on how to achieve these objectives in practical and cost-efficient terms. The descriptions of the Thematic Files provide the list of items that need to be explicitly addressed;
- **Visa Exempt (VE):** The list of visa-exempt countries¹⁵ is the following and remains unchanged. It does not influence the methodology applied for the study¹⁶.

¹⁵ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-policy/index_en.htm

¹⁶ A complete list of visa exempt countries is available in the Annex II of the COUNCIL REGULATION (EC) No 539/2001 of 15 March 2001, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001R0539:20110111:EN:PDF>

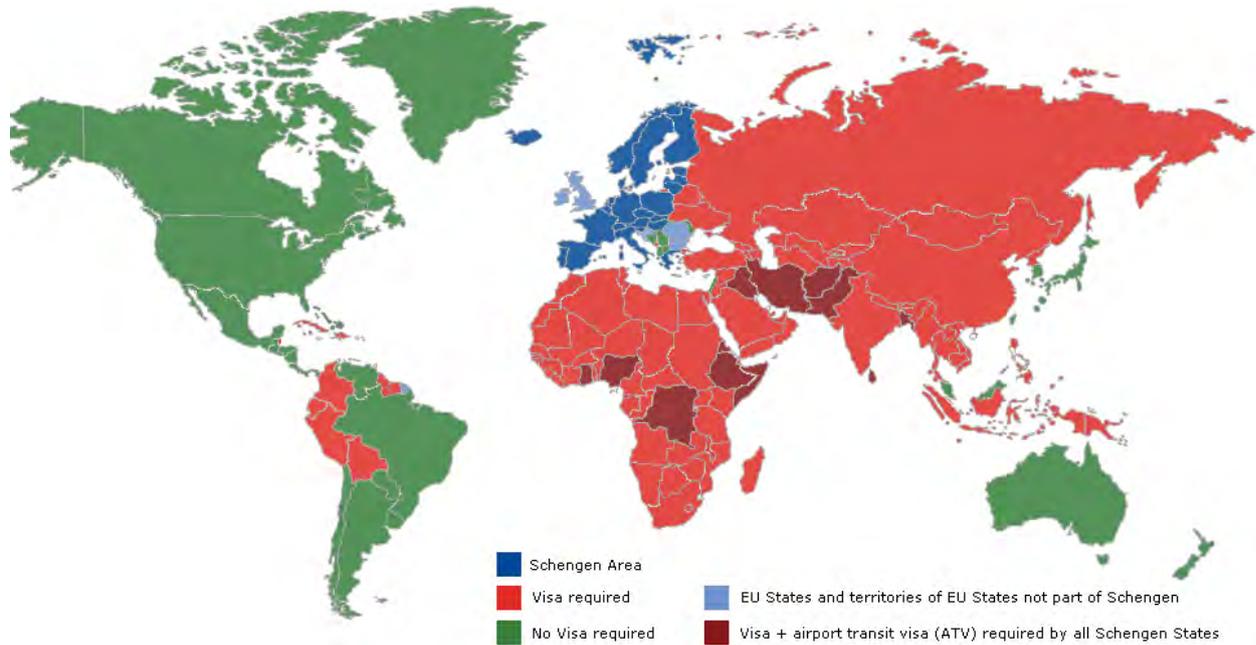


Figure 3 Visa requirements for the Schengen Area as of June 2014 (source: EC)

- The EES and RTP is assumed to go live in the course of 2020 based on the idea that after running the Pilot in 2015, legislation would be adopted in 2016 and the project completed in three years' time. For that reason, quantitative values are extrapolated from current values until 2025 as the systems must start with sufficient capacity to face the volumes of the first years;
- **Passport:**
International Civil Aviation Organization (ICAO) Standard 3.10.1 states "For passports issued after 24 November 2005 and which are not Machine Readable, Contracting States shall ensure the expiration date falls before 24 November 2015". As a result, all non-Machine Readable Passports should have expired by that deadline and consequently, only Machine Readable Passports will be valid after that deadline. ICAO's Assembly¹⁷ endorsed the standard which allows both MRTDs and e-MRTDs as MRPs. Whether to issue a MRTD or e-MRTD is at the discretion of the issuing state.

It can be observed that ICAO invested in the establishment of technical standards for e-MRTDs (i.e. travel documents that contain a radio-frequency identification (RFID) readable chip as well as an MRZ) with digitised facial image, and in a global PKD¹⁸ that allows its members to verify the integrity of these e-MRTDs. By the end of 2013 out of 198 countries and territorial entities that are part of ICAO, the situation of the use of e-MRTD's is as follows, when making the split between those that are EU/EEA and the requirements as regards visas

¹⁷ <http://www.icao.int/publications/Pages/doc7300.aspx>

¹⁸ 45 Countries are participating at the ICAO PKD for the exchange of certificates <http://sp2010.icao.int/Security/mrtd/Pages/PKD-Participants.aspx>

	Countries issuing e-MRTD's	Countries not issuing e-MRTD's	Total
EU/EEA/CH	32	0	32
Countries whose nationals are visa exempt (VE)	31	12	43
Countries whose nationals must be in possession of a visa	60	63	123
Total	123	75	198

The following assumptions will be used throughout the study:

Visa Exempt (VE):

At the end of 2013, out of 43 non-EU countries, 31 issue e-MRTD's. The twelve that do not (Antigua and Barbuda, Barbados, Bermuda, Costa Rica, El Salvador, Guatemala, Honduras, Mauritius, Nicaragua, Paraguay, Seychelles, Uruguay) account for a small number of travellers entering the Schengen area.

As passports have a maximum validity of 5 to 10 years, the existing MRTD's in circulation are being replaced by e-MRTD's. Therefore by 2020 (6 years from this point in time), all VE at the exception potentially of the 12 countries cited, will circulate with e-MRTD's¹⁹.

By 2020, VE travellers having an MRTD are to be handled as an exception case, meaning occurring rarely.

Visa Holder (VH):

All VH will travel either with an MRTD or an e-MRTD, always with a visa (by definition). Currently already 60 countries out of the 123 whose nationals require a visa, issue e-MRTD's. The issuers of the largest amounts of e-MRTD's like China with 7 million e-MRTD's per year and India with 48 million e-MRTD's per year are among these countries. While the proportion of newly issued e-MRTD's and MRTD's was about 50-50 in 2013, the expectation is that by 2017 about 90% of newly issued visas will be e-MRTD's.

By 2020 (in fact already in 2015), all visas will be in VIS (roll-out completed). All travel documents held by VH have FPs and a good FI in VIS.

Cases of bad facial image in VIS to be handled as an exception case:

- There should not be a bad FI in VIS for e-MRTD bearers if the Consular Post (CP) is equipped with e-MRTD readers;
- There will continue to be a low proportion of bad FIs in VIS for MRTD bearers, just as there are today.

¹⁹ IMS Research forecast cited in <http://globalpapersecurity.com/100-countries-issue-epassports.htm> on March 26, 2012

There **Data access:** ID data will be read from the MRZ/chip. Facial images can be read freely yet securely by the Inspection System (IS) (i.e. the passport reader).

When an e-MRTD is used, passive authentication (PA) shall be used for ensuring that the content of the chip has not been tampered with. In addition, where possible, active authentication (AA) should be used to identify any cloning and copying of the chip.

- **Biometric identifiers:** Both the EES and RTP will make use of the same biometric identifiers (i.e. fingerprints and facial image²⁰) to maximise re-usability and interoperability;
- **Law Enforcement Access (LEA):** Should not be the primary driving requirement objective for the EES system since the main objectives of the EES are related to border control. Under the current legal proposal, access to the EES for law enforcement purposes may only be given following an evaluation to be carried out after the system has been in operation for two years;
- **ABC gates:** Will continue to primarily compare the facial images from live photos against the facial data stored in the chip. Where applicable, FPs will also be used for verification purposes. Their current configuration and setup will be reused to the greatest extent possible, in order to ensure cost effectiveness;
- **Acceding Schengen Member States:** As indicated in the legal proposal for the EES the use of EES also encompasses EU Member States that does not yet fully apply the Schengen acquis. In an answer to Romania on this issue in the negotiations in the Frontiers Working Party of the Council, the Commission clarified it as follows.

"Since the EES will replace the provisions establishing an obligation to verify the length of stay and to stamp passports of third country nationals, which are applied by acceding Member States upon accession to the European Union, the EES will be applicable to all Schengen Member States including those that do not yet fully apply the Schengen acquis. The use of the EES as described in the proposal for a Regulation amending the Schengen Borders Code is part of the border checks that are mandatory for all Member States. Romania will therefore have access to the EES in the same way and under the same conditions as other Member States."

The Study analysis shows that in principle this should not have an impact on the EES, as it is described in the report. There could however be practical implications that might need to be specifically addressed. An example of this is the situation of a Member State Schengen state not yet having fully implemented the Schengen acquis, that would have to use EES but has not yet implemented the VIS. Since the EES process relies on the use of VIS, alternative solutions for such a situation would have to be looked at for the duration in between the accession to the EU and the full implementation of the Schengen acquis.

²⁰ While the current legislative proposals (2013) only foreseen the use of FP as biometric identifier, the Study examined the use of other biometric identifiers with particular attention at the combination of FP and FI.

– **Relevant sources of law**

When considering the use of databases such as EES and RTP, the rights of individuals are mainly covered by two fields of EU law: data protection law and immigration law. This Study focuses on the definition of options for a Pilot and their impact on data protection law and immigration law.

The Study's starting point is represented by the three legislative proposals comprising the Smart Borders Package, which were submitted by the EC in February 2013:

- Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union;²¹
- Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme;²²
- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP).²³

The aforementioned proposals already identified relevant legislation:

- Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code);²⁴
- Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention;²⁵
- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation);²⁶
- Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code);²⁷
- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice;²⁸

²¹ COM(2013) 95 final, 28.2.2013.

²² COM(2013) 97 final, 28.2.2013.

²³ COM(2013) 96 final, 28.2.2013.

²⁴ OJ L 105, 13.4.2006.

²⁵ OJ L 405, 30.12.2006.

²⁶ OJ L 218, 13.08.2008.

²⁷ OJ L 243, 15.09.2009.

²⁸ OJ L 286, 1.11.2011.

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;²⁹
- Regulation (EC) No. 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions bodies and on the free movement of such data.³⁰

In addition, since the Study will look into the possibility of providing law enforcement authorities with access to EES, the following source of law is also relevant:

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.³¹

Legislative proposals currently under discussion

In addition to current legislation, it is also important to be aware of the status of the most relevant legislative proposals currently under discussion. This includes:

- Proposal for a Regulation of the European Parliament and of the Council on the Union Code on Visas (Visa Code) (recast);³²
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);³³
- Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data;³⁴
- Proposal for a Regulation of the European Parliament and of the Council establishing a touring visa and amending the convention implementing the Schengen Agreement and Regulation (EC) No 562/2006 and (EC) 767/2008.³⁵

For an overview of case law from the Court of Justice of the European Union and the European Court of Human Rights, please refer to Annex E.

²⁹ OJ L 281, 23/11/1995, p. 31–50

³⁰ OJ L 8, 12/01/2001, p. 1–22

³¹ OJ L 350, 30/12/2008, p. 60–71

³² COM(2014)0164 final

³³ COM(2012)0011

³⁴ COM(2012)0010

³⁵ COM(2014) 0163 final

• **EES and RTP - Border Control Processes**

Objectives

This section examines the different options for the prospective EES and RTP processes ("to-be") and investigates the impact of the projected Smart Borders proposal on processes according to the pre-defined analysis criteria.

The analysis covers Thematic Files 4-10, which address the following topics:

- Impact of the introduction of the EES and RTP on border control processes for the different categories of travellers (see section 3.2 and 3.4.1);
- **Impact on BCP crossing time including travellers' flows** (queues) (see section 3.4.2);
- Impact in relation to LBT and residence permits in RTP (see sections 3.4.4 and 3.4.5);
- Impact on BCP organisations and resources (see section 3.4.3);
- Impact variations between air, land and sea borders (see section 3.4.5);
- Process accelerators (see section 3.5);
- Use of a separate token (see section 3.3.5).

The outcome of this section is a list of options together with their assessments, and forms the basis for defining the "target operating models" (TOMs) presented in chapter 8.

The following graph provides a high-level illustration of the elements examined in the chapter.

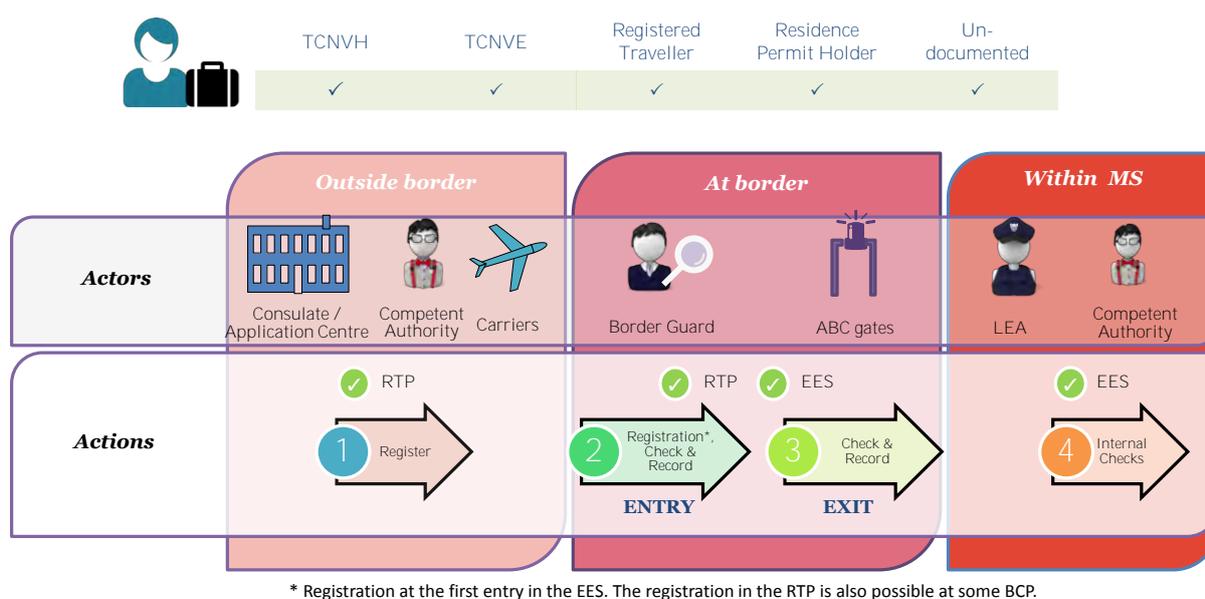


Figure 4 Scope of the chapter

Approach

The description of the “as-is” border control processes provides the reference model for analysing future “to-be” processes. Based on the “as-is” situation and the overall context, the Study analyses which new or changed activities (marked as new ) could be introduced in the border control processes as a result of the implementation of the EES and RTP.

The scope and objectives of the EES and RTP as defined in the Smart Borders Package provide the framework for the analysis of future processes. In order to address all questions of the Thematic Files, the Study describes and analyses various options, relating in particular to how data and biometrics could be used in border control processes (see also chapters 4 and 5). Options that are not aligned with the Smart Borders legal proposals are described in section 3.7 for EES and in section 3.8 for RTP.

Important note

The processes described in this chapter for the EES and RTP cover a number of options related to the future border control processes, in particular in relation to the use of data and biometrics. The process description keeps all options open. Chapter 8 includes recommendations for which options to study further in the pilot.

1.1. Context

The analysis of the future border control processes for EES and RTP is based on the following:

- The **Smart Borders Package** consisting of three legal proposals, for EES, RTP, and the amendment of the Schengen Borders Code;
- The **Schengen Borders Code**;
- **Options** that are to be studied, as referred to in the Thematic Files;
- **The VIS regulation.**

The border control processes provide the overall context for the entire report. Therefore they take into account and analyse the impact of options studied in other Thematic Files. Some of these options are key issues for the design of the future border processes and for the RTP processes, such as:

- The alphanumeric dataset to be registered in the EES (TF11);
- The number of fingerprints for registration in the EES (TF1);
- The number of fingerprints to be registered and the use of photographs as a complementary means of verification and identification in the RTP (TF2);
- The use of photographs as a complementary means of verification and identification in the EES (TF1);
- The use of e-MRTD as a source of a photo when this is used in EES and RTP processes as a biometric identifier (TF1);
- Synergies with the VIS in relation to the use of data and biometrics for EES and RTP (TF1, TF2 and TF16).

Assumptions

The main working assumptions are described in section □□ Basic assumptions.

Key figures

The chart below presents the forecasts of the border crossings at the external borders of the Schengen Area in terms of entries and exits for the years 2014, 2020 and 2025.

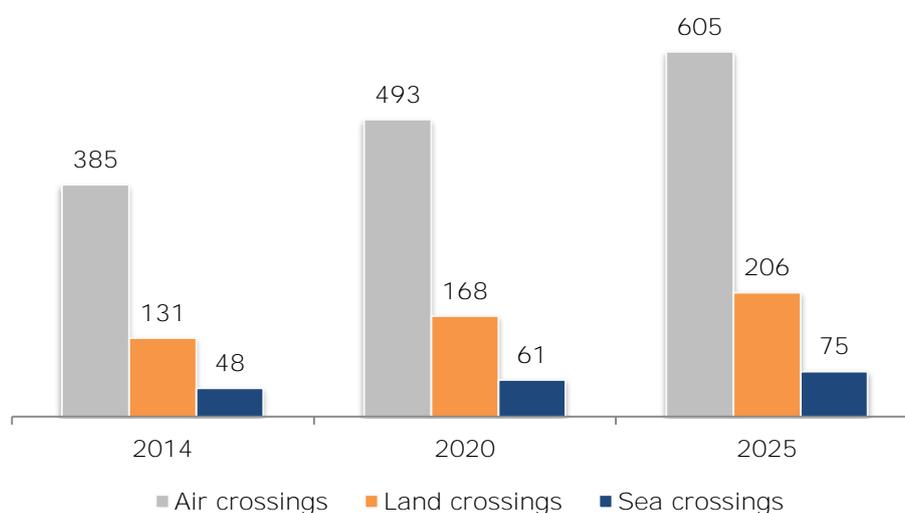


Figure 5 Forecasts of border crossings at the Schengen Area's External borders in millions

Further information on the statistical data used and on the forecasts for 2020 and 2025 can be found in chapter 7.

1.1.1. Border processes today

Table 4 Border processes at entry and exit today

	Entry/ Exit	TCNVEs TCNVHs	Description
Document check	Entry Exit	✓	Manual verifications of valid travel documents or other document authorising a traveller to cross the border and where applicable the requisite visa or residence permit. The documents are also checked to detect falsifications.
Bearer verification	Entry Exit	✓	Manual checks made to secure that the bearer of the travel document is the lawful owner of the document.
Visa check (VIS)	Entry Exit - <i>optional</i>	<i>Only TCNVHs</i>	Schengen visas are issued at consular posts around the world. The VIS is checked, using fingerprints and the visa number. ³⁶
Stamp check	Entry Exit (optional)	✓	Stamps are checked and the stay is calculated manually.

³⁶ Fingerprints are mandatory as of October 2014. At the time of delivery of this Study not all consular posts register the visa information in the VIS, but this functionality is expected to be available worldwide as of mid-June 2015.

Questions	Entry	✓	<p>Questions are asked as regards:</p> <ul style="list-style-type: none"> • the purpose of the stay; • sufficient means of subsistence for the duration of the stay and the return to the country of origin; • other supporting documents (e.g. tickets, hotel reservations or invitations to meetings).
SIS II check (and other databases)	Entry Exit - <i>optional</i>	✓	SIS II and other relevant systems are checked to verify that the person is not a threat to public policy, internal security, public health, or international relations of any of the Member States or not allowed in the Schengen area.
Stamping	Entry Exit	✓	The passport is stamped.
Authorisation to enter/exit	Entry Exit	✓	When the result of all checks can be approved, the passport is stamped and the person can be granted access to the Schengen area.
Second line checks and actions	Entry Exit	✓	Depending on the results of all the checks and on the questions and observations included at the border crossing, there could be alternative actions taken related to law enforcement, migration and asylum or to verify certain requirements (e.g. checking that the document is valid or that it is not a forgery). Those actions are not described here but can be seen as part of the overall Border Control Processes.
Internal checks		✓	After going through the border checks and gaining entry, a person can still be checked in the national territory (either as part of a police check or an identity check by authorities responsible for immigration).

1.2. The EES process (TF4.1, TF6.1, TF6.2 and TF8.1)

This section of the Study addresses the questions of:

- TF 4.1 (overall impact of the EES);
- TF 6.1 (formalisation of processes for first entry);
- TF 6.2 (formalisation of processes for subsequent border crossings);
- TF 8.1 (formalisation of the EES exit process).

The overview of the EES explains how the border control process for the different categories of travellers will be impacted by the introduction of the EES. It is followed by a formal definition of the EES processes, including the first entry and subsequent crossings.

Overview of EES

The overall concept of the EES is to register all entries and exits of TCNs at the Schengen external borders. Persons who are not registered in the EES will have their personal data added into the EES the first time they cross one of those borders. At subsequent crossings, within the data retention period, only the entry and exit information will be registered, after checking that the person's individual file has been duly registered in the EES.

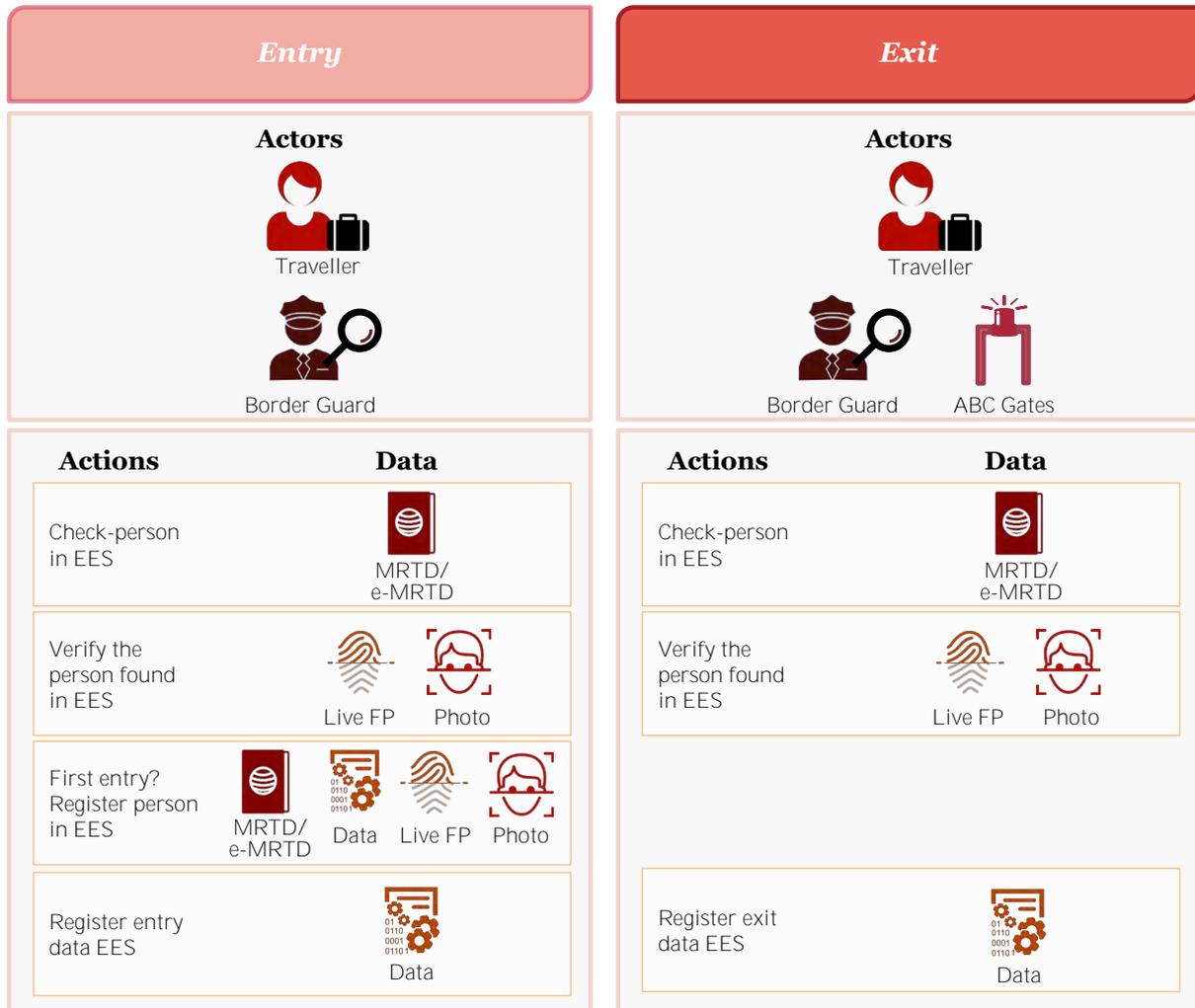


Figure 6 Illustration of the overall concept of EES

The entry and exit processes for the EES would be integrated within the existing overall border control process, as regulated in the Schengen Borders Code. The main changes to the generic process would be the following:

- At every border crossing, as part of the verification, a search is run in the EES. An option is to use only the issuing country and the document number, captured from the MRZ of the travel document (and, in addition, the visa number for VH). If need be, the date of birth and the name could be used to run an additional search. Another option would be to make the search in accordance with the legal proposal of the EES, which is requesting more fields than issuing country and document number for the search in EES.
- A 1:N identification to the EES, using fingerprints, is proposed as an option. This option would help detect duplicates in the EES, where the same person has more than 1 individual file registered.

- When a person is found in the EES, further verification is made to secure the identity of the person, by electronic use of biometric data and/or by manual verification.
- In the case of a first entry, an individual file on the person will be registered in the EES. This would include an alphanumeric dataset and the addition of biometric data in the form of fingerprints and a photo.
- All entries/exits are recorded in the EES with data specific to the crossing (e.g. date and time³⁷). This data would be an addition to the individual file of the person already registered upon first entry.
- Stamping and checking of stamps is abolished. The stakeholders concerned will be able to retrieve or receive information as regards the remaining number of days for the allowed stay.

- ***Process description***

This subsection of the study defines in detail the future processes for the border crossing of TCNs at entry and exit and also indicates the data used throughout the processes.

Note: There is no absolute sequence of activities prescribed by the Study, whether in the pictures or in the text. Some activities do have a sequence, guided by the Schengen Borders Code, and others can be done in parallel, depending on the routines and equipment at the specific border crossing point.

³⁷ See 3.2.2 "Data used in the entry and exit process".

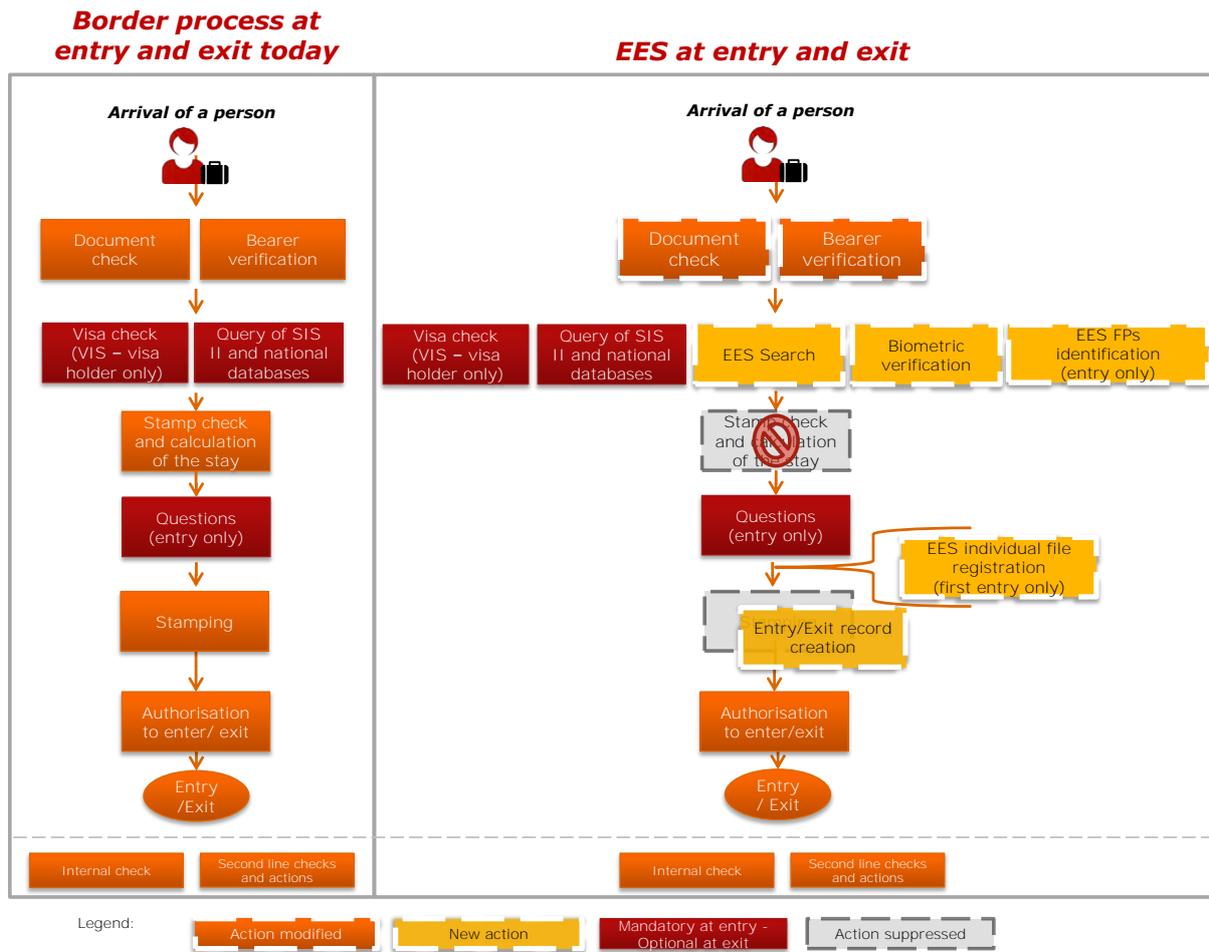


Figure 7 Comparison between the current process at the BCP, at entry and exit, and the process with the introduction of the EES

Formalisation of the process

The table below depicts both formalisation of the EES process for the first entry and formalisation of the EES process for subsequent border crossings occurring during the data retention period.

The process includes options, mainly in relation to data and biometrics used but, in some cases, an activity is optional in itself (e.g. the 1:N identification proposed as an activity in the EES process). The process description does not draw conclusions as to which options should be used.

Table 5 The description of the process at entry and exit

	Entry Exit	TCNVEs TCNVHs	Description
Document check 	Entry	✓	Verifications of valid travel documents or other document authorising a traveller to cross the border. This also includes a check of travel documents to look for falsifications.
	Exit		<p>Electronic MRTD:</p> <p><i>Note: The recommendation below is of a general nature and valid for the border processes as a whole. It is also proposed in an amendment to the Schengen Borders Code (article 7.2b) to make such a check, when it is possible.</i></p> <p>Both for manual and ABC gates, the Study confirms the need to include Passive Authentication (PA), which is a mandatory check according to ICAO. PA verifies the integrity of the contents of the various on-chip Data Groups (containing biographic information, facial image, fingerprints, etc.). Furthermore, where feasible, the discretionary Active Authentication (AA) or Chip Authentication (CA) may be added. AA/CA verifies the authenticity of the chip on which the Data groups reside.</p> <p>Non-electronic MRTD:</p> <p>In this case, the documentation check for falsifications is limited to manually checking the traditional document security safeguards (e.g. ink and optically variable elements).</p>
Bearer verification 	Entry	✓	Verification that the holder of the MRTD is the lawful owner of it.
	Exit		<p>Electronic MRTD:</p> <p><i>Note: The recommendation below is of a general nature and valid for the border processes as a whole, not only in relation to the EES and RTP.</i></p> <p>Both for manual and ABC gates, the Study recommends including biometric verification of live captured photo against the photo stored on the chip. For manual gates, this recommendation would imply that investments have to be made in camera equipment, since this type of equipment does not normally exist at manual gates today.</p> <p>This recommendation is primarily for checks at first entry and for TCNVEs. TCNVHs are considered to be verified as part of the visa application process.</p> <p>Non-electronic MRTD:</p> <p>In this case, the authentication check is limited to manually checking the picture on the document against the</p>

	Entry Exit	TCNVEs TCNVHs	Description
			document holder.
SIS II check (and other databases)	Entry Exit	✓	SIS II and other relevant systems (e.g. Interpol, national databases/watch lists) are searched (SIS II searches are optional at exit) to determine whether the person could be refused entry, is wanted and/or a threat to public security.
VIS check (VIS)	Entry Exit	<i>Only TCNVHs</i>	At entry, the VIS is checked, using fingerprints and the visa sticker number. ³⁸ At exit, the VIS check described above is not mandatory. <u>In relation to the introduction of EES, an option³⁹ could be to use the document number and country code (from MRZ) to proceed with the check in the VIS.</u>
 Questions	Entry	✓	Questions are asked as regards: <ul style="list-style-type: none"> • The purpose of the stay; • Sufficient means of subsistence for the duration of the stay and for the return to the country of origin; • Other supporting documents (e.g. tickets or invitations to meetings); • The level of detail of questions and answers is adapted according to the travel history as shown by the stamps in the travel passport.
EES fingerprint identification 	Entry	✓	It is proposed, as an option, to include a 1:N search for identification, using fingerprints. The identification is solely for the purpose of finding duplicates in the EES database, meaning the same person appearing more than once, with different names and/or documents. This option, if retained, could be used as a systematic activity or a discretionary activity. The choice of one of these two alternatives is also an option. This identification would primarily be made at <u>entry</u> and for <u>TCNVEs</u> . TCNVHs are identified as part of the visa application process and this should keep the risk of having duplicates to a minimum. The identification should be done as an automated activity in parallel with or in addition to the EES search. It could

³⁸ Fingerprints are mandatory as of October 2014. As of today, not all consular posts register the visa information in the VIS, but this will be fully implemented during 2015 (i.e. at which time the roll-out of VIS is planned to be accomplished).

³⁹ This proposal is not compliant with the legal proposal for the EES and it would require a change of the VIS regulation.

	Entry Exit	TCNVEs TCNVHs	Description
			<p>then result in the following findings:</p> <p>a) The person is not found in the EES via the EES search, due to the fact that another document number was used when the individual file was created.</p> <p>b) The person is found via the EES search, which returns only one travel document, although the person has more than one individual file using another identity and/or another document.</p> <p>These cases can only be thoroughly detected by using the proposed fingerprint identification.</p>
<p>EES Search</p> 	Entry/ exit	✓	<p>A search is made in the EES using the issuing country and the document number, taken from the MRZ. The date of birth and the name can be used automatically for further searches, if needed.</p>
<p>EES individual file creation</p> 	First entry	✓	<p>If the person is not found in the EES, a first-time registration of an individual file is made. This includes data from the MRZ (captured from e-MRTD or MRTD), possibly also the additional fields of the EES legal proposal and biometric data.</p> <p>For TCNVE, fingerprints and a photo from the e-MRTD, a live photo or a scanned photo from the MRTD could be stored in the individual file. For TCNVEs, using an MRTD, the printed photo of the MRTD could be stored. This could only be used for manual verification (ocular, using a display of the stored photo) at subsequent entries/exits, since the quality would not be good enough for current automated matching algorithms.</p> <p>For TCNVHs, the fingerprints are already stored in the VIS and no enrolment is needed for these in the EES. A photo, preferably from the e-MRTD, when available, should also be stored in the EES individual file. The absence of any form of biometric data for VHs in the EES would require a constant and mandatory consultation of both EES and VIS for TCNVHs. In addition, the photo stored in VIS is not always deemed to be of sufficient quality. The quality of photos stored in the VIS could be improved, possibly by implementing e-MRTD readers in all consulates. The latter is however outside the scope of this Study.</p>
			<p>The use of photo in the EES</p> <p>The main reasons for the use of photo as a complementary biometric identifier in the EES process are the following:</p>

	Entry Exit	TCNVEs TCNVHs	Description
			<ol style="list-style-type: none"> 1. By using the photo of the e-MRTD (chip) it is possible to make a bearer verification against a live photo, which would highly improve the security of the border process in general; 2. Storing a photo from the e-MRTD or a live photo of sufficient quality in EES, means that there would be a biometric identifier that can be used in subsequent electronic and automatic (e.g. ABC-gates) verifications, in the border control process. The stored photo could also be used for manual (ocular) verifications, by displaying the photo and compare this to the traveller being checked; 3. Scanning and storing a printed photo in EES is of limited or no use for electronic or automated verifications, but can be useful in manual (ocular) verifications, where the photo can be displayed; 4. A stored photo in EES, from any of the sources mentioned, can always be used in relation to identifying travellers believed to be overstayers; 5. The use of photo for verifying the identity of a person would be even more useful in the case where it is decided to have a transitional period where fingerprints are not mandatory to store or to use; 6. The usefulness is mainly related to TCNVEs but in certain cases (e.g. exceptions where fingerprints are not captured in the VIS) it is useful also for TCNVH.
<p>EES biometric verification</p> 	Entry/ Exit	✓	<p>If the person is found in the EES, a biometric verification is made either by using a facial image and/or fingerprints.</p> <p>At entry: For TCNVHs - the biometric verification done via the VIS check is trusted</p> <p>At exit:</p> <ul style="list-style-type: none"> • For TCNVHs, the check made against the VIS is trusted, if it is made (it is not mandatory at exit). If no VIS check were made, the verification related to EES would be manual (ocular), using the photo of the travel document or a displayed stored photo from EES; • In ABC gates a) making an automated Document check (using at least Passive Authentication), b) making a Bearer verification using the e-MRTD and facial recognition and c) ensuring the EES and VIS data exist for the traveller would validate the chain of trust and so would be seen as sufficient, also without a biometric verification against the VIS.
<p>EES entry/exit</p>	Entry/ exit	✓	Entry/Exit data is entered in the entry/exit record in EES.

	Entry Exit	TCNVEs TCNVHs	Description
record creation			
			
Authorisation to enter/exit	Entry Exit	✓	<p>Once all checks have been made and approved, and once the EES record creation is complete, the person can be granted access to the Schengen Area.</p> <p>Note: if the person is not granted access to the Schengen Area, an option could be to still create the EES individual file and the entry/exit could still be recorded. If this option is retained, there is a need for a specific field in the individual file or in the entry/exit record that distinguishes this specific case from the normal case, when a person is allowed to enter. There is a proposed amendment to the SBC, aimed at including changes related to the EES, where in Annex V part A 1b it is stated that in the case of refusal, the passport should be stamped and the reason for refusal indicated in a separate register/list.</p>
Second line checks and actions	Entry Exit	✓	<p>Depending on the results of all the checks and on the questions and observations included at the border crossing, alternative actions could be taken in relation to LEA, migration and asylum. These are not described here but can be seen as part of the overall border process.</p>
Internal checks	Entry	✓	<p>After going through the border checks and gaining entry, a person can still be checked in the national territory, either as part of a police check or security check.</p>

The picture below shows the overall process flow for EES **at entry**, including process steps for TCNVEs and TCNVHs.

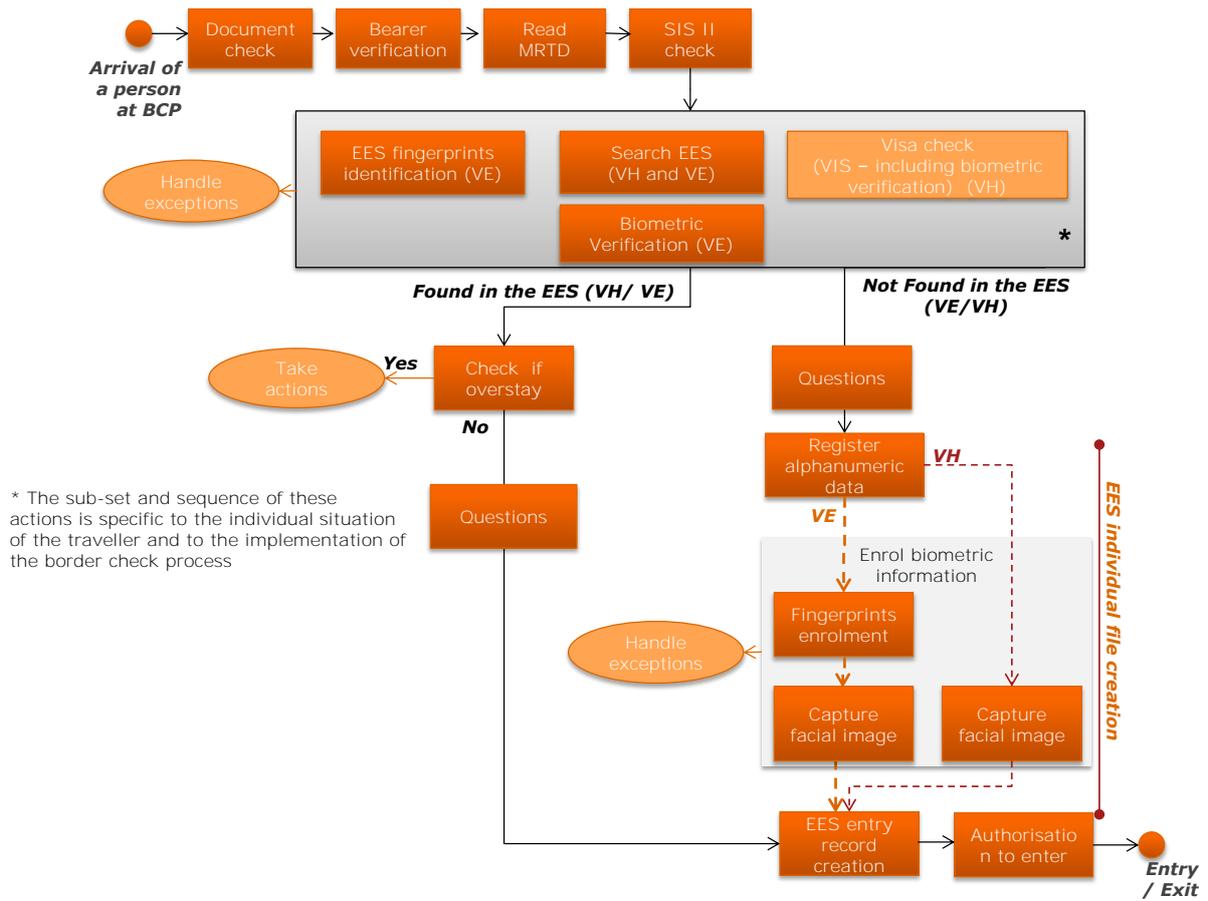


Figure 8 EES process flow at entry

The diagram below shows the EES process flow **at exit**, including the different process steps for TCNVEs and TCNVHs.

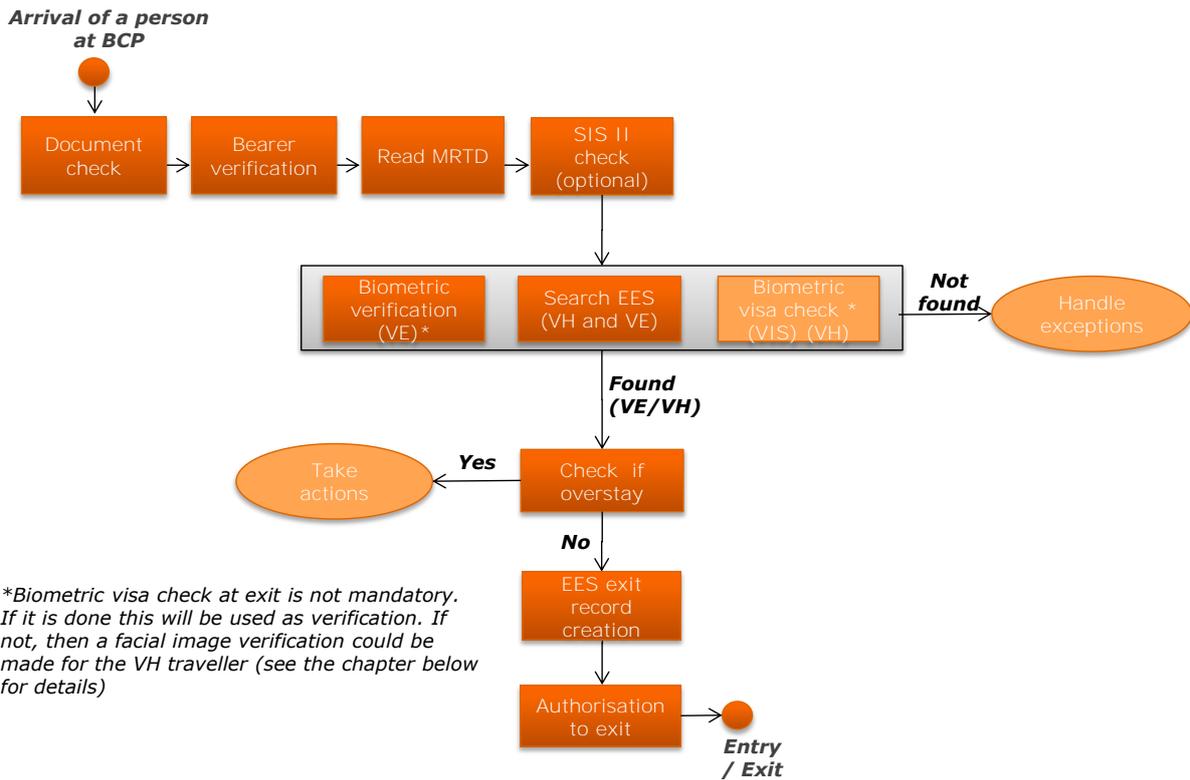


Figure 9 EES process flow at exit

Data used in the EES process at entry and exit

The table below provides an overview of the data used for the entry and exit in relation to the EES. The column entitled “Consequences for the border control processes” indicates the changes for the border control staff involved in the process. The need for IT systems and training is not taken into account here.

Table 6 EES - Data used upon entry and exit

Activity	Entry / Exit	Data used and biometrics	Consequences for the border control processes
Read MRTD	Entry/ Exit	MRZ: <ul style="list-style-type: none"> Type of document Issuing country or organisation Name (first name, family name) Document number Date of birth Date of expiry Nationality Sex Personal number 	None. This is a routine activity for all checks.

EES Search	Entry/	1. Issuing country + Doc Number	None. This is a background transaction, which could be made in parallel with searches in other systems (e.g. SIS II) where data from the MRZ also is used.
	Exit	<p>If not found and the guard is made aware that the person should be in the EES, alternative 2 below could be used (automatically).</p> <p>2. Name + DOB</p> <p>The EES records found should be displayed with the facial image to help the Border Guard find the right record. In the case of a self-service kiosk, the system could perform a facial-image search against the 'few' candidate records returned by the EES, preferably by using a live photo, since the photo in the EES usually comes from the e-MRTD.</p> <p>3. An option is to include a 1:N identification, using biometrics. It could help find persons who are using a different document (i.e. different document numbers because a new document has been issued or they have dual citizenship or have attempted fraud by using more than one document) to the one they used at previous entries.</p>	

Visa check (VIS)	Entry	<i>4-1 fingerprints</i>	<u>At entry</u> , verification is part of the existing routine for VIS checks.
	Exit	<i>4-1 fingerprints</i>	<u>At exit</u> , it is not mandatory to check the VIS.

Person found in EES

Check if overstay	Entry/ Exit	Number of days the person has stayed within the Schengen Area	Routines for handling this information must be in place.
--------------------------	----------------	---	--

Biometric verification (VH)	Entry		The VIS check (see above) includes the necessary verification.
------------------------------------	-------	--	--

	Exit		At exit, it is not mandatory to check the VIS. If the VIS check is done using FPs, this will cover the need for verification.
--	------	--	---

If verification against VIS is not done, the verification would be done using a photo, either as a manual (ocular) verification or automated if an ABC gate is used (see below)

Photo

At exit, at ABC gates that

- make an automated document check on the e-MRTD (using at least Passive Authentication),
- perform a Bearer verification consisting in a facial recognition using the e-MRTD picture against a live photo, and
- retrieve a valid EES and visa status on the basis of the e-MRTD document number and issuing country,

then the chain of trust, for the purpose of EES, would be seen as sufficient without requiring a fingerprint-based verification against the VIS.

Biometric verification (VE)	Entry/ Exit	<i>4-1 fingerprints</i>	Capturing fingerprints and verifying them against the fingerprints stored in the EES is a new activity in the process. Equipment and routines already existing at external borders, used for VIS checks, ⁴⁰ could be used for the purpose of this verification against EES.
------------------------------------	----------------	-------------------------	--

Photo

The e-MRTD photo could be used at exit for verification against a live photo, if using ABC gates. Facial recognition could also be made using the live photo of the ABC-gate against the photo stored in EES (at exit).

⁴⁰ The Commission decision of 9 October 2009 laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the VISA Information System. The VIS regulation is stating that 4 fingerprints are to be used for the verification, but that 1 or 2 fingerprints could be used if the Member State chooses this option.

If an automatic biometric verification is not made (e.g. in case fingerprints could not be enrolled), the photo from the central EES can be displayed and used for manual, ocular, verification.

Activity	Entry / Exit	Data and biometrics	Consequences for the border control processes
<i>Person not found in the EES</i>			
EES Individual file creation (data)	First Entry	a) MRZ, visa number for VHS b) MRZ, visa number and in addition all other fields of the legal proposal, including: <ul style="list-style-type: none"> • Surname at birth; • Place of birth; • Country of birth; • Travel document issuing authority; • Travel document issue date; • Nationalities. 	a) None – a system function. b) Adding this data would require manual registration. Place of birth, Travel document issuing authority and Travel document issue date could be retrieved without manual actions from an e-MRTD. These are, however, optional fields in the concerned data group of the e-MRTD (according to ICAO 9303). If they are not stored in the e-MRTD or when an MRTD is used, these fields need to be typed in manually, which takes time and creates a risk of errors. Surname at birth, Country of birth and Additional nationalities are included neither in the MRTD nor in the e-MRTD. They would always have to be typed in manually and it would be necessary to ask the person to provide the necessary documents to verify that the data entered is correct. The potential need for transliteration must be considered for this option in relation to the fields not included in the MRTD or in the e-MRTD and entered manually.
EES Individual file creation (biometrics)	First Entry	Register fingerprints <i>8 fingerprints or fewer enrolled.</i>	A new activity in the border process. For VHS: 10 fingerprints are stored in the VIS and there is no need for any enrolment specifically for the EES. For VEs: Existing VIS equipment and routines, at border crossings, might be used for enrolment. It has to be taken into account that these are currently used for capturing fingerprints and not for enrolling, which could impact the time it takes to enrol.

For the VIS, 4-1 fingerprints are captured for biometric verification against the VIS. If more than 1 fingerprint is to be enrolled in the EES, this could bring an additional element to the process that would impact the complexity and duration, in particular in those situations where **'single-finger scanners' were implemented for the VIS verification.**

First Entry	Capture photo	A new activity in the border process.
	<ul style="list-style-type: none"> a) Photo of the e-MRTD b) Live photo c) Scanned photo from the photo of the MRTD 	For VHs: A photo is already stored in the VIS but as a precaution, and in order to avoid doing a quality check of the picture in VIS, a photo should be captured also for VHs, from the e-MRTD. This would ensure that there is a photo of good quality in the EES. In the VIS there can be stored photos that are scanned from the passport, which does not make for good quality.

For VEs: The photo in the e-MRTD should be used for registration to the greatest extent possible.

General:

Using a live photo could work well for subsequent verifications, but it would entail new routines and equipment to handle the process of enrolling a live photo of acceptable quality.

Where MRTDs are used, a scanned photo could be used for storing in the individual file. It would, however, only be useful for manual (ocular) verification at later entries and exits.

EES entry / exit record creation

Entry	<p><i>The following is registered upon entry:</i></p> <ul style="list-style-type: none"> • Date and time of entry • Entry MS • Entry BCP • Entry authoriser authority • Calculation of the number of days of the authorised stay • Date of the last day of the authorised stay • Visa sticker number for VHs
-------	--

All fields registered at entry or exit, but the fields related to calculation of days and date of the last day of the authorised stay can be generated by the EES.

Exit

The following is registered upon exit:

- Date and time of exit
- Exit MS
- Exit BCP
- Visa sticker number for VHs

Entry/ Exit

As an option, additional optional fields could be included in the entry/exit record. These would be:

- Flight number
- Origin
- Final destination (if not in entry MS)
- License plate
- Vehicle Identification Number (VIN)
- Full original name (since the ICAO standard truncates and the transliteration cannot be reversed to get the original name)
- If the person is a driver or passenger in the vehicle
- Observations

It requires manual intervention to type in the extra fields. These fields are currently recorded according to the type of border, by MS having a national Entry Exit system. In the rest of this study, these fields are referred to as **"additional"**. The possibility to consider them as optional, not mandatory, and leave it up to Member States to include them or not depends on the future legal basis.

Assuming these additional data would be recorded, some information might be gathered from the API, and/or PNR, in the case of air borders. It could also be possible to obtain the full name from the chip of the e-MRTD, if available but not the original name (before transliteration).

Another aspect to be considered is that any **manual data entered via the border guard's** keyboard need to address language issues. A recommendation would be to use only English and Latin characters for fields entered (e.g. observations) and only keep original language (and the concerned diacritics) for specific fields, such as license plate number. The border guard must of course have the functions needed to enter English characters, without diacritics or with diacritics that are translated (e.g. license plates with German umlaut).

1.3. The RTP process (TF4.1, TF7.1, TF7.2, TF8.2)

This section of the report aims to define the overall concept of the RTP and to formalise the RTP processes. Two main RTP processes are taken into consideration:

- RTP application/enrolment;
- RTP entry/exit.

◦ **Overview of RTP**

The overall objective of RTP is to provide an option for TCN travellers to benefit from a simplified and faster border crossing process. In order to benefit from this “fast lane” option, travellers need to apply for and obtain RTP membership. The current legal proposal states that RTP applications may be lodged at consular posts, common application centres, used by the concerned Member State or at external border crossing points. For VIS applications, some Member States use external service providers to handle the applications and have voiced an interest that this could also be the case for RTP.

Table 7 Summary of the expected demand for the RTP over the years⁴¹

	2020 (in millions)	2021 (in millions)	2022 (in millions)	2023 (in millions)	2024 (in millions)	2025 (in millions)
<i>Growth adjustment for the RTP demand</i>	0.25	0.50	0.75	1	1	1
RTP border crossings (5% of the total with growth adjustment applied)	9	19	29	41	43	44
Estimated number of VH and VE frequent travellers (equivalent to 5% of the border crossings)	0.8	1.8	2.7	3.8	4.0	4.1
RTP border crossings (8% of the total with growth adjustment applied)	14	30	47	65	68	71
Estimated number of VH and VE frequent travellers (equivalent to 8% of the border crossings)	1.3	2.8	4.4	6.1	6.4	6.6

The above table shows the estimated demand for RTP (see section 3.3.4 for further information). It is expected that there will be a transitional period during which RTP registrations gradually increase. However, specific measures could be taken where this uptake of RTP could be increased: for instance, to make the enrolment process faster and easier by pre-registration of applications and to promote the use of RTP to TCNVHs that are applying for an MEV.

Note: The RTP process described relies on the use of the e-MRTD as a token. The justification of this assumption is provided in section 3.3.5.

⁴¹ The estimation considered two cases: 1) RTP border crossing representing 5% of the total 2) RTP border crossings representing 8% of the total. This table do not include resident permit/card holder.

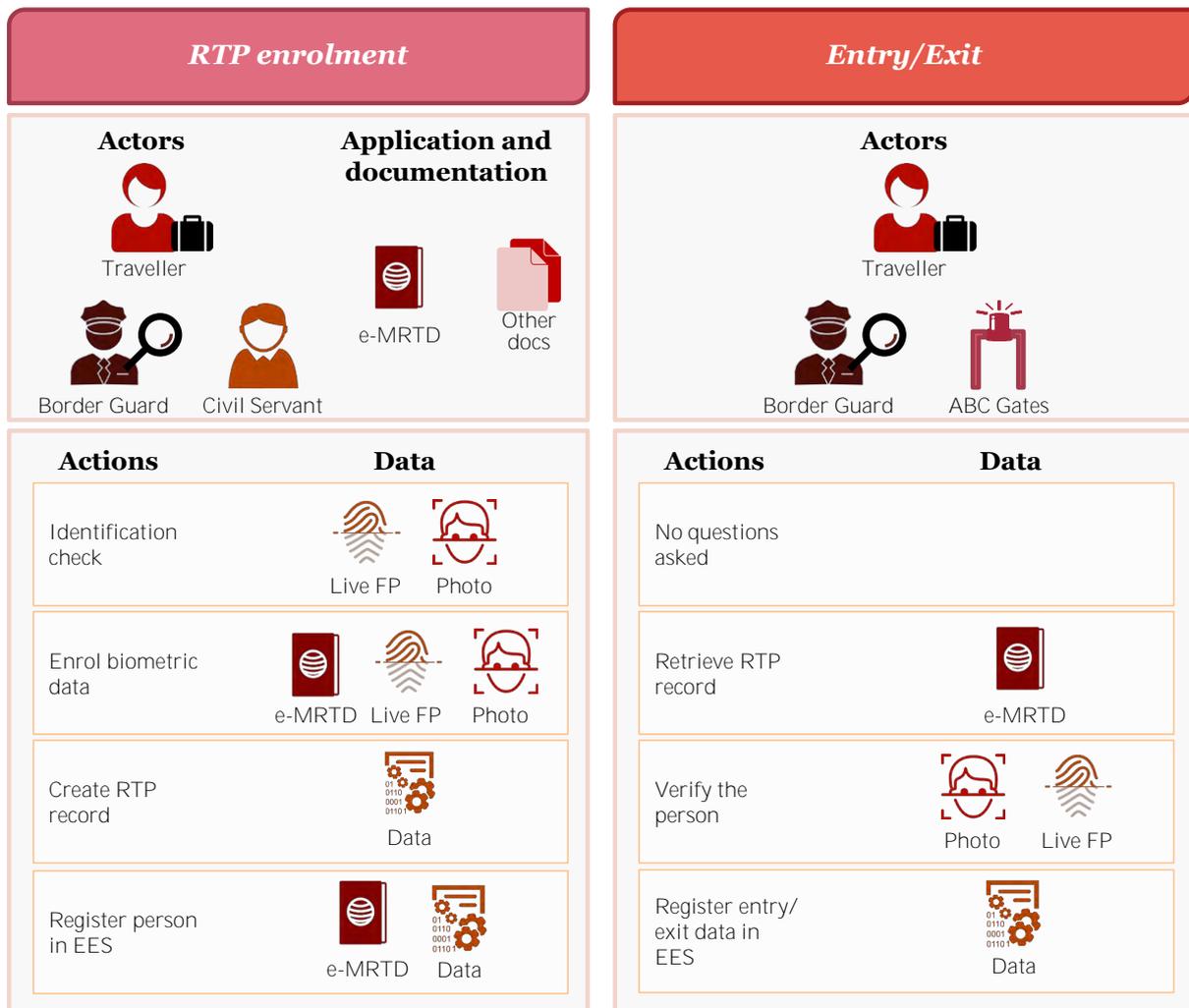


Figure 10 Illustration of the overall concept of RTP

Due to the pre-vetting done during the application process, travellers would not be subject to the questions that are part of the thorough checks for TCNs in the border control process (see table 3).

Consequently, these registered travellers (RT) should be able to use the ABC gates, where available, at Border Crossing Points. At manual gates, the RT would be checked in accordance with the process described in section 3.2, but no additional questions (such as regarding means of subsistence, reasons for the visit, etc. – see table 3) would need to be asked and no supporting documents, as for other TCNs, would need to be presented and the RT would be able to use the EU/EEA/CH lanes.

The main elements of the RTP, based on the legal proposal and options analysed in the Study, would be the following:

- The application for RTP status should be able to be filed at Consular Posts, common application centres, used by the concerned MS or at external border crossing points. Some Member States also use external service providers for visa applications and would like this model to work also for RTP. TCNVE persons would presumably form the bulk of applicants at external border crossings. It should be noted that applying for RTP status is not intended to be made at the actual border control (front line) but would be a back-office activity, preferably preceded by an on-line application;

- When submitting his/her application to the RTP, the traveller presents the application form and his/her travel document. In addition, he/she submits the required supporting documents for vetting the person before s/he is granted RTP status. In addition, fingerprints and optionally a photo are enrolled and included in the RTP system. When examining RTP applications, the fingerprints could also be **used for making a 1:N identification check, to prevent “RTP-shopping”** (i.e. that a person tries to obtain an RTP status using different identity documents);
- At external border crossing points, the RTP status of the person is retrieved using the issuing country and document number. The identity of the person is then verified via a biometric check, **using a photo of the person or the person’s fingerprints. This verification could be made locally** (typically at an ABC gate) or against the central RTP (at manual border checks or at ABC gates equipped to handle fingerprints);
- A major change for TCNVHs with RTP status is that they will use the EU/EEA/CH lanes, where normally no regular checks against the VIS are performed today. These lanes should however be equipped to make verifications using fingerprints against the VIS, for instance for family members of an EU citizen who do not hold a residence permit but travel on the basis of a visa;
- The RTP status can be extended for a maximum duration of 5 years (1+2+2 years).

◦ **Process description for application/enrolment process**

This subsection describes in detail the RTP application/enrolment process for both TCNVEs and TCNVHs. It indicates where and how this enrolment takes place and addresses the issue of how to prevent “RT shopping” by analogy with “visa shopping”.

Table 8 Description of the RTP application / enrolment process

	TCNVE TCNVH	Description
Application 	✓	<p>The person fills in a form and submits it to the authority dealing with the application.</p> <p>The legal proposal sets out the possibility of an on-line pre-registration service that could facilitate the process.</p>
Document check 	✓	<p>The person’s identity documents are checked on arrival at the place of application.</p> <p>Electronic MRTD:</p> <p>The Study recommends including a Passive Authentication (PA), which is a mandatory ICAO check. PA verifies the integrity of the contents of the various on-chip Data Groups (containing biographic information, facial image, fingerprints, etc.). Furthermore, where feasible, the discretionary Active Authentication (AA) or Chip Authentication (CA) may be added. AA/CA verifies the authenticity of the chip on which the DGs reside.</p>

		<p>Non-electronic MRTD:</p> <p>No electronic verification can be made, which makes the use of MRTDs less secure compared to e-MRTDs.</p>
<p>Bearer verification</p> 	TCNVE	<p>Verification that the MRTD holder is the lawful MRTD owner.</p> <p>Electronic MRTD:</p> <p>The Study recommends including a biometric verification of a live captured photo against the photo stored on the chip. The verification of the e-MRTD is described above.</p> <p>This recommendation is primarily related to TCNVEs. TCNVHs are also verified as part of the visa application process.</p> <p>Non-electronic MRTD:</p> <p>No electronic verification can be made, which makes the use of MRTDs less secure compared to e-MRTDs.</p>
<p>RTP identification (1:n)</p> 	✓	<p>For TCNVEs: The identification is made against the RTP database in order to avoid "RTP-shopping" but also to find if the person has an earlier application that is refused, revoked or even granted and still active.</p> <p>If 4 fingerprints were used for enrolment, then 4 fingerprints would be captured for this identification activity. If 10 fingerprints were used for enrolment, then 10 fingerprints would be used in this identification activity.</p> <p>For TCNVHs: The identification has been made as part of the visa application process. It may therefore not be necessary as part of the RTP process.</p>
<p>Interview</p> 	✓	<p>The person would be interviewed and clarifications may be requested from the applicant when need be.</p>
<p>VIS check</p> 	✓	<p>For VHs: If the application is not made at the same time as applying for an MEV, the VIS should be checked.</p>
<p>EES check</p> 	✓	<p>The EES is searched using issuing country and document number of the e-MRTD. This check is to ensure that the applicant is not an overstayer.</p>
<p>SIS II check</p>	✓	<p>The SIS II is searched⁴².</p>

⁴² The legal proposal for the RTP provides for a mandatory check in the SIS II, when examining an RTP application (Article 12g), that the person is not a person for whom an alert has been issued. The SIS II Regulation does however not allow visa authorities to search SIS II for data other than alerts on



Vetting



A vetting procedure (i.e. admissibility and examination) is performed that can also include consultations with other Member States. The procedure is defined in articles 11 and 12 of the legal proposal for the RTP.

RTP registration



Fingerprints Enrolment, data filling and data source

For TCNVEs, 4, 8 or 10 fingerprints are enrolled and a photo is captured from the e-MRTD or live. Data from the application is used to create a file in the RTP.

For TCNVHs (MEV), two options are under consideration:

- a) The fingerprints already exist in the VIS and need not be enrolled in this process. The data in the VIS could also be used for RTP application and border crossing purposes, which is why a very limited amount of data from the RTP application needs to be used to create a record in the RTP.
- b) Fingerprints are captured separately for the purpose of the RTP and the data requested is entered manually (when possible from the e-MRTD) to create a record in the RTP.

Also for TCNVH, a photo of sufficient quality (e.g. from the e-MRTD) could be captured and added to the RTP, for quality reasons and for coherence with the EES data.

The use of photo in the RTP

The main reasons for the use of photo as a complementary biometric identifier in the RTP process (for VE and VH) is the following:

Storing a photo from the e-MRTD or a live photo of sufficient quality in EES, means that there would be a biometric identifier that can be used in subsequent electronic and automatic (e.g. ABC-gates) verifications, in the border control process. The stored photo could also be used for manual (ocular) verifications, by displaying the photo and compare this to the traveller being checked. The latter is useful for instance in the exceptional cases where fingerprints could not be enrolled in RTP, or in VIS.

RTP file creation

The RTP file creation, as described here, would be made once the

documents and persons refused entry in the Schengen Area. If the issuing authority for the RTP is the visa authority, a national business process should be introduced to meet the requirement of Article 12(g) of the proposal. A protocol is to be established between the visa issuing authority and e.g. the police, for the full SIS check to be carried out. The police will then be able to inform the visa authorities of whether an alert exists in the SIS II on grounds other than those for which the visa authorities can directly access the SIS.

status is granted. The file creation is the actual registration of the data into the RTP system, for TCNVEs. For TCNVHs, the VIS is consulted in the RTP application process and a similar consultation could be made for other purposes related to the RTP application (e.g. revoking the status). This means that for TCNVHs, there is no need to duplicate this data to the RTP.

EES individual file creation



An individual file is created in the EES, without recording data on entry/exit. If the option is retained, it would make it unnecessary to perform an EES registration for the RTP traveller upon first entry, as is the case in the application process described in the legal proposal. The calculation mechanism must take this option into account, meaning that the calculation starts at the first recorded entry.

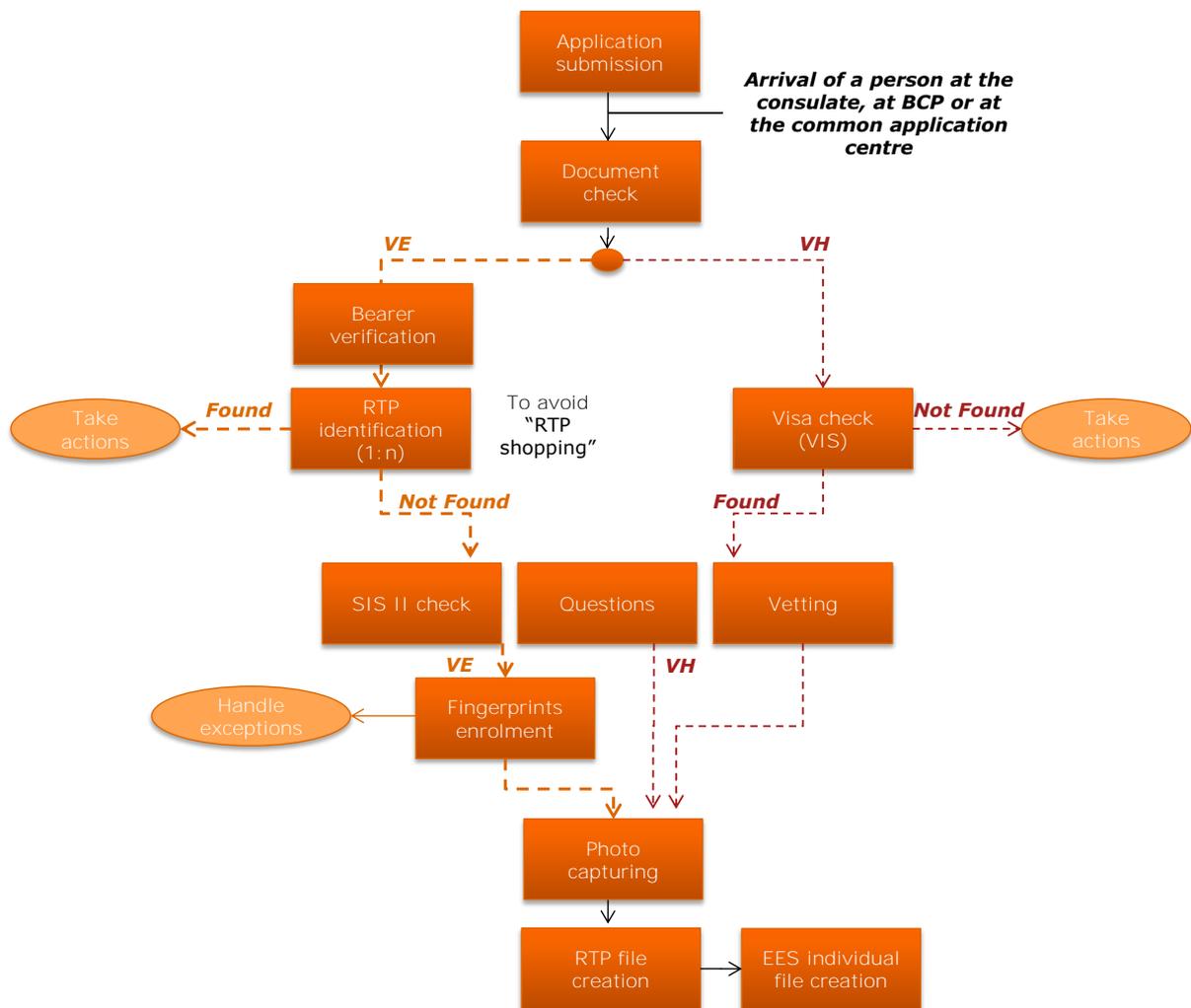


Figure 11 RTP enrolment process

> *Data to be used for each activity in the RTP enrolment process*

The table below indicates the data to be used for the RTP enrolment process. The “consequences” column provides a first insight into the impact on the authorities’ workload and on the duration of the process. The need for IT systems and training is not discussed in this section.

Table 9 *Data to be used in RTP enrolment*

Activity	Data and biometrics used	Consequences	Comment
RTP identification (1:N)	4, 8 or 10 fingerprints	<p>A new activity for the authorities that would handle RTP applications.</p> <p>In relation to the option of enrolling 4, 8 or 10 FPs: The same number of FPs will be used for identification as is chosen to use at enrolment.</p> <p>The border crossing process is not impacted.</p>	<p>This activity would be made to avoid “RTP shopping” but also to find out if the person has any earlier application(s) and to find out about the status (e.g. revoked).</p> <p>For TCNVEs, an identification against the RTP.</p> <p>For TCNVHs, an identification check has been made as part of the visa application process. It may therefore not be necessary to make this activity as part of the RTP process.</p>
Fingerprints Enrolment	4, 8 or 10 fingerprints ⁴³	<p>A new activity for the authorities that would handle RTP applications. The border crossing process is not impacted.</p>	<p>For TCNVEs only.</p> <p>As regards the option to enrol 10 fingerprints, see explanations in chapter 4, related to Thematic file 2.</p>

⁴³ For the assessment of a different number of FPs, please refer to TF2 in chapter 4.

Photo Capturing

Live photo or e-MRTD photo

A new activity for consular posts and/or back office functions at border crossings. The border crossing process is not impacted.

For VEs and also for TCNVHs, a photo of sufficient quality (e.g. from the e-MRTD) is to be added in the RTP. The reason for storing a photo for TCNVHs is that the quality of a proportion of existing photos in the VIS is often insufficient for facial recognition.

The main reason for capturing and storing a photo is to have a complementary means of (automated or manual) verification and identification. Also for verification at ABC gates, where the majority of existing installations use photos only.

RTP file creation

- Status information, indicating that access to the RTP has been requested;
- The authority with which the application has been lodged, including its location;
- Surname (family name); first name(s) (given names);
- Surname at birth (earlier family name(s)), country of birth, nationality(ies); and
- Sex;
- Date of birth, place of birth;
- Type and number of the travel document(s), the authority which issued it and the date of issue and of expiry;
- Place and date of the application;
- If applicable, pursuant to Article 9(5), details of the person liable to pay the applicant's subsistence costs during the stay, being:

This is a new activity for the authorities that would handle an RTP application. The actual border crossing process is not impacted.

For TCNVEs, all data must be registered as part of the RTP enrolment process.

For TCNVHs, the data from the existing VIS record may be consulted, in a similar way to the consultation of VIS in the RTP application process, when there is a need (e.g. revoking the status).

RTP file creation

- In the case of a company or other organisation, the name and address of the company/other organisation, surname and first name of the contact person in that company/organisation and telephone number;
- Main purposes of the journeys;
- The applicant's home address and telephone number;
- If applicable, the visa sticker number;
- If applicable, the residence permit or residence card number;
- Current occupation and employer; for students: name of educational establishment;
- In the case of minors, surname and first name(s) of the applicant's parental authority or legal guardian.
- Status information indicating that access to the RTP has been granted;
- The authority that granted access, including its location;
- The place and date of the decision taken to grant access to the RTP;
- The commencement and expiry dates of the validity of the access.

o **Process description at entry and exit**

This subsection formalises the RTP member’s border crossing process both at entry and exit. The first table gives an overview of the steps in the process. The second table below provides a detailed description of each step in the process for TCNVEs and TCNVHs, including the data and biometrics used.

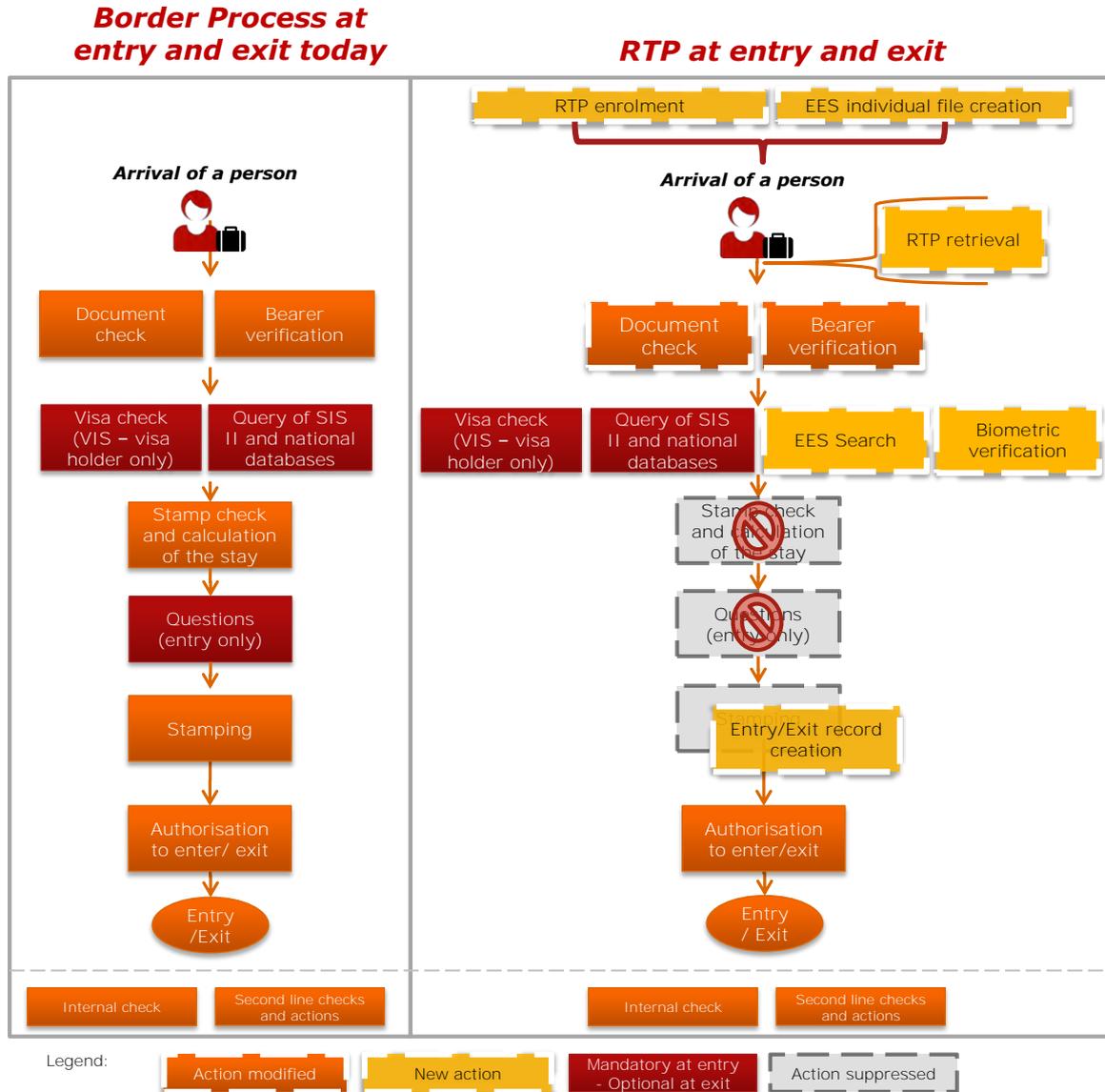


Figure 12 Comparison between the current process at the BCP, at entry and exit, and the process with the introduction of the RTP

Table 10 Description of the RTP process upon entry and exit

		TCNVEs TCNVHs	Description
Document check	Entry	✓	Verifications of valid travel documents or other document authorising a traveller to cross the border. This also includes a check of travel documents to look for falsifications.
	Exit		
			<p><i>Electronic MRTD:</i></p> <p> Note: <i>The recommendation below is of a general nature and valid for the border processes as a whole. It is also proposed in an amendment to the Schengen Borders Code (article 7.2) to make such a check, when it is possible.</i></p> <p>Both for manual and ABC gates, the Study recommends including Passive Authentication (PA), which is a mandatory ICAO check. PA verifies the integrity of the contents of the various on-chip Data Groups (containing biographic information, facial image, fingerprints, etc.). Furthermore, where feasible, the discretionary Active Authentication (AA) may be added. AA verifies the authenticity of the chip on which the Data Groups reside.</p> <p><i>Non-electronic MRTD:</i></p> <p>In this case, the documentation check for falsifications is limited to checking the traditional document security safeguards (e.g. ink and optically variable elements).</p>
Bearer verification	Entry	✓	Verification that the holder of the MRTD is its lawful owner.
	Exit		
			<p><i>Electronic MRTD:</i></p> <p> Note: <i>The recommendation below is of a general nature and valid for the border processes as a whole, not only in relation to the EES and RTP.</i></p> <p>Both for manual and ABC gates, the Study recommends including biometric verification of live captured photo against the photo stored on the chip. The verification of the e-MRTD is described above.</p> <p>This recommendation is primarily for checks at entry and for TCNVEs. TCNVHs are verified as part of the visa application process and this verification is considered to be sufficient.</p> <p><i>Non-electronic MRTD:</i></p> <p>In this case, the authentication check is limited to checking the picture on the document against the document holder.</p>
RTP Retrieval		✓	<p> The RTP record is retrieved, using the document number + issuing country of the MRZ. If the person is not found, he/she will be subject to a “normal”, manual, border check</p>

RTP biometric verification

Depending on the border crossing (see table 9), the verification could be made using:

- Facial recognition based on the e-MRTD photo and a live photo, or a live photo and the photo stored in RTP; or
- Fingerprint comparison against the central RTP, using 4-1 fingers captured; or
- Manual verification, using the printed photo or a displayed stored photo from the EES.

VIS check

Only TCNVHs

VIS is consulted as in the existing border control process (not mandatory at exit)

Note: A VH with RTP status using an ABC gate needs to be verified against the VIS using fingerprints, according to the VIS regulation. For a VH, with RTP status, to use an ABC gate, this would imply any of the following alternatives:

- a) The ABC-gates have to include the ability to verify against VIS, using FPs.
- b) The VIS is consulted using the visa number and the identity is verified by facial recognition using a live photo and comparing it to the facial image of the e-MRTD. This would be a change to the VIS regulation.
- c) The VIS is consulted using the visa number and the identity is verified by comparing a live photo to the photo stored in the VIS. This would also imply a change to the VIS regulation.
- d) The VIS is consulted using the travel document number and the identity is verified as in c). It avoids that the travellers has to present the visa number.

It should be noted that this issue is a consequence of allowing visa holders to use ABC gates and is not specifically linked to any option of what biometrics are used. The RTP verifications described for this case are sufficient for the purpose of the RTP. The alternatives described above are purely related to VIS and the use of ABC-gates.

SIS II check

SIS II is consulted (not mandatory at exit)

EES search

A search is made in the EES using the issuing country and the document number, taken from the MRZ. The date of birth and the name can be used for further searches, if needed.

The individual file is proposed, as an option, to be registered at enrolment in the RTP. An alternative would be that the individual file is registered at the first entry of the traveller that has obtained RTP status.

EES entry/exit record creation

Upon each entry/exit, the recording of the data is the same as that described in the EES process.



Authorisation to enter/exit



Once all checks have been made and approved and once the EES registration is complete, the person can be granted access to, or exit from, the Schengen Area.

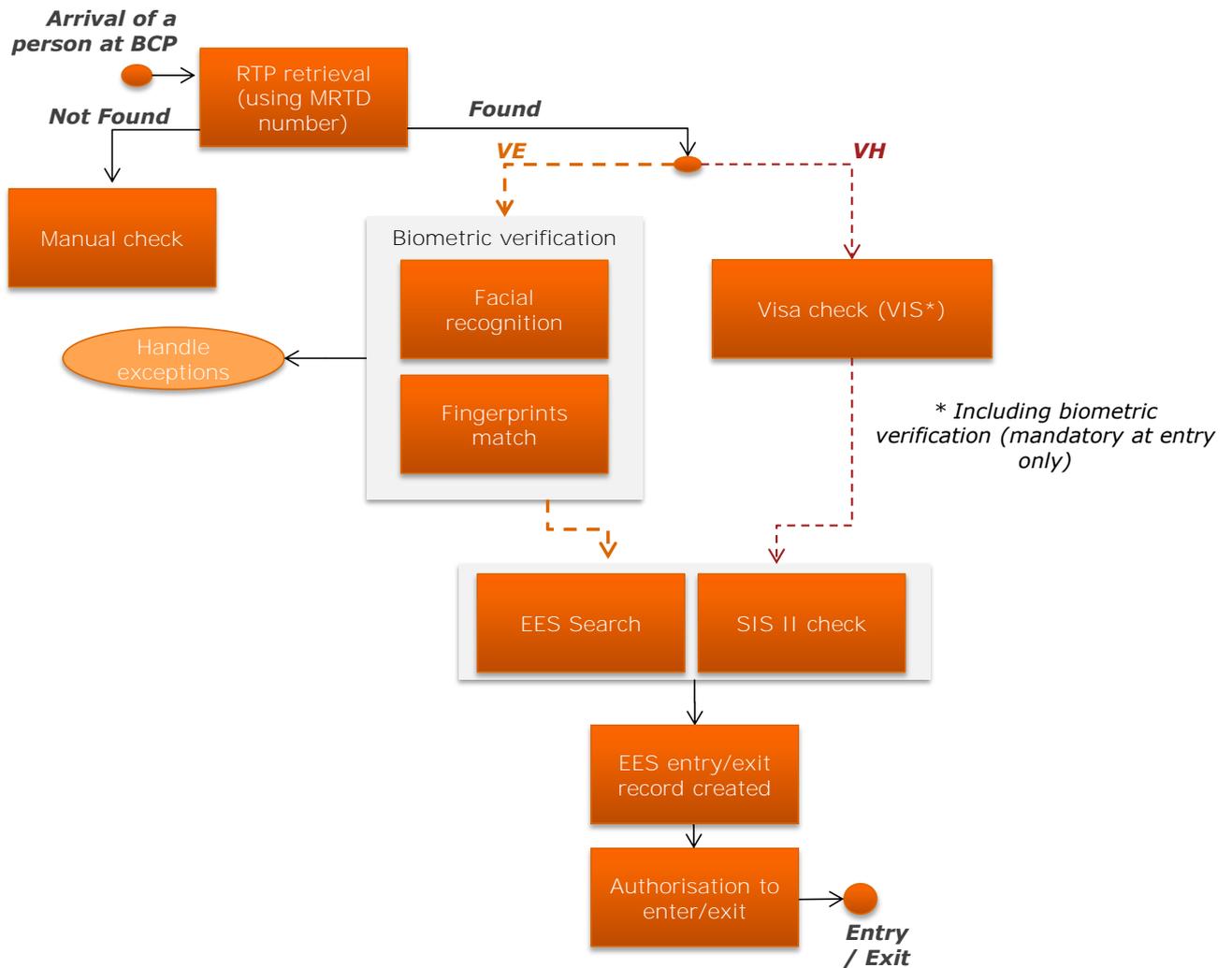


Figure 13 RTP process flow at entry/exit

> **Data to be used**

The table below provides an overview of the data to be handled in each of the process steps. The consequences column provides the impact on the border crossing process.

Table 11 Data used in the RTP process at entry and exit

Activity	Data and biometrics used	Consequences for the border crossing process
RTP record retrieval	From MRZ: • Document number	A new activity in the border crossing process.

Activity	Data and biometrics used	Consequences for the border crossing process
RTP verification (at ABC gate)	<ul style="list-style-type: none"> • Issuing country <p>From e-MRTD – live photo of the person compared to the photo in e-MRTD. An option could also be to have the ABC-gate compare the live photo to the photo in RTP.</p> <p>Live fingerprints compared against the central RTP system.</p>	<p>These are new activities in the border crossing process.</p> <p>If the existing infrastructure can be used, the main impact will be related to the number of RTP travellers that increases the total volume and possibly the potential incorporation of FP equipment at the ABC gates.</p> <p>VHs would be verified either as part of the VIS check (at entry) or, if so decided, via a verification using a live photo compared to the photo from the e-MRTD (at exit, where VIS checks are not mandatory).</p>
RTP verification (manual border check)	<p>Live fingerprints are compared against the central RTP system.</p> <p>Alternatively (TCNVHs at exit):</p> <p>A manual check by the border guard, using the displayed or printed photo of the person.</p>	<p>A new activity in the border crossing process. The existing infrastructure to compare fingerprints against the VIS can be used for the purpose of verifying travellers against RTP.</p> <p>TCNVHs would be verified as part of the VIS check at entry, using FPs. At exit, the VIS check is not mandatory. If this check is not done, the RTP verification could be done manually</p>

EES search*

EES entry/exit record creation*

* See section 3.2

◦ **Consultation of the RTP database (TF 7.3)**

TF question: This item addresses the way the RT database is consulted and also assesses whether there is a need to have the biometric data kept separate from the alphanumeric ones. In that case, an identifier needs to link these two parts of the database.

The use of the e-MRTD as a token, or having a separate token, is described in section 3.3.5. The use of a separate token could be seen as a key item in managing the potential separation of alphanumeric data and biometric data. The use of a separate token is not recommended and the explanation for this is given in section 3.3.6.

The possible separation of alphanumeric data and biometrics in the central RTP has no impact on the border control processes. As seen from an end-user point of view, the potential need to allow access to the alphanumeric data but not to biometrics, or vice versa, can be achieved by other means, such as access control. The specific issue of separating, or not separating alphanumeric data and biometrics, is analysed in the sections concerning data content/data protection (see 5.2) and architecture (see 6.3 and 6.4.4).

In short, the RTP database could be consulted, during the enrolment in RTP and during the border control process, as follows:

- Identification (1:N) at enrolment against RTP, using fingerprints;
- Registration of the person in the RTP using alphanumeric data and biometrics;
- Confirmation of the RTP status at entry and exit;
- Verification, using biometrics, at entry and exit;
- For the renewal of RTP access;
- In the event that any problems occur with facilitating registered travellers border crossing points.

The alphanumeric data and biometrics used in each activity related to RTP are described in detail in sections 3.2.2, 3.3.2 and 3.3.3. These descriptions are used as an input for the analysis of data content/data protection and for the architecture area.

◦ **Alternative options to the token (TF10)**

The legal proposal for RTP includes a separate token for proving the RTP status, in particular related to the use of ABC gates. The proposal contains the following text (footnote no 7 on page 4):

"In the context of a RTP, a token is a physical device given to the authorised user to prove his/her access granted to the RTP electronically. The token acts like an electronic key to access something, in this case to the automated gate. Technical specifications will determine whether only a bar code is used or a chip in which the unique identifier (application number) is stored."

The Study has analysed the use of a separate token (see table below for details) and the main finding is that such a solution would have very few significant advantages and, on the other hand, it would generate additional costs and increase complexity.

In relation to the issue of data protection, it should be noted that the Impact assessment for the Smart borders did not make a comparison in this respect between having a separate token and using the e-MRTD. The e-MRTD was discarded because of doubts as regards if it would be widespread enough for the purpose of the RTP.

As an alternative to a separate token, the use of e-MRTD and/or MRTD as a token has also been studied.

MRTD as a token for RTP

The MRTD would not work well in any existing or planned ABC gates, whose use by RTs would be one of the expected benefits. The vast majority of ABC gates⁴⁴ relies on the security of the e-MRTD (passive authentication – PA) and the authentication of the bearer, using the chip. These gates access the facial image stored in the passport chip and compare it with the facial image taken at the ABC gate. Therefore, as RTP travellers should use ABC systems and a fundamental re-design of the existing systems is undesirable, the MRTD has a disadvantage in this respect.

⁴⁴ Source: Frontex, 2014.

The MRTD could potentially be used at ABC gates equipped with fingerprint readers, if these gates accept MRTDs as documents, thereby not being able to make any passive authentication. At present, there is only a national solution, with a national database of fingerprints, that possibly could handle these requirements. If such a solution existed, it would anyhow only cover a limited need for the RT use of ABC-gates, since a majority (at present) of ABC-gates are not equipped in this way. RTs with an MRTD would have to be informed that they cannot use the ABC-gates, otherwise the attempts to use these could create disruptions in the flow of travellers at border crossings.

RTs with an MRTD would therefore only be able to use manual gates. Also, at manual gates, it would not be possible to reach the same security level in document checks and bearer authentications as with an e-MRTD.

Another differentiating factor is that the RT with MRTD, using the EU/EEA/CH lane, would possibly slow down the process of this lane, because of the manual (ocular) inspection needed.

EU is also requesting and promoting the use of the e-MRTD, because of security, and it is a mandatory requirement, with few exceptions, that the EU citizen who wants to use the ABC-gates must have an e-MRTD.

The 'creation' of a false MRTD is considerably easier than creating an e-MRTD, since the e-MRTD has far more security protection and security features. The risk of TCNs creating false MRTDs that contain (only) the correct RTP identifier can be seen as considerable. This risk is further increased by the fact that the MRTD will (possibly only) be checked, as document, by a border guard including a manual (ocular) facial image verification.

Should this option be retained, it should be clear that this would lead to a number of additional complications at border control when RT MRTD holders nevertheless try to pass through ABC gates and are likely to complain when this does not work.

The main finding is that MRTD would be less beneficial for the RT, would lead to a lower level of security and could not be used in electronic checks, also at manual gates, in the same way as an e-MRTD could be. The number of travellers wanting an RTP status and having an MRTD is estimated to be limited at the time RTP will be operational and the numbers will continue to decrease over the following years.

e-MRTD as a token for RTP

The table below presents an analysis as regards using the e-MRTD as token for RTP.

If the e-MRTD were used as a token for RTP, the actual "token" would be identified in RTP by using the passport number in combination with the country code, from the chip of the e-MRTD. This combination of passport and country code is unique for each and included in every e-MRTD compliant with the ICAO 9303 standard. Such a token would be unique and could be registered at enrolment in the RTP. It would later be used to find out if the traveller has RTP status, supported by a verification of the person, using biometrics, and (when possible) a bearer authentication to ascertain that the bearer of the travel document is also its lawful owner.

Using the e-MRTD as a token for proving the RTP status would have a very limited impact on border crossing processes, whether through ABC gates or manual border crossings. The e-MRTD is the main document used today for most crossings and no new routine or equipment is needed other than what is already in place.

A separate identifier in the e-MRTD (e.g. a stamp) has been discussed in order to let a person with RTP status have the benefit of a simplified border crossing also in degraded mode (especially if there is no access to the central system). It was concluded during the meeting of MS experts held on 16 April 2014 that, in the exceptional event of such a degraded mode, they would check all

passengers thoroughly as for any TCN. The use of a marker in the passport would therefore be of no value, since no proper service of the kind expected for RTP could be provided.

Description and assessment of the options

The two options analysed are:

- a. A separate token in the form of a physical device to prove the RTP status
- b. Using the e-MRTD as the token for proving the RTP status

Option	Advantages	Disadvantages
<p>a) Separate token</p>	<p>Security/data protection: A potentially added security and data-protection advantage, whereby an RTP member would need to be able to present the additional token in addition to his/her passport. The inherent link between the token and the passport details would constitute an additional check in the RTP database. The RTP member's personal details (including biometrics) could only be consulted (by default, in a normal situation) through the use of the separate token.</p> <p>Usability: An RTP member would have a tangible form of membership that could have additional promotional value in relation to the use of the EU RTP. The separate RTP token could carry an easily recognisable visual identity, which would have a "marketing" value. However, this marketing value of the token is inspired from existing national RT programmes which have a more exclusive character (e.g. the Dutch Privium programme with a membership fee of €121 for the basic version) while the current RTP is solely meant to take a frequent traveller TCN out of the queue and is therefore proposed at €20 in the legal proposal.</p>	<p>Costs:</p> <ul style="list-style-type: none"> • Production costs. These yearly costs are estimated at €20 million. • Management costs; these costs could be covered by the RT membership fee. • Logistical costs for sending the token to the RT traveller and/or for distributing it worldwide to consular posts and to border crossing posts in the Schengen Area. <p>Usability:</p> <ul style="list-style-type: none"> • Handling the loss of a token, possible revocation and renewal • Additional scanning at ABC gates: the separate token would need to be read by the passport scanner of an ABC gate, in addition to the passport. This scanning step is the most error-prone and time-consuming activity of an automated gate process and should be minimised. • One more item, besides travel documents, that the RT traveller would have to carry with him/her. <p>Standardisation:</p> <ul style="list-style-type: none"> • The token would need a specific definition and standardisation whose outcome may even delay the use of RTP.
<p>b) Using the e-MRTD as a</p>	<ul style="list-style-type: none"> • Usability: the e-MRTD is an existing item for travellers. 	<p>Usability: The RT would have no visible proof of</p>

token	<p>No additional items to carry.</p> <ul style="list-style-type: none"> • Routines and equipment for reading the e-MRTD exist already. It is well known by the border guards. • The e-MRTD is already used at ABC gates. <p>Standardisation:</p> <ul style="list-style-type: none"> • e-MRTDs follow worldwide-accepted standards both on the format, the data contents and the security features. <p>Security:</p> <ul style="list-style-type: none"> • The intention of protecting the access to personal data with the use of a specific token can also be obtained by protecting personal data by means of an appropriate access mechanism. <p>Costs:</p> <ul style="list-style-type: none"> • Producing and distributing the token will not generate any additional costs. 	his/her RTP status. If the RT database is unavailable and status cannot be confirmed, the RT traveller needs to be handled as a non-RT TCN. However, the likelihood of a long service disruption of the RT system is remote and can be mitigated by system performance requirements.
-------	--	--

Main findings

The separate token provides few significant advantages and increases operational complexity.

The e-MRTD would be less costly and less complex to implement and maintain as a token. It gives the necessary security and has no impact on duration of the crossing.

- **Identification of the possible interactions between EES and RTP (TF7.4)**

This item deals with the way the entry-exit data will be updated for an RT and leads to an investigation into the data location.

The data and biometrics used in each activity related to RTP and EES are described in detail in sections 3.3.2 and 3.3.3.

In short, the interaction between the EES and RTP would be as follows: the registered traveller's personal data (i.e. a minimal dataset as for TCNVEs) will be registered in the EES when he/she applies for RTP status or, alternatively (according to the legal proposal), when the registered traveller first enters the MS concerned. The traveller who has obtained RTP status will then have his/her entries and exits recorded in the EES, using the same data as TCN travellers who are not part of the RTP.

This means that the RTP status from a business point of view could be seen as an additional and optional attribute to a person registered in the EES. This observation is not to be interpreted as promoting one combined system for EES/RTP.

The issue of how the data should be made available to national border management systems and of the location of the data are questions for the architecture area and may also depend on data content/data protection issues.

◦ **Consulting the EES in the VIS application process**

Article 16 of the EES legal proposal states that the EES can be consulted by the authorities issuing visas. The main reason for this consultation is to check if the person applying for a visa would be an overstayer, which could be a reason for not granting a visa, for revoking it or annulling it. The Study proposes that this consultation be conducted in the same way as the EES search described in table 5 of chapter 3.2. This search uses the “issuing country” and “document number” fields as a unique identifier to find the individual file in the EES, which is the only purpose of the search. This data for the search is proposed instead of the data described in Article 16 of the legal proposal.

– **Impact of EES and RTP**

This section of the Study analyses the impact of the EES and RTP on:

- BCP crossing time (TF5);
- average border crossing time for TCNs at entry and exit (TF5.3);
- traveller flows (queues), on EU citizen flows and border crossing time (TF5.4);
- residence permits (TF4.3);
- local border traffic (TF4.4);
- organisation and resources of Border Crossing Points (TF5.5).

This section also highlights the impact differences for air, land and sea borders. The following table summarises the forecasts for the border crossings per type of border in 2020 for the whole Schengen Area (for further details please refer to Chapter 7).

Table 12 Forecast of border crossings in 2020 for the Schengen Area

2020 (in millions)				
	Air	Sea	Land	Total
EU	340	46	91	477
VE	87	10	7	104
VH	66	6	69	141
Total	493	62	167	722

◦ **Impact on Border Crossing Points crossing time, security and complexity (TF5)**

This sub-section of the Study assesses the impact of EES options on border crossing time (D), complexity (C) and security (S) for the first visit and for subsequent visits.

The impact on border crossing time is mainly related to the options for using data and biometrics in the activities of the border crossing process. The data and biometrics used in each activity of the EES and RTP processes for entry and exit are described in detail in section 3.2.3 (EES) and 3.3.3 (RTP).

> **EES (TF5.1)**

In the two pictures below all options that could have an impact on the duration of the border crossings in relation to the EES are listed. For each option, there is an estimation of the added time, if any. The TCNVs and TCNVHs will take different times to cross the border, which is why the table lists separate values for both these categories. The first entry and subsequent entries are presented in separate tables. In the text following the tables, each option (A-E) is described in further detail.

	EES FIRST ENTRY				VISA HOLDER			VISA EXEMPT		
	CRITERIA	S	D	C	Time	S	D	C	Time	
Fingerprint identification	Fingerprint identification (1:N)	N	N	N		++	-	-	20-30	
First entry? Register person in EES	MRZ (for VH also visa sticker number)	N	N	+	0	N	N	+	0	
	Additional, mandatory fields	N	N	N	60-90	+	--	--	60-90	
	8 FP mandatory	N	N	N	0	++	--	--	40-60	
	4 FP mandatory	N	N	N	0	+	-	-	<30 (vendor: 3s)	
	Photo from e-MRTD	+	N	+	0	+	N	+	0	
	Live photo	+	-	-	30	+	-	-	30	
	Photo from print	--	N	N	0	--	N	N	0	
	Date, time, border crossing point, authority, etc	N	N	N	0	N	N	N	0	
	Additional, optional fields	+	--	--	30-60	+	--	--	30-60	
	TOTAL				120-180				170-270	

Figure 14 Impact on BCP crossing time of EES-related options (first entry)

	EES SUBSEQUENT ENTRY/EXIT				VISA HOLDER			VISA EXEMPT		
	CRITERIA	S	D	C	Time	S	D	C	Time	
Verify the person found in EES	1-4 fingerprints	N	N	N	0	+	-	N	15-20	
	Photo from e-MRTD	N	N	N	0	+	-	+	15-20	
Register entry data EES	MRZ (for VH also visa sticker number)	N	N	+	0	N	N	+	0	
	Date, time, border crossing point, authority, etc	N	N	N	0	N	N	N	0	
	Additional, optional fields	+	--	--	30-60	+	--	--	30-60	
	TOTAL				30-60				45-80	

Figure 15 Impact on border crossing duration in terms of EES-related options (subsequent entry/exit)

A – Biometric verification and identification for EES

If a traveller's individual file were found in the EES by a search using issuing country and document number as criteria, the traveller's identity would be verified against the EES, using fingerprints or a photo as a biometric identifier. The use of a photo would in particular be necessary during a transition period, where no fingerprints are used.

For TCNVHs the biometric verification is presumed to be part of the normal VIS checks, at entry. At exit, the photo of the e-MRTD could be used to verify the person's identity with a live facial image, in case the VIS verification is not made, since it is not mandatory.

The impact assessment of EES alphanumeric registration and search options and the summary of main findings are provided in the table below.

The table also contains the assessment of the proposed fingerprint identification to the EES, which could be made at first entry. The objective of this is to eliminate duplicates of the individual file that could occur (e.g. persons with double citizenships, change of passport or fraud).

Table 13 Assessment of options of verification against EES

Option	Duration (s)	S	C	Comment
4-1 fingerprints (VE)	15-20	+	-	The capturing of fingerprints for verification could be done using the existing equipment for the VIS checks. Routines and training courses should already be in place. The fingerprints are verified against the fingerprints stored in EES
Photo from e-MRTD (VE/VH) or a live photo	15-20	+	+	The photo in the e-MRTD could be used to verify the persons against a live photo (for TCN using ABC gate at exit) or for manual (ocular) verification. An alternative would be to compare a live photo (i.e. in an ABC-gate, or a manual gate if this feature is available in a manual gate, could also be compared against the stored photo in the EES. The photo stored in EES would have to be also from the e-MRTD or a live photo in order for the verification to work.
Fingerprint identification (1:N)	20-30	++	-	The fingerprints captured would be used for a 1:N identification with the purpose of detecting duplicated individual files

Main findings

Including the photo in the EES individual file would give more alternatives when it comes to the verification of travellers, to identify overstayers by displaying the photo and, in particular, in the absence of fingerprints (e.g. because of transition or in exceptional cases). It also provides an alternative for verifying TCNVH at exit where fingerprint checks are not mandatory according to the VIS regulation.

The proposed identification would secure that duplicates of the individual files does not exist, causing problems with calculation of days and problems for the traveller, or existing there because of fraud. It has a certain impact on the duration of the check (20-30 sec), there would be additional costs and there are considerations in relation to data protection that must be taken into account, when further considering this proposed activity.

B - Alphanumeric part of the individual file in EES

The MRZs of e-MRTD/MRTD are used, read automatically or manually, to run searches in the SIS II for all TCNs, and to retrieve from the VIS the TCNVHs data. Using the MRZ of the e-MRTD/MRTD also for the purpose of registration in the EES is a very straightforward solution and does not require the border guard to take any additional action. According to assessments made in the study (see also the Data chapter 5) the MRZ data is sufficient for the purpose of the EES. In order to obtain a reference to the VIS, the visa sticker number should also be part of the data registered for TCNVHs.

The legal proposal contains an additional set of data, besides the MRZ data, that is proposed to be mandatory in the EES registration.

The assessment of alphanumeric registration options in EES is summarised in the table below.

Table 14 Assessment of alphanumeric registration options in EES

Option	Duration (s)	S	C	Comment
MRZ + visa number	0	N	++	The MRZ data is already captured in the existing process and would have no impact on the duration. The visa number is captured as part of the normal activities related to VIS.
MRZ + the additional data set of the legal proposal	60-90	+	--	This dataset can partially be captured from the e-MRTD. The additional data is however not mandatory to store in the e-MRTD and three of the requested fields are not in the MRTD or the e-MRTD. Therefore a manual registration would always be needed for these three fields and in many cases of all the requested fields.

Main findings

MRZ + the visa number provide a necessary and sufficient set of alphanumeric data for the purpose of the EES and does not make the border control process longer. A detailed description justifying this finding can be found in section 5.2.

C – Fingerprint enrolment in EES (TCNVEs)

According to the legal proposal it would be mandatory to enrol 10 FPs in the EES registration of the individual file of TCNVEs. The options described below include using fewer fingerprints for the EES registration. Estimates from various projects (e.g. PARAFE (FR), UIDAI (India), VIS and US visit program) have been used to assess the duration. The summary of the assessment is provided in the table below (*for the further analyses please also refer to TF 1.1 Number of FPs to be used in the EES in section □□°*)

Table 15 Assessment of EES options for enrolling fingerprints (FPs)

Option	Duration (s)	S	C	Comment
10 FPs	50-90	++	--	This will have a significant impact in relation to duration and complexity but provides very good security and also better quality in relation to identifications, which is of interest for immigration purposes and LEA to the EES.
8 FPs	40-70	++	-	Enrolling 8 FPs has less impact on duration, compared to 10 FPs, since one step (enrolling thumbs) in the enrolling process is omitted. 8 FP provide a good security and quality for making the identifications mentioned above.
4 FPs	20-30	+	-	Enrolling 4 FPs makes the process shorter while it is assessed (see the chapter on Biometrics) to be sufficient for verification purposes. It brings limitations to making the identifications mentioned above .
< 4 FPs	10-30	N	-	This operation should have limited impact on duration and adds less complexity. The enrolment is similar to the operations done for VIS verification checks and the equipment is available. The security would not be as good as for 4, 8 10 FP. The identifications mentioned above would be less reliable or not possible, depending on the number of fingerprints enrolled.
0 FP	0	N	N	If fingerprints are not enrolled and registered in the EES, the biometric verification could be made using a photo (see assessments above under "A biometric verification for EES") and/or relying on the alphanumeric data and manual verification of the traveller's identity .

Main findings

10 or even 8 FPs seem challenging to enrol in all types of border crossings and various types of conditions. State of the art mobile technology would potentially allow for a maximum of 4 FPs at the time. 8 FP could be enrolled by such a device but would require an extra step that adds some time; For the details on biometric verifications, see chapter 5.4.

D – Photo registration in EES

Introducing registration of a photo requires one of the following options to be used:

- The photo of the e-MRTD is accessible and trustful. To ensure that the photo in the e-MRTD can be trusted, the issuing country certificates must be checked (see chapter 4 on Biometrics).
- A live photo is taken.
- Photo from the printed page of the MRTD is scanned.

All of the options are discussed in the table below, highlighting the impact on duration, security and complexity of BCP.

Table 16 Assessment of photo registration options in EES

Option	Duration (s)	S	C	Comment
Photo from the e-MRTD	0	+	+	Photos from the e-MRTD are reliable (broken chips are estimated to be 1 in a 1,000), of good quality and offer trustful results. BCPs are usually equipped with e-MRTD readers.
Live photo	40	+	-	Taking a live photo must be performed in very good conditions to provide quality results (ICAO compliant quality).
Photo from print	0	--	N	The photo from the biographical page offers very limited usefulness for facial recognition purposes. It is also important to note that by 2020, an increasing number of passports are expected to be e-MRTDs (see working assumptions in chapter 2), which supports the idea of not using the photo from the biographical page for EES registration.

Main findings

The e-MRTD photo should be used to the maximum extent possible for the registration in EES. For travellers with MRTD either no photo is stored in EES or the printed photo is scanned and stored, with very limited use in subsequent verifications.

E – Recording of entry/exit data in EES

For each entry and exit, data in accordance with the table 5 in chapter 3.2 would be recorded.

MS experts have proposed registration of additional, optional fields. These would mainly relate to data on travel and transportation. In most cases they would have to be entered manually.

Table 17 Assessment of entry/exit data recording options in EES

Option	Duration (s)	S	C	Comment
Data on the entry and exit	0	N	N	All the requested data can be automatically obtained from the related systems (national border applications and EES) and would be updating EES in a background transaction. There would therefore be no impact on duration.
Additional (optional) fields	30-60	+	--	Manual registration would be required in many cases, where data cannot be obtained from other sources (e.g. API).

Main findings

The data recorded at entry and exit is sufficient for the purpose of the EES. Additional optional fields could be useful for immigration control and law enforcement purposes. These would, however, add to the duration of the crossing. The additional optional fields are described in chapter 5 and also in section 3.2.3 (table of data being used per activity)

> **RTP (TF 5.2)**

This sub-section of the Study assesses the impact of the RTP on border crossing time, security and complexity. The RT border crossing process needs to be designed in a way that the border crossing time is significantly reduced. The RT is expected to be able to use existing ABC gates but should also yield a benefit in the event that there is only a manual process at a particular BCP.

The description of RTP alphanumeric check options, as well as their impact assessment on BCP crossing time is provided in the table below (A - verification against RTP).

In the picture below, all options are listed that could have an impact on the duration of the border crossings in relation to RTPs. For each option there is an estimation of the added time, if any. There is only a limited difference made between TCNVes and TCNVHs, in relation to how the process works, since they are presented here mainly as RTP members.

There is no difference between first entry and subsequent entries in the processing.

RTP Entry/Exit	VISA HOLDER				VISA EXEMPT				
	CRITERIA	S	D	C	Time	S	D	C	Time
1-4 fingerprints		N	N	N	0	+	-	N	15-20
Photo from e-MRTD		N	N	N	0	+	-	+	15-20
Date, time, border crossing point, authority, etc		N	N	N	0	N	N	N	0
TOTAL									15-20

Figure 16 Impact on BCP crossing time of RTP related options

The retrieval of the RTP record is not considered to extend the duration of the border crossing. Only the options for A and B are presented in the assessment below. For TCNVH using manual gates there is no added time since the VIS check/biometric verification replaces any need for making a biometric verification to RTP.

A – Biometric verification for the RTP

Once the RTP record is retrieved the traveller must be verified. This is done as follows:

- **ABC gate (using photo).** The traveller is verified using a live photo compared against the photo in the e-MRTD. **It is the same verification as what is described as “Bearer verification” in Table 6 Description of the RTP application / enrolment process.** Another option could be to compare a live photo to the photo stored in the RTP;
- **ABC gate using fingerprints.** The traveller is verified using live captured fingerprints compared against to the fingerprints stored in the RTP, or against the VIS if the traveller is a TCNVH;
- **Manual gates.** The traveller is verified using live captured fingerprints compared against the fingerprints stored in the RTP or against the VIS, if the traveller is a TCNVH. If need be a manual (ocular) verification using the stored photo in the RTP could be made.

Assessment of options of verification against the RTP is provided in the table below.

Table 18 Assessment of options of verification against the RTP

Option	Duration (s)	S	C	Comment
1-4 fingerprints (VE)	15-20	+	-	<p>The verification using fingerprints can be made at ABC gates that can handle fingerprints or at manual gates, using the existing equipment for the VIS checks.</p> <p>Routines and training should already be in place. The fingerprints are verified against the fingerprints stored in the e-MRTD, or against the ones stored in the RTP or the ones stored in the VIS.</p> <p>Clarification: The negative impact, represented by the "-", as regards complexity for using fingerprints is mainly related to the fact that fingerprints in the e-MRTD are difficult to use in automated verifications (complexity of EAC key dissemination).</p>
Photo (e-MRTD)	15-20	+	+	<p>The e-MRTD photo would be used to verify the identity of the traveller against a live photo (ABC gates) or the photo stored in RTP upon RTP enrolment or by a manual (ocular) verification).</p>

Main findings

It is fair to assume that the most common case for verification of a traveller with RTP status would be ABC gates, using a live photo and checking it against the e-MRTD complemented by a successful automated check of the status in the central system on the basis of the token. In manual gates the live fingerprints can be compared with the fingerprints stored in the RTP (for VH the VIS check is trusted). Using fingerprint comparison to the fingerprints stored in the e-MRTD is an unlikely case given that the solution for a secure distribution of EAC keys to all countries issuing e-MRTD is unlikely to be in place. .

B – Recording of entry/exit data in EES

For each entry and exit, data in accordance with table 5 in chapter 3.2 would be recorded. Given the purpose of the RTP status and the aim to have a shorter time for border crossings (e.g. no questions asked at entry), it is logical, and recommended, not to include any additional optional fields.

Table 19 Assessment of the option of entry/ exit data recording in the EES

Option	Duration (s)	S	C	Comment
Data on the entry and exit	0	N	N	All the requested data can be obtained from the related systems (national border applications and EES) and would be updating EES in a background transaction. No impact on duration.

Main findings

The proposed data recorded at entry and exit is sufficient.

Main findings

EES (TF5.1): Including the photo in the EES individual file would give more alternatives when it comes to the verification of travellers, in particular in the absence of fingerprints and also for more verification of TCNVH when exiting and fingerprint checks are not mandatory according to the VIS regulation. The proposed identification (1:N using fingerprints) would secure that duplicates of the individual files do not exist.

The MRZ and visa number provide a necessary and sufficient set of alphanumeric data for the purpose of the EES and does not make the border control process longer.

Regarding FPs, 10 or even 8, seem challenging to enrol in all types of border crossings and various types of conditions. State of the art mobile technology would potentially allow for a max of 4 FPs to be read in one step. 8 FP could be enrolled by such a device but would require an extra step that adds some time.

The e-MRTD photo should be used to the maximum extent possible for the registration in EES. For travellers with MRTD either no photo is stored in EES or the printed photo is scanned and stored, with very limited use in subsequent electronic verifications but could be used in manual (ocular) verifications.

The data recorded at entry and exit is sufficient for the purpose of the EES. Additional optional fields could be useful for immigration control and law enforcement purposes. Capturing these additional data would, however, add to the duration of the crossing.

In Chapter 8, these results and the options examined so far will be combined to form different Target Operating Models (TOMs), which provide the outline of different designs for the EES and RTP. The below tables summarise the characteristics and options that will be selected for each TOM.

With reference to TOMs A, B and C:

1st entry	TOM A	TOM B	TOM C
Number of fingerprints	0 (VE)	4 (VE)	8 (VE)
	10 FP's (VH) are already enrolled in VIS		
Combinations of FI and Number of FP	e-MRTD: retrieve photo or use live photo MRTD: use scanned photo No FP	e-MRTD (retrieve photo or use live photo) MRTD: use scanned photo 4 FPs (VE)	e-MRTD (retrieve photo or use live photo) MRTD: use scanned photo 8 FPs (VE)
Expected time (duration in sec)	5	45-65	65-95

Entry/Exit (search & verification)	TOM A	TOM B	TOM C
Number of fingerprints	VH: 1, 2 or 4 live FP, against VIS (as of today)	VE: 1, 2 or 4 live FP, against EES VH: 1, 2 or 4 live FP, against VIS	
Combinations of FI and Number of FP	Use photo VH: 1, 2 or 4 live FP, against VIS (as of today)	Use photo <i>OR</i> VE: 1, 2 or 4 live FP, against EES VH: 1, 2 or 4 live FP, against VIS	
Expected time (duration in sec)	15-20	35-50	

RTP (TF5.2): It is fair to assume that the most common case for verification of a traveller with RTP status would be ABC gates, using a live photo and checking it against the e-MRTD. In manual gates the live fingerprints can be compared with the fingerprints stored in the RTP (for VH the VIS check is trusted). Using fingerprint comparison to the fingerprints stored in the e-MRTD is an unlikely case given that the solution for a secure distribution of certificates EAC keys to all countries issuing e-MRTD is unlikely to be in place.

With reference to TOMs M and N:

Type of Biometric	TOM M	TOM N (RTP alternative proposal)
1st entry	(VE) 4 FPs	No FPs - FPs retrieved from EES No photo – Photo retrieved from EES
Entry/Exit (search & verification)	Retrieve e-MRTD: photo or use live photo VE: 1, 2 or 4 live FP, against RTP VH: VIS check is trusted	Retrieve e-MRTD: photo or use live photo VE: 1, 2 or 4 live FP, against EES VH: VIS check is trusted

- ***Impact on average border crossing time for TCNs and general impact on queues at entry and exit (TF 5.3 and TF 5.4)***

The average duration of the border crossing, including queuing time, depends not only on any added activities/elements related to EES in the border crossing process, but also on a number of factors for each particular border crossing, such as:

- The relationship between the number of TCNVEs, TCNVHs and EU/EEA/CH travellers;
- The number of persons who are allowed to cross as part of regional agreements (e.g. Local Border Traffic);
- The flow of traveller and the peak pattern (e.g. travellers arriving from a ship or a flight in large numbers to the border check or travellers departing from an airport, arriving in a period of around 2 hours before the boarding of the flight);
- Infrastructure (e.g. technical equipment, ABC gates, number of booths and lanes);
- Space (e.g. constraints in the space for making checks);
- The use of biometrics and data sets for EES registration;
- The options chosen in relation to the use of biometrics and data (e.g. enrolling 8 or 4 fingerprints in the individual file).

Main findings

The main findings are based on the analysis of added durations and the simulations of border crossing flows at air borders and land borders that have been executed.

An added duration below 60 seconds at first entry has very limited impact on service levels and average dwelling time. An added duration below 30 seconds at subsequent entries and exits, has virtually no impact on services levels or dwelling time. It should be noted that this relates to the overall situation. Depending on how queues are arranged any added duration would have an certain impact on the individual TCN.

An added duration above 60 seconds would have an progressively increasing impact on service levels and dwelling times. The use of the duration of 60 and 30 seconds as a reference in this assessment is corresponding roughly to the maximum added durations of the TOMs that are presented in chapter 8.

> *Impact on average border crossing time*

Sections 3.4.1.1 and 3.4.1.2 gives the estimated added duration for various options and also a potential total added duration, with a range, if all possible options would be retained.

Simulation of border control processes

For indicating the impact on average border crossing time an activity simulation was performed together with Frontex, using a proven tool. The simulation and the results are described in detail in Annex J.

Real data from an air border and a land border was used in the simulations. For the air border both the entry and exit processes were simulated, and also the use of ABC gates (which gives indications relevant for RTP travellers). For the land border only the exit process could be simulated as the entry process and in particular the queuing occurs on the side of the border of the neighbouring non-EU country.

One part of the simulation is the analysis of the impact on service levels in relation to added duration of the border check. The service levels are to 2, 5 and 10 minutes for the concerned air border. For the land border simulation the services levels of 10 and 30 minutes were used. This service levels defines the objective to serve the traveller within a given time and includes the dwelling time (i.e. the time from when the passenger arrived to the queuing area till the check is made). These levels can be seen as indicating average durations for the border crossing process.

The simulations also included how the dwelling time is impacted in relation to added duration of the border checks and the potential impact on workload. Observations in relation to dwelling time and workload are used in subsequent chapters, assessing queue impact and workload.

Simulation observations – Service levels at air borders

1. An added duration of less than 60 seconds in average, at first entry, has a very limited impact on **“service level 2” and no impact on the other service levels. It should be noted that the service level of 2 minutes is extremely challenging and basically used only for ABC gates.**
2. An added duration of more than 60 seconds in average, at first entry, has the following impact:
 - **A measurable impact on the “service level 2”, which has the objective to serve a traveller within 2 minutes. Once the additional tasks implied by EES equals 60 seconds the decrease of services level becomes steeper.**
 - Services levels of 5 and 10 minutes are in principle not affected by this duration.
3. At subsequent entries and exits an added duration of 30 seconds or less has in principle no impact on service levels.

Simulation observations –impact of RTP at air borders

For the air border both the entry and exit processes were simulated, and also the use of ABC gates (which gives indications relevant for RTP travellers). In this section only the observations related to the use of ABC gates are presented.

1. The use of ABC gates for RTP travellers makes it possible to keep a higher service level than at manual gates. The service level (2 min) used in the simulation includes dwelling time;
2. The general trend is that the more crossings made by RTP travellers the more improvements can be seen in terms of service level compliance at the manual gates, less dwelling time and less workload. In the case of 5 % of RTP crossings the service level of the ABC gate is not impacted while the manual service level is improved with 2 % and the service level of 5 minutes improves 3%;
3. The simulation also showed that in case the ABC gates are not dimensioned for the increased number of crossings, the service levels and dwelling time for the ABC gates are impacted negatively. Of course if the number of EU/EEA travellers increase beyond what the configuration of ABC gates can handle, this has the same impact. The positive impact on the manual gates would still remain, also in this case.

Simulation observations – Service levels at land borders

1. At a volume of 16000 vehicles/month and an added duration of 60 seconds per vehicle, at exit the services level compliance of 30 minutes decreases with around 2%, which corresponds to an average added duration of 36 seconds per vehicle. It should be noted that the service level includes dwelling time.
2. It should be noted that the added duration, caused in relation to EES, is simulated per vehicle. An added duration of 60 seconds corresponds, in the case studied, to an added time per person of around 30 seconds (for verification only, since this is an exit) as there were on average two persons per car.

> Impact on traveller flows and queues

A. Traveller flows and queues (TCNs)

The elements that could cause added time for queuing, in relation to the implementation of EES and RTP are described in sections 3.2 and 3.3. As mentioned the choice of options have a consequence on the potential added queues that could be a result of new activities in the border check process.

The simulation made together with Frontex (see Annex J for all details) provides results that can be used in respect of assessing flows and queues.

B. Traveller flows (EU/EEA/CH)

Since EU/EEA/CH travellers can use dedicated lanes when arriving at an entry or exit border crossing, these flows should not be impacted by the introduction of EES. Some elements, however, could impact the flows for EU/EEA travellers:

- RTP travellers are supposed to use the EU/EEA/CH lanes and ABC gates. Depending on the volumes of travellers enrolling for RTP and how this increased demand is met at the specific checkpoint, there could be an impact on duration and queues. The management of queues is up to the local authorities within the legal framework set out in the SBC;

- Extended duration of checks for TCNs possibly causing growing queues in certain cases could lead to the need for allocating lanes normally used for EU/EEA/CH travellers as TCN lanes, thereby possibly reducing the services provided to EU/EEA/CH travellers.

The Study proposes the option to allow TCN use ABC-gates at exit. This could also have an impact on the volumes of travellers using ABC-gates. The assessment above is only related to the use of the EU/EEA/CH queues, which does not include TCN in general, but only RTP members and some other cases (e.g. TCN that are family members of EU citizens).

Simulation observations – traveller flows at air borders

In line with the results for the service level presented in section 3.4.2.1, the introduction of the EES has a limited impact on the average dwelling time at the first entry⁴⁵, going from 1 minute 50 seconds to 2 minutes 6 seconds, and virtually no impact on subsequent entries and at exits⁴⁶. Further details can be found in Annex J.

Simulation observations – traveller flows at land borders

At a volume of 16000 vehicles/month the addition of 60 seconds per vehicle for the introduction of the EES, increases the dwelling time with around 3 minutes. An added duration of 30 seconds (as could be the case for subsequent entries or exits) has, instead, showed no impact on the dwelling time.

◦ ***Impact on the resources of Border Crossing Points (TF 5.5)***

This chapter analyses the potential impact on resources, in relation to the implementation of EES and RTP, at the external border crossing points. The impact on resources is dependent on the following factors:

- The specific conditions at the concerned border crossing point (e.g. land border, volumes, management of lanes, categories of travellers, infrastructure);
- The pattern of arrival to the border checks (e.g. there could in one BCP be a continuous flow that is quite even for a longer time over the day while another BCP may have a pattern with massive numbers of passengers arriving in a quite short time, creating peaks);
- The current situation as regards the organisation of lanes, as described in the Schengen Borders Code;
- The analysis of options for use of data and biometrics;
- The assessment of durations (see section □□);
- The use of EU/EEA/CH lanes for RTP travellers;
- The proposal to make use of automated exits for TCN travellers (see 3.5.5).

The simulation results as regards impact on the workload can be used for indicating if and to what extent more resources could be needed. It is based on real data from an airport and from a land

⁴⁵ Assuming an estimated additional 60 seconds due to the introduction of the EES.

⁴⁶ Assuming an estimated additional 30 seconds due to the introduction of the EES.

border. It should be noted that the results might not be generically true for any BCP but could be used as an indication on the potential impact on resources. This result cannot be used to make the conclusion that additional resources are needed. The need for a resource increase is also related to the specifics of the border crossing (e.g. peak patterns over the day or over a period).

Main findings

A general conclusion, with the reservations described above, would be that an added duration above 60 seconds could cause a more significant increase in the workload, temporary or over a longer period. The calculated increase would be around 10 % for 60 second of added duration. This assessment is based on simulations of entry checks at air border and exit checks at land border.

Simulation observations – impact on workload at air borders

1. At subsequent entries and exits an added duration of 30 seconds or less has in principle no impact on the workload.
2. An added duration of more than 60 seconds, at first entry increases the workload by around 9 % (at 60 seconds) of the workload necessary for the entry checks;

Simulation observations – impact on workload at land borders

3. At a volume of 16 000 vehicles/month, 44 % of the time the guards are active with checks, if no time is added. At 60 seconds of added duration the usage factor becomes 56 %, an increase of around 12 %. This gives still a margin to handle peak situations.

1.3.1. Impact in relation to Local Border Traffic (TF 4.4)

Local border traffic is often creating high volumes of border crossings, in particular at land borders.

The question here is whether travellers in possession of a local border traffic permit would be negatively impacted by the implementation of EES and RTP. If this were the case, then it would be of interest to study mitigations related to this consequence.

Overview of existing provisions for local border traffic

TCNs living in a border region can apply for and travel on the basis of a permit (called LBT) which simplifies border crossing, rather than using a short stay visa. With this LBT they may travel up to 30 km within the neighbouring Schengen country and stay in that area up to a maximum 3 months. The precise duration of the stay is determined in the Local Border Traffic agreement between the Member State and the neighbouring country. This permit and the conditions to be fulfilled in Local Border Traffic Agreements are defined in Regulation (EC) No 1931/2006, which provides an exception to the Schengen Convention. The local border traffic regime constitutes a derogation from the general rules governing the border controls on persons crossing the external borders of the Member States of the EU which are set out in the Schengen Borders Code (Article 35 of the SBC)..

Today eight Schengen countries (Spain (ES), Hungary (HU), Latvia (LV), Norway (NO), Poland (PL), Romania (RO) Croatia (HR) and Slovakia (SK)) issue LBT permits with at least one non-EU neighbouring country. The figure below provides statistics regarding the total number of LBT permits issued along with the average number of permits issued per year over the past six years.

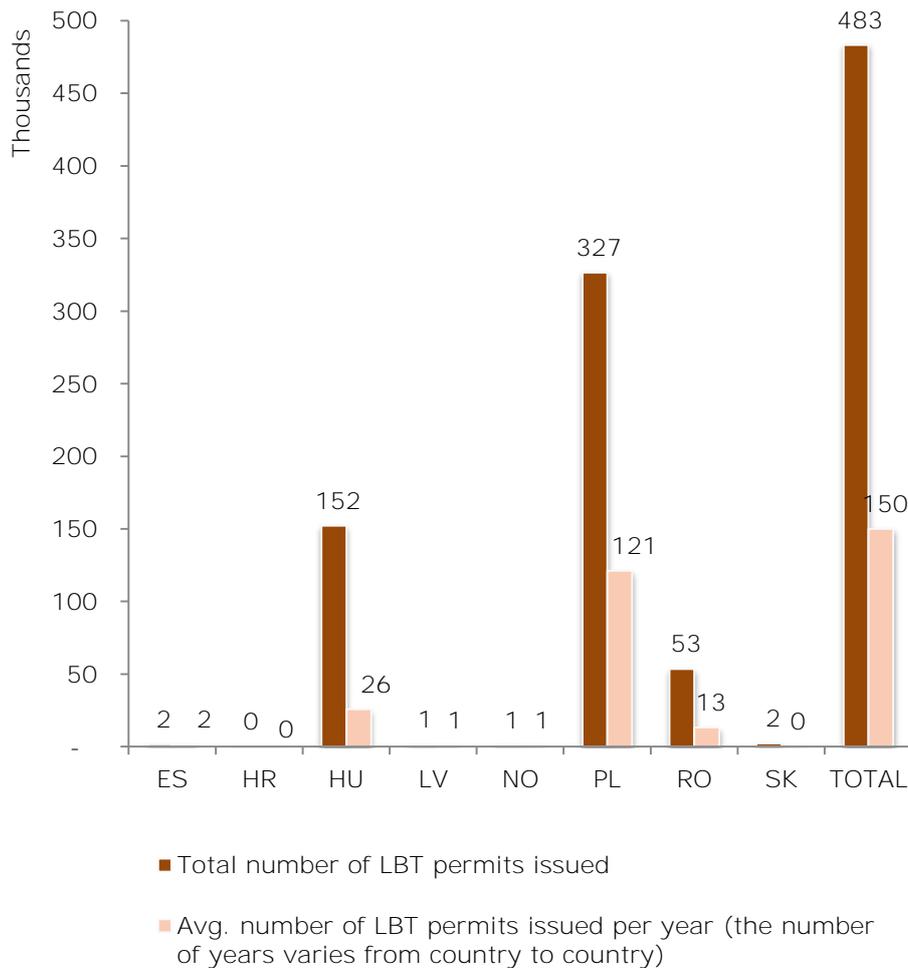


Figure 17 Total and average number of LBT permits issued by country; Source: DG Home Affairs 2014

The total number of LBT permits issued since 2009 is currently less than 500,000. However they account for an estimated 7.5 to 10 million border crossings at land borders as LBT permit holders have a need to cross the border very frequently, otherwise granting of the permit would not even have been considered.

Persons carrying these permits do not have their passports checked for former stamps as their passports are not stamped when they cross the border. According to the information provided in an expert meeting⁴⁷ involving the countries presently handling LBT permits, the permit holders entries and exits are registered in their national EES (entry exit system). The main reason is to keep a record for checking the length of their stay with respect to what the permit allows. By analogy with the existing routines it was clearly stated that particularities different to normal EES stay duration would have to be coded in the calculation of stay module in the central EES in case LBT entries and exits would also be included. The added value, besides calculating the stay, could be that other countries can use the information in cases where a person with an LBT permit misuses the rights this permit gives.

⁴⁷ The meeting was held on 29 April 2014. The remaining MS that use LBT permits, but that did not participate in the meeting, have answered via e-mail, along the same lines as the MS that participated.

The experts participating did not express any request for any automatic registration of persons with LBT permits in the RTP, and saw the application to RTP as a separate process, to be carried out as for any TCN applying for short-stay in the Schengen area.

Description and assessment of the options

With the background information on existing provisions for local border traffic permits, the following options that are not all mutually exclusive could be envisaged:

- a. The LBT process remains as it is and could work well for the persons carrying the permits and for the border checks, after implementation of the EES and RTP. At present, there are no stamps or stamp checks made for these persons, and the purpose of the EES, which is to replace the stamps, would not affect the LBT permit holders as far as the stamping is concerned.
- b. The persons holding an LBT permit are entered into the EES. This option could give the concerned Member States support as regards calculation of the stay related to the LBT permit. If the need arises, other Member States would also be able to see the persons with LBT permits in the EES. However, the authorised period of stay in the LBT is computed differently than that of short stay as defined in the SBC (i.e. 90 days within any 180 day period). The holder of a local border permit can move freely within the border area for a period up to three months if his/her stay is uninterrupted and has a new right to a complete period of stay each time his/her stay is interrupted. Moreover, the stay of the holder of a local border permit must be regarded as interrupted as soon as the person concerned crosses back into his/her state of residence irrespective of the number and frequency of border crossings made. This would imply that a specific calculation method would need to be included in the EES for this category.
- c. The person holding an LBT permit, in addition and if desired, could apply for RTP status with the prerequisites and rules as for any other TCN – this could be justified in case the person has other legitimate (professional or personal) interest to travel outside the area covered by the LBT. The RTP status is fully separated from the LBT permit; assuming that the authorities would not revoke the LBT permit, this could still be used for local border crossings.
- d. In the case a negative impact is detected on the conditions applicable for these travellers when crossing the borders (longer queues and/or additional dwelling times) at a particular border crossing point, the dedication of specific lanes could be envisaged (this option is not included in the table below – see instead section on Process accelerators, 3.5). This should be decided on the basis of the logistical constraints and opportunities applicable in the given BCP and depending on whether EES and RTP are applicable to these persons. Art 15(b) of the LBT Regulation provides that the bilateral agreements may provide for border crossings to be eased, whereby Member States may, inter alia, reserve specific lanes to border residents at border crossing points.

The options of EES and RTP solutions that would address facilitation and security of LBT permits are assessed in the table below. The table addresses also in which extent travellers in possession of a local border traffic permit would be negatively impacted by the implementation of EES and RTP.

Table 20 Description and assessment of the options related to Local Border Traffic

Option	Advantages	Disadvantages
a) LBT process remains the same	This option would work well also with the introduction of EES. It cannot be concluded at	LBT permit holder overstays would not be detected by the EES. Risk of LBT overstay would be addressed by the same means as currently.

Option	Advantages	Disadvantages
	<p>present that these persons would be significantly impacted by the implementation of the EES and RTP (see also section 3.4 as regards assessments of duration and simulations made by Frontex).</p> <p>At any rate, as long as the persons with LBT permits share the same lane as other TCN, any added duration due to EES would impact all persons queuing.</p> <p>It would keep the EES calculation mechanism more simple</p>	
<p>b) The persons holding an LBT permit are entered into the EES</p>	<p>The EES could manage the calculation for the LBT permits and other MS would be aware of that a person with an LBT permit was allowed to enter.</p> <p>A simplification occurs as regards the number of systems to be used by Border Guards: These travellers would be recorded in the same way as other travellers are recorded in EES and entry/exit dates are checked vs. the entitlement that gives access to the Schengen area. This advantage can however be achieved without entering LBT data into EES, by adapting national systems.</p>	<p>EES is not a solution aimed at decreasing the duration at border crossings. Entering these persons in the EES can therefore never be seen as a measure for making the border crossing more efficient, for persons with LBT permits.</p> <p>If entered in EES the impact on duration is assessed as moderate (depending on options retained) in relation to duration of the border crossing.</p> <p>The rules for the calculation of stay for persons with an LBT permit are different from those for TCNs that have entered the Schengen area on other grounds (VE of VH). This would add some complexity to the EES process, in particular as regards the LBT permit data that would have to be hosted, even if this data set remains minimal.</p> <p>Moreover, for those persons reaching another Member State, there would be no means to enforce the rule that remain specifically applicable only to the Member State that issued the LBT.</p> <p>The need for other MS to know about persons with LBT permits staying in the Schengen territory is not obvious. An MS survey conducted in 2013 by the Council WP on Frontiers/False Documents concluded that there were few abuses of LBT and this is why the benefit of other</p>

Option	Advantages	Disadvantages
		Member States finding the registrations in EES would be limited.
<p>c) The person holding an LBT permit, in addition and if desired, could apply for RTP status with the prerequisites and rules as for any other TCN</p>	<p>Applying to the RTP is a separate process, available for all TCN that are VE or VH with MEV and otherwise eligible for this program.</p> <p>As regards the option for persons with LBT permits to apply for RTP status there are no specific aspects to include.</p> <p>These persons also have a LBT permit must be taken into account as a separate fact at the concerned border checks.</p>	

Main findings

Persons holding an LBT permit do not currently have their travel document stamped.

Entering these persons in the EES would add to the duration of the border crossings since they would have to be enrolled in the EES and their entry/exit records entered in this system.

As long as persons with LBT permits share the same lane as other TCN they are impacted by any added duration of the border crossing that the EES could bring. Organisational solutions (see section 3.5) should therefore be looked at to remedy this fact.

The proposal of entering them in the EES, to facilitate the calculation of stay related to the LBT permit, is of limited added value compared to the complexity of the calculation of the authorised stay of this category in the EES and added duration at border checks this would bring.

- ***Impact in relation to residence permits in EES and RTP (TF4.3)***

The objective of this sub-section of the Study is to analyse any potential negative **impact in relation to persons having a residence permit, due to the implementation of EES and RTP**.

Overview of residence permits

A Member State can issue a **temporary (short-term - ST) residence permit** only valid for the country where the person resides. The validity of this permit is normally one, two or three years and it can be renewed.

The Schengen Convention⁴⁸ states that: "*Aliens who hold valid residence permits issued by one of the Member States may, on the basis of that permit and a valid travel document, **move freely for up to 90 days in any 180-days period** within the territories of the other Member States,*

⁴⁸ Article 22 of the Schengen Convention as amended by Regulation 610/2013

provided that they fulfil the entry conditions referred to in Article 5(1)(a), (c) and (e) of Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) () and are not on the national list of alerts of the Member State concerned."*

A TCN residing for more than 5 years in the same Member State may receive a **long-term (LT) residence permit**. For the long-term residence permit there is an EU Directive⁴⁹ while at the same time there are still **national long-term residence permits being issued**. The EU LT residence permit also contains provisions for residing in an EU Member State different from the Member State that issued the residence permit. It is estimated⁵⁰ that there are 2.5 to 3 million EU LT residence permits and 2.5 to 3 million national long-term permits.

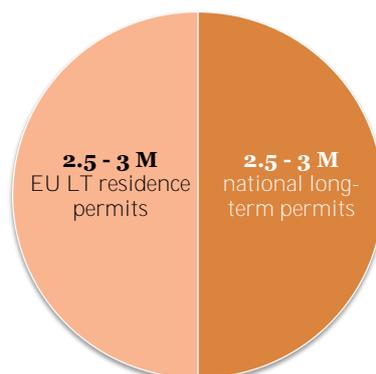


Figure 18 Estimation of the number of resident permits in Europe. Source: DG Home Affairs (2013)

Albeit person holding a residence permit of any kind today could⁵¹ have his/her passport stamped, the stamping is not needed for any calculation related to the allowed stay within the Schengen territory, for VE and VH persons, but would rather be used by the Member State which issued the residence permit to verify that the holder of this permit is not absent from its territory for a longer period, which would entail the loss of the residence rights in the given Member State. Residence permits are normally checked upon arrival at the external border and in other relevant situations.

Description and assessment of the options

There are three options to investigate in this area:

- a. **Persons with residence permits are treated the same way as today by some Member States.** The stamping made today, to verify that the holder of the permit still respects the conditions for the issuance of the permit, could be done;
- b. **Registering persons with residence permits in the EES.** The main reason for such an arrangement would be to have the EES providing calculations that can be used to determine whether the person has stayed too long **outside** the territory of the Member State which issued the residence permit, which would entail the loss of the residence permit. However, in such a case, the calculator needs to be adapted for the holders of residence permits as the main purpose of the EES is the verification of the respect of stay **within** the Schengen area (90 days

⁴⁹ [Directive 2003/109/EC](#) of 25 November 2003

⁵⁰ Source: DG Home Affairs, 2013

⁵¹ In the opinion of the Commission this is not a necessary measure for holders of residence permits

within any 180 days period) and not to verify whether a person might have stayed outside the Schengen area for a longer period than accepted by the Member State which issued the permit;

- c. Registration of persons with **EU residence permits in the RTP**. Persons holding a valid residence permit may apply, be checked and granted RTP status by a competent authority and pay the fee for this. It has been made clear at Member State expert meetings that no automatic registration of residence permits should be made in the RTP. This last option is the one contained in the existing legal proposal.

The table below provides the options of residence permits in relation to the EES and RTP.

Table 21 Description and assessment of the options related to residence permits

Option	Advantages	Disadvantages
a. Persons with residence permits are treated the same way as today	Since they would not be registered or checked in the EES, the duration of their border check, at the crossing, should not be impacted.	
b. Registering persons with residence permits in the EES	Adds a possibility of calculating whether the person has stayed too many days outside the Schengen area to keep the permit	This proposal would have the following disadvantages: <ul style="list-style-type: none"> • The calculation of stay for residence permit holders in EES would be a separate and new function, in relation to what is proposed for the EES; • Any added duration due to the EES process adds to the duration of the check compared to the situation of today this would have a negative impact on border crossing duration for these persons.
c. Registration of persons with EU residence permits in the RTP	This would be treated as for any TCN that would apply for RTP status. RTP status would provide increased facilitation at the border crossing.	

Main findings

Given the above consequences and the fact that any stamping made today is for the purpose of controlling the obligations related to the residence permit and not for their right to stay in the territory as VE or VH, it would be recommended not to register persons with residence permits in the EES.

◦ **Variations for air, land and sea borders (TF4.2/TF8.3)**

This section aims at describing and assessing constraints and conditions for air, land and sea borders where certain options related to the EES and RTP could be challenging to manage. The

impact assessments in earlier sections of section 3.4 (e.g. 3.4.1) are still valid in general for all border types and should be used as a reference when reading this section.

The impact assessed in this section mainly relates to the use of data and biometrics in the EES and RTP, since these are vital for the processes but can also bring challenges when it comes to implementing the same requirements at all types of border crossings.

Below is a non-exhaustive graph that depicts the types of border crossings that have to be looked at. The percentage presented in the picture, given by border type, reflects the number of Border Crossing Points (in total 1800).

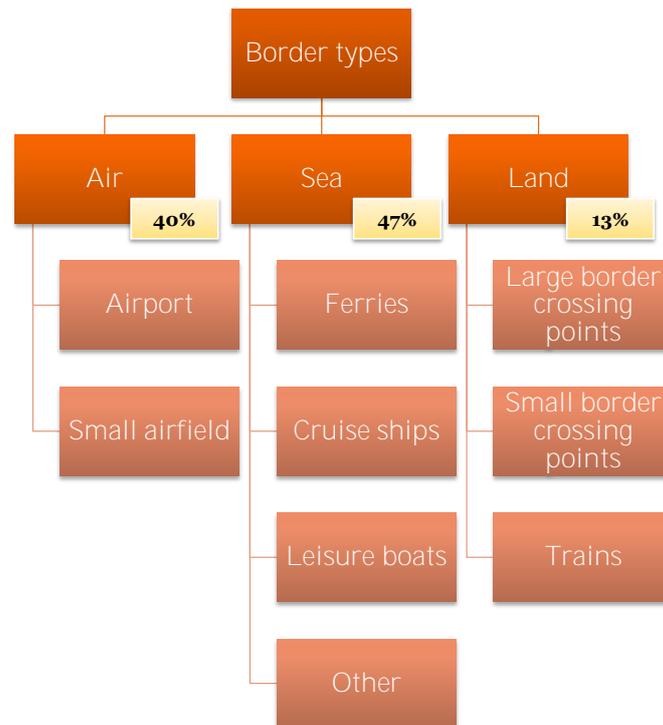


Figure 19 Border types. Source: Official Journal Annex 4

> *EES - Differences in conditions at borders*

The difference of impact is not only relevant to assess based on the type of border but also in relation to the size of the border crossing, i.e. the number of border crossings. A large land border or a ferry terminal can most often be seen as equal to a large airport, in terms of the equipment in place, queue arrangements and resources.

The impact of EES, in relation to the use of data and biometrics, could therefore be similar in all these larger border crossings but more significant or complex to handle with the desired requirements in a small border crossing, be it an airfield, a small land border, a train or a small port. The Impact Assessment of the RTP⁵² estimated an average time for border checks for visa holders on entry at air borders of 1 minute 44 seconds, for visa-exempt third-country nationals, 1 minute 3 seconds and for EU citizens 15 seconds. The average time at air borders on exit is 1

⁵² European Commission, Impact Assessment: Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council Establishing A Registered Traveller Programme, SWD(2013) 50 final, 28.2.2013, p. 16.

minute 11 seconds for visa holders, 52 seconds for visa-exempt nationals and 15 seconds for EU citizens. Average border checks for third-country nationals at land borders last 10-30 seconds longer than at air borders.

The following elements should be taken into account when looking at the impact the EES could have at various types of borders:

- The alphanumeric search and registration of alphanumeric data in the EES, using a limited data set (MRZ), would have a limited impact (see also chapter 3.4.1.1, table 12), regardless of the type and size of border crossing. Today the MRZ is already used for checks in the SIS II, and these checks are mandatory for any kind of border crossing.
- According to the VIS regulation, all types of first line controls at borders should be equipped and able to capture as many fingerprints as used for the check in the VIS. This equipment and the routines that exist should be taken into account when looking at the need for fingerprint enrolment and verification at various types of borders.
- Small Border Crossing Points, be it air, land or sea, and border checks in trains should have the same possibility since they are also subject to the VIS requirements.

Note: All the descriptions below, related to the implementation of EES in various conditions, follow the same process as described in section 3.2. This means for instance that the registration of the individual file of a person, in the EES, is only made a first-entry within the data retention period for the EES.

Summary of conditions and options for checks at different border types

The equipment in the summary should be seen as the minimal requirements, for the border type, related to Schengen Border Code and other relevant instruments (e.g. SIS II and VIS regulations). The options for use of biometrics are based on assessments of feasibility described in the biometric chapter. Some of the options and the related constraints could be proposed to further check in the pilot (e.g. using handheld devices for enrolling 4 FP). This summary is based on currently (2014) widely available technology and does not yet take into account new evolutions in biometric capturing devices.

The summary relates only to the use of biometrics and electronic use of data from the e-MRTD. Checks where MRTD are used are not part of this table, but would be carried out as of today, or as described in the EES process, if relevant.

Note: The descriptions of options in the table below are to be seen as constraints that must be taken into account in the assessment and choice of options to check in the pilot. The Border types are to be seen as indicative and not as a strict definition. There could be small border crossings extensively equipped and with good spacing facilities and there could be large border crossings that are not having the type of equipment or conditions listed in the table. It is recommended and assumed that the number of fingerprints to enrol for the individual file would be the same at any border crossing.

Table 22 Summary of the specific conditions and options for air borders

Border type	Equipment/infrastructure	Conditions and constraints	Options for biometrics (photo)	Options for biometrics (FP)
Air border				
International airport (regular Schengen flights)	<ul style="list-style-type: none"> Fixed equipment for control and use of e-MRTD Fixed fingerprint scanners for 1-4 FP verification to VIS Fixed workstations for border control applications Lane separation with flexible usage ABC gates (optional) Kiosks (optional) 		<p>Photo from e-MRTD can be read and used for verification</p> <p>Live photo could be used in ABC gates</p>	<p>4-8 FP possible for enrolment in EES</p> <p>1-4 FP for verification</p>
Airfield with limited/irregular non-Schengen flights	<ul style="list-style-type: none"> Fixed or mobile equipment for control and use of e-MRTD Fixed or mobile fingerprint scanners for 1-4 FP verification to VIS Fixed workstations or laptop/mobile devices for border control applications 	<p>Checks could have to be made outdoors in some cases, depending on limited infrastructure.</p> <p>In these cases cold weather can make it difficult or impossible to capture fingerprints. In such conditions other solutions (e.g. indoor, permanent or temporary, facilities). This is subject to MS decisions and constraints.</p>	<p>Photo from e-MRTD can be read and used for verification</p>	<p>4 FP possible for enrolment in EES using a mobile device in a one-step action. 8 FP is possible to enrol but adds an extra step in the use of the device.</p> <p>1-4 FP for verification</p>

Table 23 Summary of the specific conditions and options for land borders

Border type	Equipment/infra-structure	Conditions and constraints	Options for biometrics (photo)	Options for biometrics (FP)
Land border				
Large border crossing	<ul style="list-style-type: none"> Fixed equipment for control and use of e-MRTD Fixed fingerprint scanners for 1-4 FP verification to VIS Fixed workstations for border control applications Lane separation with flexible usage ABC gates (optional and presently used only for pedestrians) 	<p>Checks could have to be made outdoor in some cases</p> <p>Travellers are checked when inside a vehicle or have to leave the vehicle for checks</p> <p>Cold weather can make it difficult or impossible to capture fingerprints. In such conditions other solutions (e.g. indoor, permanent or temporary, facilities). This is subject to MS decisions and constraints.</p>	<p>Photo from e-MRTD can be read and used for verification</p> <p>Live photo could be used in ABC gates</p>	<p>4-8 FP possible for enrolment in EES</p> <p>1-4 FP for verification</p>
Small border crossing	<ul style="list-style-type: none"> Fixed or mobile equipment for control and use of e-MRTD Fixed or mobile fingerprint scanners for 1-4 FP verification to VIS Fixed workstations or laptop/mobile devices for border control 	<p>Checks could have to be made outdoor in some cases</p> <p>Travellers are checked when inside a vehicle or have to leave the vehicle for checks</p>	<p>Photo from e-MRTD can be read and used for verification</p>	<p>4 FP possible for enrolment in EES using a mobile device in a one-step action. 8 FP is possible to enrol but adds an extra step in the use of the device.</p> <p>1-4 FP for</p>

	applications		verification
Train (on-board)	<ul style="list-style-type: none"> • Mobile equipment for control and use of e-MRTD • Mobile fingerprint scanners for 1-4 FP verification to VIS • Mobile devices for border control applications 	<p>Checks are made on-board with limited space and no fixed infrastructure</p> <p>Problems sometimes occur with signal strength and penetration for online connections and such connections must be secure with full end-to-end data encryption</p> <p>When existing, tunnels prohibit online consultation of central systems. Alternatives shall exist as it is not legally and technically feasible in the foreseeable future (and not security proof) to envisage a copy of the central data on the portable devices.</p>	<p>Photo from the e-MRTD can be read and used for verification</p> <p>4 FP possible for enrolment in EES using a mobile device in a one-step action. 8 FP is possible to enrol but adds an extra step in the use of the device.</p> <p>1-4 FP for verification</p>

Table 24 Summary of the specific conditions and options for sea borders

Border type	Equipment/infrastructure	Conditions and constraints	Options for biometrics (photo)	Options for biometrics (FP)
Sea border				
Ferry terminal	<ul style="list-style-type: none"> • Fixed equipment for control and use of e-MRTD • Fixed fingerprint scanners for 1-4 FP verification to 		Photo from the e-MRTD can be read and used for verification	4-8 FP possible for enrolment in EES 1-4 FP for

		VIS		verification
		<ul style="list-style-type: none"> Fixed workstations for border control applications Lane separation with flexible usage 		
Large harbour	<ul style="list-style-type: none"> Fixed equipment for control and use of e-MRTD Fixed fingerprint scanners for 1-4 FP verification to VIS Fixed workstations for border control applications 		Photo from the e-MRTD can be read and used for verification	4 FP possible for enrolment in EES using a mobile device in a one-step action. 8 FP is possible to enrol but adds an extra step in the use of the device. If fixed equipment is installed for enrolling FP, 8 FP should be possible.
				1-4 FP for verification
Small port	<ul style="list-style-type: none"> Fixed or mobile equipment for control and use of e-MRTD Fixed or mobile fingerprint scanners for 1-4 FP verification to VIS Fixed workstations or laptop/mobile devices for border control applications 	Infrastructural conditions and availability 24/7 can vary depending on available premises (e.g. harbour masters office, nearest police station)	Photo from the e-MRTD can be read and used for verification	4 FP possible for enrolment in EES using a mobile device in a one-step action. 8 FP is possible to enrol but adds an extra step in the use of the device.
				1-4 FP for verification
Ship/ferry (on-board)	<ul style="list-style-type: none"> Mobile equipment for control and use of e-MRTD Mobile fingerprint scanners for 1-4 	Checks are made on board with limited space and not always with a fixed infrastructure (e.g. dedicated	Photo from the e-MRTD can be read and used for verification	4 FP possible for enrolment in EES using a mobile device in a one-step action. 8 FP is

<p>FP verification to room) VIS</p> <ul style="list-style-type: none"> • Mobile devices for border control applications 	<p>possible to enrol but adds an extra step in the use of the device.</p> <p>1-4 FP for verification</p>
--	--

Land borders

Checks on road traffic

To ensure effective checks on travellers, Member States may install or operate separate lanes at certain border crossings. This can facilitate the conditions for taking fingerprints. However, depending on weather conditions, it can be difficult to always capture the desired number of fingerprints. In addition, there could be constraints related to having passengers out of their vehicles and capturing fingerprints in a reasonable time. Also, a mixture of TCN and EU/EEA passengers can be in single vehicles, complicating the separation of people.

For instance, Estonia, Latvia, Poland and Slovakia already started performing fingerprint checks for VIS purposes at land borders. One or four fingers are the most common choices regarding the number of FPs to use.⁵³

Frontex reports that for the purpose of performing the VIS checks, MS had to undertake minor changes of infrastructure, the most common being the replacement of the windows in the booths. For example, Latvia plans to create new windows with a drawer permitting the easy passing of the scanner to travellers during fingerprint verification, thus protecting the device from humidity, extreme temperature and direct sunbeam. MS have been accumulating experience using mobile equipment for FP checks and have been faced with related operational challenges. In fact, connectivity, autonomy and weather conditions might affect their functioning. For example, Latvia installed a secure Wi-Fi network at the Zilupe railway BCP, while the Finnish Border Guard has made specific investments with an Internet provider, both in order to ensure the necessary connectivity for mobile equipment.⁵⁴

By 2020, the technological advancements and the accumulated experience from the VIS checks are likely to have a positive influence on reducing the issues linked to the implementation of EES and mitigating the operational challenges that are faced today.

⁵³ Frontex's Best Practices at EU land BCPs (draft version - 18/02/2014)

⁵⁴ Frontex's Best Practices at EU land BCPs (draft version - 18/02/2014)

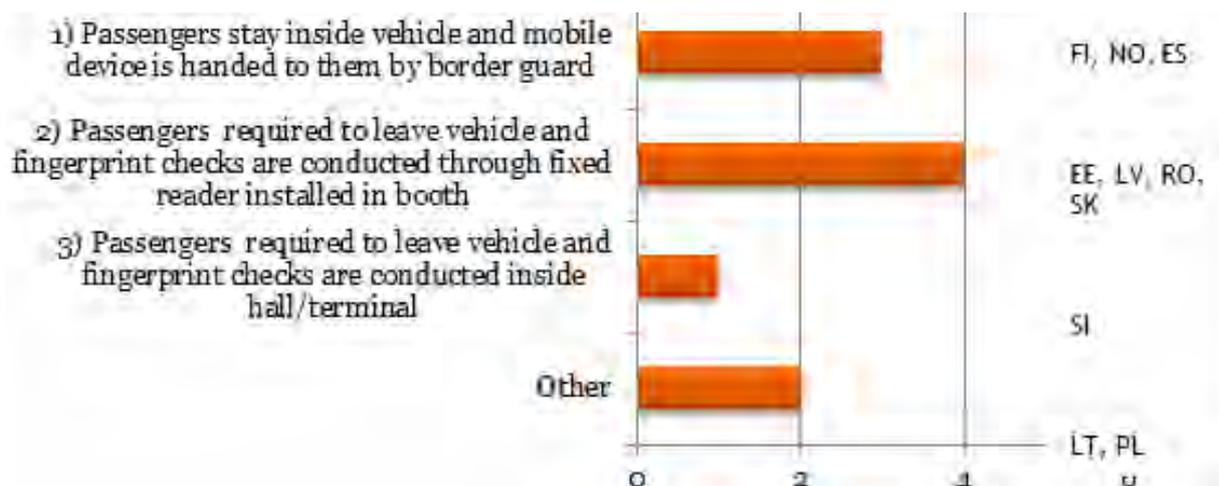


Figure 20: VIS checks- MSs' procedures to collect the fingerprints of persons travelling in private vehicles. Source: Frontex's Best Practices at EU land BCPs (draft version - 18/02/2014)

The table below provides the processing time values according to the different types of vehicles.

Table 25. Estimated average processing times at land BCPs (minutes)

Member State	Buses	Trucks	Cars	Pedestrians	Trains
Bulgaria	15'	5'	2'	40-60'	1' per traveller
Estonia	30-40'	10'	3'	1' per EU citizen, 2-3' per TCN	30-45'
Finland	1-2' per traveller	1-2' per traveller	1-2' per traveller	n/a	2' per traveller
Hungary	15-20'	5'	3'	1'	20'
Latvia	20-30'	5' per EU citizen, 7-10' per TCN	2-3' per EU citizen, 4-5' per TCN	1' per EU citizen, 2-3' per TCN	Travellers- 45', cargo-30'
Lithuania	up to 30'	1-5'	1-5'	1-2'	20-50'
Poland	up to 40'	up to 10' on departure, up to 20' on entry	up to 5' on departure, up to 10' on entry	2'	1 officer can check 20 travellers in 60'
Romania	2' per traveller	10'	5'	2'	n/a
Slovakia	30-45'	10-30'	10'	30'	2'

Source: Frontex's Best Practices at EU land BCPs (draft version - 18/02/2014)

The following two figures illustrate the situation at different land borders on different days. The figures capture the high variability that characterises these types of borders and their volumes which is consistent with the high variance of the processing times reported in the table above.

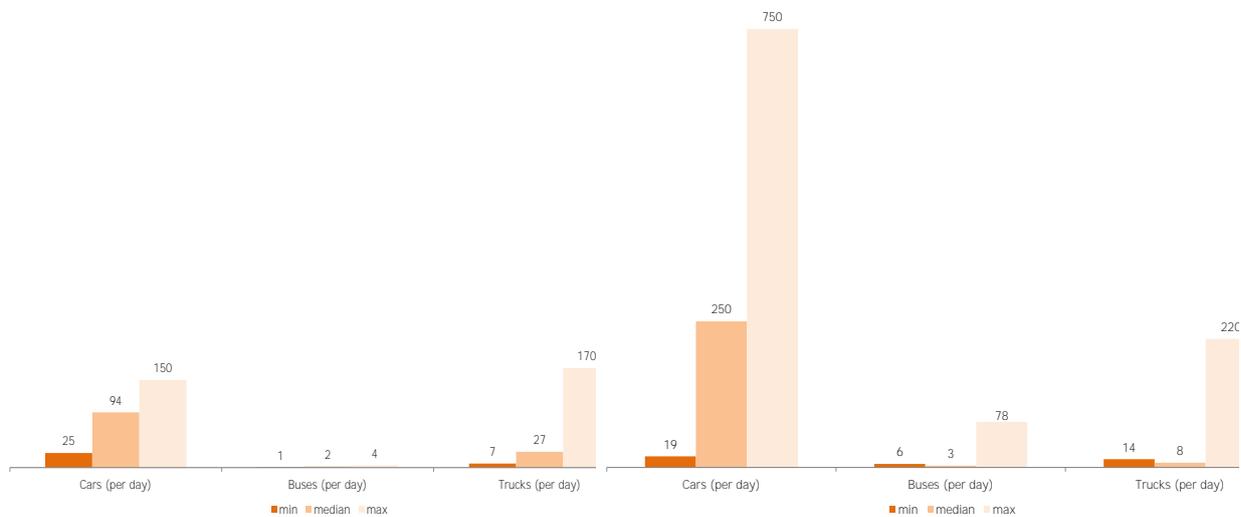


Figure 21 Aggregated overview of the number of incoming vehicles (road) during a **normal day** (calculation based on the situation at Bulgarian, Latvian, Polish and Romanian BCPs)

Figure 22 Aggregated overview of the number of incoming vehicles (road) during a **busy day** (calculation based on the situation at Bulgarian, Latvian, Polish and Romanian BCPs)

Checks on rail traffic

Checks are carried out both on train passengers and on railway staff on trains crossing external borders, whether this is done on the platform, at the first station of arrival/departure, on the territory of an MS or on the train (moving or being stopped at a BCP). In the latter case when using a mobile device, with limited space, it will be difficult to handle more than 1-2 or 4 fingerprints.

Air Borders

Checks at international airports

When carrying out checks at this type of Border Crossing Points, Member States have created conditions to channel passenger traffic and handle large volumes of travellers. It is assumed that the constraints and conditions referred to in this chapter do not relate to border checks in international airports. These are supposed to be equipped good enough to cope with the requirements of the EES and RTP. Large air borders do have other challenges in relation to the use of EES and RTP, which are described in chapter 3.4 and also in the Annex J (simulation of air borders, using EES and RTP).

It is worth mentioning that for certain situations, like flights with short connection times, it can be considered difficult to enrol more than 4 fingerprints.

Checks in aerodromes

Travellers are also checked at airports that do not hold the status of international airports under the relevant national law (aerodromes) but through which the routing of flights from or to third countries is authorized.

In these types of Border Crossing Points, capturing a photo from the e-MRTD, to be used in the EES search/registration of the individual file, requires adequate equipment in the form of a passport reader. Given the conditions at such a small border crossing, mobile solutions might be needed for enrolling fingerprints for registration and/or reading the e-MRTD. Reading the e-MRTD is a standard function on a number of mobile devices, whereas enrolling more than 4 fingerprints, even if possible, could be a constraint.

Therefore the impact for the mandatory requirement to enrol more than 4 fingerprints can be considered to be high whereas for capturing photos the impact can be considered to be medium/low.

Sea borders

Checks on ships shall be carried out at the port of arrival or departure, on-board the ship (at the port or during the voyage) or in an area located in the immediate vicinity of the vessel set aside for this purpose (no border-control check will take place for passengers on vessels that remain within the Schengen zone).

Cruise ships

Border guards are informed of the nominal lists of passengers and crew at least 24 hours before the arrival at each port in the territory of the Member States or, where the journey to the port lasts less than 24 hours, immediately after the boarding is completed at the port of departure. Therefore an EES search and possibly a preliminary registration of the individual file, if it is a first entry, could be possible before the arrival of the ship. The enrolment of a minimum number of fingerprints or capturing photos would be done either in a stationary border crossing, where passengers leave and enter the ship or it can be done on-board with mobile equipment. The latter method could be a way to solve time constraints for carrying out border checks, where otherwise a large number of passengers must be checked in a very short time when arriving to the harbour.

Pleasure boating, cargo ships/coastal fishing, ferry connections

Pleasure boats are obliged to follow the sailing route indicated and when arriving at a port they must visit the nearest official border crossing office. For instance, this can be the harbour master or a police station. It is assumed that, at least in smaller ports, the infrastructure in these offices is not always adequate for the requirements of EES.

Ferry connections often have a similar setup as an airport, albeit not always with the same size and volumes of travellers. The impact for the requirement to enrol more than 4 fingerprints and/or for capturing the photo can be considered to be medium/low for ferry connections.

For cargo ships and coastal fishing, the crews of these boats have special conditions in the Schengen Borders Code and are not supposed to have their passports stamped or have stamps checked as long as they stay on the boat or near the boat if in a harbour. This means that they are only checked as TCNs when leaving the boat, for instance to have a period of holiday, to finish a period of work or to go on temporary leave.

RTP - Differences in conditions at borders

The impact of using data from the MRZ to retrieve the RTP record would be very limited and equal for any type and size of border crossing. The reason is that, today, checks against the VIS and SIS II using the MRZ must be done at all border crossings.

The introduction of verifications against the RTP at manual gates, using fingerprints, is of limited impact (see chapter 3.4.1.2), since this verification is comparable to the mandatory verification for VIS. On the other hand, it might be difficult to give the RTP traveller the expected services when

arriving at a small border (air, land, sea). The concept of RTP is however aimed at facilitating border crossings for frequent travellers, in order for them not to be impacted by the potential **queues for a “normal” TCN. This normally relates to border crossings with high volumes, where** queues can be expected. The smaller border crossings where the RTP traveller cannot get the expected service are typically not places with long queues and waiting times.

A general conclusion is that, in a degraded mode (e.g. RTP system not available), the RTP travellers would have to be checked manually. In certain variants of degraded mode they might still be treated as RT (e.g. no questions asked) but if the RTP system would not be available, they would have a full manual check as any TCN.

For air borders the RT would be able to use ABC gates, whereas at other border crossings (e.g. land borders) this is, as of now, not possible. In some smaller border crossings there might not even be separate lanes for EU/EEA/CH citizens. The RT would still benefit from not being asked questions, etc but the benefits would be less.

> ***Main findings – variations for land, sea and air borders***

According to the type of border (air, land, sea) and the data and biometrics to be captured, the impact on processes may be more or less important. For this reason the implementation of the same requirements for all type of border crossings will be challenging.

EES: The difference of impact is not only relevant to assess based on the type of border but also in relation to the size of the border crossing. The impact of EES, in relation to the use of data and biometrics, could therefore be similar in all these larger border crossings but more significant or complex to handle with the desired requirements in a small border crossing. Summarising the constraints found in the analysis, for border crossing where mobile equipment is used, it would be challenging to enrol more than 4 FPs. At border crossings where the check is made outdoors, the environmental conditions can bring problems to enrol FPs properly. Photo can be taken from the e-MRTD in all places equipped with e-MRTD readers, but it is not certain that such readers would exist in all border crossings. A general reflection is that there is an obligation to check FPs for the VIS verifications, at all border crossings, which should imply that the necessary equipment, at least for enrolling 4 FPs or less to the EES, would be in place.

RTP: The impact of using data from the MRZ to retrieve the RTP record would be very limited and equal for any type and size of border crossing. Verifications against the RTP at manual gates, using fingerprints, is of limited impact. In a degraded mode, the RTP travellers would have to be checked manually. For air borders the RTP travellers would be able to use ABC gates, whereas at other border crossings this is, as of now, not possible. No questions are asked but if it is not possible to use the EU/EEA/CH lane their benefit from having the RTP status is less.

– ***Process accelerators***

The section of process accelerators investigates how innovative approaches could speed up border crossing times. This section highlights potential process accelerators that could positively impact the duration of the border crossing processes for the implementation of EES/RTP systems.

1.3.2. Decreasing the average crossing time (TF9.1)

The border crossing point is a sensitive place for collecting data given the time pressure. Therefore particular attention should be given to how data collection can be prepared or automated. The measures under review include gathering information from transport companies before arrival, self-pre-registration before the border check and organisational measures.

The process accelerators could be divided into the following categories:

1. **Data gathering** before border crossings
2. **Pre-border checks**
3. **Data retention**
4. **Organisation** of border crossing points

Of course, the implementation of the potential accelerators is dependent on the selection of the options according to the Target Operating Model (TOM), otherwise the accelerator is useless e.g. if the full data set of the legal proposal is not seen as essential for implementing the EES, there is limited value in implementing a solution where this data can be registered beforehand.

> *Data gathering*

Any data that can be gathered before the person arrives at the border crossing point could speed up the checks, accelerate processing time and enhance security.

The data gathered could be used for example to check travellers in EU systems and national systems, optimize queue management and prepare the registration in the EES.

The description and assessment of data gathering options for process acceleration are provided in the table below.

There are several data gathering options that could accelerate the border crossing processes:

A. API (Advanced Passenger Information)

API are a set of 9 data elements (see list further) that are collected by the carriers and transmitted to border control authorities of the requesting country prior to flight arrival, and made available on the primary line at the border crossing point.

All the arrangements are made between Member State authorities and the carriers; there is **no European central system** or central administration.

Directive 2004/82/EC on the obligation of carriers to transmit passenger information⁵⁵ has the objective of improving border control and combat illegal immigration by the transmission of advance passenger data by air carriers to the competent national authorities. The information is composed of passenger lists transmitted electronically (or in case of failure by any appropriate means), in advance of departure, to the authorities of the first authorised border crossing point.

These lists should include:

1. The number and type of travel document used;
2. Nationality;
3. Full names;
4. The date of birth;
5. The border crossing point of entry into the territory of the Member States;
6. Code of transport;
7. Departure and arrival time of the transportation;
8. Total number of passengers carried on that transport;
9. The initial point of embarkation.

⁵⁵Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to transmit passenger information

B. PNR (Passenger Name Record) data is information provided by passengers during the reservation and booking of tickets and when checking in on flights, as well as collected by air carriers for their own commercial purposes. It contains several different types of data, such as:

1. Travel dates;
2. Travel itinerary;
3. Ticket information;
4. Contact details;
5. Travel agent through which the flight was booked;
6. Means of payment used;
7. Seat number;
8. Baggage information.

The data are stored in the airlines' reservation and departure control databases and the following five fields are compulsory to complete the booking:

1. Passenger name;
2. Contact details for the travel agent or airline office;
3. Ticketing details, either a ticket number or a ticketing time limit;
4. Itinerary of at least one segment, which must be the same for all passengers listed;
5. Name of the person providing the information or making the booking.

The Commission's proposal for a PNR directive⁵⁶ provides for the transfer by air carriers of PNR data of passengers of international flights to and from the Member States, as well as the processing of that data, including its collection, use and retention by MS and the exchange between them. PNR data collected in accordance with the Directive may be processed only for the purposes of the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

C. Passenger lists from ships (e.g. cruise ships and ferries)

These lists are very similar to API and used in a similar way. According to the Schengen Borders Code⁵⁷ they contain (the example shown below is for cruise ships), certain information that is related to what is relevant for the use of EES:

1. First name;
2. Surname;
3. Date of birth;
4. Nationality;
5. Document number and type of travel document;
6. Visa number, if relevant.

D. Crew lists

Crew lists are mainly used for trade, fishing, etc. and are subject to specific rules of the Schengen Borders Code. As long as the crew stays in or near the port where their ship docked, they are not

⁵⁶ Proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime COM(2011) 32

⁵⁷ The general provision for requesting these list is in Annex VI, section 3.1.2. The fields referred to here are those requested for cruise ships.

subject to checks or stamps of documents. It is only when the crew leave their ship to enter a country that a check is made. Then it is a normal check as for any TCN.

The assessment of options related to gathering information is provided in the table below.

Table 26 Assessment of data gathering options for process accelerators

Options	Advantages	Disadvantages
<p data-bbox="177 479 331 510">) API data</p>	<p data-bbox="421 479 975 741">EES individual file: It could be an option to make a search in EES using the document number, date of birth and name from the API to find out if the person is already registered in the EES, or not, and create a subset of the result, potentially used for simpler and faster access upon arrival.</p> <p data-bbox="421 779 975 981">Queue management: The data (e.g. number of travellers per category – VE, VH EU/EEA) could be used to prepare and optimise lanes management according to the pattern of travellers arriving in a certain time period.</p> <p data-bbox="421 1048 975 1480">Not specifically related to the EES, but having a positive impact on the border crossings in general, is the possibility to use the API data for security checks against SIS II, Interpol, national databases and other sources: the passenger list data can be used for searches in those systems. The results of these checks can be forwarded to the border guards and/or made available in the systems used by the border guards, alerting them before the arrival of the person⁵⁸.</p>	<p data-bbox="975 479 1426 712">EES search: The data on the issuing country is not included in the API fields, which means that the normal EES search, which is composed of issuing country + document number, would not yield any results.</p> <p data-bbox="975 750 1426 1279">EES registration of the individual file: It is quite doubtful if keeping a subset of the result of a search in EES, with persons not being registered and persons being registered in EES, really would decrease the duration of the border crossing. The subset needs to be managed, found by the border guard and the actual time to make the search in EES at the physical arrival of the person to the border guard is very short, or negligible in relation to the overall duration of the check.</p> <p data-bbox="975 1317 1426 1585">Integration with national end-user systems: To use the API data would require interfacing with the national border management systems, where EES and RTP are integrated at end-user level. This requires national systems interfacing to be developed.</p> <p data-bbox="975 1624 1426 1845">Consistency within Member States: API is implemented in a heterogeneous way; it is up to each MS to decide whether to implement it and how API is used depends on each MS's choice and conditions. As a result, it is</p>

⁵⁸ To be validated by border guards.

		currently not used consistently across Member States. It is not undergoing any common quality assurance, which makes it difficult to trust the content of the data. Quality concerns raise questions with regard to the protection of the right to personal data. In addition, safeguards should be put in place in order to ensure that authorities accessing API have the legal authority to API data for the risk assessment of travellers.
) PNR	The data could potentially be used for preparing the checks related to EES.	<p>The PNR is mostly a useful tool for second line checks. It also has the same constraints as API as regards that it is not a uniform tool used, or even not used, in the same way in all MS. The data does not contain document number and is collected on by MS on their initiative from the reservation and booking companies. It is not undergoing any common quality assurance, which makes it difficult to trust the content of the data.</p> <p>The scope of the Commission proposal for a PNR directive is limited to the purposes of the prevention, detection, investigation and prosecution of terrorist offences and serious crime, <u>which means that is not supposed to be used for the purposes of the EES or the RTP.</u></p>
) Passenger lists from ships	EES individual file and queue management: this data could be potentially be used in the same way as API data.	See the assessment of API above
) Crew lists	-	As mentioned in section 3.4.4.1, the crews are subject to specific regulations and once they go through a border check they are treated as any TCN. The use of the crew lists in relation to EES and RTP, as an accelerator, would not provide any benefits.

Main findings

Data from API and other sources of traveller data could potentially give MS information that could accelerate the border crossing processes at air borders and sea borders in relation to queue and lane management, in advance of the arrival of the travellers. The implementation and use of API is

under MS responsibility and so is the operational queue management. It is only the concerned MS that could make the assessment, on a case-by-case basis, of the usefulness, in relation to investments needed, of having such data in advance.

The use of API data for preparing the EES verification/registration at air border and sea borders (at land borders there is no such common data gathered) would not bring much added value (in relation to the EES) to the border control process. Any subset of persons registered in EES, or not, must be maintained locally since it cannot be centrally registered until the traveller arrives, found by the border guard and the time gained compared to making the search and start the registration when the person actually arrives is assessed to be quite limited. It is only the concerned MS that could make the assessment, on a case-by-case basis, of the usefulness, in relation to investments needed, of having such data in advance.

PNR is not seen as useful for queue management or any preparations of the EES verification and registration, basically since it, according to the directive, is to be used for second line activities (e.g. security, risk assessment) and it also has the same disadvantages as API when it comes to not being uniformly used and of uncertain data quality.

> *Pre-border checks*

In recent years, there has been a tendency (e.g. implementation of self-service kiosks at the airport of Orlando, for TCN) to gather personal data when the traveller is usually queuing at the gate, for example, with self-service kiosks where the traveller is guided by the system to perform the necessary activities.

Such a **pre-border check** could typically include the following:

1. Recording of **Traveller Data** (e.g. MRZ and additional data to be used in the registration of the individual file in the EES)
2. Recording of **Biometrics** (i.e. live fingerprints and photo)
3. Making **checks** against relevant databases
4. MRTD or e-MRTD **authenticity checks**

The table below provides the description and assessment of features in a pre-border check that could accelerate the border process (using kiosks for example), in relation to EES.

Traveller that is already registered in the EES:

- a) Recording of **MRZ data**
- b) **EES search**, if the person is found, taking a **live photo/ live fingerprints** and verifying this against the biometrics stored in EES and VIS.

Travellers entering for the first time (in addition to a and b):

- c) Recording of **additional data** (if more data is required than MRZ data).
- d) Capturing **fingerprints** and a **photo** from e-MRTD and **live photo**
- e) **Preliminary creation of the individual file**, to be validated by the border guard.

The Schengen Border Code has a proposed amendment (article 7a(2)) that would allow TCN under certain conditions (i.e. fingerprints exist in the VIS or the person has an e-MRTD) to use an automated border control. This supports the proposal in this chapter. The article also states

that the process shall be monitored and there must be an individual decision by a border guard to authorise or refuse entry.

Table 27 Assessment of pre-border checks options for process acceleration in the EES

Potential accelerators	Advantages	Disadvantages
1. Recording of MRZ data	Prerequisite for pre-border checks.	No time saving as such.
2. EES search⁵⁹	Prerequisite for pre-border checks.	No time saving as such.
3. Biometric verification	Decreases border guard EES verification time to process for persons found in the EES. Only questions remain to be handled by the border guard.	The verification must be supervised to ensure security
4. Full alphanumeric dataset registration (as in the legal proposal)	Decreases border guard EES registration processing time as data could either be captured automatically from the e-MRTD or the travellers could enter this data manually. Then the travellers could also enter the three fields that are not contained in the e-MRTD or MRTD. (surname at birth, country of birth and additional nationalities).	Manual registration would be needed. The concerned data that could be captured from the e-MRTD is optional to store in the chip. Three fields (that are not in the e-MRTD/MRTD) must be entered manually and controlled by the border guard.
5. Enrol fingerprints for registration	Saves between 10-90 seconds if the enrolment of the fingerprints is done before the border check (depending on the number of fingerprints that are mandatory to be captured).	Fingerprints enrolment might require support and supervision. TCNVHs: no enrolment needed and therefore no time saved (see EES process in section 3.3.2)
6. Capturing a live photo for registration	A live photo captured in good conditions would enhance the quality of the photo stored in EES. The captured photo can also be used in the biometric verification (see above). This capturing is also valid for TCNVHs (see chapter 3.3.2).	

⁵⁹ The search should be integrated with current border guard activities to avoid any duplication of checks.

7. Preliminary creation of the individual file

Saves time by having the registration already performed and only verified by the border guard.

Support might be required to assist travellers in preliminary registration.

Main findings

Pre-border checks could have a (very) positive impact on border crossing time by limiting border guard manual interventions and thus making it possible to allocate more time to decision-making.

Activities such as capturing photos or fingerprints are time consuming. Any automation of those activities can save significant time to process (see chapter 3.4 for assessments of the duration).

The benefits from such an investment would mainly be foreseeable if a large volume of traveller's is handled at a specific border crossing point. The potential use of pre-border checks would therefore mainly be useful at international airports, large land border crossings (rail or road) and ferry/cruise ship terminals.

TCNVE will mainly benefit from this accelerator because TCNVH do not have their fingerprints enrolled in the EES process, which means less time is saved by this accelerator.

> ***Data retention (in relation to border crossing processes)***

This section highlights the impact of the data retention periods on border control processes. The aspects of data retention are described in detail in chapter 5.6.

In relation to the border crossing process there are two main issues where the length of data retentions has an impact:

- The longer the data retention period in the EES is, the lower the number of **first-time entries** will be. Therefore the number of registrations of the individual file will decrease and the border crossing time will be reduced.
- For RT a shorter data retention period of EES would mean that these travellers regularly have to go to the manual gates and have an EES individual file registered. This would of course lessen the benefit of the RT status.

These issues above are also indicated in the chapter describing the data retention in detail.

1.3.3. Organisation of Border Crossing Points (TF9.2)

The objective of this section is to envisage what type of measure can be taken from an organisation point of view to accelerate the processing time and limit the EES and RTP impacts. The table below provides the description and analysis of different options:

a) **Separate TCNVE and TCNVH lanes**

When fingerprints are introduced as part of the EES registration, the average processing time for TCNVEs will (depending on options retained) possibly be higher than for TCNVHs. Consequently, the temporary or permanent introduction of separate lanes, depending on the situation at the border crossing, can be of advantage to decrease average processing time. It will make it possible to have similar processes at any time and not to alternate between TCNVEs and TCNVHs.

Another option could be to open more gates (e.g. using electronic signpost to change the flow) for TCNVEs, to balance the overall flow between TCNVEs and TCNVHs. The SBC already provides that Member States may install separate lanes for visa exempt persons (Article 9.2 and Part B1 of

Annex III – “visa not required”). This article should provide the necessary basis for the option to make such a separation. It is however the Member States that would have to assess if they see such an investment giving added value.

b) **Flexible use of lanes**

At border crossings where there is a need to eliminate temporary imbalance in traffic flows it is already possible (see Article 9 §4 of the SBC and the Borders best practices guide) to waive the rules relating to the use of the different lanes. The usefulness of this depends also on how the lanes are equipped.

c) **Waiting areas**

The waiting areas can make it possible to collect data and biometrics when travellers are waiting. This can accelerate the processing time at the border when combined with the pre-border checks.

For land borders, when using waiting areas the vehicles do not have to wait in the queue, but can wait in the waiting area, and only go to the border crossing when their number comes up. This makes the process more efficient and helps accommodating changes in the flow.

Table 28 *Description and assessment of options relating to the organisation of border crossing points*

Option	Advantages	Disadvantages
a) Separate TCNVE and TCNVH lanes	This possibility is already provided in the SBC and is optional for MS. Making use of it would streamline the average processing time by increasing productivity due to specialisation. The uniformity of checks only being made for one category in the concerned lane could decrease average time for checks. The balancing of flow of VE and VH, allocating extra lanes for one of the categories when need be, can also decrease the overall time needed.	Limitations in terms of space in certain situations. Additional costs could be envisaged to make the separation.
b) Flexible use of lanes	Minimising impact of EES/RTP by using flexible lanes where allocation to lanes can be made depending on the type of categories arriving.	Additional costs could be envisaged to make use of flexible lanes.
c) Waiting areas (land borders)	Data and biometrics could be collected in the waiting areas, thereby reducing the time at the border check. This could be made similar to what is proposed for the pre-border checks, but concretely related to practical problems at land borders with high volumes of heavy traffic.	Additional costs for building the facilities.

Main findings

Separation of TCNVE and TCNVH lanes, optimisation of lanes usage and waiting areas (for land borders) are all valid average processing time savers to be considered on a case-by-case basis.

1.3.4. Minimising the number of documents used (TF9.3)

The objective of this section is to look at how to minimise the number of documents used when interacting with the EES and RTP. All documents legally required from the traveller shall remain in its possession.

The documents that could be used for border crossings, in relation to EES and RTP, are:

1. MRTD – passport;
2. e-MRTD – passport;
3. Visa sticker (affixed in the passport but can be seen as a document of its own);
4. Residence permits;
5. LBT permits.

The issue of minimising the number of documents that need to be handled at border crossings has been addressed in the preceding chapters. The measures envisaged here in relation to the processing time are the following⁶⁰:

- a) Maximising the use of the e-MRTD;
- b) Using the e-MRTD as a token for RTP;
- c) Using the document number of the MRTD to search for the VIS.

The assessment of the options that would minimise the number of documents used is given in the table below.

Table 29 Assessment of document use options

Option	Advantages	Disadvantages
a) Maximise the use of the e-MRTD	<p>Increases rapidity and security of the processes since the e-MRTD includes all alphanumerical data needed for EES and also a photo that can be used for verification.</p> <p>Since this is available electronically, the time for the border check is decreased.</p> <p>Further to this, only one document would be needed for all the purposes included in the border process, for both old and new activities.</p>	<p>In some cases, travellers might still have an MRTD.</p> <p>This would make it impossible to use the data and biometrics stored in the chip for automatic searches, verification and registration.</p>

⁶⁰ The LBT permits are addressed in section 3.4.4. Residence permits are addressed in section 3.4.5.

b) Use the e-MRTD as a token for RTP	See section 3.3.5	
c) Use document number of the MRTD/e-MRTD to search the VIS	Decreases processing time by removing one step in the border process.	The VIS legal basis would have to be amended to allow using the document number for searches in the VIS, at border checks. In the case the VIS legal basis is not amended, the visa number would be used, as it is done today.

Main findings

Using the e-MRTD as the sole document needed when interacting with the EES and RTP can reduce processing; no other documents would be needed to facilitate the process for the traveller in the RTP and the border guard during the manual control; the automation is facilitated for the RTP (see sections 3.2 and 3.3 for details).

1.3.5. Process automation (TF8.4)

This section focuses on the automation of border crossing using ABC gates for TCN travellers⁶¹. The number of ABC gates in operation is increasing steadily, 260 ABC gates have been installed within the Schengen Area as of June 2014⁶², and with more installations planned around Europe.

The usage of ABC gates at **entry** provides only a benefit for EU nationals and for TCN who are registered in RTP. From a technical point of view a TCN using an e-MRTD could also pass an ABC gate at entry but as the Schengen Border's Code provides that each TCN should also be submitted to thorough check including questions, the benefit of using the gate in terms of border control duration would be close to zero. When TCN register as RT, they submit the evidence justifying that these questions would not be asked again. Therefore ABC gates at entry only provide a benefit to RT's whose border crossing time becomes identical to the ones of EU travellers, so going down at air borders from 1min 44 seconds for TCNVH and 1 min 3s seconds for TCNVE to 15-20 seconds.⁶³

The usage of ABC gates at **exit** should be made possible for all TCNs and not only RT's if the following prerequisite conditions are met:

1. Travellers have an individual file in the EES, created **at first entry**.
2. They are in possession of an e-MRTD passport.
3. A biometric verification can be made with the photo of the e-MRTD checked against a live photo.

The Schengen Border Code has a proposed amendment (article 7a(2)) that would allow TCN under certain conditions (i.e. fingerprints exist in the VIS or the person has an e-MRTD) to use an automated border control. This supports partly the proposal in this chapter, but refers to that

⁶¹ A TCN that becomes part of the RTP would be able to use any ABC gates, upon entry into or exit from the Schengen area. This will speed up processing time at border control and optimise resource utilisation. This automation is described in further detail in the chapter dealing with the RTP.

⁶² Source: Frontex, June 2014.

⁶³ European Commission: Impact Assessment. Already cited.

supervision is mandatory, whereas the proposal of this chapter refers to the use of an ABC-gate, being a fully automated exit, where manual intervention only occurs on a case-by-case basis.

Table 30 Assessment of the option to use ABC gates

Option	Advantages	Disadvantages
Use of ABC gates	<p>Automating most of the process at exit will significantly reduce average processing time in comparison with manual processing.</p> <p>Increases security, as it includes an automatic biometric bearer verification (for the ABC gates that can handle facial recognition) proving that the person using the e-MRTD is the lawful owner of that e-MRTD.</p> <p>Decreases border guard’s workload. The advantage can mainly be made true and has already been implemented at air borders. The advantage could also be achieved at other border crossings (example like trains and cruise ships) but would require a detailed process and infrastructure design first.</p>	<p>If the conditions listed above are met, no disadvantages could be seen as regards speed and security except the requirements to adapt the capacity of the gates.</p>

Main findings

Automation of the process by using ABC gates at exit for TCN is a significant accelerator as it decreases the average **processing time and limits the impact of EES and RTP on the border guards’ workload. The use of this option depends on where MSs decide to install ABC-gates, which at present is mainly at air borders. It might be that MSs decide to also introduce ABC-gates at large sea borders (e.g. ferry terminals) or at large land borders. If so, then this option could be of value also at such crossings.**

Use of state of the art technology

The use of state of the art technologies will help in facilitating the border controls and in mitigating any adverse effect that the increased security and checks might have on the border control processes and on the crossing time.

Among the new technologies that are currently on the horizon, touch-less FPs sensors are believed to be promising in simplifying the capture of FPs and at the same time being more hygienic. As this technology is rather new and with limited real-life applications so far, it is proposed that it should be tested in the pilot.

1.3.6. Using iris as an accelerator

During the recent years an increased interest in iris can be observed, both at a global and at a European scale. The Indian UIDAI large-scale project includes iris, and various Member States have expressed their interest in the use of it.

Even though the Study has not analysed the impact or use of iris in the border control processes, it could be of interest to look at iris features in the pilot, e.g. to gather facts on duration, quality, complexity, etc. and to understand the feasibility of using this as a biometric identifier.

Today iris scanners are used in a number of ABC-gates in the EU but not in manual gates.

Iris technology rose to the forefront due to a combination of factors. The original technology was patented and under a license, however those patents have now expired. Iris information can easily be captured, is stable over time, and has a high degree of accuracy. Finally, an iris-based system is seen as a highly non-intrusive solution, which facilitates user acceptance, across different regions and cultures worldwide.

Iris recognition uses the pattern that is formed by the muscle tissue and cell structure in the iris region of the eye. The iris image is captured using infrared illumination and a camera.

A short introduction to and evaluation of iris technology is provided in appendix D.

1.3.7. Process Accelerators – summary

The existence of process accelerators can possibly decrease the duration of the border crossing processes in the context of the implementation of EES/RTP systems.

Decreasing the average crossing time (TF9.1)

The border crossing point is a sensitive place for collecting data given the time pressure. Therefore particular attention should be given to how data collection can be prepared or automated. The implementation of the potential accelerators is dependent on the selection of the options according to the Target Operating Model (TOM), otherwise the accelerator is useless. The process accelerators could be divided in:

Data gathering

API data could possibly be used for proactive queue management but the use of this data for preparing the EES verification/registration at air and sea borders would not bring much added value to the border control process. Any subset of persons registered in EES, must be maintained locally, since it cannot be centrally registered.

It is only the concerned MS that could make the assessment, on a case-by-case basis, of the usefulness, in relation to investments needed, of having such data in advance. PNR is not seen as possible to use, as the legal basis for PNR puts restrictions to its usage that de facto excludes their use for the EES.

Pre-border Check

Pre-border registration/checks could have a (very) positive impact on border crossing time by limiting border guard manual interventions and thus making it possible to allocate more time to decision-making. Activities such as capturing photos or fingerprints are time consuming and any automation can save significant time. The benefits from such an investment would mainly be **foreseeable if a large volume of traveller's is handled at a specific border crossing point**. The potential use of pre-border checks would therefore mainly be useful at international airports, large land border crossings (rail or road) and ferry/cruise ship terminals. TCNVE will mainly benefit from this accelerator because TCNVH do not have their fingerprints enrolled in the EES process, which means less time is saved by this accelerator. A concern in this area is the need for supervision of **the "kiosks" where the pre-border registration/check would be done**.

Data Retention

Any period longer than legally proposed data retention period would decrease the number of registrations of the individual file in EES. A data retention period that would be synchronised with

the length of the RTP status would decrease the number of occurrences where an RTP traveller had to make a new individual file in the EES.

Organisation of Border Crossing Points (TF9.2)

Separation of TCNVE and TCNVH lanes, optimisation of lanes usage and waiting areas (for land borders) are all valid average processing time savers to be considered on a case-by-case basis.

Minimising the number of documents used (TF9.3)

Using the e-MRTD as the sole document needed when interacting with the EES and RTP can reduce processing. No other documents would be needed to facilitate the process for the traveller in the RTP and the border guard during the manual control. The automation is facilitated for the RTP.

Process automation (TF8.4)

Automation of the process by using ABC gates at exit for TCN is a significant accelerator as it **decreases the average processing time and limits the impact of EES and RTP on the border guards'** workload. The use of this option can currently mainly be envisaged at air borders where almost all (only Finland is an exception to this) ABC gates have been implemented till now. It might be that MS decided to also introduce ABC-gates at large sea and/or land borders. If so, then this option could be of value also at such crossings.

Iris

The Iris could be used in complement to the FPs and FI, similarly to the Indian experience, potentially improving the accuracy and performances of the biometric matching system. Alternatively, it could be used as a replacement for FI or FP, for the biometric verification, taking advantage of its high degree of accuracy, low intrusiveness and thus facilitating the user acceptance. The limiting factor would be the lack of coherence with the VIS technical and legal framework which relies on FPs and photo, therefore limiting the re-use of the equipment already deployed for the VIS.

It would be of interest to investigate further within the pilot the feasibility of the Iris as a biometric identifier, to assess and gather real-life data on its performances and on how it could be integrated best in the border crossing points and processes.

1.4. The RTP process – alternative proposal

This chapter provides an alternative proposal regarding the RTP application and membership processes.

While the previous RTP process is close to the one provided by the current legal proposal, this alternative proposal developed during the Study in order to minimize the impact on consular posts and border crossing points. Nevertheless this proposal should not be seen as a comprehensive and detailed description, as further analysis will be needed if this alternative is retained. If interest for this proposal is further confirmed it should be further developed.

1.4.1. Overview of the RTP (alternative)

An alternative approach to the RTP application process

This alternative departs from the existing proposal for the RTP process in the following way:

1. Registration in the EES, through normal border crossing procedures, would be a prerequisite to apply for RTP status. (A minimum number of entry/exit combinations would be defined);

2. No new enrolling of photo or fingerprints would be needed in the RTP application process;
3. The existing biometric data in the EES (VE) and VIS (VH) would also be used for biometric verifications in the RTP process upon entry and exit;
4. No visit in person to a consular post or a border crossing point would be needed. It is proposed that the application would only be made online.

This approach would simplify the enrolment process, decrease the workload of consular posts/border crossing points as regards applications and make the RTP system less complex, since no additional biometrics would need to be stored.

Application prerequisites

In order to raise travellers' awareness of the RTP programme, it would be advisable to set up an information campaign similar to the one carried out when the VIS was launched.

To apply for the RTP programme, the traveller (TCN) should comply with the following prerequisites:

- The individual file exists in the EES.
- There is the defined minimum number of entries and exits without any overstay. There should of course be at least 1 entry and 1 exit recorded in EES (no history of overstaying), but this number can be chosen to be higher in order to be more restrictive.
- The traveller must be in possession of an e-MRTD which was referenced in the individual file.
- If the applicant is a visa holder, the visa must be an MEV which was referenced in the individual file.
- In general, the requirements of the Schengen Borders Code must be followed.

Exceptions for persons with residence permits and cards

The Study recommends that these persons are not registered in the EES, hence this alternative application process would not work well for these categories, which often are frequent travellers. A way to solve this situation could be to allow for these persons to apply for RTP status, even without being registered in the EES, given that they do have a valid residence permit/card.

Another condition would be that after applying for RTP but before these travellers obtain their RTP status, they would have to pass an external border, go to a manual gate and get their individual file registered in the EES. After this, and after the same vetting as for other travellers, their status could be granted by the competent authority. The difference between residence permit and card holders vs. other TCN with RT status would be that entries and exits would not be recorded. For residence permit and card holders, the RT status would merely work as a border crossing facilitation mechanism.

All other prerequisites would be the same for these travellers as for others that apply for RTP (e.g. they need to have an e-MRTD)

Application process

The application process starts when the traveller submits an RTP application form. In this alternative, the application is always made via an online registration service.

The applicant would need to indicate the exact e-MRTD (and MEV (VH)) details previously used to create the EES individual file. The data to be provided when filing an application would be in accordance with the RTP legislative proposal.

Online registration service

The online registration service should preferably be set up as a centralised webpage that could serve any traveller applying for the RTP. For example, this could take the form of a webpage administered by a central EU institution/agency. The administration of the website has no bearing **on the decision to grant RTP status, which is assumed to be made by the MS's competent authority.**

The online application form would be forwarded to the relevant Member State. Once it receives the application, the Member State concerned is then responsible for granting or denying RTP status.

To determine which Member State should be the recipient of the application form, several options could be considered and further developed at a later stage.

- For TCNVEs — one option would be to send the application to the Member State which the applicant last exited;
- For TCNVHs (MEV) — one possibility would be to use the Member State where the visa holder **registered as "Intended Border of First Entry" for the MEV.**

The details pertaining to the online registration service would need to be further developed if this alternative was retained. Such details would need to specify the payment process, any needs to interact with the user (e.g. to provide information to the user if he/she is eligible or not), the degree of involvement of the MS and the roles and responsibilities as well as the need for communication with the applicant.

Vetting

The vetting process is in principle not changed by this proposal, except that an interview in person would not be conducted.

Granting of RTP status

The Member State granting RTP status would be responsible for informing the traveller about the decision taken. This could be done by sending an e-mail.

The current active RTP status would **simply be referenced in the person's existing individual file** (including the necessary biometric data).

RTP Status

The duration of RTP status and rules are not affected by this proposal.

RTP at entry and exit

In principle, this alternative proposal changes **nothing in the use of the traveller's RTP status and the related necessary verifications.** The process would be as described in chapter 3.3 at entry and exit.

The only difference with the description in chapter 3.3 is that, in the case of biometric verifications for VE travellers, the EES would be consulted instead of the RTP. For VHS, the VIS biometric check is trusted, as described in chapter 3.3.

1.4.2. Consequences for the report

This chapter outlines the changes that this alternative process for the RTP would have on the report as a whole if the option was retained and the study report is used as a basis for future descriptions of the process.

Processes

The changes brought about by the alternative application process and the use of the RTP status at entry/exit is outlined in the preceding parts of this chapter. If this alternative is retained, the description would need to be enriched and complemented.

The other areas that would require change, if this proposal is retained, are the following:

- Consultation of the RTP database (3.3.4)
 - The RTP database would only be consulted, for retrieving the RTP status. In particular the biometrics are no longer stored in the RTP database. As mentioned above, for VE the biometrics in the EES are used and for VH the ones in VIS.
- Interaction between EES and RTP (3.3.6)
 - **The interaction would be limited. There would be no need for a “pre-registration” at the end of the RTP application;**
 - The EES would be used to verify VE travellers with RTP status.
- Impact assessments in relation to the RTP (3.4.1.2)
 - The assessments related to entry/exit would not change in terms of time, complexity and security. The consultation of the RTP database would have to be replaced by the consultation of the EES for verifications.

The need to visit consular posts or Border Crossing Points in order to apply for RTP status would be taken out of the document. Should an interview still be deemed necessary, an option could be to indicate possible questions to be asked (annexed to the RTP application file) by a border guard at the next entry or via a telephone interview. In this case, RTP status would not be granted until these questions were answered.

Biometrics

The analysis carried out with regard to the biometric identifiers to be used for the RTP in Chapter 4 is not applicable to this RTP proposal as it would rely on the EES for biometric verifications.

Architecture

The following areas would be impacted:

- The NUI would not need the services for enrolling/capturing and verifying biometrics against the RTP;
- The requirements regarding the sizing of the system (e.g. databases, performance) would be lower due to the lower number of transactions and biometrics to be stored;
- The argument for having the EES and RTP as one system would be further strengthened by the fact that the RTP would rely on the EES to a large extent for its functioning. The only data

stored in the RTP would be data that proves the eligibility and status of the person as an RTP member;

- The online application solution for the RTP should be further defined in architectural terms and in relation to the central RTP.

Data

The data used for the RTP would basically remain the same. Any reference to biometrics used for the RTP could be taken out since the biometrics used for verification, when using the RTP status at border crossings, would be either the ones in EES (for VE) or the ones in VIS (for VH).

The retention period for individual EES files and corresponding entry/exit records would need to be **'long enough' to prove a 'bona fide' travel history and to allow the TCN to apply, while keeping the existing individual record.** Any retention period of less than 1 year would probably lead to problematic situations for this RTP alternative.

Legal compliance

The table related to legal compliance would need to be updated to fit the alternative proposal. All references to biometrics used for RTP applications and their compliance with the current legal proposal must be taken out.

TOMs and options for the pilot

TOM N describes the alternative proposal for the RTP.

Smart borders: EES and RTP summary of options

This chapter describes the possible sets of options detailed for each step of the whole border control process, in relation to EES and RTP. The options recommended by the Study are marked as **"R", while the rest with Optional ("O")**

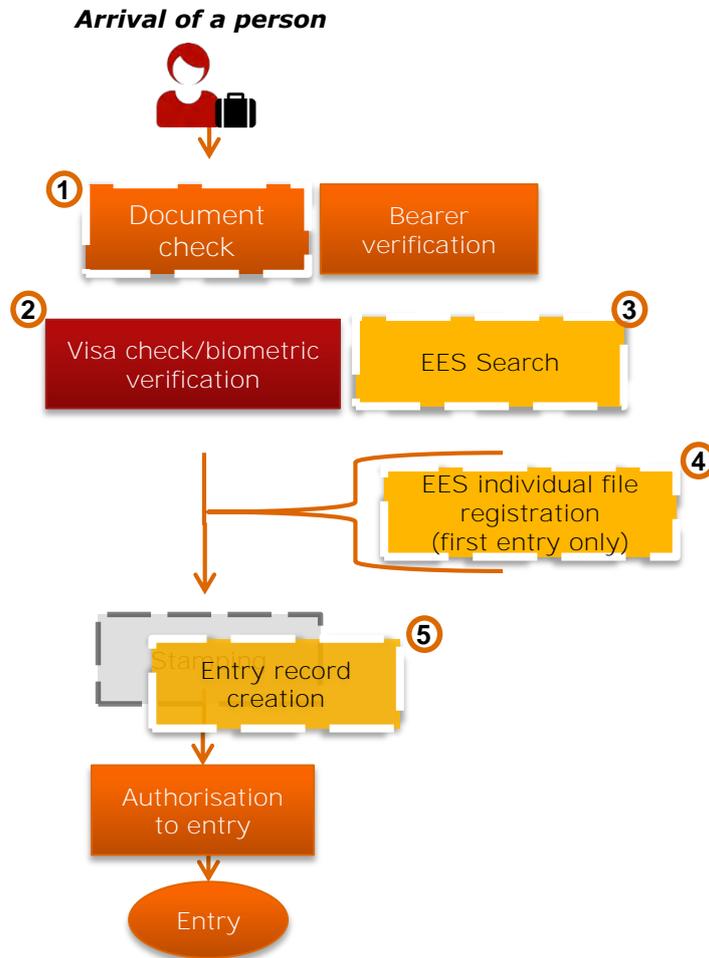
Please note that the tables focus on changes of the processes, which is why for instance manual checks and manual (ocular) verifications (e.g. document check and checking the bearer of the document by manually comparing the person in front of the guard with the photo of the passport) are not mentioned explicitly in the tables.

The tables present the categories of TCNVE and TCNVH separately, to highlight difference, although many activities and the use of data and biometrics are quite similar.

- **EES**

- > **TCNVH**

TCNVH options at entry



Step 1: Document check – (ABC and manual gate) ⁶⁴

**Main objective: Authentication of e-MRTD (chip) and check for falsifications
(Authentication of MRTD and check for falsification remain unchanged)**

n°	Action	Status
1.1	Passive Authentication (PA)	R ⁶⁵

⁶⁴ The bearer verification is performed within the VIS framework. No change proposed.

⁶⁵ R: Recommended option

1.2	Active Authentication (AA)	O ⁶⁶
1.3	Chip Authentication (CA)	O

Step 2: VIS check

Main objective: retrieve visa information from VIS

n°	Action	Store vs check	Status	ABC-gate vs manual gate
2.1	VIS check and verification by using visa number and live FP	Check	Mandatory action - <i>(unchanged)</i>	Manual gate
2.3	VIS information retrieved by using document number	Check	O	Manual gate

Step 3: EES Search

Main objective: record at all subsequent entries and exists

n°	Action	Store vs check	Status	ABC-gate vs manual border gate
3.2	Retrieve EES individual file: issuing country and document number of MRZ (MRTD/e-MRTD)	Check	R	Manual gate

⁶⁶ O: Optional

Step 4: EES individual file creation

Main objective: Create individual file in EES, at first entry				
n°	Action	Store vs check	Status	ABC-gate vs manual gate
4.1	First entry: FI (e-MRTD or live)	Store	R	Manual gate
4.2	First entry: MRZ data + visa number for TCNVH	Store	R	Manual gate
4.3	First entry: MRZ + all additional fields of the legal proposal	Store	O	Manual gate

Step 5: Entry/exit record creation

Main objective: record at all subsequent entries and exists				
n°	Action	Store vs check	Status	ABC-gate vs manual gate
5.1	Fields in entry/exit record (according to legal proposal + visa number)	Store	R	ABC/ Manual gate
5.2	Additional fields in entry/exit record ⁶⁷	Store	O	Manual gate
5.3	Create specific field for access denial (i.e. refusal of entry)	Store	O	Manual gate

With reference to TOMs A, B and C (EES)

	TOM A	TOM B	TOM C
1st entry	e-MRTD: retrieve photo from chip or use live photo	e-MRTD (retrieve photo from chip or use live photo)	e-MRTD (retrieve photo from chip or use live photo)
	MRTD: scanned photo	MRTD: scanned photo	MRTD: scanned photo

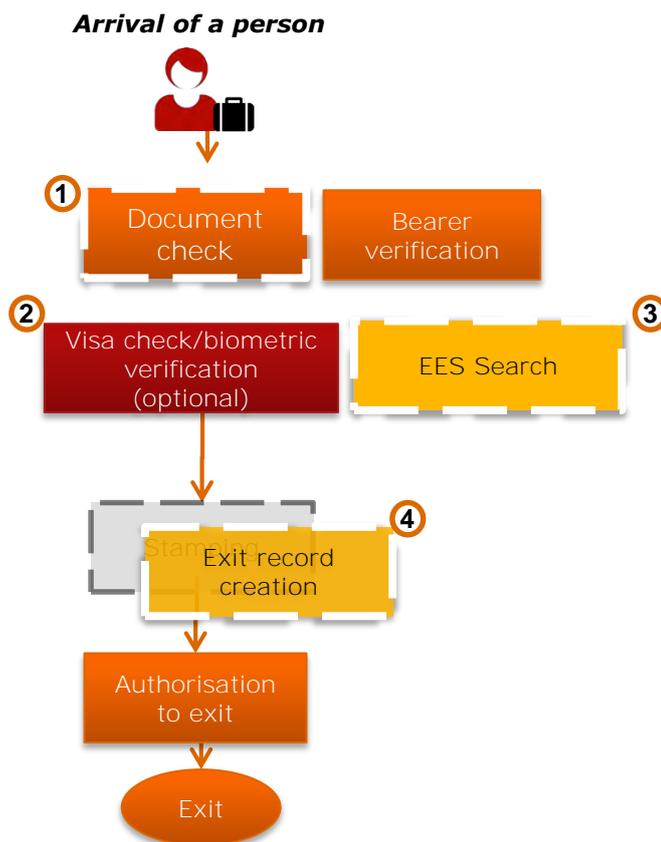
⁶⁷ Fields that would be registered, in most cases manually, at entry/exit (flight number, origin, final destination, license plate, vehicle number (VIN), full original name, if the person is a driver or a passenger, observations).

**Entry/Exit
(search &
verification)**

VH: 1, 2 or 4 live FP,
against VIS

VH: 1, 2 or 4 live FP, against VIS

TCNVH options at exit



Step 1: Document check – (ABC and manual gate)⁶⁸

**Main objective: Authentication of e-MRTD (chip) and check for falsifications
(Authentication of MRTD and check for falsification remain unchanged)**

n°	Action	Status
1.1	Passive Authentication (PA)	R
1.2	Active Authentication (AA)	O

⁶⁸ The bearer verification is performed within the VIS framework. No change proposed.

Step 2: VIS check (optional)**Main objective: retrieve visa information from VIS**

n°	Action	Store vs check	Status	ABC-gate vs manual gate
2.1	VIS check and verification by using visa number and live FP (<i>unchanged</i>)	Check	R	ABC and manual gate
2.3	VIS information retrieved by using document number	Check	O	ABC and manual gate

Step 3: EES Search**Main objective: record at all subsequent entries and exists**

n°	Action	Store vs check	Status	ABC-gate vs manual border gate
3.1	Retrieve EES individual file: issuing country and document number of MRZ (MRTD/e-MRTD)	Check	R	ABC ⁶⁹ and manual gate

Step 4: Entry/exit record creation**Main objective: record at all subsequent entries and exists**

n°	Action	Store vs check	Status	ABC-gate vs manual border gate
4.1	Fields in entry/exit record (according to legal proposal + visa number)	Store	R	manual gate
4.2	Additional fields in entry/exit record ⁷⁰	Store	O	manual gate

⁶⁹ ABC is proposed to be only used at exit, for TCN, where this is possible.

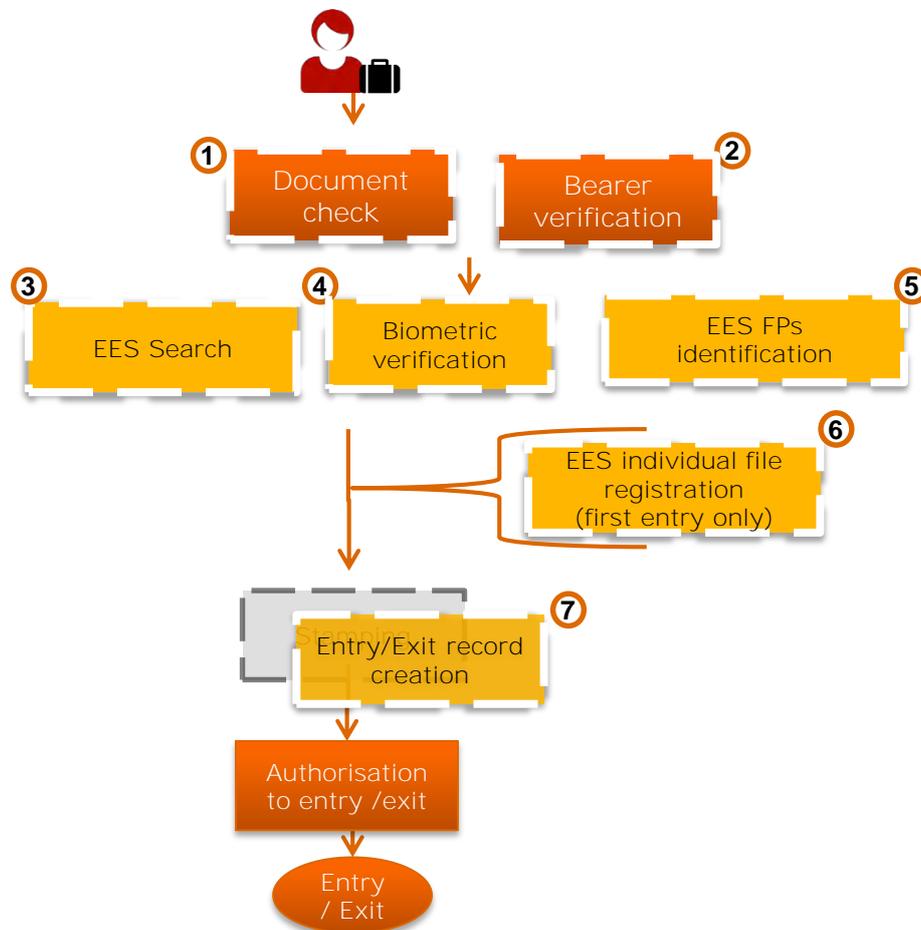
⁷⁰ Fields that would be registered, in most cases manually, at entry/exit (flight number, origin, final destination, license plate, vehicle number (VIN), full original name, if the person is a driver or a passenger, observations).

With reference to TOMs A, B and C:

	TOM A	TOM B	TOM C
Entry/Exit (search & verification)	VH: 1, 2 or 4 live FP, against VIS (optional)	VH: 1, 2 or 4 live FP, against VIS (optional)	

> *TCNVE*

TCNVE options at entry



Step 1: Document check – (ABC and manual gate)

**Main objective: Authentication of e-MRTD (chip) and check for falsifications
(Authentication of MRTD and check for falsification remain unchanged)**

n °	Action	Status
1.1	Passive Authentication (PA)	R
1.2	Active Authentication (AA)	O
1.3	Chip Authentication (CA)	O

Step 2: Bearer verification

**Main objective: verification that the holder of e-MRTD is the lawful owner
(Visual verification that the holder of the MRTD is the lawful owner is unchanged)**

n°	Action	Status
2.1	Live FI against e-MRTD (where available)	R

Step 3: EES Search

Main objective: record at all subsequent entries and exists

n°	Action	Store vs check	Status	ABC-gate vs manual border gate
3.2	Retrieve EES individual file: issuing country and document number of MRZ (MRTD/e-MRTD)	Check	R	Manual gate

Step 4: EES Biometric verification

Main objective: Biometric identification and verification of TCNVE

n°	Action	Store vs check	Status	ABC-gate vs manual gate
4.1	Verification: <ul style="list-style-type: none">1,2 or 4 FP against EESLive FI against e-MRTD or against FI in EES (ABC at exit)Manual (ocular) verification using FI	Check	R	Manual gate

Step 5: EES Biometric identification

Main objective: Biometric identification and verification of TCNVE

n°	Action	Store vs check	Status	ABC-gate vs manual gate
5.1	Perform 1:N identification, using biometrics -live or e-MRTD ⁷¹ FI -live fingerprints ⁷²	Check	O	Manual gate

Step 6: EES individual file registration

Main objective: Create individual file in EES, at first entry

n°	Action	Store vs check	Status	ABC-gate vs manual gate
6.1	First entry: live FP ⁷³ - FI (live, e-MRTD, scanned)	Store	R	Manual gate
6.2	First entry: FI (e-MRTD or live)	Store	R	Manual gate
6.3	First entry: MRZ data	Store	R	Manual gate
6.4	First entry: MRZ + all additional fields of the legal proposal	Store	O	Manual gate

⁷¹ e-MRTD should be used to the maximum extent possible to ensure quality and feasibility of verification.

⁷² A number of 4 FPs is recommended by the Study.

⁷³ 4 or 8 fingerprints are proposed to be enrolled for the individual file (see TOM B and C)

Step 7: Entry/exit record creation

Main objective: record at all subsequent entries and exists

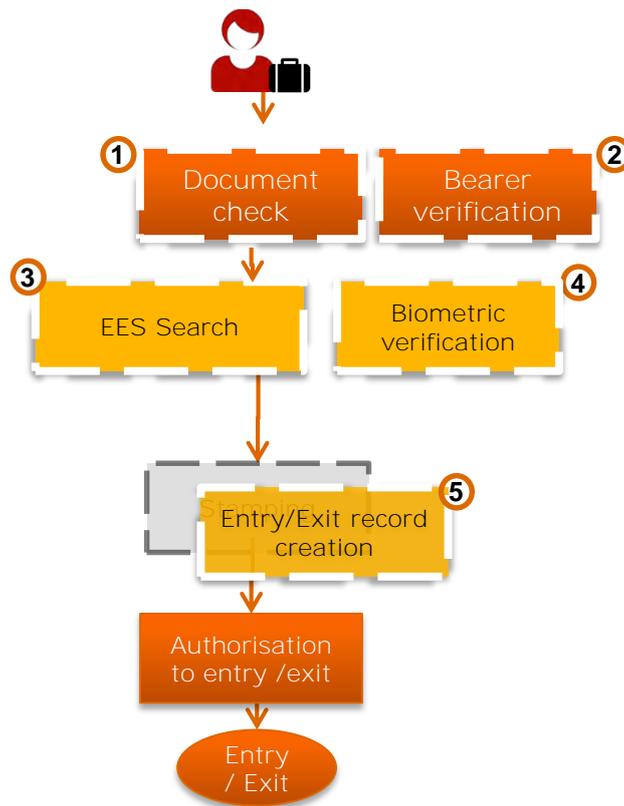
n°	Action	Store vs check	Status	ABC-gate vs manual gate
7.1	Fields in entry/exit record (according to legal proposal + visa number)	Store	R	ABC/ Manual gate
7.2	Additional fields in entry/exit record ⁷⁴	Store	O	Manual gate
7.3	Create specific field for access denial (i.e. refusal of entry)	Store	O	Manual gate

With reference to TOMs A, B and C (EES)

	TOM A	TOM B	TOM C
1st entry	e-MRTD: retrieve photo from chip or use live photo MRTD: scanned photo No FP	e-MRTD (retrieve photo from chip or use live photo) MRTD: scanned photo 4 FP	e-MRTD (retrieve photo from chip or use live photo) MRTD: scanned photo 8 FP
Entry/Exit (search & verification)	Verification of FI from e-MRTD against photo in EES	1, 2 or 4 live FP, against EES	

⁷⁴ Fields that would be registered, in most cases manually, at entry/exit (flight number, origin, final destination, license plate, vehicle number (VIN), full original name, if the person is a driver or a passenger, observations).

TCNVE options at exit



Step 1: Document check (ABC and manual gate)

**Main objective: Authentication of e-MRTD (chip) and check for falsifications
(Authentication of MRTD and check for falsification remain unchanged)**

n °	Action	Status
1.1	Passive Authentication (PA)	R
1.2	Active Authentication (AA)	O
1.3	Chip Authentication (CA)	O

Step 2: Bearer verification

**Main objective: verification that the holder of e-MRTD is the lawful owner
(Visual verification that the holder of the MRTD is the lawful owner is unchanged)**

n°	Action	Status
2.1	Live FI against e-MRTD (where available)	O

Step 3: EES Search

Main objective: record at all subsequent entries and exists

n°	Action	Store vs check	Status	ABC-gate vs manual border gate
3.1	Retrieve EES individual file: issuing country and document number of MRZ (MRTD/e-MRTD)	Check	R	ABC ⁷⁵ and manual gate

Step 4: EES Biometric verification

Main objective: Biometric identification and verification of TCNVE

n°	Action	Store vs check	Status	ABC-gate vs manual gate
4.1	Verification: <ul style="list-style-type: none">• 1,2 or 4 FP against EES• Live FI against e-MRTD or against FI in EES (ABC at exit)• Manual (ocular) verification using FI	Check	R	Manual gate

⁷⁵ ABC is proposed to be only used at exit, for TCN, where this is possible.

Step 5: Entry/exit record creation

Main objective: record at all subsequent entries and exists

n°	Action	Store vs check	Status	ABC-gate vs manual border gate
5.1	Fields in entry/exit record (according to legal proposal + visa number)	Store	R	manual gate
5.2	Additional fields in entry/exit record ⁷⁶	Store	O	manual gate

With reference to TOMs A, B and C (EES)

	TOM A	TOM B	TOM C
Entry/Exit (search & verification)	Verification of FI from e-MRTD against photo in EES	1, 2 or 4 live FP, against EES	

⁷⁶ Fields that would be registered, in most cases manually, at entry/exit (flight number, origin, final destination, license plate, vehicle number (VIN), full original name, if the person is a driver or a passenger, observations).

1.4.3. RTP (entry –exit)

> TCNVH entry-exit options

Main objective: verification of the person having a RTP membership

n°	Action	Store vs check	Entry vs Exit	Status	ABC-gate vs manual border check
1.1	Live FP ⁷⁷ checked against VIS	check	Entry / Exit	R	ABC and manual gate
1.2	Live FI against e-MTRD ⁷⁸	check	Entry / Exit	O	ABC and manual gate
1.3	Live FI against RTP	check	Entry / Exit	O	ABC and manual gate

> TCNVE entry-exit options

Main objective: verification of the person having a RTP membership

n°	Action	Store vs check	Entry vs Exit	Status	ABC-gate vs manual border check
2.1	Live FP ⁷⁹	check	Entry / Exit	R	ABC and manual gate
2.2	Live FI against e-MTRD ⁸⁰ or against RTP	check	Entry / Exit	O	ABC and manual gate

⁷⁷ Check against EES (TCNVEs) or VIS (TCNVHs) or RTP depending on the option chosen for the RTP enrolment procedure.

⁷⁸ e-MRTD should be used to the maximum extent possible to ensure quality and feasibility of verification.

⁷⁹ Check against EES (TCNVEs) or VIS (TCNVHs) or RTP depending on the option chosen for the RTP enrolment procedure.

⁸⁰ e-MRTD should be used to the maximum extent possible to ensure quality and feasibility of verification.

1.4.4. Main general recommendations for successful implementation of EES and RTP (processes)

	Action	Recommended	Optional
	For biometric verification, the use of FI is key in the transition period towards FP use, if the decision to have such a transition period without FP at the beginning is taken: e-MRTD FI should be used to the maximum extent possible to ensure quality and feasibility of verification, for MRTD holders, the printed photo is scanned and stored as a minimum requirement	✓	
	A maximum of 4 or 8 FPs enrolled for TCNVEs (in accordance with mobile technology potential and to avoid extra delays)		✓
	LBT permits and residence permit holders should not be included in EES: entering these persons in the EES would add to the duration of border crossing and brings no added value to the specific objective of the EES. LBT permits and residence permit holders could, however, be included in the RTP.	✓	
EES	Pre-border checks (via self-registration in kiosks) could accelerate the border crossing processes (air and sea borders) for preparing EES registration and verification		✓
	Separation of TCNVE and TCNVH lanes and making better use of the time for travellers at waiting areas (land borders) to prepare and make checks , are likely to accelerate border crossing		✓
	Automation of the process at exit for all TCNs : using ABC gates at exit could reduce the amount of time and workload of guards		✓
	A minimum dataset is recommended to be used, for saving time and ensuring data quality, for: <ul style="list-style-type: none"> • EES search (issuing country + document number) • EES individual file (MRZ + visa sticker number for TCNVH) 	✓	

- **EES entry/exit record (date, time, BCP, etc.⁸¹)**

	Use e-MRTD as token for RTP status : no separate token is needed ⁸²	✓
RTP	Only e-MRTD holders as potential RTP candidates (note that opening the RTP enrolment to MRTD holders would complicate verifications and include higher risks for fraud)	✓
	Live FI checked against e-MRTD FI should be used to the maximum extent possible to ensure quality and feasibility of verification at ABC gates	✓

⁸¹ See table 5 in chapter 3.

⁸² The separate token provides little determining advantage and adds operational complexity. Using e-MRTD reduces costs and complexity, maintains level of security and has no negative impact on the duration of the border crossing.

– **Compliance with the EES legislative proposal and with other legal instruments**

The table below gives an overview of options included in the Study, which are not compliant, partially or fully, with the EES legislative proposal. The overview does not explain all details as regards the usage of data and biometrics. It does also not justify or assess the options. This is explained in detail later in other parts of the study (e.g. chapter 3.4 includes assessments in relation to impact on border crossing duration and flow of travellers)

Option	Instrument and articles	Impact⁸³	Impact on legislative proposal
Search in EES to retrieve the individual file using: issuing country and document number	EES: 15	Limited	Currently the EES legislative proposal provides for that a search in EES for verification at external borders can take place with the surname, surname at birth, first name, date of birth, country of birth, nationality/is and sex in combination with some or all of additional data enlisted in art.15. Although the proposal already includes the issuing country and the document number among the data that can optionally be used for search purposes, it provides for different data to be used for the verification as listed above. Therefore, if the option retained would only include for search purposes the issuing country and the document number, then the EES legislative proposal would require a modification in order to reflect this option.
Registration of TCN by creating the individual file entering the following data: MRZ and visa number	EES: 11	Limited	The EES legislative proposal currently includes a higher number of alphanumeric data to be collected at the moment of registration compared to the number suggested by this option. This option establishes that the data to be registered in the individual file would be limited to: MRZ and the visa number (for visa holder). If this option is chosen, then the legislative proposal would need to be reviewed.
Insert additional optional fields (such as license plate, flight number) at each entry/exit of TCN	EES: 11	Limited	This option introduces additional fields that are not mentioned in the current legislative EES proposal. Therefore, if accepted, the legislative proposal would need to be amended.

⁸³ **Limited impact:** only one legislative proposal of the Smart Borders Package is impacted **Extensive impact:** at least two legislative proposals are impacted **Very extensive impact:** at least one legislative proposal and at least one legislation in force are impacted.

Registration of TCNVE by creating an individual file that contains less than 10 FP	EES: 12(1)	Limited	The current EES proposal provides that, in the absence of a previous registration of a third country national in the EES where a decision has been taken to authorise the entry of TCNVE, the border authority shall enter 10 fingerprints in the individual file of the person. If the option retained would include less than 10 fingerprints, then the legislative proposal would need to be amended.
--	------------	---------	--

Option	Instrument and articles	Impact ⁸⁴	Impact on legislative proposal
Biometric verification of live captured photo against the photo in the e-MRTD) to support verification	EES: 15; 18; 23	Extensive(a Iso RTP)	The legislative proposal composing the Smart Borders Package currently does not include biometric verification using photo. Such an option would require a modification of the proposals. This specific option relates mainly to ABC gates. Similarly, the RTP legislative proposal would need to be amended because it does not include biometric verification using photo either. (note: since the photo is used for a verification it needs to be a digital picture also called facial image (FI))
Biometric verification of live captured photo against the photo stored in EES for verification at entry/exit	EES: 11; 12; 15 ; 18; 23.	Extensive (also RTP, see below)	The legislative proposals composing the Smart Borders Package currently do not include biometric verification using live photo against the storing of photo in EES. Such an option would require a modification of the proposals. This option could be implemented by border guards doing manual (ocular) verification or by an automated verification, if the right equipment exists in the manual gate. In addition also the storage of this personal data would need to be provided.
Use document number in the context of EES to find data in VIS (instead of visa sticker number)	EES: 16. VIS 767/2008: 18.	Very extensive	Currently VIS Regulation 767/2008 states the possibility for the competent authorities to search in the VIS by using the visa sticker number in combination with verification of fingerprints of the visa holder. If instead of the visa sticker number, the option retained would include the use of the document number and the country code for the search, then the VIS Regulation would need to be amended.
Identification in EES at entry using fingerprints, for	EES: 19	Limited	Currently the EES legislative proposal states the possibility to use fingerprints for identification purposes only for those persons who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member

⁸⁴ **Limited impact:** only one legislative proposal of the Smart Borders Package is impacted **Extensive impact:** at least two legislative proposals are impacted **Very extensive impact:** at least one legislative proposal and at least one legal instrument in force are impacted.

all TCNVE.

States. This option aims at generalising identification to all TCNVE. If considered to be in line with data protection legislation it would require a modification of the EES legislative proposal.

Verification at exit made against VIS for TCNVH	EES: no article exists VIS: 18 SBC: 7(3) (c)	Very extensive	Currently the Schengen Borders Code does not include any obligation with regard to checks to be carried out in VIS at exits. If such an option would be retained, then a modification of VIS Regulation is required. In addition, such verification would need to be included in the EES legislative proposal as well An alternative to this option entails the verification with a photo from the e-MRTD, as described above (see option Use the e-MRTD photo against the photo stored in EES for verification at entry/exit).
EES individual file and entry record created for persons refused entry	EES: no article exists	Very extensive	Currently the EES legislative proposal does not include that persons refused entry could be entered in the EES. This option would make available the information of the refusal to all border crossing points at the external border, which could bring added value to a more secure border control process. In addition the SBC in Article 13 provides for the obligation to affix an entry stamp on the passport cancelled by a cross in indelible black ink and to write opposite it on the right hand side also in indelible ink the letter(s) corresponding to the reason(s) for refusing entry, the first of which is given on the standard form under annex V for refusing entry. MS should also if applicable enter the refusal of entry in the SIS.
VIS Check at entry using ABC gate	EES: no article exists	Very extensive	The legislative proposal allows for persons with RTP status to use ABC gates. This implies that VH with RTP status could use ABC gates. A check to the VIS, using fingerprints, is a mandatory action at entry. The consequence of this would either be that it is imposed that ABC gates can use fingerprints or that the verification of the ABC gate (using photo) in combination with checking the VIS using visa number, would be accepted. The latter would require a change in the VIS legislation.
Collect the e-MRTD FI (if available) or a high resolution picture at entry and store it in	EES: 5; 11;12		For TCNVE this option would require foreseeing including a change that supports storage of FI taken from e-MRTD or taken as a live picture. For TCNVH it could also be an option, if the quality of images in VIS is not considered

the EES

sufficient.

Collect the e-MRTD FI (if available) or a high resolution picture at visa application and store it in the VIS only.

Regulation 810/2009: 13(2)

This option only concerns TCNVH and the procedure to be followed at the moment of the submission of a visa application. Today in VIS images are scanned from the paper version or a live picture with format of average resolution is taken. In the future it is necessary to take into consideration the possibility to collect facial image from e-MRTD (when it exists) and support higher resolution format in the context of the visa application procedure.

LBT PERMITS

TCNs holding an LBT permit are entered in EES

EES: no article exists
Regulation (EC) No 1931/2006: 6

Very extensive

Currently the EES legislative proposal excludes LBT from its scope, since they are not subject to any stamping when they cross the EU Schengen Borders. Therefore any modification going towards the inclusion of individuals holding a LBT permit would require a modification of the EES legislative proposal.

In addition it would require a modification of Regulation (EC) No 1931/2006 to include within the scope of the entry exit system TCNs holding a local border traffic permit and it could require an amendment of the SBC.

RESIDENCE PERMITS

TCNs holding a residence permit are registered in EES

EES: no article exists
SBC

Very extensive

Currently TCNs holding a residence permit are not included in the EES legislative proposal, hence if retained, the EES legislative proposal would need to be amended. This option would require including a different and separate calculation of authorised stay in the EES, and possibly Directive 2004/38/EC as their stay is not limited to 90 days within 180 days and the provision granting equal treatment with nationals with regard to free access to the entire territory of the MSs concerned would need to be amended because EU citizens fall outside the scope of the entry/exit system...

PROCESS ACCELERATORS

Collect data in waiting areas

EES: no article exists
SBC: Annex II
Registration of information.

Extensive

Currently such option is not provided by the EES legislative proposal and it is assumed that the proposed accelerator might be outside the scope of the EES legal instrument. If this option would be retained it could require an amendment of the Schengen Borders Code. The SBC do make a reference to the possibility of TCN using automated checks, under supervision, in article 7a) 2) . It is however not clear that this would cover all the options of a pre-check and pre-registration in waiting areas.

EES data retention time aligned to RTP data retention and status	EES: preamble (20). Limited	The data retention time is currently set to 181 days for the EES and 5 years only for overstayers. If the EES data retention period was aligned to the RTP status, then the EES legislative proposal would need to be amended. This option takes into account that the RTP proposal currently includes a first registration of one year followed by two subsequent periods of two years each. The data retention for RTs in the EES should be limited to the length of their actual access to the RTP. Since RTs might not want to extend such access to for the full 5 years, then as soon as their period of access the RTP has expired they should re-register in the EES.
Separate lanes for VH and VE	EES: no article exists. Very extensive RTP: no article exists. SBC: 9; Annex 3.	Currently such an option is not included in the legislative proposals composing the Smart Borders Package. It is however not seen as necessary, but it would require an amendment to the Schengen Borders Code. The Schengen Borders Code currently provides that MS shall provide separate lanes at air borders and may provide separate lanes at sea and land borders bearing the indications of annex III of the SBC i.e. EU/EEA/CH citizens, Visa not required, all passports etc. TCN who are not obliged to possess a visa when crossing the external borders of the MS and TCN who hold a valid residence permit or long-stay visa may use the lane VISA not required. They may also use the lane ALL passports. The provision of a separate lane 'VISA not required' is not obligatory.

1.5. Compliance with the RTP legislative proposal and with other legal instruments

The table below describes options included in the Study, which are not compliant, partially or compliant with the legal proposal for RTP.

Option	Instrument and main articles	Impact ⁸⁵	Impact on legislative proposal
1: N identification against the RTP, using FP. (for VE) when submitting the RTP application	RTP: article 31(5) currently foresees it but should be amended in order to only cover VH	Limited	The RTP legislative proposal currently provides this possibility. It should be amended in order to only cover VH and to carry out such identification systematically
Store the photo of the e-MRTD in the RTP for verification purposes	RTP: recitals and articles 3; 5; 8; 25; 31; 32; 37; 48; Annex I	Extensive	The RTP legislative proposal currently does not provide the possibility to store a photo in the RTP for verification purposes. Such an option would require a modification to the RTP proposal
Registration of the individual file in EES once an RTP application is considered to be admissible	RTP: article 14 EES: articles 11, 12	Extensive	The EES and RTP legislative proposals do not include the possibility of creating an EES individual file once an RTP application is considered to be admissible. Should this option be retained, it would require several modifications of the proposals, including the calculation of authorised stay that should be done as from date of actual entry and not from the registration in the EES. Specific provisions for residence card holders, residence permit holders and D-visa holders could be included in order to ensure that no entry/exit record would be created for these categories of RTs.
e-MRTD used as a token	RTP: 1; 2; 3; 5; ; 18; 21 ; 22; 23; 27 Chapter VI; 31; 3	Extensive	The RTP legislative proposal, part of the Smart Borders Package, currently envisages issuing a token. This latter and the number of the travel document are to be provided on arrival and departure at the border in order to verify that access has been granted to the RTP.. If the option retained excludes the use of a separate

⁸⁵ **Limited impact:** only one legislative proposal of the Smart Borders Package is impacted **Extensive impact:** at least two legislative proposals are impacted **Very extensive impact:** at least one legislative proposal and at least one legislative instrument in force are impacted.

	2; 33; Chapter VIII; 34; 36; 37; 38; 39; 63; SBC legislative proposal: art 9.2(a)		token, then the RTP legislative proposal would need to be amended. This option includes also that the RTP record would be retrieved by using the issuing country + document number, which makes also for a change to the legal proposal. The Schengen Borders Code legislative proposal foresees that if RTs they are holding biometric passports they may also use the lanes indicated by the signs in Part D of Annex III. However, if the option retained implies the use of the e-MRTD as a token, RTs would always be holding a biometric passport.
RTP 10 fingerprints	RTP: 8	Limited	Currently the RTP legislative proposal provides the enrolment and processing of four fingerprints. Any modification to this number would require an amendment to the RTP legislative proposal. The collection of 10 fingerprints should be justified (in particular, the measure shall be proportionate and necessary).
Data stored in the VIS are used as basis for the RTP of VH(verification and storage)	RTP: 5;8, 25,31, 32,40,41, Annex I VIS Regulation	Very extensive	The RTP legislative proposal establishes that the RTP system should store also data of visa holders, which are currently also stored in the VIS. If this option is retained and is considered compatible with data protection principles, then the RTP proposal and the VIS Regulation would need to be modified.
Collect the e-MRTD FI (if available) or a high resolution picture at entry and store it in the RTP	RTP: 3; 5; 8; 25; 31; 32; 37; Annex I	Extensive	For TCNVE as well as for TCN holding a residence permit, a residence card or a D-visa this option would require foreseeing a change that supports storage of FI taken from e-MRTD or taken as a live picture. For TCNVH it could also be an option, if the quality of images in VIS is not considered sufficient.
Collect the e-MRTD FI (if available) or a high resolution picture at visa application and store it in the VIS only (VH)	Visa Code: art. 13(2)	Very extensive	This option only concerns TCNVH and the procedure to be followed at the moment of the submission of a visa application. Today in the VIS, images are scanned from the paper version or a live picture with format of average resolution is taken. For the future it is necessary to take into consideration the possibility to collect the facial image from the e-MRTD (when it exists) and support higher resolution format in the context of the visa application procedure.

<p>VIS check for VH that are RTP members using ABC gates at entry and exit. an option could be to include FI verification against the FI in the VIS if the ABC-gate cannot handle FP verification to the VIS</p>	<p>EES: 11; 12;18 RTP: 5; 8; 25;31; 32; VIS Regulation Schengen Borders Code</p>	<p>Very extensive</p>	<p>This option is an alternative for making the mandatory VIS check. It would require changes to the VIS regulation since this only includes biometric verifications using FP</p> <p>This option seems also not to be in line with Article 7 (2) of the SBC. and art 7(3)(c)(i) of the SBC. Therefore such an option would require amendments to the SBC if retained.</p>
<p>Rely on FP stored in VIS (for TCNVH only) on entry and exit</p>	<p>RTP: 5;8; 25; 31;32 VIS Regulation SBC</p>	<p>Very extensive</p>	<p>This option would be of application only for TCNVH.</p> <p>This option seems also not to be in line with Article 7(3)(c)(i) of the SBC. Therefore such an option would require amendments to the SBC if retained.</p>
<p>Checking e-MRTD against live photo for ABC gates</p>	<p>RTP 7a</p>	<p>limited</p>	<p>This option entails the possibility of checking the e-MRTD against live photo in RTP in ABC gates.</p> <p>Currently paragraph 2 of Article 7a of the proposal amending the Schengen Border Code opens the possibility to use ABC means in combination with "self-service kiosks" by travellers where the fingerprints are stored in the VIS or in the travel document (biometric passport) and where these fingerprints can be accessed by the border guard authorities.</p> <p>Introducing the possibility of checking e-MRTD against live photo would entail the modification of the proposal in order to foresee such an automated check also for e-MRTD against live photo. Also in this case the process shall be monitored and followed by an individual decision by the border guard to authorise or refuse entry.</p>

• ***Use of biometric characteristics***

– ***Objectives, approach and structure of this chapter***

◦ ***Objectives***

This chapter examines the use of biometric recognition as a means to enhance and strengthen identity checks at external borders and the overall security of border controls. This chapter further explains the advantages, drawbacks and specifics of biometric identifiers in order to answer the following Thematic Files:

- TF1 Biometrics in EES;
- TF2 Biometrics in RTP;
- TF3 Transition period.

◦ ***Approach***

Biometric characteristics plays a role in each of the four process families (see Figure 1). Their primary objective is to strengthen identity checks at external borders. Therefore, the focus is on the key factors that contribute to this strengthening. For the purpose of the analysis, security (S), impact on duration of the border crossing (D) and implementation complexity (C) criteria have been considered, together with transversal criteria such as costs and data protection. It should be noted that the present chapter only provides the answers to the Thematic Files, and concludes with a section on legal aspects and data protection. Further analysis with regard to the various criteria has been performed in the chapter on Target Operating Models.

Security has at least two major relevant domains in the EES AND RTP context:

- Added value of the biometric functionality in strengthening identity checks at external borders; and
- System security (e.g. defence against hackers, malware, business continuity).

Security has been limited to the first domain (the added value in the identity checks). This document assumes that the system will be implemented with adequate system security considerations and after eu-LISA Risk Analysis. However, these fall outside the scope of the Thematic Files.

It should be noted the study intentionally provides answers to Thematic Files in terms of options rather than in terms of recommendations.

Finally, the vocabulary used in this section is based on the standard⁸⁶ biometric terminology, which is described in the glossary.

⁸⁶ ISO/IEC 2382-37 Biometrics – Vocabulary

- **Structure**

This chapter first introduces biometric recognition and describes how this relates to the EES and RTP. Then assumptions are described with regard to biometric recognition in an EES and RTP context. Subsequently, analyses of key aspects related to the criteria are provided. The answers to the Thematic Files are provided next. Finally, legal and data protection aspects are addressed.

For the sake of completeness, a more detailed description of biometric recognition, its security and performance, as well as e-MRTDs is provided in appendix.

- **Context**

- **Biometric characteristics related to the EES and RTP**

Although similar in some aspects, human beings differ in appearance, behaviour and biological traits. Various recognition technologies can be used to create and maintain a reliable identity repository. For the purposes of EES AND RTP, the most important ones are recognition of digital images of the face, and of fingerprints.

Other technologies exist, but are currently considered less relevant to EES and RTP. These include iris, hand geometry, voice, vascular patterns, dynamic signature verification, keystroke dynamics, vein/palm scans, DNA and gait.

A typical system architecture for a biometric system is depicted below.

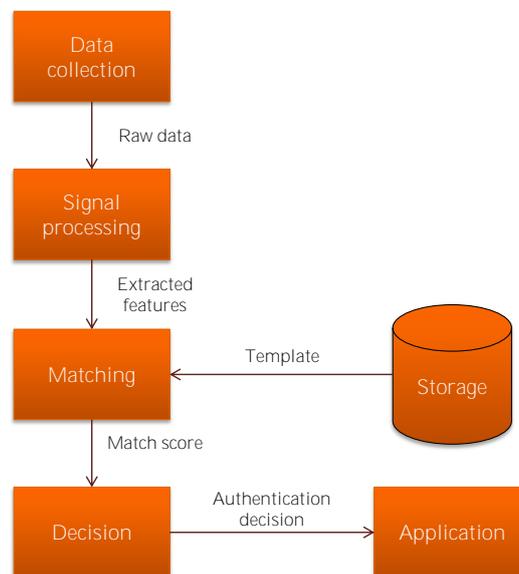


Figure 23 A typical biometric system architecture

Initially, raw data is collected and processed into features, which are stored in the form of a template in a database. The original raw data is also kept, to facilitate interoperability. Upon subsequent data collection at a later point in time, the newly collected data features can then be compared with the already stored template.

Possible uses for biometric characteristics in the context of the EES and RTP include:

Table 31 *Biometric Use Cases in the context of the EES and RTP*

#	Description of possible use	Application to border control processes (EES)	Application to border control processes (RTP)
1	1:1 verifications FP/FI versus database	Verification of persons already present in the EES, at all entries, exits and in-territory checks.	Verification of persons already present in the RTP, at all entries and exits
2	1:1 verification of document holder versus document bearer	Verification of whether the document holder equals the legitimate document owner	Verification of whether the document holder equals the legitimate document owner
3	1:n identification at entry in EES and RTP	Identification of persons at entry will make it possible to find persons with double, possibly fraudulent identities, and to find persons with two or more passports that could (legally) contain slightly different data which would enable them to stay in the Schengen area almost indefinitely. It can be observed this was technically not yet possible with the VIS technology in 2006, and was not provided for on a systematic basis in the Legal Proposal.	Identification of persons at RTP enrolment. The identification search may be limited to rejected RTP applicants.
4	1-n identification ("re-documentation") searches for travellers that lost their travel documents	Check performed within the territory and at the exit (i.e. travellers with a temporary document different from the entry document or realising the loss of the document at the exit).	Not valid for RTP
5	1:few searches with FI	Identification of persons found in the EES, using FI plus a less exact key to search (e.g. gender, date of birth or name). Such identification is made against a subset of data from individual files in the EES.	Not valid for RTP
6	1:few searches with FP	Identification of persons found in the EES, using FP plus a less exact key to search (e.g. gender, date of birth or name). Such identification is made against a subset of data from individual files in the EES.	Not valid for RTP
7	1-n law-enforcement searches	Not part of the border control processes, but for checks within the territory	Not valid for RTP
8	1-n latent searches	Not part of the border control processes, but for checks within the territory	Not valid for RTP

The usage of iris as a biometric identifier had previously been excluded from the study. While reference projects doing identifications (1:n searches) in databases of over 1million persons were previously non-existent, the UID programme in India has proven that iris can be an appropriate biometric identifier for identifications in very large databases. This report simply states that iris technology seems to be sufficiently mature and tested to be used in the Smart Borders scenarios where it could potentially replace the fingerprints, both for identifications and verifications. This technology has not been analysed for the purpose of this report.

Assumptions

The hypothetical biometric services rest on the following assumptions:

- As a consequence of ICAO Standard 3.10.1⁸⁷ all non-MRPs should have expired by November 2015. Consequently, only Machine Readable Passports will be valid after this deadline;
- As explained in the general assumptions, it is expected that all ICAO members will gradually perform a transition to e-MRTDs;
- An e-MRTD/MRTD can be used as the only credential for RTP (no other token than a MRTD passport is required for RTP);
- Due to security concerns, only RTP members with an e-MTRD passport will be allowed to use automated gates (ABC gates);
- ID data can be read from the MRZ as well as from the chip, if available. Facial images can be read relatively easily by the Inspection System (IS). For e-MRTD, facial image data is protected from an access control perspective by the Basic Access Control (BAC) mechanism and by the more secure Supplemental Access Control (SAC)⁸⁸. Other data such as fingerprints is protected by Extended Access Control (EAC), which mandates the use of certificates. The latter is considered relatively cumbersome, as such certificates are not always available. A full analysis of the different data groups stored and protected in an e-MRTD is available in appendix;
- Although not provided for by the current legal basis, it could be evaluated whether both the EES and RTP could make use of the same/a subset of biometric identifiers, i.e. fingerprints taken live (on the spot) and facial image read from the chip, to maximise re-usability and interoperability;
- **When fingerprints are taken, they are taken as flat (also referred to as 'plain') fingerprints**, not as rolled fingerprints. This is identical to how fingerprints are taken for the VIS. While rolled fingerprints make it possible to capture more information than flat fingerprints, their taking requires assistance from an operator. This introduces further delays in the enrolment process. As flat fingerprints offer sufficient functionality for the purposes of EES and RTP, this report always implicitly refers to flat fingerprints, unless explicitly indicated otherwise;
- Taking 10 fingerprints at entry may not be possible in all situations;
- As EES and RTP are primarily border-control systems, Law Enforcement Access should not be the driving requirement;

⁸⁷ Source: ICAO, <http://www.icao.int/publications/Pages/doc7300.aspx>

⁸⁸ The Supplemental Access Control (SAC) will become mandatory for the new European passports as from December 2014.

- Today, most ABC gates compare facial images or fingerprints against images stored in the chip and one of the goals will be to re-use as much as possible their current configuration and setup, to be more cost-effective;
- Finally, with regard to document security, e-MRTD verification steps should follow the Frontex 'Best Practices'⁸⁹.

- ***Sources used for the TF analysis***

This study does not intend to provide its own assessment of current biometric systems, service providers or components. This study is based on a broad range of public domain information and **vendor consultation, complemented by DG Home Affairs' experience.**

The main sources of information used to support the analysis in this chapter are:

- Experience with the VIS and its BMS;
- Consultations:
 - **With Member State representatives during the study's workshops;**
 - With representatives from the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) on the specific topic of protection mechanisms of e-MRTDs;
 - Vendors of biometric solutions.
- Literature review of reports from:
 - Unique Identification Authority of India (UIDAI);
 - The US National Institute of Standards and Technology (NIST);
 - The US Department of Homeland Security (DHS);
 - The German Federal Office for Information Security.

⁸⁹ Source: Frontex, Best Practice Technical Guidelines for Automated Border Control Systems, http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf

– **TF analysis**

To formulate the answers to the questions raised in the Thematic Files, the rationale for deploying a biometric system is first summarised; this rationale is mainly based on the security services it offers. The intended security service level is a trade-off between several factors, including the type of biometric characteristics used, biometric recognition performance, and constraints such as database size, additional delays and increased complexity.

First, the most important factors are described, and then they are analysed in the context of EES and RTP.

◦ **Evaluation factors that contribute to the TF analysis**

A biometric system is composed of the following subsystems: Data Acquisition, Signal Processing, Data Storage, Comparison and Decision. Security performance assessment is based on the errors generated by these subsystems. The two main classes of error types are acquisition and matching errors:

- Acquisition errors are Failure To Enrol (FTE) and Failure To Acquire (FTA);
- Matching errors are False Non-Match Rate (FNMR) and False Match Rate (FMR).

When used in verification (1:1) transactions, and focussing on the outcome of the transaction, FNMR and FMR correspond to False Rejection Rate (FRR) and False Acceptance Rate (FAR).

When used in identification (1:n) transactions, they correspond to False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR).

Various error types are summarised below; a more detailed description can be found in appendix.

Summary of the **acquisition error types**:

- Failure To Enrol (FTE): proportion of user enrolment transactions that cannot be completed according to the enrolment policy;
- Failure To Acquire (FTA): probability of user attempts during verification or identification for which the system cannot acquire an appropriate sample.

The root cause for FTE and FTA can be the same, but they are differentiated because they belong to a different part of the process. Allowing enrolment of lower quality samples (i.e. allowing a lower FTE or FTA) might result in more matching errors.

Summary of the **matching error types**:

- False Non-Match Rate (FNMR): is calculated as the proportion of samples from genuine attempts that cannot be matched against enrolled templates of genuine users;
- False Match Rate (FMR): is calculated as the proportion of samples from imposter attempts that are successfully compared against enrolled templates of genuine users.

FNMR and FMR are **attempt-based** rates. They are based on a single attempt, and not on a verification or identification transaction. Such a transaction may allow multiple attempts in a single transaction.

Summary of the **verification transaction error types**:

- False Acceptance Rate (FAR): when an intruder is incorrectly accepted. FAR is determined by **both the 'False Match Rate' and the system's decision policy**. FAR is often considered the most important single rate;
- False Rejection Rate (FRR): when a genuine user is incorrectly rejected. FRR is determined by both the False Non-Match (FNM) rate and the decision policy. FRR determines the manual workload since such users will most likely complain and will have to be handled manually;
- True Acceptance Rate (TAR): is defined as $TAR=1-FRR$. For example if $FRR = 1\%$, $TAR=1 - 0.01 = 99\%$.

FAR and FRR are transaction-based. A transaction results in either acceptance or rejection. The **system's policy may allow e.g. 3 failed verification attempts before rejecting the user**. In the case of such a failed verification transaction, there are 3 False Non-Match errors, but only a single False Rejection. Furthermore, it can be observed that the Equal Error Rate (EER) is the intersection between the FAR and FRR curves, where each is equally probable. The Detection Error Trade-off (DET) curves plot the FAR/FRR or FMR/FNMR as a function of the threshold.

With regard to the security performance of identification transactions, it is customary to consider **the concept of "candidate list"**. A candidate list is a list of enrolled users that are the most similar to the input sample provided. The identification rank r of a user is the smallest-sized candidate list of which the user is a member. The **identification transaction error types** are summarised as (a more detailed description can be found in appendix):

- Open set-search: samples from persons not enrolled in the system are used, in addition to **samples from enrolled persons**. This is considered to simulate "real-world use" of biometric characteristics. False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR) are used to report on "open-set" performance;
- Closed set-search: samples are from the same population as the enrollees. Only false claims of identity within the set can occur. This is not considered a real-world simulation. Cumulative Match Characteristics (CMC) curves are used to report on "closed-set" performance.

Furthermore, the term **Accuracy** is used to represent "1-FRR". It is mainly used for one-to-many search/identification transactions.

All of these attempts and transactions require a certain processing time. Time is influenced by the desired quality level; capturing higher quality data takes more preparation, and sometimes also more time. The total transaction time is the sum of the time of its component steps, which may be executed locally or remotely. For example, capturing is typically performed locally, but storing and comparing may be performed remotely, after which the resulting decision is communicated back to the local application. In the case that a communication between local and remote components is involved, there will be local processing time, remote processing time and network transit time.

- **Observations related to these factors**

- > **With regard to security performance**

On the basis of experiences of DG Home Affairs with VIS/BMS and best practices as discussed with vendors, the following observations are formulated:

Verification

Since the ability to detect imposters is typically considered to be the single most important security characteristic, FAR is considered the single most important security performance rate for verification. The biometric characteristics that are most mature for verification are fingerprints. Facial image recognition is also considered sufficiently mature for verification. Obviously their FAR **does not determine the system's security performance on its own, but further system parameterisation is typically driven from the decision to fix the FAR at a certain value. For Border Control systems, the FAR is typically set at 0.1% (value used for VIS' FAR for fingerprints), or better.** Vendors indicate the FAR can be improved by several orders of magnitude using today's technology and 8 or 10 fingerprints.

The desired FAR should be achieved under a compromise between FTE and FRR. A stricter enrolment policy leads to a higher FTE, but this yields a lower FRR as a consequence of the better quality of the data. End-users of the system appreciate a low FRR, but a higher FTE results in more persons that cannot be handled or require manual intervention to succeed in enrolling. It can equally be argued that there is value in fixing the FTE rate at zero, meaning all persons encountered in the process should somehow be enrolled, without exceptions but possibly compromising the data quality and thus increasing the FRR.

Verifying that the document holder corresponds to the document owner is and will continue to be possible by simple visual inspection performed by the Border Officer. The automation of this inspection, relying on facial image recognition (comparing live captured face versus stored image) is also popular, and is used at many ABC-gates.

The following figures are from the VIS-BMS:

Table 32 *Performances for the VIS-BMS: 1:1 verifications / permutations activated / fixed central processing time of 2 seconds*

# of fingers	FRR	FTE	FAR
1	0.01%	6%	1%
2	0.01%	2.5%	1%
4	0.01%	1.5%	0.1%

It should be noted the VIS-BMS uses technology from 2006. The FRR is lowered on purpose (with a detrimental effect on FAR) as the greater majority of visa holders are indeed expected to be the genuine holders of the visa. This lower FRR results in very few visa holders being falsely rejected.

The number of active fraudulent cases is estimated to be low. The impact of a slightly higher statistical FAR on this limited set of imposters is hence very limited.

Identification

Under a given FTE and FAR, accuracy of recognition based on fingerprints will vary depending on the number of fingers used for comparing. Under values representative for FAR and FTE in an EES and RTP context, vendors claim that accuracy can range from 90+% for a single finger to approximately 99.5% for 4 fingers and 99.9% for 8 fingers or more.

Furthermore, observations with regard to facial image recognition alone indicate diverging opinions. However, the vendors claim that in general, it cannot be considered to be sufficiently **accurate for identification in "stand-alone" mode towards high candidate lists or large database sizes.**

Obviously, processing time is also influenced by database size as well as the number of fingerprints used.

The current implementation of the VIS-BMS leads to an overall measured FTE of around 5% due to a quality control and rejection mechanism. The accuracy of the BMS AFIS has been measured to be better than 99.9% in this case.

However, it should be mentioned that the performance of an identification system such as the VIS-BMS correlates strongly to the database size. Therefore, the claimed numbers (assuming the current state of VIS-BMS with only some million entities) are not representative for EES and RTP with 70-300+ million identities (depending on storage duration). The numbers in the table below should be seen in this light.

An implementation of the VIS-BMS for 2014 or 2015 would lead to an FTE of 0%, where all fingerprints regardless of their quality would be accepted. The expected accuracy of the BMS AFIS would then drop to 99.5% (statistical value).

Table 33 Performances for the VIS-BMS: 1:n identifications / database of 70M records / Response time: 10 min / Best practices used

# of fingers	Accuracy (=100 – FRR)	FTE	FAR
10	99.9% (measured)	5%	< 0.01%
10	99.5% (statistical)	0%	< 0.01%

The VIS-BMS uses technology from 2006.

Literature review from UIDAI led to the following observations.

The Indian project is today the biggest on-going biometric project in the world. At the time of **compiling this report, approximately 600 million people were enrolled.** Given the project's size, the information published on the UIDAI website has been consulted. However, it should be noted that UIDAI reports are oriented towards a representative population of challenging cases, e.g. manual workers and rural persons. This is not a representative population for the envisaged EES and RTP systems. Nevertheless, selected figures are included because they provide insight into the security ambitions of this uniquely sized project.

Fingerprint Security:

- Based on the extrapolation of NIST reports, UIDAI has come to the conclusion that using 10-finger comparing against a database of 1 billion, it is possible to achieve a FAR of 1.4% at a FRR of 2%, and a de-duplication accuracy (TAR) greater than 95%.

These terms are recalled for clarity's sake: False Acceptance Rate (FAR) means, as the name implies, false acceptance, or not distinguishing look-alikes, False Rejection Rate (FRR) means making erroneous rejections. The True Acceptance Rate (TAR), is a measure of accuracy, calculated as $TAR = 1 - FNMR$, where FNMR is the false non-match rate. It can be observed that the UIDAI report uses the term FNMR rather than FRR. As a recall when used in verification (1:1) transactions, FNMR and FMR become False Rejection Rate (FRR) and False Acceptance Rate (FAR). When used in identification (1:n) transactions, they become False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR).

- Based on additional research carried out by UIDAI on data captured locally from Indian citizens, it can be expected to achieve a 99% TAR with about 1% FAR, using a four-finger slap sensor.

Facial Image Security:

UIDAI⁹⁰, building on analysis performed by NIST, does not consider facial images to be a sufficiently stand-alone biometric identifier for identification purposes. No opinion is formulated with regard to verification.

> *With regard to timing for enrolment*

The following observations can be made:

- VIS experience: 50 seconds for 10 FPs with sufficiently good quality for subsequent identification (source: Official VIS statistics from DG Home Affairs);
- US experience: 20 seconds (4 slap fingers) to 30 seconds (single finger) for 10 FPs (source: unofficial US DHS statistics).

From Vendor White Papers⁹¹ on EES and RTP, the following data can be added:

- Fingerprints:
 - Capturing 10 NIST Fingerprint Image Quality (NFIQ⁹²) level 1, 2 or 3 quality flat impressions can be done in < 20 sec in supervised self-service kiosks. The figures received from the AFIS vendors indicate that images with NFIQ levels 4 and 5 result in TAR values below 60% which are typically unacceptable to their customers;
 - 1:N identification feasible using 10 plain fingerprints, in 10 seconds database search time for databases the size of the envisaged EES and RTP systems.
- Facial image:
 - Non-ICAO quality⁹³ < 20 seconds (less suitable for automatic comparison);

⁹⁰ "Biometrics Design Standards For UID Applications Version 1.0 (December 2009)", available at <http://uidai.gov.in/resource-center.html>

⁹¹ resulting from the AFIS vendor workshop organised by DG HOME on 30 April 2014

⁹² NFIQ number is a *prediction of a matcher's performance*; it reflects the predictive positive or negative contribution of an individual sample to the overall performance of a fingerprint matching system. NFIQ's5 levels of quality are intended to be predictive of the relative performance of a minutia based fingerprint matching system. NFIQ=1 indicates high quality samples, so lower FMR and/or FNMR is expected.

⁹³ ICAO image quality is specified in 9303 Part 1 Volume 1 Appendix 11 to Section IV.

- ICAO quality < 40 seconds (suitable for automatic comparison).

It should be considered that the size of EES and RTP storage will largely depend on the storage period (i.e. retention period), and that this size will influence the various timings.

From the UIDAI *Proof-of-Concept* reports, the following additional observations can be made:

- Total enrolment time (FI-FP-Iris) = 3 min, of which 10 FPs= 2 min (using a population selection representative of challenging cases – e.g. manual workers and rural persons);
- Typical verification time using 1 or 2 FPs = 200 msec.

> **With regard to operating conditions**

In general, devices such as fingerprint scanners do not operate in minus temperatures. This means that countries located in northern Europe will additionally have to address the challenges posed by freezing temperatures and their impact on FP scanner functionality. Therefore, further consideration should be given to the influence of low temperatures on the duration of border control processes where a FP scanner is used.

– **Biometric characteristics in the EES (TF1)**

◦ **Number of fingerprints to be used (TF1.1)**

The answer to TF question – *how many fingerprints are to be used (separated for enrolment and identification/verification)* – depends in the first place on whether fingerprints will be the sole biometric identifier used in border control processes Use Cases. In TF1.1, the assumption is made that fingerprints will be the sole biometric identifier. In TF1.5, fusion of fingerprints with facial image is addressed.

For all tables included in this chapter, unless indicated otherwise, the values reflect the **professional judgement of DG Home Affairs’ experts combined with information collected from the various vendors**. These figures are based on the following assumptions:

- Unless otherwise stated, the number of records to be compared against is assumed to be 100+ million;
- Unless otherwise stated, the figures refer to a single capture attempt (no repeated capture of fingerprints or facial image as long as minimum quality is reached);
- False Match Rate: FMR in 1: N is assumed to be set at 0.1%, which is best practice in border applications like ABC gates or VIS-BMS;
- Failure To Enrol: FTE rate is assumed to be set to 0%; i.e. for all input data that passes the initial quality checks, biometric templates will be generated and stored.

Obviously, the impact on performance and hardware requirements will vary depending on how many fingerprints are used. In general, having fewer fingerprints enrolled has a negative impact on security and on the probability that an individual will be identified or not. Every additional fingerprint increases accuracy and comparison speed. The latter is counter-intuitive but is due to the multi-stage structure of the matching algorithms. All 10 fingerprints will be used for pre-search filtering, thus reducing the search space. The actual comparison will then typically be performed with fewer fingerprints, e.g. 4 only.

Enrolment

The number of fingerprints for enrolment is driven by the requirements for subsequent verification and/or identification. The more fingerprints are enrolled, the more options are open for subsequent use cases. Furthermore, enrolment for identification has higher quality requirements than for verification.

For selecting the appropriate number of fingerprints for enrolment, the assumption is that the following conditions are sufficiently representative for the purpose of this study: a FAR of 0.1% or better, which is achieved under an appropriate compromise between FTE and FRR. Furthermore, Failure to Enrol (FTE) and Failure to Acquire (FTA) should be minimised. The latter is a question of policy.

With regard to the number of fingerprints, the following alternatives can be chosen:

Table 34 Overview of arguments for/against different numbers of fingerprints (applicable for 100M < database size < 350M)

Number of fingerprints	Arguments in favour	Arguments against
10	<p>Richest information set</p> <p>FRR below 1%</p> <p>Accuracy > 99%</p> <p>Highest number of alternatives remain open for verification and identification transactions</p> <p>Best security performance for identification, verification and Law Enforcement (highest number of latent print checks possible)</p> <p>Fastest (having more fingerprints decreases processing time due to possible pre-filtering)</p>	<p>Timing: most significant increase in border control processing time</p> <p>Usability: both hands required</p> <p>Highest complexity</p> <p>Largest gallery size</p> <p>Most expensive</p> <p>Highest storage/network bandwidth/processing power requirements</p> <p>Vendors indicate there is only marginal improvement in accuracy (1:n) over 8 FPs</p>
8	<p>Enrolment of 8 FPs is faster than enrolment of 10 FPs and yields almost identical accuracy (1:n) > 99%</p> <p>Since 8 fingers are enrolled, many alternatives are open for verification and identification</p>	<p>Timing: only marginally faster than 10 FPs</p> <p>Usability: requires use of both hands during enrolment.</p>
4	<p>Timing: combines an accuracy rate of approximately 98 % or better, with a short enrolment time (4 fingers can be enrolled at once in many border control use cases; obviously, there can be exceptions)</p> <p>Usability: single hand is sufficient (as opposed to both hands)</p> <p>Still significant redundancy in the case of problems with recognition of a finger</p>	<p>Less rich information, reduced number of alternatives that remain open for verification and identification compared to 8 and 10 FPs</p> <p>LEA possibilities significantly reduced since fingerprints for 'other hand' are missing</p>

Number of fingerprints	Arguments in favour	Arguments against
2	<p>Timing: since the number of FPs is reduced, enrolment speed is relatively high</p> <p>Usability: convenience for traveller at time of enrolment is relatively high</p> <p>Low storage/network bandwidth/processing power requirements</p> <p>Still minimal redundancy in the case of problems with a specific finger</p>	<p>Slower for identification than when using more FPs (having fewer fingerprints increases processing time due to lack of possible pre-filtering)</p> <p>Even smaller set of alternatives available for verification and identification</p> <p>LEA possibilities drastically reduced since fingerprints for 'other hand' are missing</p>
1	<p>Timing: since the number of FPs is reduced to a single finger, enrolment speed is high</p> <p>Usability: convenience for traveller at time of enrolment is high</p> <p>Lowest storage/network bandwidth/processing power requirements</p> <p>Lowest complexity</p> <p>Smallest gallery size</p> <p>Least expensive</p>	<p>Only one finger available for verification and identification. This decreases redundancy in the case of problems with that specific finger.</p> <p>Experience of AFIS vendors has shown that use of a single finger leads to a relatively high FRR, which is annoying for travellers.</p> <p>Least favourable for LEA and identification transactions</p> <p>Slowest for identification (having fewer fingerprints increases processing time due to lack of possible pre-filtering)</p>

Identification

The preceding table introduced the various possibilities for selecting the number of fingerprints for enrolment. This information is further complemented by the table below, which provides an approximation of the possible number of fingers enrolled versus False Rejection Rate.

Table 35 False Rejection Rate against the number of FPs enrolled

# FPs	FRR fingers only (false non match)
1	8%
2	2,7%
4	2.2%
8	0.8%
10	0.7%

The colour green indicates a favourable characteristic, while orange and red indicate increasingly less favourable characteristics.

Detailed quantitative security performance information is available from the VIS/BMS experience. For security reasons, this information can be discussed only in closed membership meetings. In general, the security performance of VIS meets expectations.

Verification

Verification can be performed using 1 finger alone, but having more fingers increases performance and decreases processing time.

Vendor information indicated that matching accuracy also depends on the fingerprint image quality. This is equally confirmed in the public domain report NISTIR 7112. This report is based on the NIST Algorithmic Test Bed, which is a version of the FBI IAFIS. From those sources it can be observed that the poorest image quality results in a TAR of approximately 50%. Using the highest quality images results in a TAR above 99%.

As for verification, the security performance for identification by EES should be similar to that of the VIS-BMS. Detailed quantitative security performance information is available from the VIS-BMS experience. However, as this information is not publicly available, it can be discussed in closed membership meetings. In general, the security performance of VIS meets expectations.

Main Findings of the number of fingerprints to be used (TF1.1)

In TF1.1 the assumption is made that FP will be the sole biometric identifier. In general, having more fingerprints enrolled has a positive impact on security and on the probability that an individual will be identified. All 10 fingerprints can be used for pre-search filtering, thus reducing the search space. The actual comparison will then typically be performed with fewer fingerprints, e.g. 4 only.

The more fingerprints are enrolled, the more options are open for subsequent use cases. I.e. with 8 fingers enrolled, many alternatives are open for verification and identification, but with 4 fingers there is still significant redundancy in the case of problems with recognition of a finger.

In terms of verification, 1 finger alone can be used, but having more fingers increases performance and decreases processing time. The matching accuracy also depends on the fingerprint image quality (poorest image quality: TAR≈ 50%, highest image quality: TAR≥ 99%). Finally, the security performance for identification by EES should at least be similar to that of the VIS-BMS, since the one of VIS meets expectations.

With reference to TOMs A, B and C:

N° of fingerprints	TOM A	TOM B	TOM C
1 st entry	0	4 (VE)	8 (VE)
Entry/Exit (search & verification)	VH: 1, 2 or 4 live FP, against VIS (as of today)	VE: 1, 2 or 4 live FP, against EES VH: 1, 2 or 4 live FP, against VIS	

- ***EES and RTP biometric options capturing fingerprints (TF1.2)***

How and when to capture fingerprints for EES and RTP (incl. preferably anti-spoofing measures) is discussed below. Special attention is given to hand-held equipment.

Enrolment

Enrolment for EES and RTP is different. The technology allows the capturing of rolled and/or flat fingerprints. While rolled images contain twice as much information as flat ones, they are primarily intended to be used in an LEA context, since they offer the most possibilities for comparing latent prints. However, to capture a rolled image, an operator must guide the individual rolling of each finger, which is time consuming. As comparing latent prints is not a primary objective of the EES system, rolled fingerprints are less appropriate there. For RTP, LEA access is out of scope as per legal proposal.

Comparing latent prints can also be done against flat fingerprints. Consideration should then be given to the fact that enrolling 4 or fewer fingerprints makes this comparison process much less conclusive. If a latent print can only be compared against 4 or fewer fingerprints (implicitly assumed to come from the same hand), the chances for a match immediately drop an additional 50% since the latent print and the enrolled print in this case can come from different hands.

TCNVEs

In the case of TCNVEs, live fingerprints should be captured upon first entry in EES. A flat image, using a slap capture device can be used. Such devices can typically capture up to four flat (plain) fingers in a single scan. Using such a flat slab capturing device, fingers can be captured in a 4-4-2 mode, or a 4-1-4-1 mode. The latter is more convenient since it allows the enrollee to have one hand available all of the time (but inherently leads to longer acquisition times).

The capturing should preferably be done in a controlled environment where sufficient attention can be given to the quality of the captured data as well as liveness detection. For such liveness detection, **reliable techniques should be applied (more details are provided below in the 'anti-spoofing' section).**

TCNVHs

Under the assumption that RTP would have access to VIS, in the case of TCNVHs, fingerprints need not be captured but the fingerprints present in VIS-BMS could be used. This is obviously subject to legal evaluation.

Verification

For both TCNVEs and TCNVHs, live fingerprints should be captured at the moment of verification.

Increasing the number of fingerprints checked increases the reliability of the verification. For the purposes of verification, Table 34 in TF1.1 lists the arguments for and against the use of different numbers of fingerprints for verification. Table 35 in TF1.1 illustrates how FRR improves with an increasing number of fingerprints used. FAR and FRR rates can be represented on Detection Error Trade-off (DET) curves.

For security reasons, quantitative security performance information such as FAR/FRR and DET is available from the VIS/BMS experience. This information can be discussed in closed membership meetings. In general, the security performance of VIS meets expectations.

Identification

For both TCNVE and TCNVH, fingerprints should be captured at the moment of identification. For the purpose of identification, as many fingerprints as possible should be captured, because this increases both security and speed. For TCNVH, identification could be done against the VIS. For TCNVE, it could be done against the EES.

As stated above for verification, for security reasons, quantitative security performance information on identification is available from the VIS-BMS experience. However, as this information is not publicly available, it can be discussed in closed membership meetings. In general, the security performance of VIS meets expectations.

Anti-spoofing

Fingerprints may be spoofed in latex or similar material. Liveness detection can mitigate this in controlled circumstances. Spoofing should be mitigated by dedicated checks that are specific to the selected capturing devices.

State-of-the-art anti-spoofing features include a comparison of the captured sample with regard to regular human skin features. Such comparison addresses spectroscopic and optical features with regard to specific parameters of the human tissue and its circulatory features. This prevents applications from attacks with fake fingers and from being spoofed by cut-off fingers.

The capturing devices to be selected should preferably both be FBI certified and demonstrate their effectiveness through public domain channels such as the International Fingerprint Liveness Detection Competition (LivDet).

The necessity of Presentation Attack Detection⁹⁴ applies to all events where a biometric modality is processed, and particularly in unsupervised conditions. Devices should undergo a dedicated security certification (e.g. ISO 15408 Common Criteria). Applicable Protection Profiles are available, e.g. from the BSI.

Finally, such anti-spoofing checks and related best practices should preferably be shared among the Member States. Furthermore, attention should be paid to operating capturing devices under adequate supervision.

Hand-held equipment

There are limitations to the quality of finger images obtained on hand-held devices, as well as to the number of images obtainable in a reasonable turn-around time.

Device characteristics cover the number of fingers that can be scanned at the same time, scan resolution, pixel depth and dynamic range. Handheld capturing devices are typically limited to capturing a single finger, and they achieve lower image quality.

Capturing multiple fingerprint images on handheld capturing devices requires that each single finger, or a maximum of two fingers at a time, be placed on the scanner platen and this process repeated until all required fingers are enrolled. There is currently no reliable statistical information on the capture times and fingerprint quality on such devices in large-scale operational conditions.

⁹⁴ As described in the current ISO/IEC 30107 draft

High-quality flat images of 10 fingers are generally taken on a reader that is fixed on a stable counter. Taking such flat images of 10 fingers requires operational conditions as commonly found in airports, where slap readers can be installed on counters and supervised during operation.

Self-service kiosks

While self-service kiosks could probably provide a means to reduce waiting times and queues at border-control by letting passengers enrol their fingerprints in a non- or semi-supervised mode, there are negative quality and security implications to be expected.

The AFIS industry warns about a likely reduction in fingerprint image quality which would have direct adverse effects on accuracy and result in other performance issues. The possible attainable fingerprint quality and the necessary quality control means should be further investigated.

In addition, there could be a real issue when persons enrol their fingerprints or facial image for somebody else or when persons enrol fake fingerprints due to the non-supervision of the kiosk. The required supervision process should be evaluated during the pilot.

Main findings of the EES and RTP biometric options for capturing fingerprints (TF1.2)

Enrolment for EES and RTP can be different, possible integration depending on many different factors, also including the legal aspects and data protection.

As comparing latent prints is not a primary objective of the EES system, plain fingerprints are to be used, and rolled fingerprints are less appropriate there. For RTP, LEA access is out of scope as per legal proposal.

Comparing latent prints can be done on flat fingerprints. For both *TCNVEs* and *TCNVHs*, live fingerprints should be captured at the moment of verification and identification. For *TCNVEs* fingers can be captured in a 4-4-2 mode, or a 4-1-4-1 mode, the latter is more convenient and identification can be done against EES. Attention should be given to the quality of the captured data as well as liveness detection. For *TCNVHs* fingerprints do not need to be captured; the fingerprints present in VIS-BMS could be used, also for identification. The former is subject to legal evaluation.

Fingerprints may be spoofed in latex or similar material. Liveness detection can mitigate this in controlled circumstances. For anti-spoofing reasons, the capturing devices should satisfy security standards (i.e. FBI and International Fingerprint Liveness Detection Competition (LivDet)) and undergo a dedicated security certification (e.g. ISO 15408 Common Criteria). Ideally, anti-spoofing checks and related best practices should be shared among the Member States.

Regarding hand-held equipment, there are limitations to the quality as well as the number of captured images in a reasonable time (bearing in mind the currently installed readers for VIS at the BCPs are typically low quality/1 finger devices, since they are oriented towards verification only). There is currently no reliable statistical information on the capture times and fingerprint quality on such devices in large-scale operational conditions. High-quality flat images of 10 fingers are typically taken on a reader that is fixed on a stable counter (as in airports).

Finally for self-service kiosks, the supervision process should be evaluated during the pilot as despite the probability to reduce waiting times and queues, negative quality and security implications are expected.

- ***Synergies with other systems (VIS, RTP) (TF1.3)***

The section below addresses Thematic File 1.3 question: synergies with other systems recording biometrics VIS and RTP including for example the rationale for storage of the facial picture in EES (for VH and VE).

Verifying a TCN's identity is a pre-requisite before evaluating his/her eligibility to cross the external border. From an overall cost/benefit perspective, it can be expected that synergies with VIS and RTP may yield benefits. Also, from a technical biometric perspective, it is assumed that TCNVH biometric characteristics will remain in VIS.

It can be argued that to increase convenience for the traveller, biometric characteristics should be captured only once. Technically speaking, for TCNVHs it would be beneficial to continue relying on the fingerprints stored in VIS, since this would avoid live re-capturing. For facial images the situation is different, as the quality of facial images stored in the VIS varies greatly and cannot always be relied upon. As a consequence, for e-MRTD TCNVH holders it should be envisaged to read the facial image from the e-passport (should facial image be not available, a high resolution picture is taken) and to store it in the EES database and then to proceed with a comparison of the picture against a live picture as per the process description. Whether this database is shared or separated for VIS, EES and RTP is addressed in the architectural part of the study.

For TCNVEs, biometric data will be entered in EES and stored in the appropriate biometric store.

With regard to seeking synergies, a distinction should be made between the different functions of Front Office (Border Control Points where capturing takes place) and Back Office (temporary data storage and comparison). From a biometric perspective, these activities are completely different and can be decoupled. Different options can be envisaged depending on the different requirements of EES and RTP. From a biometric perspective, it makes sense to have dedicated Front Office functionality (EES and RTP have different business requirements) and shared Back Office functionality (the development and operation of an effective matching engine is complicated and expensive, as a consequence sharing makes more sense).

Options with regard to distributing the Front and Back Office functionality for VIS, EES and RTP are addressed in the architectural part of the study.

Main findings of synergies with other Systems (VIS, RTP) (TF1.3)

It is commonly agreed that biometric characteristics should be captured only once in order to increase convenience for the traveller. For TCNVHs it would be beneficial to continue relying on the fingerprints stored in VIS. For e-MRTD TCNVH holders, since the quality of facial images stored in VIS varies greatly, the facial image could be read from the e-passport, be stored in the EES database and then be compared with the live picture. For TCNVEs, biometric data will be entered in EES and stored in the appropriate biometric store.

Regarding seeking synergies, it should be clear that from a biometric perspective, these Front Office (Border Control Points where capturing takes place) and Back Office (temporary data storage and comparison) functions are completely different and can be decoupled. However it makes sense to have separate dedicated FO functionalities for EES and RTP, but a shared BO functionality.

◦ **Impact of the use of the biometric identifier on the border control process as well as on enrolment time (incl. degraded mode⁹⁵) (TF1.4)**

Border control process

The impact due to the interactions with biometric technology in the border control processes is documented in chapter 3. In order not to negatively impact processes, it is recommended that, using live captured fingerprints, system parameters ensure that:

- Verification transactions should be completed within 3 seconds;
- Identification transactions should be completed within 10 seconds.

With regard to the degraded mode, if EES and/or RTP is not available, the border control procedures should resort to manual verification.

Enrolment time

Specific information with regard to the impact of biometric systems on enrolment is presented below.

From DG Home Affairs’ VIS/BMS experience as well as from vendor input and informal DHS statistics, below are the typical capture times using current technology.

Fingerprints

Table 36 *Fingerprint capturing time*

Single finger versus 4-finger scanner	1 finger	10 fingers
Single finger scanner	Approximately 3 seconds	Approximately 30 seconds
4-finger scanner platen	Approximately 3 seconds	Approximately 20 seconds (4-4-2 or 4-1-4-1)

Facial image

Table 37 *Facial Image capturing time*

ICAO compliance	1 face
ICAO compliant facial image	Approximately 40 seconds
Non-ICAO complaint facial image	Approximately 20 seconds

From the UIDAI literature study, the following observations on enrolment times were made for different age classes. As explained in the UIDAI ‘Proof-of-Concept’ document [POC2011], these

⁹⁵ Degraded mode refers to a situation when the EES and RTP would not be available or where there would be an exceptional situation as defined in the Schengen Borders Code (see article 8- Relaxation of Border Controls in Regulation (EU) No. 562/2006).

enrolment times were derived in a monitored environment, using a structured enrolment process and trained operators.

However, the population was selected on purpose to represent challenging cases such as rural workers and manual labourers. The latter does not apply to the expected users of the EES and RTP systems.

Table 38 'Enrolment times for face and 10 fingerprints by age'⁹⁶

Age	Under 20	20 to 30	30 to 40	40 to 50	50 to 60	60 to 70	70 to 80	Above 80
Face	0:00:31	0:00:31	0:00:33	0:00:35	0:00:37	0:00:38	0:00:40	0:00:45
10 FP	0:01:45	0:01:52	0:01:43	0:01:45	0:01:53	0:01:56	0:02:08	0:02:14

Furthermore, measuring the impact of biometric technology on enrolment assumes that the correct operational conditions are present for the technology selected.

The following items are particularly relevant:

- For face: camera controlled by enroller, controlled lighting environment, control of pose, accessories, and preferably after capture, performance of a quality check. It is noted that capturing good quality facial images requires tightly controlled conditions. It should also be made clear that typical border control booth situations do not provide such conditions and cannot easily be adapted. It can be concluded that, for a good quality facial enrolment solution, dedicated equipment is necessary;
- For fingerprints: either multi-print flat (i.e. 'plain' or 'slap') reader or mobile reader handling 1 print. The number of fingers selected defines the time required. The presence of a trained operator is recommended. After the capture, a NIST Fingerprint Image Quality (NFIQ) check should preferably be performed. Also, temperature and humidity should be controlled.
-

Main findings of impact of the use of the biometric identifier on the border control process as well as on enrolment time (incl. degraded mode) (TF1.4)

In order not to negatively impact processes, it is recommended that, using live captured fingerprints, system parameters ensure that:

- Verification transactions should be completed within 3 seconds;
- Identification transactions should be completed within 10 seconds.

With regard to the degraded mode, if EES and/or RTP is not available, the border control procedures should resort to manual verification.

Specific estimates with regard to the impact of biometric systems on enrolment (Fingerprint capturing time, Facial Image capturing time, Enrolment times (FP+FI) for different age groups) is presented. It is also suggested that it should be taken into consideration that quality of FI is highly dependent to capturing conditions (usually not present at typical border control booths) and for FP, temperature and humidity should be controlled, a trained operator should be present and an image quality check of the capture should be performed immediately.

⁹⁶ Source: [POC2011 Annexure 2 p.29]

With reference to TOMs A, B and C:

Expected time (duration in sec)	TOM A	TOM B	TOM C
1st entry	5	45-65	65-95
Entry/Exit (search & verification)	15-20	35-50	

- **Use of facial recognition in combination with the use of fingerprints (TF1.5)**

Fusing facial imaging and fingerprints is beneficial both for verification and identification. The table below provides an approximation of possible improvement in False Rejection Rates when fingerprints (ranging from 1 to 10) are fused with a facial image for verification.

Table 39 False Rejection Rates using fingerprints only vs. fingerprints and facial image

# FPs	FRR fingers only (false non-match rate)	FRR fingers fused with facial image
1	8%	3%
2	2.7%	1%
4	2.2%	0.6%
8	0.8%	0.3%
10	0.7%	0.25%

As illustrated by the table above, facial recognition in combination with the use of fingerprints is a viable option for reducing the number of fingerprints to be captured.

However, the following considerations should be kept in mind when using multi-modal biometrics:

- The system should support fingerprints and facial image to reduce the FTE and FTA (allowing enrolment/acquisition of travellers that are challenged e.g. by lack of fingers);
- Given that fingerprints are the most proven and mature technology, the use of facial images in combination with it should aim at increasing processing speed and using less fingerprints. It should not lead to situations where a FI match and a FP match-failure would lead to automatic classification of a "successful" match.

Furthermore, both the UIDAI reports and the US NIST 'Study of Biometric Fusion' [NISTFUSION] support the conclusion that combining fingerprints with facial images can lead to significant FRR improvements.

Finally, it can be observed there are at least the following options for obtaining the facial image in the event that fusion with fingerprints would be desirable:

- Live capture (which requires appropriate conditions, e.g. specified in the ICAO 9303 standards, and appropriate image quality, e.g. specified in the NIST standards);
 Capture from the chip (in which case at least Passive Authentication (PA) should be applied);
 (as a reminder, all TCNVE currently carry e-MRTDs).

Main findings of use of facial recognition in combination with the use of fingerprints (TF1.5)

Use of combination of FI and FP is judged beneficial for both verification and identification, leading to FRR to lower. Introduction of a combined solution can lead to a reduction of the number of FP needed. Considerations should be kept in mind when using multi-modal biometrics: the aim is to reduce the FTE and FTA and that fingerprints are the most proven and mature technology and facial images are introduced to increase the enrolment, processing speed and traveller's convenience.

With reference to TOMs A, B and C:

Combinations of FI and No of FP	TOM A	TOM B	TOM C
1st entry	e-MRTD: retrieve photo or use live photo MRTD: use scanned photo No FP	e-MRTD (retrieve photo or use live photo) MRTD: use scanned photo 4 FPs (VE)	e-MRTD (retrieve photo or use live photo) MRTD: use scanned photo 8 FPs (VE)
Entry/Exit (search & verification)	Use photo VH: 1, 2 or 4 live FP, against VIS (as of today)	Use photo OR VE: 1, 2 or 4 live FP, against EES VH: 1, 2 or 4 live FP, against VIS	

◦ ***Facial image/fingerprints possibly captured from the travel document (TF1.6)***

Technically speaking, the relationship between fingerprints and electronic passports is characterized by the following observations:

- Electronic passports contain maximum 2 fingerprints;
- Access to fingerprints requires the EAC keys. Such keys need to be obtained through bilateral exchange;
- Relying on the contents of the fingerprints provided by the chip requires successful use of PA.

The relationship between facial images and electronic passports is characterized by the following observations:

- Electronic passports contain the facial image of the document owner;
- Reading this facial image can be done using BAC, which is always available;
- Relying on the contents of the facial image provided by the chip requires successful use of PA.
-

In short, it can be said that:

- Capturing facial images from passports is relatively simple. Either there is no access control, or only Basic Access Control (BAC) is present. Furthermore, it should be remembered that Passive Authentication (PA) is mandatory according to ICAO Doc 9303. PA offers protection of integrity and authenticity of the data stored in the chip. It requires validating the certificate chain of Document Signer and Country Signing CA;
- Capturing fingerprints from passports is difficult/may be impossible in certain cases, as access is currently limited to the issuing Country/Member State through EAC keys, which are in practice hardly exchanged.

It has to be noted that, currently, a trust assessment for non-EU passports is not always possible. For instance, Germany, one of the leading countries in the trust assessment, is able to validate the trust chain of only 59 countries (June 2014). Additional measures have to be put in place to make the use of the passport's facial biometric data trustworthy. Such additional measures should be based on the specific cryptographic protection implemented by the issuer, or should provide assurance on the integrity of the binding between the physical document and the chip from where the facial image would be read, or should be a combination of both these measures.

With regard to the exchange of certificates required for cryptographic processing (PA as well as other techniques), the creation and operation of a shared certificate masterlist at European or Schengen level should be considered. An entity could be given the responsibility for obtaining and sharing the certificates currently obtained through individual bilateral exchanges between the Member States and Third Countries, and between Member States. For masterlists, the ICAO PKD arrangements apply.

Main findings of facial image/fingerprints possibly captured from the travel document (TF1.6)

The relationship between fingerprints and electronic passports and facial images and electronic passports are presented. In short, capturing facial images from passports is relatively simple, while capturing fingerprints from passports is difficult and may be impossible in certain cases. It has to be noted that, currently, a cryptographic trust assessment for non-EU passports is not always possible and additional measures have to be put in place to make the use of the passport's facial biometric data trustworthy. With regard to the exchange of certificates required for cryptographic processing, the creation and operation of a shared certificate masterlist at European or Schengen level could be considered.

– **Biometric characteristics in RTP (TF2)**

◦ **Biometric identifier(s) to be used for RTP (TF2.1)**

The biometric identifiers to be used for RTP depend in the first place on the relationship between EES, RTP and VIS, as well as on the RTP enrolment process and on the biometric characteristics selected for EES.

Multiple options can be identified as in the table below. Options for EES include no biometric characteristics at all, fingerprints only, but ranging from 1 to 10, facial image only, and the combination of facial image and a fingerprint range. The leftmost column indicates the 'base', the options for EES. The 3 columns labelled 'Corresponding RTP option for biometric' are defined in relation to what has been selected in the base column.

Table 40 TF 2.1.1 EES and RTP biometric options

EES option for biometric characteristics:	Corresponding RTP option for biometric characteristics		
Fingerprints and/or Facial Image			
No biometric used	Selection of FPs only	FI only	Selection of FPs combined with FI
10 FPs (no FI)	Same as EES	Subset of 10 FPs	Zero (no fingerprints used in RTP)
8 FPs (no FI)	Same as EES	Subset of 8 FPs	Zero
4 FPs (no FI)	Same as EES	Subset of 4 FPs	Zero
2 FPs (no FI)	Same as EES	Subset of 2 FPs (i.e. 1)	Zero
1 FP (no FI)	Same as EES	n/a	Zero
Facial Image (no FPs)	Same as EES	n/a	Zero (no face used in RTP)
Facial Image + Selected Fingerprints	Same as EES (FI + FPs)	Subset of FPs	Zero

Fingerprints, facial image or combination

Where the options involving fingerprints, facial image or their combination are used for RTP, the selected security performance should match the role the RTP biometrics (enrolment, verification, and identification) takes on in the border control processes. In the context of the currently envisaged RTP functionality, the main purpose of RTP will be to facilitate the travel experience of regular travellers.

RTP does not address functionality with regard to eligibility-status check or entry-exit checking and recording. As a consequence:

- The main biometric services that can be called upon are for verification purposes;
- Identification checks are not the primary focus of RTP.

The limited usability and necessity of identification checks against the RTP leads to a possible reduction in the number of fingerprints and an increased possibility of using facial image (only).

Given the relatively low number of RTP travellers, the identification supporting the prevention of RTP shopping would apply only to a limited set of stored fingerprints. **Where EES would be using fingerprints, RTP could either use the same fingerprints, a subset, or none at all ('zero').**

Using the same or a subset of biometric characteristics for EES and RTP would make sense for the following reasons:

- Only one biometric capture for RTP and EES (in which case the same biometric characteristics would be used and copied or entered once if the system were to be a combined EES-RTP system); however from a data protection point of view such a possibility could be considered only if RTP and EES would not be conceived as individual and independent systems but rather as complementary modules part of an integrated border management system. In this case, biometric characteristics would be captured once (for the purpose set by the integrated border management system) and used where considered appropriate during the different phases of the border management process;
- The majority of RTP members will end up with an individual file in EES, since the majority of TCNs (VEs & VHs) are subject to the Schengen short-stay rules;
- The mandatory biometric capture for EES could precede the application for RTP status leading to the EES biometric data being used for both EES and RTP.

If a subset were to be used, the selection of a specific subset could be based on the security performance requirements for RTP.

Using no biometrics for RTP could be envisaged since the border control process include checks that comprise at least verification, and if the identity claimed matched the identity stored with RTP status.

Where EES would be using a combination of fingerprints and facial image, RTP could make use of the same or a subset of the fingerprints, combined with the facial image.

Furthermore:

- For TCNVHs, it is assumed that the verification against the fingerprints stored in VIS as per border check process applicable as from 11 October 2014 fulfils the RTP objectives; and
- For TCNVEs, the biometric characteristics will need to be captured at enrolment time or as an alternative option, previously captured biometric data for the EES individual file could be re-used. The latter would imply that a person would need to have entered Schengen previously and be registered in the EES.

ABC gates

With regard to ABC gates, it can be observed that today most of them handle facial image recognition (exceptions for France and Spain) and no other biometric identifiers. The inclusion of the facial image in the RTP could enable a uniform verification process at ABC gates, for both TCNs and EU Citizens. Such gates would still need to be equipped with fingerprint readers as well to check TCNVHs against the VIS at least for entry gates. In any event, the addition of fingerprints to ABC gates is considered to be feasible by all Member States.

Furthermore, it can also be observed that at least entry gates may use only the facial image plus the travel document number for MEV-holders that have RTP status.

Main findings of the biometric identifier(s) to be used for RTP (TF2.1)

The biometric identifiers to be used for RTP depend in the first place on the relationship between EES, RTP and VIS, as well as on the RTP enrolment process and on the biometric characteristics selected for EES. Since the main purpose of RTP will be to facilitate the travel experience of regular travellers, it does not address functionality with regard to eligibility-status check or entry-exit checking and recording but serves verification purposes.

The limited usability and necessity of identification checks against the RTP and the low number of RTP travellers, leads to a possible reduction in the number of fingerprints and an increased possibility of using facial image (only).

Using the same or a subset of biometric characteristics for EES and RTP would make sense for the several reasons, including the existence of only one biometric capture for RTP and EES, even though from a data protection point of view such a possibility could be considered only if RTP and EES would not be conceived as individual and independent systems but rather as complementary modules part of an integrated border management system; the majority of RTP members will end up with an individual file in EES; the mandatory biometric capture for EES could precede the application for RTP status.

If a subset were to be used, the selection of a specific subset could be based on the security performance requirements for RTP. However, using no biometrics for RTP could be also envisaged since the border control process include checks that comprise at least verification, and if the identity claimed matched the identity stored with RTP status.

Regarding ABC gates, most of them today handle facial image recognition and no other biometric identifiers. The inclusion of the facial image in the RTP could enable a uniform verification process at ABC gates, for both TCNs and EU Citizens. gates. In any event, the addition of fingerprints to ABC gates is considered to be feasible by all Member States.

With reference to TOMs M and N:

Type of Biometric	TOM M	TOM N
1st entry	(VE) 4 FPs	No FPs - FPs retrieved from EES No photo – Photo retrieved from EES
Entry/Exit (search & verification)	Retrieve e-MRTD: photo or use live photo VE: 1, 2 or 4 live FP, against RTP VH: VIS check is trusted	Retrieve e-MRTD: photo or use live photo VE: 1, 2 or 4 live FP, against EES VH: VIS check is trusted

- ***Impact of the use of biometric identifier(s) on the border control process (TF2.2)***

The impact due to the interactions with biometric technology in the different use cases of the border control process is documented in Chapter 3.

The same remark on ABC gates as in the answer to TF2.1 applies here as well.

As this section is short, no summary is provided.

- ***How and when to capture them? (TF2.3)***

Assuming the border control process requires an identical level of security performance for biometric verification of a TCN regardless of whether he/she has RTP status, the answers provided under TF1 apply. Appropriate options will need to be selected. Please refer to the tables in the preceding sections, that describe the options for enrolment using 1-10 fingers, and the possibilities for FRR.

The assumption can be made that no hand-held equipment will be used during the RTP application process.

The use of hand-held equipment at Border Control for manual verification of RTP members follows the exact same logic as verifications against EES with regard to how and when to capture them.

As this section is short, no summary is provided.

- ***Synergies with other systems recording biometrics, Visa information System (VIS) and EES (TF2.4)***

As introduced in TF 2.1, using the same or a subset of biometric characteristics for EES and RTP would make sense for the following reasons:

- Only one biometric capture for RTP and EES (in which case the same biometric characteristic would be re-used and copied twice or entered once if the system were to be a combined EES-RTP system);
- The majority of RTP members will end up with a personal file in EES⁹⁷, since the majority of TCNs (VEs & VHs) are subject to the Schengen short-stay rules;
- The mandatory biometric capture for EES could precede the application for RTP status leading to the EES biometric data being used for both EES and RTP.

Performing the verification of a TCN's identity is a pre-requisite before checking his/her RTP status (see Figure 13 in the RTP 3.3.4. *Process description at entry and exit*). From an overall cost/benefit perspective, it can be expected that synergies with VIS and EES may yield benefits as the EES does not amend the already applicable VIS based fingerprint verifications. Also, from a technical biometric perspective, it is assumed that TCNVH biometric characteristics will remain in VIS.

⁹⁷ unless already existing because of previous travels, which is likely for TCNVH

To increase convenience for the traveller, biometric characteristics should be captured only once. Technically speaking, for TCNVHs it would be beneficial to rely on the fingerprints stored in VIS, since this would avoid live re-capturing and data duplication.

For facial images, the situation is different, as the quality of facial images stored today in the VIS varies greatly and cannot yet always be relied upon. As a consequence, it should be envisaged to read the facial image from the e-passport and store it in the database. Whether this database is shared or separated for VIS/EES/RTP is addressed in the architectural part of the study.

As envisaged in the previous sections, in order to further increase convenience for the VH RTP traveller, an option could be to perform a facial image comparison at the ABC-gate, against the e-MRTD, against the VIS or even both. In this particular case, the facial image recognition could supersede the VIS fingerprint verification, making the latter unnecessary at border crossing points that implement FI recognition.

During a manual border-control process, the fingerprint verification would most probably work better than facial image recognition. The reason for this is the inherent better FAR and FRR, as well as the better capacity to tackle look-alikes with FP.

For TCNVEs requesting RTP status, biometric characteristics will be entered in the central database and stored in the appropriate biometric store.

Main findings of synergies with other systems recording biometrics, Visa information System (VIS) and EES (TF2.4)

From an overall cost/benefit perspective, it can be expected that synergies with VIS and EES may yield benefits as the EES does not amend the already applicable VIS based fingerprint verifications.

- ***Impact of the use of biometric identifiers on the border control process including the degraded mode (TF2.5)***

The impact due to the interactions with biometric technology in the border control processes is documented in the border control processes chapter.

If RTP were to require biometric enrolment, please refer to the impact of biometric enrolment in TF1.4.

With regard to the degraded mode, if the RTP system were not available, the border control process should resort to manual verification of the live person against what is visually available from the travel document. Also, the traveller would have to be reassigned to the regular process flow, as there would probably be no possibility to check the RTP status.

As this section is short, no summary is provided.

– **Transition period (TF3)**

This TF is aimed at analysing the consequences of not using biometric characteristics from the start. This can be done either by having a transition period or a phased approach.

A transition period is a period during which no biometric data would be used in the EES thus relying only on the alphanumeric data of the travel documents. The use of biometric characteristics would be introduced after the transition period.

A phased approach consists in creating the possibility of including biometric characteristics in EES from the start by Member States that are ready and letting the other Member States join in progressively, so as to reach full implementation by a target date.

◦ **Broad analysis of possible options**

The existing legal proposal for the EES contains a clause stating that biometric characteristics must be used after a transitional period of 3 years. Fingerprints could be used, if the proposal was amended in that sense, before this period, but the Member States would then need to decide whether to use them for registration and at checks. The definition of biometric characteristics is limited to fingerprints in the legal proposal.

TF 3 of the technical specifications for this study has requested an analysis of the impact and alternatives in relation to having a transitional period. The options presented here are developed in response to this request, focusing on the consequences with regard to the border crossing processes.

The options presented also include photographs as biometric identifiers; in certain cases such photographs could be used as the sole identifier and in other cases they could be used in combination with fingerprints.

In the table below, four options for implementing biometric characteristics are presented. The discriminating factor between the options is the time at which biometric characteristics become mandatory – Entry Into Operation (EIO), and which biometric characteristics should be used.

Table 41 Four options for implementing biometric characteristics (the order of the options is not significant for the analysis)

Options	Biometric characteristics		Graphical representation
	Photo	Fingerprints	
<p>Option A</p> <p>FI only, no fingerprints ever</p>	EIO	Never	
<p>Option B</p> <p>Biometric characteristics can be registered and used for verification but this usage is only mandatory 3 years after entry into operation.</p>	EIO+ 3y	EIO + 3y	

Options	Biometric characteristics	Graphical representation
<p>Option C</p> <p>Only photos are registered in the EES and used for verification directly from the start. Fingerprints are optional at first.</p>	EIO EIO + 3y	
<p>Option D</p> <p>Biometric characteristics must be registered and used in verification as of entry into operation.</p>	EIO EIO	

For a TCNVH traveller, fingerprints and a photo are already registered in the VIS. Fingerprints must be used for verification in the VIS system as of October 2014. The difference for TCNVHs, in the options described, relates to the possible use of photos for verification (i.e. facial recognition using the centrally stored photo).

> *Option A*

The table below summarises the main characteristics of this option.

Table 42 *Option A – facial image only, no fingerprints ever*

General	
<ul style="list-style-type: none"> Registration in EES through use of MRZ plus facial image on entry-exit; Biometric identification capabilities are limited since facial image only has a limited TAR. 	
Advantages	Disadvantages
<ul style="list-style-type: none"> Simplicity. 	<ul style="list-style-type: none"> Limited capability to identify (fraudulently) undocumented persons - using the EES and 1:N comparing of facial images.
<ul style="list-style-type: none"> Can be assumed to be the least costly option. 	<ul style="list-style-type: none"> Limited LEA value - 1:1 or 1:N searches of fingerprints cannot be used.

> *Option B*

The table below summarises the main characteristics of the transitional period.

Table 43 *Option B – photo and fingerprints: EIO+3y*

General	
<ul style="list-style-type: none"> Registration in EES through use of MRZ plus additional data beyond MRZ on entry-exit; No reliable verification can be made using biometric characteristics during the first three years. 	
Advantages	Disadvantages

- Gives Member States more time to implement necessary processes and equipment for biometric registration and checks.
- No reliable verification can be made using biometric characteristics during the first three years.
- No time advantage for pre-border kiosks – limited accelerator during the transition period.
- Impossible to identify undocumented persons - using the EES and 1:N comparing of fingerprints or photo would not be possible.
- Limited LEA value - 1:1 or 1:N searches of fingerprints cannot be used.

> *Option C*

The table below summarises the main characteristics of the transitional period.

Table 44 *Option C – photo: EIO; fingerprints: EIO+3y*

General	
<ul style="list-style-type: none"> • Registration in EES through use of MRZ plus additional data on entry-exit with the addition of a photo; • Photo can be used for facial recognition to verify the person’s identity; • No fingerprints are mandatory to enrol until 3 years after EIO. 	
Advantages	Disadvantages
<ul style="list-style-type: none"> • Gives Member States more time to implement necessary processes and equipment for fingerprint registration. 	<ul style="list-style-type: none"> • A TCNVE person (found in the EES) cannot be verified using fingerprint checks with the central system.
<ul style="list-style-type: none"> • A TCNVE person (found in the EES) can be systematically verified by using facial recognition in relation to the central system. 	<ul style="list-style-type: none"> • Impossible (or at least increased difficulty) to identify (fraudulently) undocumented people - using the EES and 1:N comparing of fingerprints would not be possible
Advantages	Disadvantages
<ul style="list-style-type: none"> • If the photo can be captured in the pre-border kiosk, this could have a positive impact on border crossing times and photo quality. 	<ul style="list-style-type: none"> • Measures to cope with the co-existence of records with and without biometric characteristics must be taken into account (e.g. invalidating records, mandatory addition of biometric characteristics upon subsequent entry/exit after the transition period, searches cannot be reliable using biometric characteristics.) • Limited LEA value - 1:1 or 1:N searches of fingerprints cannot be used.

> *Option D*

The table below summarises the main characteristics of option D.

Table 45 *Option D – photo: EIO; fingerprints: EIO*

General

- Registration in EES through use of MRZ plus additional data on entry-exit with 10 (or fewer) fingerprints and a photo;
 - Verification of TCNVE persons in the EES could be made using facial recognition and/or fingerprint comparing with respect to a central AFIS.
-

Advantages

- Homogeneous records: all records have biometric characteristics. Significant potential for having more homogenous process as well.

Disadvantages

- Can be expected to be the most complex from the start.
-
- Undocumented persons could be identified using 1:N searches against the EES immediately.
 - Can be expected to be the most expensive from the start.
-
- Pre-border checks, or any similar solutions for enrolling fingerprints and taking a photo, would be of interest, in particular for certain border types/situations.
 - Gives Member States less time to implement necessary processes and equipment for biometric registration and checks.
-
- LEA could use the EES for 1:1 or 1:N searches using fingerprints (captured live or latent prints).
-

- **Advantages and disadvantages of an alphanumeric-only EES transition period (TF3.1)**

Since the fact that a transition period is defined as a period during which no biometric data would be used in the EES, the consequence of not having such a transition period is that biometric characteristics would be used from the very start of the EES system.

Hence the following main advantages and disadvantages of not having such an alphanumeric-only transition period can be formulated:

Table 46 Advantages and disadvantages

Advantages of not having an alphanumeric-only EES transition period	Disadvantages of not having an alphanumeric-only EES transition period
The reliability of the generated entry/exit records will immediately benefit from the use of biometric characteristics.	The system will be launched with a complexity that will be higher than without biometric characteristics. This can potentially lead to a more cumbersome roll-out for Member States. Not having an alphanumeric-only transition period will result in Member States having less time to adapt their border crossing points.
The capability to measure overstayers will immediately be impacted for the better.	Convenience for travellers might suffer from the initial higher queue-times that are a consequence of the requirement to enter everybody's biometric characteristics from the very start of the system.
The information collected can immediately be expected to be more precise with regard to the capacity to verify or identify a traveller.	There will be less time to try out biometric options in parallel but disconnected from the operational production system. Having such parallel but disconnected set-up could allow further testing and comparison.
It allows a smooth transition from the end of the roll-out of biometric technology at borders for the VIS, i.e. it builds on the VIS without creating a deferral of efforts.	

- ***Consequences of having an EES transition process without biometric identifiers (TF3.2)***

Having a transition period without using biometric identifiers has as a consequence that the border control processes must rely on alphanumeric-only checks.

- > ***Consequences for travellers***

Implementing an EES based on alphanumeric-only checks can be expected to only marginally increase the processing time in the border crossing process.

Since no biometric characteristics needs to be enrolled or to be captured for verification or identification, there will be no additional time added to the border control processes for biometric aspects.

- > ***Consequences for the border control process***

On the one hand, from a border control process perspective, such a transition period will temporarily yield simplicity (for the time of the transition period).

On the other hand, it can be observed that:

- Since today there is no EES in place, having an EES transition period without biometric identifiers can be expected to have no significant impact on the security checks at the borders, because these checks will not change;
- The reliability of the generated entry/exit records will not benefit from the use of biometric technology. This benefit will only materialise after the transition period;
- The information collected will not benefit from the additional precision and assurance derived from the use of biometric characteristics.

- > ***Consequences for LEA***

Having a transition period without using biometric identifiers has as a consequence that law enforcement processes must rely on alphanumeric-only checks. Until the end of this transition period, law enforcement will not benefit from additional information-enriching capabilities of biometric characteristics:

- To search for information on the travel and cross-border movements of suspected persons;
- To detect persons subject to an alert with regard to the use of different identities to cross the borders;
- To identify suspects that lost or destroyed their travel documents.

- **Advantages and disadvantages of a phased approach (TF3.3)**

A phased approach is defined as consisting in the creation of the possibility of including biometric characteristics in EES from the start by Member States (potentially at selective border control points only) that are ready, and letting the other Member States join in progressively, so as to reach full implementation by a target date. The main advantages and disadvantages of this approach can be described as follows:

Table 47 *Advantages and disadvantages of a phased approach*

Advantages	Disadvantages
Higher degree of individual freedom for the Member States with regard to the timing of the implementation of the biometric characteristics compared to the transition approach.	Full benefits only available at the end of the phased approach.
Increased possibilities for integration and acceptance testing.	Potential for operational complexity if Member States include biometric characteristics according to a different timing, resulting in less effective checks when a TCN's entry and exit Member States are different.
Increased possibilities for system tuning.	There is a risk of uneven levels of security at the external borders, as persons not subject to the visa obligation could effectively chose whether their fingerprints will be recorded or not by choosing to enter the Schengen area via a Member State that postpones biometric enrolment and identification/verification. .
Benefits of using biometric characteristics will immediately be present in those Member States that include biometric characteristics in EES from the start.	

- **Data protection considerations**
 - **Extension of the use of biometric characteristics for identification purposes to all TCNs**

The EES legislative proposal provides for the use of biometrics in the form of fingerprints to **“Support the identification of irregular migrants; by storing biometric characteristics in the EES on all persons not subject to the visa requirement, and taking into account that the biometric characteristics of visa holders are stored in the VIS, Member States' authorities will be able to identify any undocumented irregular migrant found within the territory that crossed the external border legally; this will in turn facilitate the return process.”** According to the EES Impact Assessment, biometric data provides a reliable means of identifying a person who is suspected of a crime or a crime victim such as victim of trafficking in human beings. Notably it helps to identify TCNs that have destroyed their documents. In addition, the proposal considers that the use of biometric characteristics could also help law enforcement authorities that are investigating a crime through the use of fingerprints and wish to establish an identity.

Currently the EES proposal limits the use of biometric characteristics for identification purposes:

“Solely for the purpose of the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States, the authorities competent for carrying out checks at external BCP in accordance with the Schengen Borders Code or within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to search with the fingerprints of that person.”⁹⁸

However, one of the options brought forward by this Study provides for the systematic use of biometric characteristics for identification purposes to all TCNs subject to EES. This would mean an extension of such systematic check to TCNVE (since the systematic check for TCNVH already takes place when enrolling at the consulate). Among the reasons brought forward by this Study, the identification of all TCNs will make it possible to find persons with double, possibly fraudulent identities and to find persons with two or more passports that (legally) contain slightly different data. While TCNVE should be searched in the EES, TCNVH should continue to be searched in the VIS. It can be observed that this option was technically not yet possible with the VIS technology in 2006, while it will be possible once the EES and RTP become operational. The extension of the use of biometric characteristics for identification purposes to all TCNs would have a negative impact on the protection of personal data of TCNs, therefore the expected benefits of extending the identification to all TCNs should be carefully assessed in light of the opportunities that such a measure would bring to find persons with double identities and to find persons with two or more passports that might contain different data. Therefore the proportionality of such an extension should be carefully assessed. In particular, it should be assessed against the existence and effectiveness of less intrusive measures that could be used in order to identify people with double or fraudulent identity or persons with passports that contain slightly different data.

A similar assessment should be carried out with regard to the use of biometric characteristics for identification purposes in RTP. Currently, the legislative proposal only provides for the possibility of using fingerprints for verification purposes at the external borders. The reason brought forward by

⁹⁸ COM(2013) 95 final, Article 19

the Study to introduce identification in RTP relates to a reduction in the risk of RTP shopping. This risk was already identified by the RTP Impact Assessment.⁹⁹

> ***Introduction of facial image recognition in EES and RTP***

The use of facial images is currently not considered an option in the context of the Smart Borders Package, although, as the RTP Impact Assessment explains "(...) all visa-exempt third countries issue e-MRTDs with only the facial image as biometric identifier".

It can be observed that the visual (non-automated) use of facial images is already provided for by the VIS. However, matching is not performed nor envisaged. In addition, as pointed out by this Study, it is accepted that digitised facial images will become increasingly available (although with exceptions) and by 2020 an increasing number of passports of ICAO countries will be an e-MRTD with biometric data in a chip. Furthermore, nowadays the majority of ABC gates handle facial image recognition (exceptions for France and Spain). Based on these considerations and given the added value that the use of facial images would bring when used together with fingerprints, the Study analyses the introduction of facial images as one of the options to be considered. The Study highlights that in order to guarantee that the quality of the photo in EES is good enough it should at least meet the requirements set by the ISO/IEC 19794-5 standard.

> ***Reduced number of fingerprints for EES***

The Study brings forward a variety of options, going from no fingerprints to 10 fingerprints in the context of EES. The number of fingerprints to be stored and processed is evaluated against the percentage of accuracy as well as the different purposes for which they can be used.

◦ ***Main options analysed***

The Study puts forward three main options with regard to biometric characteristics:

- 1) Use of fingerprints only, for both the EES and the RTP;
- 2) Use of facial images only for both of the EES and the RTP;
- 3) Combined use of fingerprints and facial images, for both the EES and the RTP.

Biometric data considered in this Study are personal data and therefore may only be processed if there is a legal basis. The proposed legal basis consists of COM (2012) 95, 96 and 97.

The proposed EES Regulation COM (2012) 95, explicitly introduces the use of biometric characteristics¹⁰⁰, particularly the use of 10 fingerprints:

Explanatory Memorandum

Reference

Subject

⁹⁹ SWD(2013)50, p.33.

¹⁰⁰ Please note that in the present section of the report, we use the words characteristics and data interchangeable. This is due to the fact that the entire report strives to use the vocabulary of ISO 2382-37, while this is not the case in the legal proposal

Explanatory Memorandum	Reference	Subject
Support for identification of irregular migrants by storing biometric characteristics of all TCNVEs in the EES and taking into account those of TCNVHs (to facilitate return process).	p. 3	Identification required
EES designed as centralised system with biometric data, retention period of 6 months (ordinary cases) and 5 years (overstayers).	p. 5	Retention time defined
Transitional period of 3 years for biometric recognition	p. 5	Transitional period
Proposal for a Regulation	Reference	Subject
EES to process biometric data	Art. 2 p. 15	Biometric characteristics are expected
Definition (biometric characteristics = FPs)	Art 5 p. 17	Biometric characteristics corresponds to FPs only
Creation of EES individual file with 10 FPs for VE	Art 12 p. 21	Enrolment of FPs for VE.
Use of the EES for examining and deciding on visa applications	Art 16	Access to the collected in the EES, including the FPs
Access for verification at external borders	Art 15	Verification required / access of the Competent Authority
Access for verification within the territory of the Member States	Art 18 p. 23	Verification required / access of the Competent Authority
Access for identification	Art 19 p. 24	Identification required / access of the Competent Authority
Commission shall adopt ... specifications for the resolution and use of FPs for biometric verification in EES	Art 23 p.25	Verification required with FPs
Use of data for reporting and statistics	Art 40	The number of individuals exempt from the requirement to give FPs

Explanatory Memorandum	Reference	Subject
Annex	Reference	Subject
For TCNVHs, BMS will be used for purpose of entry and exit	p. 44	Reuse of BMS

The proposed RTP Regulation COM (2012) 97 explicitly provides for the use of biometric characteristics:

Explanatory Memorandum	Reference	Subject
Use of fingerprints	p. 3	In ABC gates the fingerprints of the travellers would be compared to the ones stored in the Central Repository and other databases, including the Visa Information system (VIS) for visa holders.
Reference to use 4 fingerprints and to the re-use of fingerprints	p. 5	Four fingerprints should be stored to ensure accurate verification of a registered traveller at the external border crossing point. The re-use of fingerprints stored in the repository is foreseen
Reference to use of 1 or 2 fingerprints	p. 6	Storing only one or two fingerprints may cause problems for the travellers and for border authorities at the external borders as fingerprints may be smudged, distorted or fragmented..
Proposal for a Regulation	Reference	Subject
Use of fingerprints	p. 13, recital 12	Use of fingerprints for reliable verification
Retention period	p. 14, recital 21	Retention period of 5 years introduced
Re-use of fingerprints previously stored	p. 14, recital 22	In order to facilitate the procedure for any subsequent application, fingerprints can be copied from their first entry into the Central

Repository within a period of 59 months.

Use of token combined with fingerprints during verification at ABC gates	p. 14 recital 25	Verification done by physically producing the token and fingerprints at the same time
Biometric characteristics = fingerprints	p. 19, art.3 (11)	Reconfirmation
Fingerprint collection	P20, art 5(3)	Appearance in person compulsory in order to provide fingerprints for interview and for the travel document to be checked.
Fingerprint collection	p. 21, art 5(6)	Obligation to collect the fingerprints
Collection of 4 fingerprints	p. 22, art 8	Exceptions, possibility to re-use previously stored fingerprints and method for collection
Split biometrical/alphanumeric data	p. 31, art 22	The alphanumeric data and the biometric data shall be recorded in separate sections
Data to be entered in the application file where an application is admissible	p. 33, art 25(5)	Fingerprints are included among these data
Use of data for examining applications, lost or stolen token or problems occur with facilitating registered travellers' border crossings	Art. 31 (4) and 31(5)	Identifies the conditions where competent authorities can search : -with biometric data alone - if the token and fingerprints are presented by the registered traveller at the same time Identifies the cases where competent authorities can have access to the biometric data
Verification of the identity of the RT at external borders crossing points	p.36, art 32	Verification of fingerprints

Specifications for the resolution and use of FPs for biometric verification in the RTP	P 38, art 37 (1)(a)	An implementing measure defining the specifications for the resolution and use of fingerprints for biometric verification in the RTP shall be adopted by the Commission in comitology
Information to be provided to the RTP applicant	P 44, art 48 (2)	Information to be provided in writing to the RTP applicant when the data from the application form and the fingerprint data are collected.
Monitoring and evaluation	P 50, art 63(4°)	The overall evaluation of the RTP to be produced by the Commission shall include an examination of the implementation of the collection and use of biometric data
Harmonised application form	P 53 and 55, Annex I	- Indication on whether the fingerprints were collected previously for the purpose of applying for a Registered Traveller Programme - Consent for the taking of fingerprints,

Annexes	Reference	Observation
n/a	n/a	n/a

Furthermore, the processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which the personal data are collected and/or further processed. The relevant legal framework setting up the requirements is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹⁰¹ and Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions bodies and on the free movement of such data. The Study highlights below a number of key issues to be taken into account when assessing the different options thus supporting the assessment of alternative, less intrusive means to achieving policy objectives".

¹⁰¹ OJ L 281, 23.11.95.

- ***Use of fingerprints only, for both EES and RTP***

Fair and lawful processing: the question on the fair and lawful processing of fingerprints in the context of EES and RTP is not addressed further in this Study since both Impact Assessments already dealt with this question. Furthermore, the use of the same biometric data is consistent with previous policy choices as in the context of VIS.¹⁰²

Specific and lawful purpose: the purposes for which fingerprints will be collected and processed are clearly described in both legislative instruments and have been assessed in the context of the both Impact Assessments¹⁰³. It is not the objective of this Study to modify the purposes of either of the systems and therefore this aspect is not further analysed in this Study.

Adequate, relevant and not excessive: currently, the EES legislative proposal provides for the processing of 10 fingerprints, while RTP provides for 4. The rationale behind this differentiation has to do with the different purposes that the two systems have and the different volumes they process. The number of individuals needing to be identified as RTP members is a small subset of the total number of individuals being recorded in EES.

The Study investigated the possibility of capturing a reduced number of fingerprints compared to the one provided for today. Options vary from no fingerprints at all to 10 fingerprints. With regard to the EES, on the one hand, enrolling a smaller number of fingerprints compared to the 10 provided for today has the advantage of reducing the impact on the protection of personal data and providing some level of data minimisation. On the other hand, a higher amount of fingerprints (8-10) decreases the probability of false rejection because there are more fingerprints against which to check.

Accurate: fingerprints present a high accuracy rate for identification. However, this may be negatively influenced by low quality of the data or non-consistent acquisition process or representation, which may lead to higher false acceptance or rejection rates. To mitigate such risks, adequate measures should be undertaken, for example by providing for human supervision for enrolment and identification tasks. In the case of the VIS such mitigations measures have proven to be effective and sufficient. The number of fingerprints and their accuracy should also be evaluated by taking into account the possibility of combining fingerprints with facial images.

- ***Use of facial images only***

The use of facial images only is currently not considered an option in the context of the EES and RTP legislative proposals, although, as the RTP Impact Assessment explains "(...) most if not all third countries issue e-MRTDs with only the facial image as biometric identifier".¹⁰⁴ In addition, as pointed out by this Study, it is assumed that digitised facial images from an e-MRTD will become increasingly available (although with a few exceptions) and by 2020 an increasing number of passports of ICAO countries will be an e-MRTD with biometric data in a chip.

¹⁰² SWD (2013) 47, p. 21 final and SWD (2013) 50 final p.52.

¹⁰³ SWD(2013) 47, p.20-22 and p.27, p34-36 and SWD (2013) 50, p.33

¹⁰⁴ SWD (2013) 50, p. 26.

Fair and lawful processing: For facial images to be processed fairly and lawfully, the method of obtaining the data should be clearly identified together with clearly determining how data are processed. In addition, it should be ensured that further processing for purposes other than the one for which the data was initially collected does not take place.

Specific and lawful purpose: The purpose of the processing of facial images should be specific and lawful. In this respect it should be pointed out that this characteristic is widely accepted by users, and that it is already lawfully used in the VIS and other large scale systems.

Adequate, relevant and not excessive: In order to be in line with data protection requirements, the collection and processing of facial images should be adequate, relevant and not excessive compared to the objective for which they are collected. The EES's main objective would be to record travellers' cross-border movements while the RTP's main objective would be to facilitate border crossing for pre-vetted, frequent third country travellers.

The processing of facial images should thus help reach these objectives without having a disproportionate impact on the individuals' right to data protection. An important aspect to be taken into account while assessing this option entails the fact that facial images have been traditionally used in border control. Facial recognition provides a fast way to verify an individual at border crossing. This is true for manual as well as for automated border checks. Indeed, in the digital age, photos are not only stored in paper passports but also in chips of electronic passports in digital form. Pictures stored in electronic passports can be used for automated border crossing, speeding up the border crossing process, thus contributing to the overall objective of improving border crossing management.

Accurate: In order to be in line with data protection requirements, facial recognition should be reliable. ISO/IEC 19794-5 defines requirements for facial images and implementation requirements should be in compliance with that standard. Therefore, careful consideration should be given to the recording conditions and the context of applications. When evaluating the option for the pilot, an important element to be taken into account concerns the fact that facial recognition is not considered being sufficiently accurate for identification in 'stand-alone' mode without using appropriate alphanumeric filtering criteria.

- ***Combined use of fingerprints and facial images, for both EES and RTP***

This option would combine the use of fingerprints with facial images. The necessity to use fingerprints in the context of EES and RTP has been already demonstrated by the respective impact assessments. In the context of EES the use of fingerprints would contribute to the fight against illegal migration as it would allow the identification of undocumented illegal migrants apprehended in the territory of Schengen States as well as prevent identity fraud.¹⁰⁵ In the context of RTP, the use of fingerprints would be used to verify the identity of travellers and prevent 'registered traveller shopping', if the fingerprints of the re rejected applicants would be stored as well.¹⁰⁶

The introduction of facial images has been assessed taking into account the purposes of both EES and RTP as well as the results of the work carried out in the context of the VIS. In light of this, it is considered that facial images are necessary to reach the objectives of EES and RTP because they

¹⁰⁵ SWD(2013) 47 final p.33-34

¹⁰⁶ SWD(2013) 50 final, p. 33-34.

enable to establish a reliable link between the genuine holder and the document as well as facilitate the border crossing with increased speed and convenience.

This Study also assessed the proportionality of the introduction of facial images in combination with fingerprints. The result of the assessment is reported below. **Fair and lawful processing:** currently the EES and RTP legislative proposals establish the processing of fingerprints only. Therefore in order to fairly and lawfully process fingerprints and facial images of TCNs, the legislative proposals part of the Smart Borders Package would need to be amended. Only if there is a legal basis for the processing of both fingerprints and facial images, such a processing would be considered legitimate.

Specific and lawful purpose: currently the EES and RTP legislative proposals do not foresee the use of facial images and therefore both legislative proposal would need to be amended in order to clearly spell out the specific purpose for which facial images (together with fingerprints would be used).

Adequate, relevant and not excessive: the use of facial images as a complementary measure to verify the identity of TCNS in the context of EES and RTP is considered to be adequate and relevant because on one hand it is a combination of two already accepted biometric characteristics, and on the other hand this combination does not add any new functionality outside the scope of those offered by the two respective biometric characteristics already used (FP and FI). It does add speed and convenience, but these are not seen as functionality, rather as non-functional system features.

Accurate: fingerprints present a high accuracy rate for identification. However, this may be negatively influenced by low quality of the data or non-consistent acquisition process or representation, which may lead to higher false acceptance or rejection rates. To mitigate such risks, facial images could be enrolled as well, increasing the degree of accuracy. To guarantee the highest level of accuracy it is recommended to use the ISO/IEC 19794-5 specifications for facial images.

– Impact of the different options on legislative proposals and relevant legislation in force

The table below specifies the impact on legislative proposals and on the relevant legislation in force that the aforementioned options would have if chosen. Options are presented, with a reference to instrument and articles where applicable. It should be noted that given the envisaged TOM the appropriate subset of options would apply.

Option	Instrument and articles	Impact ¹⁰⁷	Explanation
Use of identification (1:N)	Art. 19 of the EES provides for access to data for	Extensive	Compared to the technology used for VIS which dates back to 2006, the current AFIS vendors all claim they can do a systematic 1:N identification

¹⁰⁷ **Limited impact:** only one legislative proposal of the Smart Borders Package is impacted **Extensive impact:** at least two legislative proposals are impacted **Very extensive impact:** at least one legislative proposal and at least one current piece of legislation are impacted.

Option	Instrument and articles	Impact ¹⁰⁷	Explanation
within the border control process, e.g. in EES enrolment (new)	identification at the border or within the territory. Art. 31 of the RTP proposal provides for the search of the RTP for examining, inter alia, applications with FP, and Art 32 provides for the verification of identity with FP		check at enrolment time, without significant impact on the process time. Such identification check could be based on fingerprints, or on a combination of fingerprints and facial image. This would add increased possibilities for security, but is not provided for in the current legal basis.
No fingerprints	EES: 11; 12; 15; 18; 19 RTP: 8 SBC: 7a	Extensive	The legislative proposals composing the Smart Borders Package currently provide for the enrolment and use of 10 or 4 fingerprints (EES and RTP respectively). Hence, aspects related to the entry and use of biometrics would need to be amended to exclude fingerprints, if this option were retained.
4 fingerprints (enrolment)	EES: 11; 12	Limited	The EES legislative proposal currently provides for the enrolment of 10 fingerprints. The adoption of such option would require the amendment of the number of fingerprints that should be entered in the individual file of the person only in the context of the EES legislative proposal, because the RTP legislative proposal already provides for the enrolment of 4 fingerprints.
1-4 fingerprints (verification)	EES: 15; 18; 19.	Limited	The current proposal is not completely clear on this point. If article 15 of the EES proposal should be interpreted as establishing that checks with fingerprints are optional for subsequent entries, then a systematic verification would require amending the proposal.
4-8 fingerprints (enrolment)	EES: 11; 12 RTP: 8	Extensive	The proposal currently provides for the enrolment of 10 fingerprints for visa exempt travellers. This is not necessary for visa holders because 10 fingerprints are already in VIS. Enrolling 4-8 fingerprints would create a difference between the number of fingerprints enrolled for visa holders and the one for visa exempt travellers.
Introduction of facial images (only)	EES: 5; 11; 12; 15; 18; 19; 23. RTP: 3; 5; 8; 25; 31; 32; 37 SBC: 7a	Extensive	Facial images are not included as part of the biometric data to be used in the context of EES and RTP. Thus, the use of facial images instead of fingerprints would require a modification of both the EES and RTP legislative proposals. Similarly in the context of RTP, the provisions where the use of biometric data is mentioned

Option	Instrument and articles	Impact ¹⁰⁷	Explanation
			<p>should be amended by replacing the use of fingerprints with facial images.</p> <p>In addition in both proposals also the definition of biometric data would need to be amended accordingly.</p> <p>Finally, also the proposal to amend the Schengen Border Code would require to be amended where the use of biometric data is mentioned.</p>
Photo from e-MRTD (in case of MRTD or not working e-MRTD)	EES: 5; 11; 12; 15; 18; 19; 23. RTP: 3; 5; 8; 25; 31; 32; 37 SBC: 7a	Extensive	Photos from e-MRTDs are currently not provided for in the proposal. The implementation of such an option, in addition to fingerprints or as a replacement of fingerprints, would require the addition of this biometric data to the legislative proposals composing the Smart Borders Package.
Photo from print	EES: 5; 11; 12; 15; 18; 19; 23. RTP: 5, 8, 25, 31; 32; 37. SBC: 7a	Extensive	Photos from print are currently not provided for in the legislative proposals composing the Smart Borders Package. The implementation of such an option, in addition to fingerprints or as a replacement of fingerprints, would require adding this biometric data to the proposals.
No transitional period to the use of biometric characteristics or phased approach	EES: preamble and 10	8 Limited	Currently, the EES legislative proposal provides for a transitional period for the use of biometric characteristics. If the option retained did not provide for any transitional period or if it provided for a phased approach, whereby those Member States that are ready could introduce the use of biometric characteristics earlier, then the proposal would need to be amended accordingly.

• **Data**

– **Context**

The EES legislative proposal part of the Smart Borders Package provides for the establishment of a centralised system to store entry and exit data of TCNs (both visa holders and visa exempt travellers) that all have the right to stay in the Schengen territory for a maximum of 90 days in any 180 day-period. The EES legislative proposal provides for the collection and processing of data relating to the identity and travel document of the visitor and authorised period of stay. The data will be entered in the system on entry and will be checked on exit, to ensure that the TCN has not exceeded the maximum permissible stay. Data will also be entered in an entry/exit record on each entry and each exit: the date and time of entry and of exit and the MS and border crossing point of entry and of exit. At entry the calculation of days of authorised stay and the date of the last day of authorised stay shall also be entered in the record. Initially, the system will be based on alphanumeric data and, after three years, will see the introduction of biometric data in the form of fingerprints.

In parallel, the Smart Borders Package also provides for the establishment of a voluntary registered traveller programme for frequent travellers to the Schengen Area. TCNs may apply for registered traveller status and benefit from faster border crossings. The RTP is proposed to be based on a central repository containing alphanumeric and biometric data and a token containing a unique identifier held by the traveller.

With regard to the collection and processing of alphanumeric data, the Study identified a number of options that diverge from the current legislative proposals and each of these options is analysed in detail below (biometrics are not addressed here since a specific section addresses this question in detail). In particular, the options that will be analysed are:

- The minimum dataset required to fulfil the EES and RTP objectives;
- The retention period;
- Law enforcement access;
- Output of EES and RTP systems.

– **Minimum dataset required to fulfil the EES and RTP objectives (TF11.1)**

Objectives

The purpose is to identify the minimum (and sufficient) dataset required to proceed with the EES and RTP related processes while ensuring data protection and privacy by design principles and maximising data automation. Priority should be given to the less intrusive implementations achieving the policy objectives.

Approach

The EES and RTP dataset proposed respectively in the EES and RTP legislative proposal was taken as a basis of reference. Based on this proposal, a data model was designed describing the different data categories and the cardinalities between the different categories.

EES minimum data set:

- The minimum EES operational dataset needed to perform checks at external borders was already defined in section 3.2.2. **A teleconference with the Member States' experts was organised on the 15th of April, 2014** in order to identify data currently collected by the MS, starting with the MRZ and biometric data as a minimum dataset, and assess the potential impact of collecting additional non MRZ data;
- Several potential data sources were identified for the purposes of data collection and re-use and their impact was then assessed in relation to various evaluation criteria;
 - Once the minimum EES operational dataset was defined, the required data related to the calculation of the duration of the authorised stay and to the conditions for entry could then be identified.
- Finally, the impact of collecting additional data (the data gap between the EES Minimum dataset and the EES legislative proposal dataset) that are not part of the minimum dataset was then assessed.

RTP Minimum dataset

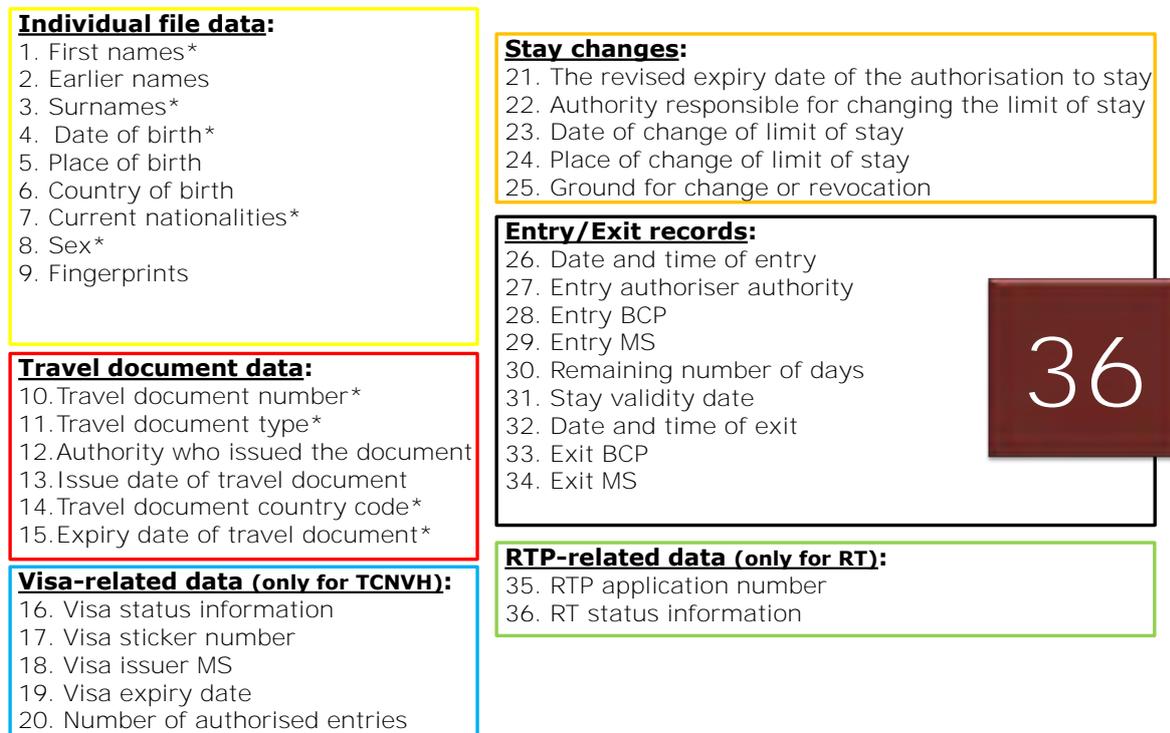
- The RTP legislative proposal dataset was compared to the VIS dataset and differences were analysed.

The following set of EES and RTP processes were considered:

- Processes prior the entry and exit: RTP enrolment/ application;
- Processes prior subsequent entry: identification, LEA, information to carriers, information to travellers;
- Processes during the entry and exit: document check, bearer verification, registration, biometric verification, individual file creation, entry/ exit record creation;
- Processes after the entry and exit: requirements for statistics and reporting.

◦ **Dataset foreseen by the EES legislative proposal**

The EES legislative proposal suggests registering the following 36 data-elements that are shown in the figure below.



* = MRZ

Figure 24 Data elements suggested by the EES legislative proposal

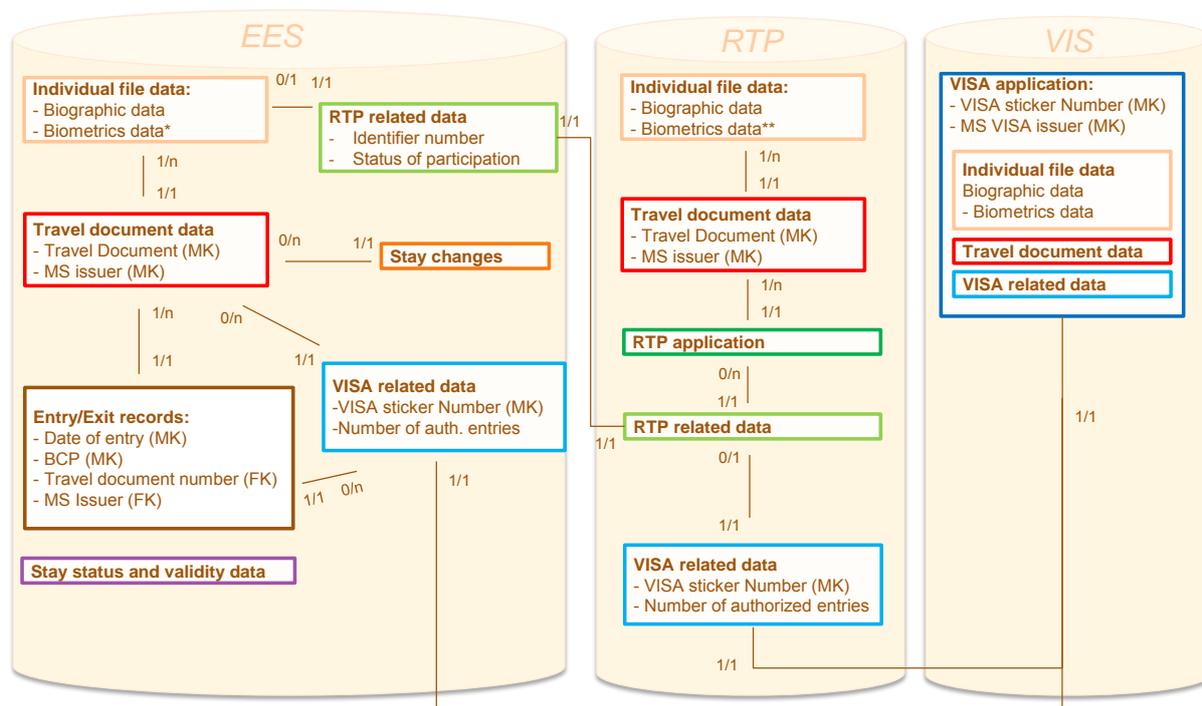
◦ **Proposal of a data model for EES and RTP**

The above-mentioned data could be classified in different categories according to their common characteristics:

- **Individual file data:** alphanumeric and biometrics data related to a person's individual file;
- Travel document data;
- Entry/Exit records: transactional data of an individual;
- Change of stay limit;
- RTP related data;
- Visa related data.

Building up on these categories of data, the following referential data model was designed as a proposal, taking into account the cardinalities and the way data categories are linked:

Data model of EES and RTP as separated systems as per the legislative proposal



* For TCNVE only, as biometrics of TCNVH are stored in the VIS

** Duplication of biometrics stored in the VIS (article 8 of the current RTP legislative proposal)

Figure 25 Data model of EES and RTP as separated systems as per the legislative proposal¹⁰⁸

From this data model the following can be outlined:

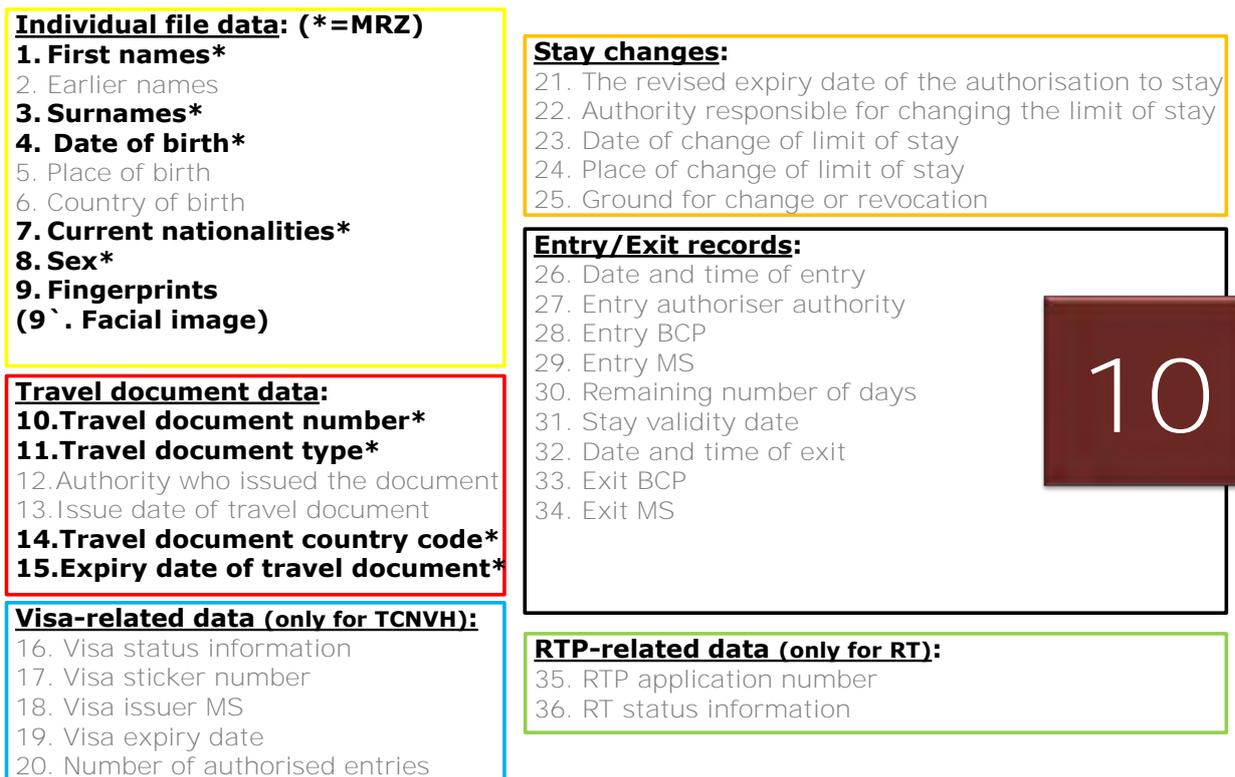
- One individual person can have different travel documents;
- One individual person can have different visas (but only one at a time);
- An RTP application can only be associated to one travel document (and one visa, if applicable);
- A travel document (in this case an e-MRTD) is a pre requisite to apply to an RTP;
- One entry-exit record can only relate to one individual person, to one visa (when applicable) and to one travel document;
- A travel document could be related to zero (TCNVE), one (TCNVH) or to multiple visa (i.e. when a minor is covered by the parent's MRTD and there are therefore 2 visa stickers in the MRTD);
- In VIS, all information is duplicated and linked for each visa application.

¹⁰⁸ Cardinalities are represented according to the French model, so the figure should be read as followed: e.g. a travel document data in EES can be associated to one-to-many entry/exit records, while an entry/exit record can only be associated to one and only one travel document data.

◦ **EES minimum dataset**

1. Data necessary for identification and authentication checks:

Based on the Member States' insights, out of the 36 data fields suggested in the proposal for the ESS Regulation, 9 alphanumeric data contained in the MRZ and biometrics data would be sufficient for border guards to perform the identification and authentication checks at the external borders ("Data used in entry and exit" on section 3.2.2). The question whether one or two biometrics should be collected is addressed in the biometrics factors section 4.5.4. The outcome is that 10 data elements (considering the biometrics as one) would be sufficient for identification and authentication.



* = MRZ

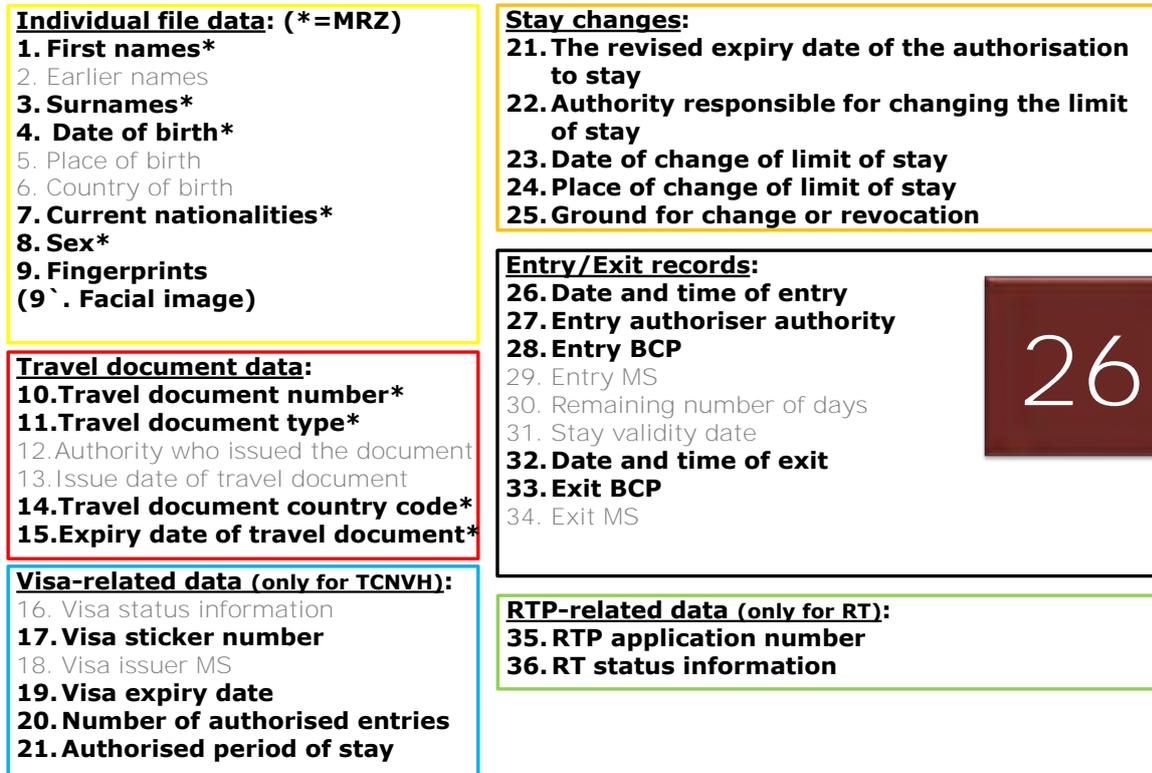
Figure 26 Data elements necessary for identification and authentication checks¹⁰⁹

Specific case of persons without passport: the person's name, date of birth, country and the document number of the parents or spouse's passport should be entered manually in the EES, as an individual file. The parent's or spouse's individual file would be created as per the normal procedure. For TCNVH travelling on multi-person or family passport the individual visa sticker data can be used for registration in EES.

¹⁰⁹ Data fields in brackets represent data not proposed in the legislative proposal and additionally collected by MS.

2. Data necessary for calculation and monitoring of the authorised stay:

On the top of the above individual file and biometric data, border guards would need 16 additional data in order to calculate and monitor the authorised stay:



*=MRZ

Figure 27 Data elements for EES entry / exit record creation on the top of individual file and biometric data

- 4 data related to visa

Authorised period of stay, Visa expiry date, visa sticker number and the number of authorized entries should be either duplicated from VIS in EES or captured manually from the visa sticker. The authorised period of stay is necessary because for one single entry visa the period of authorised stay may not correspond to the visa expiry date. If the TCN used the entire time of authorised stay the system should flag it. However, if the period is not fully used then the visa expiry date should be used to calculate overstay. The visa sticker number is necessary because a travel document can be linked to multiple visas. The number of authorized entries is necessary for system performance reason as this data will be needed to perform entry check;

- 5 data related to the changes (extension or revocation) of the authorized limit of stay. Data fields 22, 23 and 24 are not necessary for the verification checks and will be available in the audit log;
- 7 data related to entry and exit records to allow the calculation of remaining allowed time;
- 2 data related to RTP, if applicable
- RTP related data is needed to make sure that EES is updated un-ambiguously when using ABC. RT status information will be needed for the calculation of data retention period, if the option of different data retention periods for RTs and non-RTs was chosen.

3. Additional data collected by Member States

On top of the data foreseen in the legislative proposal, some Member States are currently collecting additional data such as the full name, the full original name, observations, transportation data, etc. (data in brackets in the below figure). Those data are currently not part of the legislative proposal.

With the exception of the full name, which can be useful to solve issues related to the identification of persons (mainly in the second line checks) because the name in the MRZ can be truncated, MS additional data are not needed for border checks and therefore should not be collected for the EES.

4. Data gap between EES Minimum dataset and the EES legislative proposal dataset. The image below highlights in red those data that are not part of the minimum dataset but that are in the current legislative proposal.

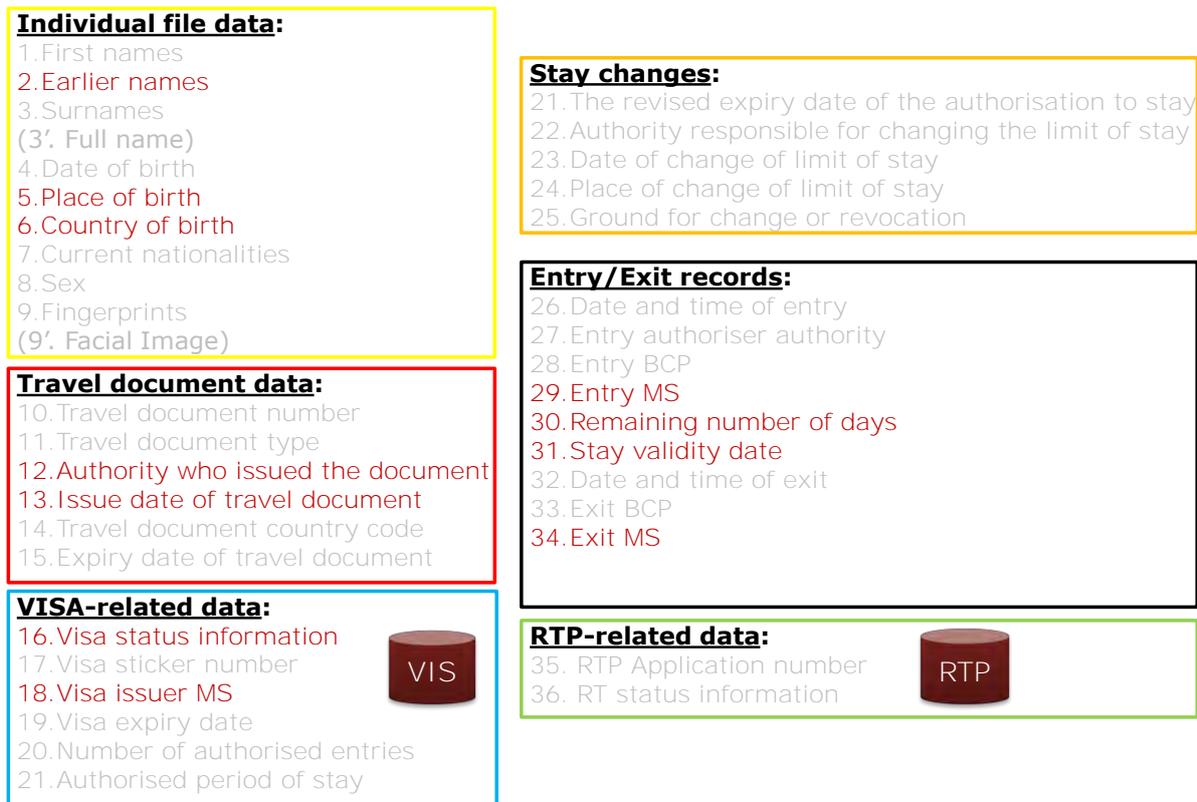


Figure 28 Data gap between the EES minimum dataset and the EES legislative proposal dataset

Some of the data suggested in the legislative proposal is not systematically stored in the chip or even on the paper passport. Ensuring the reliability of the information inserted manually will be in some cases challenging, if not impossible (this is the case for the Data field N°3; surname at birth, N°5; the place of birth, N°6; the country of birth and N°12; travel document issuing authority).

Article 5 (1)(a)ii of the SBC specifies that the passport must be issued within the 10 previous years. Therefore it might seem necessary to collect the travel document issuing date (data field N°13). Yet, given that travel document expiry date will be maximum 10 years, the travel document issuing date entry check will be implicitly performed during the travel document expiry date check. Capturing the travel document issue date appears thus to be unnecessary.

By using standard codification such as ISO standard 3166 for codifying country/region/city, combined with the Border Crossing Point reference as per the annex of the SBC,¹¹⁰ the MS Entry and Exit location could be included in the BCP Entry and Exit data (data field N°29 and 34).

The legislative proposal also suggests storing a dedicated field for the remaining number of days and stay validity date (data field N°30 and 31). Those data are calculated based on authorised period of stay. Thus information is duplicated which increase the risk of data inconsistencies. The data owner need to be defined as well as the underlying legal responsibilities related to the accuracy, the display at border and the output provided to carriers and travellers, if any.

An alternative option to the legislative proposal would be the one already described in the legislative proposal. This option entails to recalculate/rebuild the remaining number of days and the last day of the authorized stay (data field N°30 and 31) via a service, by querying the historical entry/exit records at each consultation. In this case this information is not stored anymore. Such option would reduce the risk of inconsistencies brought by the data duplication.

5. Reporting and Statistics objectives

As stated in article 40 of the EES legislative proposal, competent authorities responsible for assessing the EES for reporting and statistics purposes should only have access to EES data which do not allow identifying individuals. This limited anonymised set of data would ensure proper reporting and statistics but would prevent the identification of individuals.

The archiving of anonymised entry/exit records and of other individual file data could reduce the risk of negative impacts on system performance. In addition such a measure would be in line with data protection requirements while enabling to keep historical entry and exit records for statistical reasons.

6. EES minimum dataset

While the EES legislative proposal suggests storing a set of 36 data, the EES minimum dataset considered necessary to fulfil the objective of the EES while maximising automation is composed of 26 data grouped as follows (please also refer to Figure 27):

- Individual file data (first names, surnames, date of birth, current nationalities, sex and fingerprints (facial image));
- Travel document data (travel document number, travel document type, travel document country code, expiry date of the travel document);
- Visa-related data (visa sticker number, visa expiry date, number of authorised entries, authorised period of stay);
- Stay changes data (the revised expiry date of the authorisation to stay, authority responsible for changing the limit to stay, date of change of limit of stay, place of change of limit of stay, ground for change or revocation);
- Entry / exit records (date and time of entry, entry authoriser authority, entry BCP, date and time of exit, exit BCP);
- RTP-related data (RTP application number, RT status information).

¹¹⁰ OJ L 105, Annex 5 Part B, 13.4.2006.

Some MS that already have national EES collect additional data such as location of residence during the stay, transportation data, purpose of stay etc. Due to the complexity of reliable manual checks and inconsistencies of mandatory data contained on the MRTD and e-MRTD across different TCN, the collection of additional data on top of the minimum EES dataset suggested by this Study would:

- Go against the minimisation and proportionality principles for 1st line border control purposes;
- Not provide an added value for the first line checks; this data can possibly be accessed in the 2nd line from the appropriate national source;
- Slow down border crossing time during the registration process.

The collection of additional data would only be beneficial for Law Enforcement Access.

Main findings

Despite the initial EES legislative proposal of 36 datasets, a total of 26 datasets are suggested. In addition to the core (initial) 10 data, including personal information and biometrics, another 16 datasets are proposed as part of the minimum EES dataset. The selection of these datasets is considered necessary to fulfil the EES objective while maximising automation. The collection of additional data to the minimum set data would go against the minimisation and proportionality principles, not adding value for the first line checks and slow down border crossing time.

◦ **Analysis of the candidate data sources for EES**

Several data sources can be considered for capturing the minimum dataset needed for EES, varying in terms of automation, scope of data and security.

Table 48 Candidate data sources for the EES

Candidate data sources for the EES	Scope of data						Analysis criteria					
	Individual file data	Travel document data	Entry/Exit records	Change of stay limit	RT related information	Visa related information	Duration of the crossing border	Security	Quality of data	Leverage on existing systems	Legal acts	Implementation complexity
Re use of VIS						x ¹¹¹	++	++	++	++	--	N
Re use of RTP					x		++	++	++	++	--	--
Chip of the e- MRTD	x	x					++	++	+	-	N	+
MRZ scanning (in MRTD or e-MRTD)	x	x					++	+	++	-	N	+
Paper travel document (passport and visa sticker)	x	x				x	--	++	-	--	N	++

¹¹¹ Visa sticker number, visa expiry date, number of authorised entries and authorised period of stay.

With regard to EES, there are different approaches that could be followed to use these data.

One approach would be to capture the minimum EES datasets by taking existing data stored in RTP (i.e. captured during the RTP enrolment). However in the design of currently existing large-scale IT systems (SIS II, VIS, Eurodac) the direct links at central level between systems has been avoided to meet data protection concerns.

In order to use RTP data of TCNVE in the context of EES, it would be possible to use the travel document number and the issuing country code which are the primary keys for both systems. However, from a data protection point of view, such an option could be envisaged only if EES and RTP would not be conceived as two separate systems.

Chips in passports can also be used to collect the minimum dataset, in particular for non-RT TCNVE. However, apart from MRZ and the facial image (the two fingerprints that can be stored in the chip are optional) the ICAO standard does not impose any additional mandatory fields, so the scope of data can vary from one country to another. In addition, chips are also sometimes - albeit rarely - defective (unreadable, damaged or broken). In this case, most of the individual file data can be collected by scanning the MRZ. Biometric data can also be collected manually during the registration process and the possible few additional data can be collected manually from the passport (not from chip). Even though the case of manual collection of data will be considered as an exception, the impact on the border crossing time could be significant depending on the number of additional data on top of the MRZ data that should be mandatorily collected.

During the verification process, a data consistency check could be performed between the data contained in the chip and the data already stored in VIS and/or in RTP.

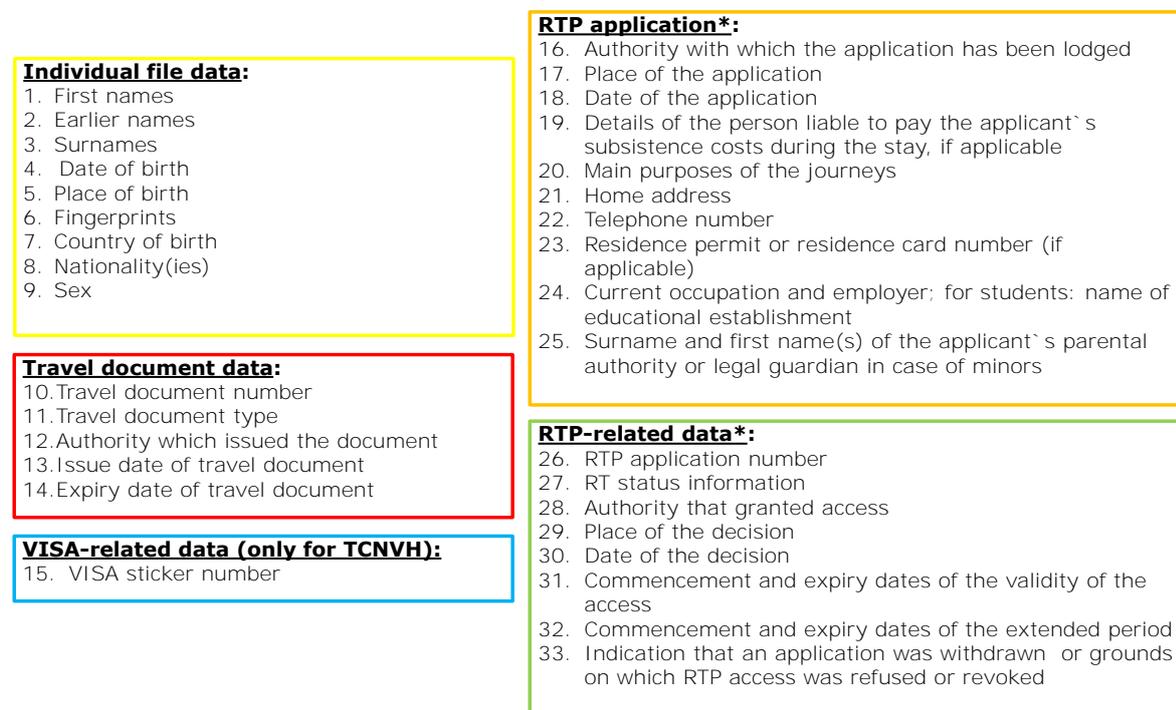
Finally, some of the data suggested in the legislative proposal might not be systematically stored in the chip or even found in the paper passport (i.e. Surnames at birth, Travel document issuing authority). These fields would need to be typed manually, which would take time and create a risk of error. Thus, the reliability control regarding the data source would be challenging. It would be necessary to ask the person to provide the necessary documents to verify that the data entered is correct and also check the authenticity and reliability of the documents submitted and on the veracity and reliability of the statements made by the TCN.

Main findings

Several data sources can be considered for capturing the minimum dataset needed for EES. The approach of taking data stored in RTP for the purposes of EES could present difficulties related to data protection. Chips in passports is another alternative, in particular for non-RT TCNVE, but the scope of collected data can differ from country to country and there could be cases of defective chips. Manual collection of data on top of MRZ should be considered an exception as the impact on border crossing time could be significant. Finally it should be taken into consideration that some of the data suggested in the legislative proposal might not be systematically be stored in the chip or even found in on the paper passport.

o **Dataset outlined in the RTP legislative proposal**

Dataset outlined in the RTP legislative proposal is presented in the figure below.



*If common data was shared between EES and RTP, RTP application and RTP-related data would be accessed via unique identifier

Figure 29 The RTP dataset outlined in the legislative proposal

If common data, namely individual file data and travel document data, were shared between EES and RTP, RTP application and RTP-related data would be accessed via unique identifier, such as RTP application number.

The scope of data suggested for the RTP is very similar to the one for VIS, with the exceptions presented in the table below.

Table 49 Data discrepancies between VIS regulation and RTP legislative proposal

Data discrepancies between VIS regulation and RTP legislative proposal	VIS regulation	RTP legislative proposal
Photograph/ Facial Image	✓	✗
Nationality at birth	✓	✗
Member state of destination	✓	✓ ¹¹²
Intended day of arrival	✓	✗
Intended day of departure	✓	✗

¹¹² The RTP legislative proposal requires address of the hosting person or company / organisation.

Data discrepancies between VIS regulation and RTP legislative proposal	VIS regulation	RTP legislative proposal
MS of first entry	✓	✗
6 data fields related to visa examination discontinued only in case visa authority representing another MS	✓	✗
5 data fields related to visa: <ul style="list-style-type: none"> Manually filled VISA sticker Visa issuing MS Duration of the stay Visa type Number of authorised entries 	✓	✗
Resident permit or resident card number	✗	✓
Telephone number	✗	✓

Given the high similarities, the Study compared VIS and RTP datasets independently of the type of travellers considered (TCNVE and TCNVH).

The discrepancies identified above are explained by the difference in the objectives pursued respectively by the RTP and the VIS. The decision whether the Facial Image should be added to the RTP legislative proposal is presented in the **previous section “Biometrics used in RTP” (Section 4.4)**.

From a data perspective, the following arguments justify the use of the Facial Image in RTP processes:

- Greater majority of ABC eGates using facial-images for biometric verification;
- Increase the accuracy level of the identification checks and homogenise accuracy level between TCNVE and TCN VH.

Main findings

The scope of data suggested for the RTP in the legislative proposal is very similar to the one determined by the VIS legislation, which is already in force. The discrepancies between VIS dataset and RTP dataset appear only because of process differences. Thus the RTP dataset as per the legislative proposal is sufficient to meet RTP objectives.

◦ ***EES and RTP data management***

This item discusses the options for the EES and RTP data management model, which addresses the question of data ownership particularly in the cases of errors, the need to amend the data etc. The section highlights advantages and disadvantages of the following potential technical options:

- **Distributed model:** the whole dataset (static and transactional data) is duplicated for each transactional occurrence. Data ownership issue is avoided but this model has an impact on the size of the database;
- **Federated model:** the static data are centralized and linked to each transactional occurrence. With this model, the size of the database is reduced but the management of data ownership is more complex.

More details on the models are given in the following sections.

Firstly, the existing data management model of VIS is analysed. Then the options for EES data management are examined and afterwards the options for RTP data management are reviewed.

VIS data management model

The VIS data model has been designed according to a distributed data management model meaning that the data of the individual file of visa applicant are duplicated for each visa application. This model eases the management of data ownership as each MS is the owner of its own visa application including individual file data. However, the size of the database is higher but nonetheless manageable.

EES data management model

With regard to the EES, the following technical options for the data management model are identified:

- **Distributed model:** duplicating the individual file data for each entry/ exit record in the EES. The MS who records the entry/exit is appointed as the data owner. The TCN does not have to repeat the procedure of the individual file creation including biometrics enrolment as the file is copied from the previous one. If the amendment of the individual file is needed, it is done in the copy of the file. Individual files could be linked for example at the moment of the creation; the subsequent could be linked with the previous one(s);
- **Federated model:** with no ownership of the unique individual file, i.e. no responsibility for entering, amending or deleting the data. The option would be in line with the principle of data minimisation, however it would raise important data protection questions and therefore is not analysed further in the Study;
- **Federated model:** if an update of an individual file data field is needed, the former record is deleted. All the previous data attached to a different individual file are lost. The owner of the individual file is the MS, which last modified the data. There would be significant issues in cases of appeal as the history of his travels is lost i.e. deleted before the expiry period ends. Therefore this technical option is not analysed further in the Study;
- **Federated model:** if an update of an individual file data field is needed, the update is recorded, however the former record is not deleted.
-

Table 50 Advantages and disadvantages of the EES data management options

Option	Advantages	Disadvantages
Option 1: duplication of individual file data	<ul style="list-style-type: none"> • Data ownership is unambiguously defined. • Good compliance of individual file records. The identity management methods suggest keeping a history of biographic data and biometrics to ensure the overall identity of a person in terms of its history at the time of the decision and in retrospect in case of appeal. Such duplication / historization of the data also help to have the most appropriate algorithm for determination, insurance of identity of the person, throughout the life of the data. 	<ul style="list-style-type: none"> • Substantially more data storage would be needed, especially in the case of a long data retention period. However this would not have a major impact on the costs. Please refer to section 4.4 for further explanation. • The option would not be aligned with the data minimisation principle.
Option 2: federated model with history of the former record	<ul style="list-style-type: none"> • The responsibility for the data is easily ensured. • Less data storage would be needed. • The option would be in line with data minimisation principle. • There would be good compliance of individual file records as per option 1. 	<ul style="list-style-type: none"> • The option would be more complex to implement.

Main findings

Both options 1 and 2 implement clear data ownership however option 1 is not aligned with data minimisation principle and requires substantially more data storage.

The data models should be further examined and determined not only based on the representation i.e. number and quality of data and database type, but mostly based on the ability to actually operate efficiently search algorithms on demanding datasets, such as biometric, both on the spot (border crossing, issuance of title or of rights) and a posteriori (in cases of investigation and / or appeals).

It is recommended that these options should be further analysed and evaluated in later stages of the Study, once the architectural options would be determined.

RTP data management model

With regard to the RTP, the following options for data management are envisaged:

- **Distributed model:** implemented as in the VIS;
- **Federated model:** implemented as in the EES (if an update of an individual file data field is needed, the update is recorded, however the former record is not deleted), but with no shared data;
 - **Federated model:** implemented as in the EES (if an update of an individual file data field is needed, the update is recorded, however the former record is not deleted) with the sharing of

the individual file data between EES and RTP. This model will apply in case EES and RTP form one system.

Table 51 Advantages and disadvantages of the RTP data management options

Description of an option	Advantages	Disadvantages
Option 1: implementation of the VIS data management model	<ul style="list-style-type: none"> • Simple implementation of the data model. • There would be no issues with the ownership of individual file data. • As in the VIS, links would allow an overview on the traveller, irrespective of the travel document used previously. • Synergies with VIS which would lead to lower development costs. • Security, data integrity and system availability would be more easily ensured, because of clear ownership and limited access to the data. 	<ul style="list-style-type: none"> • There would be duplication with respect to individual file data stored in the EES, so more data storage would be needed.
Option 2: implementation of EES data management model (option 2), but no sharing of static data	<ul style="list-style-type: none"> • Less data storage would be needed. • The option would be in line with data minimisation principle. • Consistency between both system data management, which facilitates the work of the end-user in charge of the RTP application data entry and examination. 	<ul style="list-style-type: none"> • The option would be more complex to implement. • Limited synergies with VIS and higher development cost. • Duplication of information in two systems, which induces a risk of possible inconsistency. For example a subsequent individual data change in the EES would not be automatically replicated on the RTP.
Option 3: sharing of static data between EES and RTP	<ul style="list-style-type: none"> • There would be no risk of data inconsistency between the EES and the RTP. • Less data storage would be needed, but this would have only a marginal advantage on costs. 	<ul style="list-style-type: none"> • There would be conflicts between data retention periods of EES and RTP, unless changes are made to the current legislative proposal. Please refer to section □□ for further explanation. • Limited synergies with VIS and higher development cost.

Main findings

Options 1 and 3 implement clear data ownership, whereas option 2 suggests storing the less data possible and is in line with data minimization principle.

It is recommended that these options should be further analysed and evaluated in later stages of the Study once issues under review would be clarified.

◦ ***Identification of the biometric identifier(s)***

To check the entry and exit flows of TCNs there must be elements which identify a person in such a way that he/she is distinguishable from all other persons and recognisable as an individual. Given that names are not unique and that even adding the date, place of birth, nationality and document number may not be sufficient to uniquely identify a person, biometric data are considered necessary to identify a person uniquely. The list of the EES and the RTP biometric options is provided in sections 4.4 and 4.5 of the Study.

From a data protection perspective, once the necessity of collecting biometric data has been confirmed, one must assess the proportionality of the envisaged solution. For this purpose the Study takes into account:

- **The type, quantity and processing of biometric data:** only the biometric data necessary to reach the objective of the EES and the RTP should be collected, stored and processed. Both fingerprints and facial images allow for the automated identification, authentication/verification of persons and as such potentially have a high impact on the privacy and the right to data protection of individuals. Biometrics aspects are further analysed in the chapters □□ Biometric characteristics in the EES (TF1) and □□ Biometric characteristics in RTP (TF2)
- **Data retention:** the longer the retention period, the greater the impact on data protection. Please refer to the section □□ for more details on this aspect. However, sometimes to the benefit of the traveller, notably when it comes to RTP, storing the data longer in the EES will avoid that the traveller re-enrols in the EES every six months.
- **Data storage:** the larger the number of fingerprints that would be enrolled per TCN for identification purpose, the bigger the data storage needed. The table below highlights the difference of data storage needed for different options of fingerprints enrolment and their impact on costs. The comparison of costs shows that impact of the choice of biometric identifier on costs of EES and RTP implementation would be negligible.

Table 52 Impact of biometric options on data storage

Biometric identifier	Size of data storage ¹¹³		Costs of data storage of 1 m records in EUR ¹¹⁴	
	Min. size	Max. size	Min. size	Max. size
10 FPs (no FI)	120 kb	173.3 kb	4440	6412
8 FPs (no FI)	96.6 kb	140 kb	3612	5235
4 FPs(no FI)	48.3 kb	70 kb	1787	2590
2 FPs (no FI)	24.3 kb	35 kb	900	1295
1 FP (no FI)	13 kb	17 kb	480	630
FI (typical size)	15 kb	20 kb	580	775

- **Data transfer:** the greater number of fingerprints would have a negative impact on message processing and transmission capabilities, and the network load. The impact of biometric options on data transfer size is shown in the table below.

Table 53 Impact of biometric options on data transfer size

Biometric identifier	Size of data transfer ¹¹⁵		
	Min. size	Average	Max. size
10 FPs (no FI)	160.0 kb	195.6 kb	231.1 kb
8 FPs (no FI)	128.8 kb	157.7 kb	186.7 kb
4 FPs(no FI)	64.4 kb	78.7 kb	93.3 kb
2 FPs (no FI)	32.4 kb	39.6 kb	46.7 kb
1 FP (no FI)	17.3 kb	20 kb	22.7 kb

¹¹³ Figures for FPs include only images and are based on VIS - BMS project.

¹¹⁴ Median price of five vendors (EMC, IBM, Microsoft, Oracle and Teradata) based on publicly available data.

¹¹⁵ The figures for FPs are calculated on the basis of VIS - BMS project taking into account base64 encoding.

Comparison

The table below summarises the overall comparison of biometric identifiers options.

Table 54 Assessment of biometric identifiers options

Options of biometric identifier	Evaluation criteria				
	Duration of the border crossing	Data protection	Implementation complexity (system architecture)	System performance	Cost
10 FPs (no FI)	--	--	N	+	-
8 FPs (no FI)	--	--	N	+	-
4 FPs(no FI)	-	--	N	N	-
2 FPs (no FI)	-	--	N	-	N
1 FP (no FI)	-	--	N	--	N
0 FP	+	+	N	--	N
FI	+	--	N	--	N

Explanation of the scoring scale:

(--) highly negative impact

(-) limited negative impact

(N) neutral impact

(+) limited positive impact

(++) highly positive impact

Main findings

The comparison of biometric options shows that if no biometric data are enrolled, the need for data protection measures is less. However, once facial image and fingerprints (independently from the number of collected fingerprints) are collected the need for setting up measures to protect personal data greatly increase. In fact the risk related to data protection is related to the traces of biometric data and the potential mis(use). Thus from a data protection point of view the discriminant element is whether biometrics are collected or not. However, from a border crossing time perspective, the greater the number of fingerprints enrolled, the longer the border crossing time would be (for further analysis, see section 1.6).

– **Retention period (TF12)**

The following section analyses the different options related to the data retention period to be envisaged for EES and RTP. The retention period covers personal data, i.e. it is not applicable to **the system's operational data (such as the time of user login etc.)**, which does not encompass personal data.

The key requirement to determine the data retention period applicable in the context of EES and RTP is that it must entail only what is necessary in relation to the main purpose of the system.

◦ **RTP and EES data retention as per the legislative proposals**

RTP data retention

With regard to RTP, the data retention period is assessed against the objective of speeding up the border process. The Study has not identified any disadvantages derived from the data retention period as set up by the current RTP legislative proposal and therefore no alternative options have been investigated.

As indicated in the RTP Impact Assessment "It is appropriate to keep the data for a maximum period of five years, in order to enable data on previous applications to be taken into account for the assessment of the subsequent RTP applications, renewal of the access to the RTP and also taking into account the re-use of fingerprints stored in the repository (59 months). Furthermore, a five year retention period would allow granting access to the RTP for five years without a new application. This would be in line with the issuance of a multiple entry visa for trusted travellers (maximum period 5 years) whose data is kept in the VIS for 5 years."¹¹⁶

In conclusion, given the advantages derived from a data retention period of five years compared to a shorter period, the Study does not have any evidence to suggest alternative options to the data retention period as provided for under the current RTP legislative proposal.

EES data retention

With regard to EES, the data retention period is assessed against the objectives set out in Article 4 of the EES legislative proposal, i.e.:

- "improving the management of the external borders and the fight against irregular immigration,
- the implementation of the integrated border management policy,
- the cooperation and consultation between border and immigration authorities by providing access by Member States to the information on the time and place of the entry and exit of third country nationals at the external borders and **facilitating decisions related thereto.**"¹¹⁷

In contrast to RTP, the current data retention rules established by the EES legislative proposal **present a series of disadvantages with regard to the border crossing** process and therefore the Study has investigated alternative options to overcome these drawbacks. Under the EES legislative proposal, the minimum period to be taken into account for the purpose of EES is 181 days because it makes it possible to calculate all short stays during a period of 180 days and to verify whether the maximum 90-day period of stay has not been exceeded. An illustration of this

¹¹⁶ SWD(2013)50, p.52.

¹¹⁷ COM(2013)95 final.

rule is provided in Figure 34 which illustrates the data retention period as provided for under Article 20 § 1 of the EES legislative proposal.

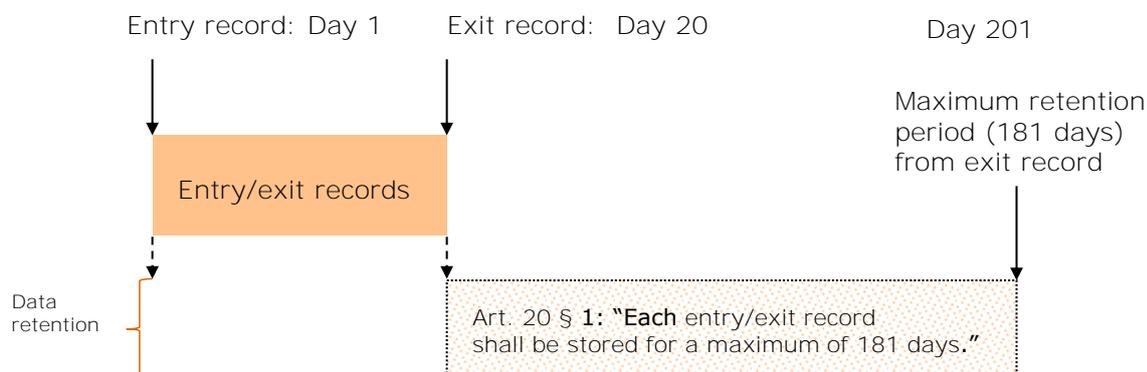


Figure 30 Exemplary case of data retention as per Art. 20 § 1 of the EES legislative proposal

Besides the general data retention rule described in the previous paragraph, the proposal also outlines an exception to this general rule. According to the second paragraph of article 20, the individual file with the linked entry/exit records will be retained for a maximum of 91 days after the last exit record, if there is no entry record within 90 days following the last exit record. Figure 35 illustrates the rule as laid down in Article 20 § 2 of the EES legislative proposal.

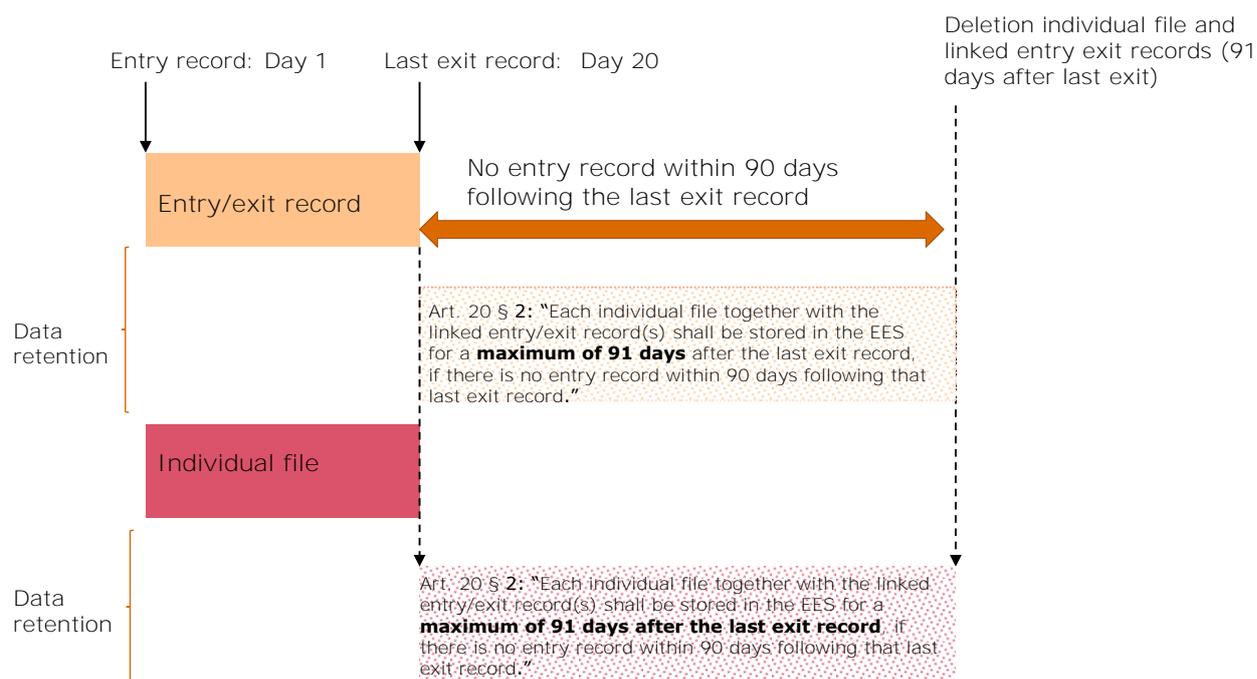


Figure 315 Exemplary case of data retention as per Art. 20 § 2 of the EES legislative proposal

The consequences of applying the rules as laid down in Article 20 § 2 are that if a TCN enters again after 90 days, but before the expiry of his/her right to stay in the Schengen territory, the whole individual file would need to be created again. However, for frequent travellers returning again before the 90 days have elapsed, the individual file would not be deleted.

The Study identified a number of drawbacks if the data retention rules as established by the current EES legislative proposal were to be implemented:

- For TCNs: loss of time due to the fact that the EES individual file would need to be created more often, increasing the time spent at border crossing and the dwelling time (please refer to table 49 below for further information). The length of the data retention period indirectly impacts the length of the border crossing process because once data are deleted, the TCNs would need to enrol their data again; as a result, the shorter the data retention period, the more time is lost by TCNs. At the same time, the longer the data retention period, the greater the risk from a data protection point of view. It is thus necessary to strike the right balance between the principles of necessity and proportionality and the objectives to be met by the EES and RTP. The table below illustrates the impact that the enrolment of an individual file would have on TCNs when crossing the borders, depending on: biometric data enrolled and type of operation undertaken.

Table 55 Impact of the EES individual file creation for TCNs

Process step	Time
1. e-MRTD : Retrieve photo (if available and chip can be read securely); otherwise, use a photo (or scanned photo)	5 s
MRTD : Use photo (scanned photo)	10 s
2. Enrolment	20-30 s
a. 4 FPs	
Enrolment	40-60 s
b. 8 FPs	
3. 1:N identification:	20-30 s
a. Systematic (only VEs)	
Total loss of time for 1 TCN	5-100 s*
Dwelling time	Depends on border crossing organisation

**Depends on the choice of target operating model*

- For border guards: the loss of time is similar to the one experienced by TCNs (please refer to the table above). It should also be mentioned that border guards currently are able to see the exact travel history of a TCN (VE&VH) through the entry/exit stamps in the MRTD. Under the current proposal, only the history from approximately the last 180 days would be visible.
- For visa authorities and authorities issuing the RTP: since exit records, which do not have exit data immediately following the date of expiry of the authorised length of stay, remain in the system for 5 years (even if exit took place at a later stage)¹¹⁸, there would be no impact with regard to tracking overstayers. Based on the current art. 20 § 3 of the EES proposal, if after 90 days, a TCN applies for a visa again, the authority will have his/her data on previous overstays. This is represented in Figure 36 below. However, like border guards, the visa authorities would be able to see a shorter travel history of TCNs, if compared to the travel history through the entry/exit stamps in the MRTD.
- With regard to overstayers, the EES proposal provides for a 5-year retention period following **the last day of the authorised stay**. As referred to in the EES impact assessment on page 29, "it is considered necessary to retain the data for a longer period for this category of TCNs. A 5-year retention period would guarantee that data are sufficiently accessible to support the identification and return process, while remaining proportionate by setting a limit to the retention period. It would also be coherent with the retention periods for the VIS and RTP".

¹¹⁸ A combined reading of recital 16, Article 10 and Article 20 of the EES legislative proposal supports this interpretation.



Figure 6 Exemplary case of data retention as per Art. 20 § 3 of the EES legislative proposal

- For law enforcement authorities: as described in section 4.4, the data retention as established in the legislative proposal would limit the usability for LEA.
- For RTP members: the data retention rules as provided for under the current EES legislative proposal would lead to a misalignment between the EES data retention period and the RTP active status (the former is set to a maximum of 181 days, while RTP is granted for a minimum of 1 year). Such a misalignment would reduce the benefits of having an RTP status, because RTP members would need to enrol in EES at least once every six months, although their RTP membership would still be active, slowing down their border crossing time. Besides the time needed for individual file creation (indicated in Table 55), the RTP member would lose time changing lanes, i.e. going to the manual control from ABC gates if the border crossing point is equipped with them.

In addition, if data continued to be retained as per the current EES legislative proposal, it would be impossible to implement the alternative RTP solution (for more information, please refer to section 3.6). This is due to the fact that according to that alternative RTP solution, EES registration would become a pre-requisite for granting RTP status and a TCN could apply for RTP status only after having been registered in the EES. However, that option would not be viable without retaining the individual data for a longer period compared to the current EES proposal, because at the time of applying for RTP status, the data in EES might already have been deleted since the individual file should, as a general rule, be kept for a maximum of 181 days.

To overcome the drawback for the RTP, an option would be to align the retention period of RTP travellers stored in EES with the length of validity of the RTP status or to 181 days, whichever is longer. For more information about the proposed options please refer to section 4.4.

The aforementioned considerations should also be analysed in light of the fact that the data generated by the entry/exit system could support law enforcement authorities in the fight against terrorism and serious crime both as an identity verification tool and as a criminal intelligence tool.¹¹⁹ For example, the data could be used to identify individuals on the basis of evidence found at a crime scene or to track the travel routes of a person suspected of having committed a crime.

For law enforcement purposes, however, it might be necessary to provide for a longer data retention period. Firstly, because investigations may take a long time to start. Secondly, because law enforcement authorities might need to go back in time to carry out their investigations.

¹¹⁹ SWD (2013) 47 final, p.22.

However, a longer data retention period for LEA might be difficult to justify, since LEA is not the primary objective of the EES. Nevertheless, it is useful to recall that already the Impact Assessment of the EES justified the need for a longer retention period for LEA and suggested a 5-year retention period.¹²⁰

As highlighted by the EES impact assessment, the negative impact on data protection derived from providing access to law enforcement authorities should be reduced by means of appropriate technical safeguards against misuse, clear legal limitations for access and data retention periods which are as short as possible.¹²¹

Main findings

With regard to RTP, the data retention period is assessed against the main objective of RTP, i.e. speeding up the border process. The Study has not identified any disadvantages derived from the data retention period as set up by the current RTP legislative proposal and therefore no alternative options have been investigated.

In contrast to RTP, the current data retention rules established by the EES legislative proposal present a series of disadvantages with regard to the border crossing process and therefore the Study has investigated alternative options to overcome certain drawbacks, mainly focusing on the decrease of the time spent at border crossing by TCNs as well as border guards and the requirements of law enforcement authorities if such an access would be granted.

- ***Alternative options in case of EES and RTP as separate systems***

This section of the Study determines alternative data retention options to what is outlined in the EES legislative proposal in case of EES and RTP are built as separate systems. For more information about this architectural option please refer to section 6.3.2.

Option A

Data retention of individual file for non-RTs: maintaining the rules of the EES legislative proposal: the individual file shall be stored in the system for a maximum of 91 days after the last exit record if there is no entry record within 90 days after that last exit record.

Data retention of entry/exit records for non-RTs: maintaining the data retention rules as laid down in the current EES legislative proposal for non-RT TCNs (for 181 days, 91 days or 5 years in the case of overstay).

Data retention of individual file and entry/exit records for RTs: in order to overcome the drawbacks derived from having to create the individual file again for RTP members as a result of Article 20 of the EES legislative proposal, this option would be to make the data retention period for RTP members in the EES as long as their RT status, or to fix it at 181 days from the last exit, whichever is longer.

For overstayers: maintain the rule as per EES legislative proposal: the individual file and the linked entry/exit records should be stored 5 years from the last day of authorised stay.

The advantages and disadvantages of this option are discussed in the table below.

¹²⁰ SWD(2013)47 final, p.29 and 30.

¹²¹ SWD(2013) 47 final, p.17.

Table 56 Advantages and disadvantages of the alignment of the EES data retention period of the TCN's individual file with the length of RTP status while maintaining the other retention rules as per the legislative proposal

	Advantages	Disadvantages
<i>Onetime</i>		<ul style="list-style-type: none"> • System complexity would be marginally higher due to data retention alignment with the length of the RTP status. • Accordingly, the EES development costs would be marginally higher. • Changes to the EES legislative proposal would be needed.
<i>Recurrent</i>	<ul style="list-style-type: none"> • The individual file of a registered traveller in the EES would be created only once during the length of the RTP status. Contrary to the legislative proposal, the biometric enrolment procedure at border crossing would take place only once. <p>This would save time for RTP members and therefore would be aligned with the primary objective of RTP, i.e. facilitation of border crossing.</p>	<ul style="list-style-type: none"> • Data inconsistencies might occur because of complex data retention logic. • The longer the retention period, the greater the impact on data protection. • There is no alignment with the alternative RTP process (although this by itself cannot justify a longer data retention period). According to the alternative RTP proposal, a TCN can apply for RTP status only after having already entered the EU territory and after having recorded entry and exit.

Main findings

The major advantage of this option is that RTP members would not have to repeat the enrolment procedure in the EES during initial or extended access to the RTP. However, such option would limit the usability for LEA, because of short retention for non-RT data.

Option B

Data retention of entry/exit record and individual file: uniform 5-year retention period

This option implies that a uniform data retention period of 5 years would be set for all categories of TCNs in the EES. This option is introduced, as 5 years is considered to be the necessary data retention period that law enforcement authorities would need to carry out their tasks, because of the average time needed to start an investigation at national level as well as because of the need to carry out searches that go back in time and also taking into consideration the data retention rules set for other databases for which LEA is permitted, such as VIS. However, LEA is not the primary objective of EES and therefore it is difficult to use it as an argument to justify a longer data retention period.

This option should be evaluated taking into account the recent case law of the Court of Justice of the EU on the validity of the EU data retention directive.¹²² Although the directive relates to a different sector (i.e. electronic communications) compared to EES and RTP, the conclusions of the Court may have a wider impact. In particular, with regard to data retention, the Court highlights

¹²² C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others 8 April 2014.

that the time period for which data are retained should be established in light of objective criteria (64-65).

The objective criteria for which longer data retention is justified are:

- i. The need to keep a travel history of the TCN for the interests of both the traveller and the border guards. For the former, it is important in order to show that s/he is a bona fide traveller. For the border guards, it is important because the questions asked can be better targeted by **looking at a TCN's travel history**.
- ii. The need to improve border management by avoiding the registering of TCN in the EES during a period of 5 years.
- iii. for LEA a longer period than that foreseen in the EES proposal would be necessary and the IA suggested that a minimum period should be fixed at 5 years.

Table 57 Advantages and disadvantages of a uniform 5-year data retention period

	Advantages	Disadvantages
<i>Onetime</i>		<ul style="list-style-type: none"> • Changes to the EES legislative proposal would be needed.
<i>Recurrent</i>	<ul style="list-style-type: none"> • The longer the data retention period, the lower the number of first-time entries and the lower the number of individual file creations in EES. This saves time at border checks. • If the data retention period in EES were long enough, it would be possible to apply on-line for RTP membership, as personal data (in particular the biometric data) from the EES file could be used for RTP purposes. • The option is the most suitable for law enforcement purposes and for the analysis of entries/exits in order to get a precise picture of travel flows. • It helps border guards to have a more comprehensive travel history of TCNs. 	<ul style="list-style-type: none"> • The option is the least favourable from a data protection perspective.

Main findings

This option provides the benefit of short border crossing times for both RTP members and non-RTP members and is best suited for law enforcement purposes; however the proportionality of a longer data retention period will have to be justified.

Option C

Data retention of individual file for non-RTs: each individual file shall be stored in the EES for a maximum of 366 days after the last exit record, if there is no entry record within the 365 days following that last exit record.

Data retention of entry/exit records for non-RTs: each entry/exit record shall be stored for a maximum of 366 days counted from the date of the exit .

For overstayers, the individual file and the linked entry/exit records should be stored 5 years from the last day of authorised stay.

Alignment of data retention of individual file and entry/exit records of RTP members: in order to overcome the drawbacks derived from having to create the individual file and the entry/exit records again for RTP members as a result of Article 20 EES, this option could include making the data retention period for RTP members as long as their RT status or fixing it at 181 days from the last exit, whichever is longer, as envisaged in Option A.

The advantages and disadvantages of this option are described in the table below.

Table 58 *Advantages and disadvantages of a 365-day data retention period for entry/exit and the individual file data*

	Advantages	Disadvantages
<i>Onetime</i>		<ul style="list-style-type: none">• System complexity would be higher due to differentiated retention periods for different data sets (entry/exit records and individual file).• Changes to the EES legislative proposal would be needed.
<i>Recurrent</i>	<ul style="list-style-type: none">• The longer the data retention period, the lower the number of first-time entries and the lower the number of individual file creations in EES. This saves time at border checks.• A short retention period for entry/exit records yields advantages from a data protection perspective.• The option is more useful for law enforcement authorities and border guards, than option A, but less advantageous compared to option B.• Non-RTP members would enjoy the same potential benefits as RTP members in terms of reduced number of enrolments in EES.	<ul style="list-style-type: none">• The longer the retention period, the greater the impact on data protection.• Misalignment with alternative RTP process. According to the alternative RTP proposal, a TCN can apply for RTP status only after having already entered the EU territory and therefore only after being already registered in EES.

Main findings

This option is more advantageous than option A because the complexity of the system would be lower. Non RTP members would have to enrol less often in the EES as compared with Option A and RTP members would not have to repeat the enrolment procedure in the EES during initial or extended access to the RTP.

Comparison

The assessment of the data retention options is summarised in the table below. The assessment shows that longer data retention periods mean shorter border crossing times and less repetition of biometric enrolment procedures; however, longer data retention periods have a greater impact on the right to personal data protection.

Table 59 Assessment of the data retention options on the basis of two separate systems

Options	EES						Evaluation criteria					
	Static data				Transactional data		Duration of the border crossing	Data protection	Implementation complexity (system architecture)	System performance	Cost	Post Entry/Exit processes
	Individual file data	Travel document data	RT-related information	Change of stay limit	Entry/Exit records	Visa-related information						
Option A	As per the current legislative proposal for non-RTP members Alignment of the EES data retention period of the individual file of TCN with the length of the RTP status for RTP members				As per the current legislative proposal (for 181 days, 91 days or 5 years in the case of overstay)		+	-	--	N	++	N
Option B	A uniform 5-year retention period						++	--	++	-	-	++
Option C	A maximum of 366 days after the last exit record, if there is no entry record within the 365 days following that last exit record				365 days or 5 years in the case of overstay		+	-	-	N	+	N

Explanation of the scoring scale:

(--) highly negative impact

(-) limited negative impact

(N) neutral impact

(+) limited positive impact

(++) highly positive impact

Main findings

Summarising the assessment of the 3 options illustrated above, the longer the data retention period the smaller the number of enrolment procedures per TCN. As a consequence, requiring TCNs to enrol less time compared to what would result if the current legislative proposal is

maintained, would shorten the overall border crossing time. At the same time, the longer the data retention period the better for law enforcement authorities. Personal data shall not be kept for longer than is necessary for the purpose for which they were collected. Thus, the decision on whether to provide access to law enforcement authorities or not, would have an impact on the data retention period to be applied in the context of EES. If law enforcement authorities would have access to EES, a data retention period of 5 years appears to strike the right balance between the right to data protection and the objectives pursued by LEA. If law enforcement authorities will not be granted a access to EES a shorter data protection period would need to be applied in order to strike the right balance between the right of TCNs to data protection and the purposes of EES, as provided by article 4 of the EES legislative proposal. For this purpose the Study brought forward a number of options identifying for each of them advantages and disadvantages.

- ***Considerations regarding data retention in the case of a single system***

This section provides considerations regarding data retention if EES and RTP are built as a single system. Such architectural option would imply that common data, would be shared for both EES and RTP purposes. For more information about this architectural option, please refer to section 6.3.3.

Implications for non-RTP members' data

The architectural option of a single system would have no implications on the retention period of non-RTP members' data, as the data would be used only for the purpose of EES.

Implications for RTP members' data

If EES and RTP were built as a single system, one option (TOM M) provides that RTP members entering the Schengen Area for the first time would not have to repeat the biometrics enrolment procedure: the individual file would already be in the system, as the file would have been created during RTP enrolment. Another option (TOM N) could be that a TCN would not have to repeat the biometric enrolment procedure to obtain RTP status, because his/her individual file would be already in the EES system – as a condition to register in the RTP and the file would have been created when s/he entered the Schengen Area.

The table below provides the considerations regarding the data retention options described in section 6.3.3 in the light of the architectural option of a single system. They constitute the initial analysis of possible options that would need to be further examined in the light of the final technical choices made.

Table 60 Considerations regarding the data retention options if EES and RTP are built as a single system

Options	EES							Considerations regarding the (data retention) options in the case of a single system
	Static data					Transactional data		
	Individual file data	Travel document data	RT-related information	Change of stay limit	Entry/Exit records	Visa-related information		
Option A	As per the current legislative proposal for non-RTP members Alignment of the EES data retention period of the individual file of TCN with the length of the RTP status for RTP members				As per the current legislative proposal (for 181 days, 91 days or 5 years in the case of overstay)		Architectural choice between two separate systems or one single system has no implications for such data retention option.	
Option B	A uniform 5-year retention period							A straightforward application of a uniform 5-year retention period would mean that entry/ exit records could be kept in the system without a corresponding individual file. This would be the case if an individual file were created during the RTP enrolment procedure. Similarly, RTP application data would be kept without a corresponding individual file, if it were created at entry. To avoid such situation, the Study suggests amending the option by keeping individual file data for the same duration as the entry/exit records or RTP application data, whichever is longer.
Option C	A maximum of 366 days after the last exit record, if there is no entry record within the 365 days following that last exit record				365 days or 5 years in the case of overstay		As above, to avoid having RTP application data without individual file data, the option should be amended. The Study suggests keeping individual file data for the same duration as the entry/exit records or RTP application data, whichever is longer.	

Main findings

The architectural choice between having two separate systems or one single system has no implications for option A, which suggests aligning the EES data retention period of the TCN's individual file with the length of the RTP status.

Option B of a uniform 5-year retention period and option C of a maximum of 366 days after the last exit record should be amended, in the case of a single system, as the individual file data should be kept for the length of entry/exit records or RTP application data, whichever is longer.

◦ **Considerations regarding coherence with VIS data retention**

This section provides considerations regarding coherence with VIS data retention, if the biometric data for VH is taken from the VIS, as shown in the table below. Article 23 of VIS regulation establishes that:

“Each application file shall be stored in the VIS for a maximum of five years, without prejudice to the deletion referred to in Articles 24 and 25 and to the keeping of records referred to in Article 34. That period shall start:

- (a) on the expiry date of the visa, if a visa has been issued;
- (b) on the new expiry date of the visa, if a visa has been extended;
- (c) on the date of the creation of the application file in the VIS, if the application has been withdrawn, closed or discontinued;
- (d) on the date of the decision of the visa authority if a visa has been refused, annulled, shortened or revoked.”¹²³

There would be no conflicts between EES and VIS data retention, as the VH will be eligible to enter the Schengen area only having a valid visa, i.e. it will be always possible to take the biometrics for his individual file from VIS for the purposes of EES.

There should be no conflicts between RTP and VIS data retention periods as well, because VH will not be able to apply for RTP without a valid visa. Even in the case of applying for RTP on the day of visa expiry, the RTP data will be retained for five years, i.e. exactly as per VIS.

Table 61 Overview of EES, RTP and VIS data retention options

	VH			VE		
	Alpha-numeric data	Biometric data	Data retention period	Alpha-numeric data	Biometric data	Data retention period
VIS	X	FI and 10 FP images	5 years from end of visa validity date	N/A	N/A	N/A

¹²³ Article 2 of Regulation (EC) No 767/2008.

EES individual file	X	Refers to VIS	<p>Option A: alignment with the length of the RTP status for RTs and as per current legislative proposal for non-RTs</p> <p>Option B: 5-year retention period</p> <p>Option C: a maximum of 366 days after the last exit record, if there is no entry</p>	X	FI and 0, 4 or 8 FP (depending on TOM)	<p>Option A: alignment with the length of the RTP status</p> <p>Option B: 5-year retention period</p> <p>Option C: a maximum of 366 days after the last exit record, if there is no entry</p>
EES entry/ exit record	X	N/A	<p>Option A: as per current legislative proposal (for 181 days, 91 days or 5 years in the case of overstay)</p> <p>Option B: 5-year retention period</p> <p>Option C: 365 days or 5 years in the case of overstay</p>	X	N/A	<p>Option A: as per current legislative proposal (for 181 days, 91 days or 5 years in the case of overstay)</p> <p>Option B: 5-year retention period</p> <p>Option C: 365 days or 5 years in the case of overstay</p>
RTP individual file	X	Refers to VIS	A maximum of five years	X	Refers to EES	A maximum of five years
RTP application	X	N/A	A maximum of five years	X	N/A	A maximum of five years

Main findings

If the biometric data for VH is taken from the VIS for the purposes of EES and RTP, there would be no conflicts between VIS data retention and the proposed options for EES and RTP data retention.

– **Law Enforcement Access (TF13)**

This TF investigates the technical consequences of giving law enforcement authorities access to EES.

Article 50 of the EES proposal provides that the first evaluation of the EES shall specifically examine the contribution the EES could make in the fight against terrorist offences and other serious criminal offences and will deal with the issue of access for law enforcement purposes to the information stored in the system, whether and, if so, under which conditions such access should be allowed, whether the retention period shall be modified and whether access to third countries shall be granted, taking into account the operation of the EES and the results of the implementation of the VIS.

In line with the data protection principles of proportionality and purpose limitation, law enforcement authorities should be able to access EES if they can prove it is necessary for the prevention, detection or investigation of terrorist offences¹²⁴ or other serious criminal offences.¹²⁵ Restricting EES access by law enforcement authorities to the aforementioned purposes is also in line with the VIS Council Decision 2008/633/JHA¹²⁶ and EURODAC Regulation No 603/2013.¹²⁷

5.4.1. Analysis of statistics concerning LEA to VIS (TF 13.1)

This sub-section analyses statistics concerning LEA to VIS. This information is relevant in the context of this Study because VIS contains alphanumeric and biometric data (i.e. facial image and 10 fingerprints) of all TCNVHs for a 5-year period and it is accessed by law enforcement authorities under strict conditions. Therefore, knowing how often and for which operations law enforcement authorities access VIS provides useful insights into the potential use of EES by law enforcement authorities.

Law enforcement authorities carry out several operations when they access VIS:

¹²⁴See definition provided in Articles 1-4 of the Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3–7.

¹²⁵See definition provided in Article 2(2) of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision OJ L 190, 18.7.2002, p. 1–20

¹²⁶ Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.8.2008, p. 129–136.

¹²⁷ Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29.6.2013, p. 1–30.

- **Search** by alphanumeric data, which determines the hits, but returns only an abstract about each hit;
- **Retrieval**, which loads the details about a specific hit in the hit list returned by the search operation;
- **Authentication by fingerprint**, which provides the outcome for 1:1 search for verification, using fingerprints;
- **Search by fingerprint**, which provides the outcome for 1:N search for identification, using fingerprints;
- **List applications in dossier**, which provides the data of group of applications for VHs.

The statistics collected cover the period from 1 September 2013 (which is the date of entry into force of the VIS Decision¹²⁸) to 31 March 2014.

During that period, 11 searches on average per day were carried out. Out of the 11 searches, there were 5 retrievals per day. Searches and authentications by fingerprints remained very limited throughout the analysed period: from September 2013 to March 2014, only 5 searches by fingerprints were carried out and there was only one authentication by fingerprints.

The graph below provides an overview of the number of searches carried out by law enforcement authorities by a selected number of countries in the course of the first quarter of 2014.

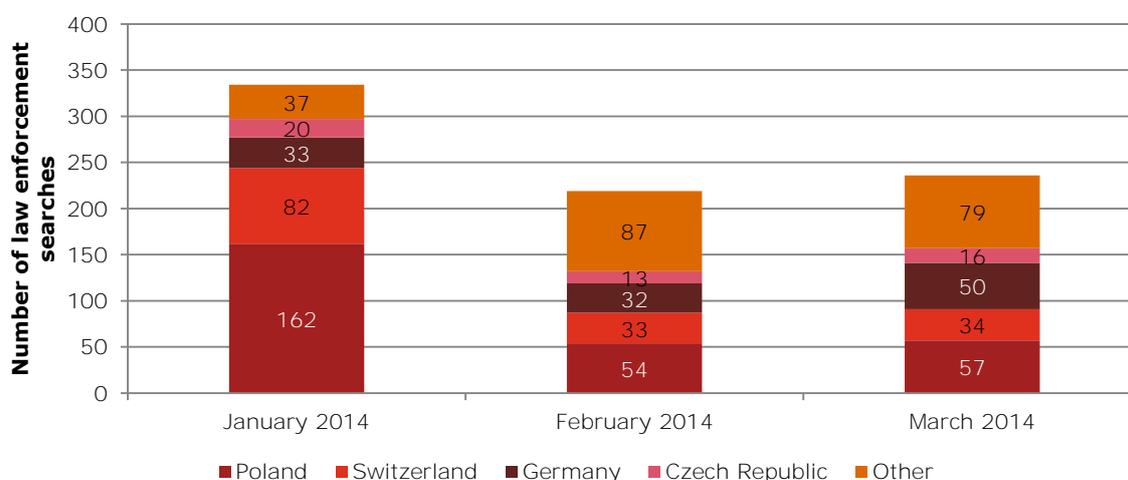


Figure 32 Number of law enforcement searches in VIS by country during the first quarter of 2014

Overall, the analysis of the available statistics shows a limited usage of VIS by law enforcement authorities, with an average of less than one access per day per country.

¹²⁸ Council Decision 2013/392/EU of 22 July 2013 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 198, 23.7.2013, p. 45–46

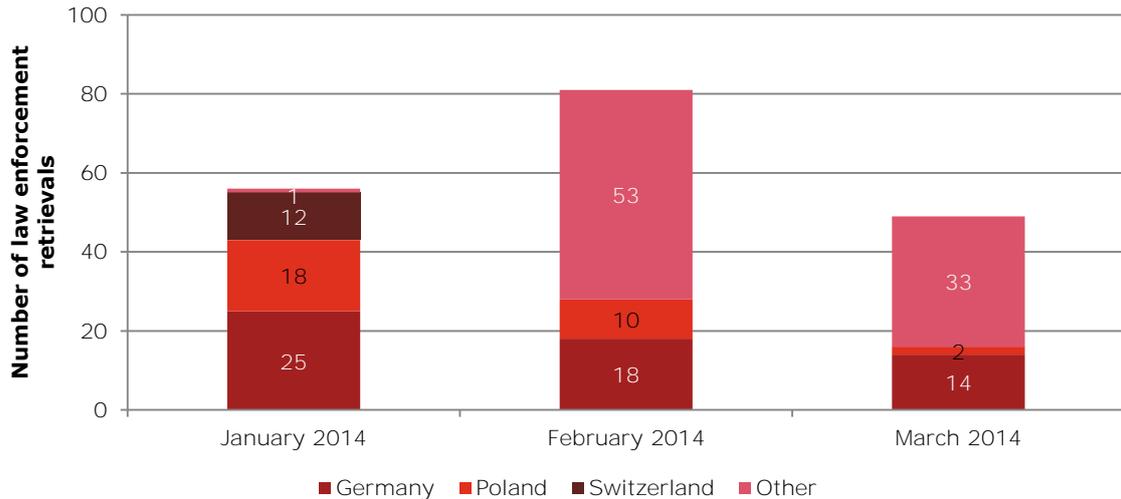


Figure 33 Number of law enforcement retrievals in VIS by country during the first quarter of 2014

Based on feedback received from MSs, the main reasons explaining the limited LEA to VIS are:

- Not all MSs may have implemented the necessary organisation and technical features to access the central VIS;
- Statistics refer to a period when the VIS did not operate at full capacity, as the worldwide roll-out will be completed by mid-2015.

Main findings

Assuming that the legal conditions for access through a national access point would remain the same for EES as they are for VIS, taking into account the above-mentioned caveats and in light of the available statistics, it is reasonable to assume that access by law enforcement authorities to EES would remain limited, as is currently the case for VIS.

5.4.2. Definition of the data required for LEA to the EES (TF 13.3)

This section of the Study examines data required for LEA to the EES taking into account the operations currently carried out by law enforcement authorities in VIS. In addition, since law enforcement authorities already access a variety of large-scale EU IT systems, including Eurodac and VIS, the Study compares the existing rules that apply for LEA to those databases and analyses to which extent similar rules could be applied to LEA to EES.

Data to carry out searches

On the one hand, in Eurodac searches can be carried out only using fingerprints¹²⁹. In addition searches by latent fingerprints is also planned to be implemented. On the other hand, searches in

¹²⁹ Articles 19 and 20 of Article 19(1) of Regulation (EU) No 603/2013 of the European Parliament and the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for

VIS can be carried out using a variety of data.¹³⁰ Enabling searches in EES by using a greater number of data compared to what is allowed in Eurodac enables law enforcement authorities to carry out a greater number and more diverse typologies of analysis compared to searches by fingerprints only. When analysed in light of EES and its objectives, the VIS model appears to be more appropriate for LEA compared to the Eurodac model since law enforcement authorities could carry out searches in EES to compute more complex searches, notably to look for travel patterns of TCNs. If the Eurodac model was applied instead, law enforcement authorities could only carry out searches by using fingerprints and only after identifying a TCN they would have access to additional data.

The figure below highlights the data that can be used by law enforcement authorities to carry out searches in VIS and compares them with the dataset currently provided for under the EES legislative proposal. Information which is used in LEA searches in the VIS is marked in black, while the dataset provided for under the EES legislative proposal are marked in grey.

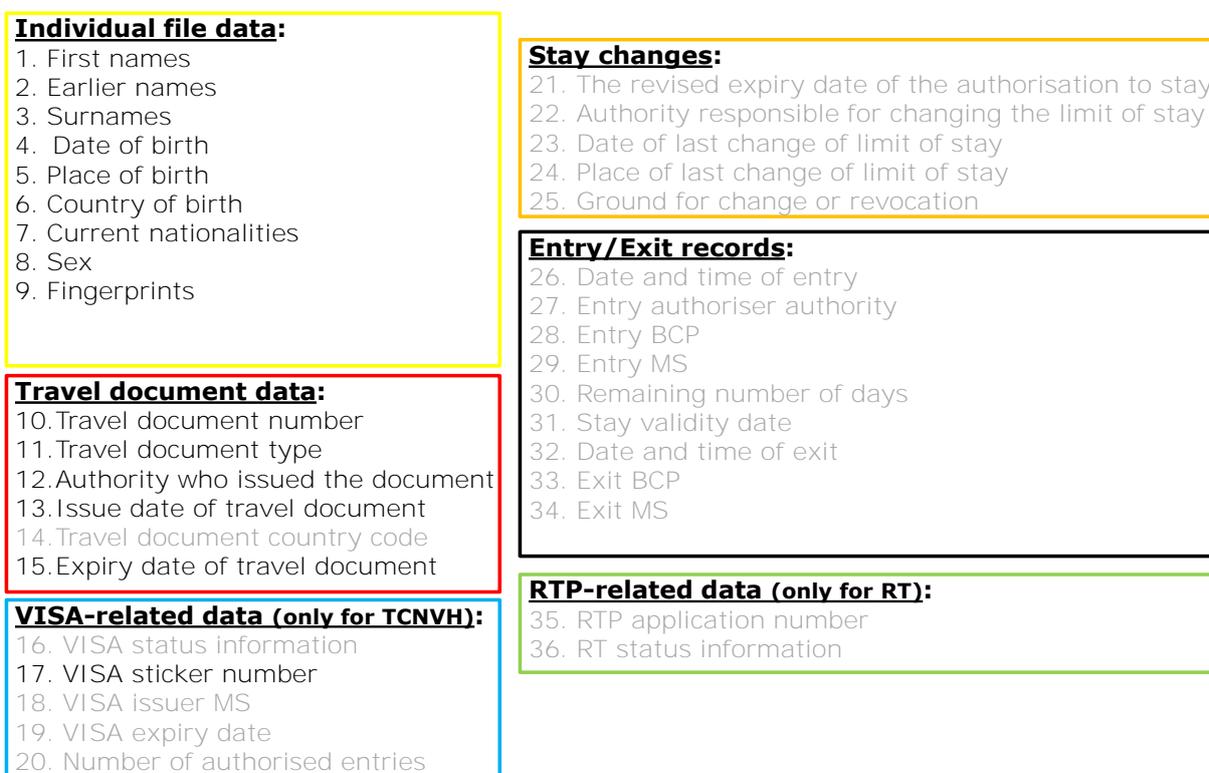


Figure 34 Information which is used in LEA searches in the VIS (marked in black) in comparison with the dataset provided for under the EES legislative proposal (marked in grey)

Figure 34, however, does not show the data which could also be used for searches for law enforcement purposes in the VIS, but is not provided for under the EES legislative proposal, such as main destination and duration of the intended stay, intended date of arrival and departure,

the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180, 29.6.2013, p. 1-30.

¹³⁰ Article 5(2) of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

intended border of first entry or transit route. The afore-mentioned information is mostly related to investigations into intended travel routes and purposes; therefore, consultation of the EES could additionally include searching with the entry/exit records linked to individual files.

<p>Individual file data:</p> <ol style="list-style-type: none"> 1. First names 2. Earlier names 3. Surnames 4. Date of birth 5. Place of birth 6. Country of birth 7. Current nationalities 8. Sex 9. Fingerprints 	<p>Stay changes:</p> <ol style="list-style-type: none"> 21. The revised expiry date of the authorisation to stay 22. Authority responsible for changing the limit of stay 23. Date of last change of limit of stay 24. Place of last change of limit of stay 25. Ground for change or revocation
<p>Travel document data:</p> <ol style="list-style-type: none"> 10. Travel document number 11. Travel document type 12. Authority who issued the document 13. Issue date of travel document 14. Travel document country code 15. Expiry date of travel document 	<p>Entry/Exit records:</p> <ol style="list-style-type: none"> 26. Date and time of entry 27. Entry authoriser authority 28. Entry BCP 29. Entry MS 30. Remaining number of days 31. Stay validity date 32. Date and time of exit 33. Exit BCP 34. Exit MS
<p>VISA-related data (only for TCNVH):</p> <ol style="list-style-type: none"> 16. VISA status information 17. VISA sticker number 18. VISA issuer MS 19. VISA expiry date 20. Number of authorised entries 	<p>RTP-related data (only for RT):</p> <ol style="list-style-type: none"> 35. RTP application number 36. RT status information

Figure 35 Proposed dataset for LEA searches (marked in black) in comparison with the dataset provided for under the EES legislative proposal (marked in grey)

With regard to the number of fingerprints, the higher the number of fingerprints enrolled the higher the relevance for law enforcement purposes because it increases the probability of finding a corresponding match. Being able to carry out a search with 10 fingerprints is the option that best meets the needs of law enforcement authorities. At the same time, law enforcement access is not the primary objective of EES, so LEA cannot be the driving factor for the choice of biometric identifier. While from an LEA point of view it would be better to access all 10 fingerprints, it is considered that accessing a lower number of fingerprints than 10 could still be of use for law enforcement purposes. Thus, law enforcement authorities should have access to the number of fingerprints that is considered necessary and sufficient to meet the primary objective of EES.

Data in the event of a hit

In the event of a hit, Article 5§ 3 of Council Decision 2008/633/JHA (VIS decision) establishes that law enforcement authorities can have access to the following additional data on top of the data used for search enlisted in Article 5 (2) of the VIS Decision 2008/633/JHA:

- (a) any other data taken from the application form;
- (b) photographs;
- (c) the data entered in respect of any visa issued, refused, annulled, revoked or extended.

Such an approach, which establishes a layered access to TCNs' data, prevents users from downloading bulk information resulting from a search. It is recommended to follow the same

approach in the context of EES as well. As a result, in addition to the data shown in Figure 35, in the event of a hit the EES could give access to all the data except RTP- related data.

RTP has the objective of facilitating the border crossing and is voluntary, thus it does not fulfil the objective of fighting against irregular migration and potentially crimes and terrorism and thus LEA should not be provided to RTP- related data. No access is therefore foreseen to the RTP for law enforcement purposes in the RTP legislative proposal.

Combinations of data for searches

After identifying the type of data that can be used, it is also necessary to establish which type of searches the system will enable. Based on feedback from MSs, the search based on any combination of data is the option that would better meet LEA needs, as it would cover the greatest amount of possible scenarios. However, enabling any kind of combination would have implications in terms of the efficacy of the EES (please refer to section 5.4.3 for further explanations) and data protection, due to the higher risk of profiling derived from unlimited search combinations.

As an alternative, the EES could enable searches via a limited number of fields as it is already the case for VIS.¹³¹

Type of access

Besides the type of searches, it is also necessary to identify how data will be accessed. For this purpose, Eurodac and VIS have been used by way of comparison since national authorities and Europol already access VIS¹³² and will be able to access Eurodac once the new Regulation¹³³ will be applicable, starting from 20 July 2015. With regard to the procedure to access the two systems the main differences are:

- In VIS, national authorities and Europol can access VIS for consultation searching via a limited set of biometric and alphanumeric data identified in Article 5(2) of the VIS Decision;
- In Eurodac, searches by national authorities and Europol are limited to the use of fingerprints.¹³⁴

The new Eurodac Regulation also includes a number of safeguards that are not in VIS. In particular, Member State's national authorities can submit a request to access Eurodac only if previous searches in national fingerprint databases, automated fingerprinting identification systems and VIS yielded no results. The Regulation also establishes that law enforcement checks may not be made in a systematic way, but only as a last resort when all the conditions for access are fulfilled. Finally, no data received from EURODAC may be shared with third countries.¹³⁵

In the context of EES both approaches could be used. The main difference entails the fact that mirroring the VIS approach would enable law enforcement authorities to carry out more

¹³¹ Article 5, OJ L 218, 13.08.2008

¹³² OJ L 218, 13.08.2008

¹³³ OJ L 180, 29.06.2013

¹³⁴ Article 20 of Regulation 603/2013 Eurodac recast

¹³⁵ Cf. Articles 20 and 27, respectively, of Regulation 603/2013 Eurodac recast

diversified searches compared to the Eurodac approach where initial access is allowed by carrying out searches only by means of fingerprints' comparisons. The advantage of following the VIS approach is that law enforcement authorities will be able to analyse travel patterns, by enquiring for example entry/exit records. If the Eurodac approach were to be followed, then once a TCN was identified in a national database no access to the EES would be allowed thereby limiting the access to EES to identification of TCNs.

Main findings

Independently from the approach chosen, access to EES by law enforcement authorities should include a number of conditions. Both the new Eurodac Regulation and the VIS Decision 2008/633/JHA provide useful input in this regard. Below we enlist key conditions that could be taken into account regarding data required for LEA to EES:

- Member States shall designate the authorities that are authorised to access the system in order to limit the number of persons authorised to access and subsequently use the data (cfr Article 5(1) new Eurodac Regulation);
- if the Eurodac approach is chosen, the comparison with fingerprints is necessary in a specific case (i.e. systematic comparisons shall not be carried out) (cfr Article 21(1)(b) of new Eurodac Regulation);
- If the VIS approach is chosen, access for consultation must be necessary in a specific case (cfr Article 5(1)(b) of the VIS Decision 2008/633/JHA);
- There are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. (cfr Article 21(1)(c) of new Eurodac Regulation and VIS Decision 2008/633/JHA Article 5(1)(c));
- Enable search only with a limited set of data that are relevant to carry out investigations related to serious crimes and activities related to terrorism (cfr Article 5(2) of the VIS Decision 2008/633/JHA or Article 20(2) of new Eurodac Regulation depending on which approach is chosen).

5.4.3. Technical consequences of LEA (TF 13.2, 13.5)

The purpose for LEA will be defined by the co-legislators in the negotiations on the EES proposal. However, it is already clear that giving law enforcement authorities access to EES could require the introduction of additional functionalities to the EES, thus slightly increasing the implementation costs.

As already described by the EES Impact Assessment on page 27, the system would be developed in such a way that only specific data sets would be accessible and/or modifiable by specific authorities.

A general access layer or standard access management tool would have to give law enforcement authorities access to specific services, namely search, retrieval, search by fingerprint and authentication by fingerprint. Like in the VIS, a search by alphanumeric and biometric data should determine the hits, whereas retrieval should enable download of the details about specific hits. Authentication by fingerprint should provide outcome for 1:1 searches and searches by fingerprint would enable 1:N searches. Law enforcement officers would submit a request to the national system, which would identify officer's role and then send the message to the central system. The

access control mechanism would check if the submitted user role is authorised to use the requested service. If the check fails, then an error message is sent back to the law enforcement officer and the flow is aborted. If the check is successful, then the ownership mechanism checks if the officer has the necessary rights to access the data. If all checks are positive, the result of the request is sent back through the national system to the officer.

Apart from an access control mechanism, appropriate technical safeguards against misuse should be implemented such as unique user identification, automatic logoff, encryption and decryption of the message, audit controls etc. User identification is a way to identify a specific user of a system, typically by name and/or number.

Automatic logoff means implementation of procedures that terminate an electronic session after a predetermined time of inactivity. The encryption and decryption of the message means converting an original message into encoded text and afterwards converting it back to original message. Audit controls mean implementation of hardware, software, and procedural mechanisms that record and examine each activity of the users of the system. However, it is important to note that the aforementioned technical safeguards would have to be implemented independently of the decision to give LEA to the EES.

More specifically, the Study identified the following additional functionalities to be taken into account when developing the EES:

- Specific search **transactions labelled as 'LEA transactions' containing specific search criteria not** subject to be used by competent authorities for border checking purposes. This would create **additional development costs. Please refer to section "Law enforcement authorities' access" of the Cost Report** for further information;
- Possible specific logging functionalities for data consultation operations carried out by law enforcement authorities;
- Complex searches such as approximate matching. This type of search (known as partial and inexact searches in the VIS) is the technique of finding strings that match a pattern approximately; it therefore has longer response times. Depending on the number of complex searches, more processing power might be needed and there could be a negative impact on network costs;
- A retention period of up to 5 years for all data would require extra processing capacity and data storage space. Contrary to what was demonstrated in section □□ for data storage where the impact on costs would be marginal, the implementation and the operation could require substantial financial amounts if the number of LEA operations was high. Please refer to section **"Law enforcement authorities' access" of the Cost Report** for further information;
- In case of choice of the 5-year retention period, 'filtering' of different combinations of data necessary for law enforcement access would increase the complexity and the costs of EES architecture (in comparison with what is necessary to achieve the primary objective of EES);
- Possibility of searching with latent / partial prints on all the fingerprints taken under the primary objective of EES (for the analysis of the possibility of searching with latents, please refer to section □□*), requiring different and possibly more expensive software etc. Please **refer to section "Law enforcement authorities' access" of the Cost Report** for further information.

Main findings

A general access layer or standard access management tool which would give law enforcement authorities access to specific services, will have technical consequences to the EES. These can be mainly summarised in the need to include access control mechanisms for the verification of identity and access rights of the officers, including appropriate technical safeguards against misuse. As a result, the system should be developed in such a way that only specific data sets would be accessible and/or modifiable by specific authorities and specific search transactions and logging functionalities should be envisaged. This can lead to additional development costs.

5.4.4. Impact of LEA on the border control process (TF 13.4)

LEA should not be the primary purpose of the EES and therefore the **border control process should not be customised around the needs derived from giving law enforcement authorities access** to the EES. Nevertheless, the Study analysed whether the introduction of LEA to EES might have an impact on the border crossing time and the organisation.

Border crossing time

Based on feedback from MSs, a bigger number of fingerprints enrolled would be primarily beneficial for law enforcement purposes. At the same time, a bigger number of fingerprints would mean that more time would be needed to collect them and this would **negatively impact the border crossing time**. Section 3.4.1 of the Study explains the impact of different biometric identification options on border crossing times.

In addition, it is important to mention that, as indicated in section 3.4.4 of the Study, the enrolment of more than 4 fingerprints would, due to specific constraints and conditions, be difficult to achieve in the following BCPs:

- Airfield with limited/ irregular non-Schengen flights;
- Small land BCPs;
- Land border crossings by train (on-board);
- Large harbours;
- Small ports;
- Sea borders crossings by ship / ferry (on-board).

Organisation

The main modifications in border crossing organisation relate to the choice of biometric identifier and the data retention period. The number of fingerprints might influence the choice of equipment, space availability and BCP organisation for enrolling TCNVEs and therefore should be further examined during the Pilot. Please refer to chapter 9 of the Study for more detailed information about options for the Pilot.

Main findings

LEA should not be the primary purpose of the EES and therefore the border control process should not be customised around LEA needs related to EES.

– Output of EES and RTP systems (TF14)

Objectives and approach

This TF analyses the feedback given to the travellers, the border guards and the carriers after verifying the remaining authorised number of days in the EES.

TF 14.1 Need to provide the traveller with information on the remaining number of days of authorised stay at entry as well as at exit (incl. impact on the infrastructure) - this TF addresses the questions of **when** (at entry or at exit, or both) and **how** (on a display, on a print-out, direct

access to the system, searching criteria to be used when querying the system, etc.) the traveller will be informed of the remaining number of days he/she is allowed to stay in the Schengen area.

TF 14.2 Need to provide the border guards and possibly carriers with information allowing the identification of VH with a single entry visa having already used their visa - the need to address the feedback to the border guard is obvious. As regards the carriers, this stems from their obligation to check at departure whether TCNVH already used their single or double entry visa. Since EES would remove the stamping of visas and passports, carriers can no longer visually check this information in the passport and visa. Carriers would need to be given access to sufficient data to meet their obligation.

- ***EES/RTP System outputs – information to be provided to the border guards***

Border guards should be able to access any data stored in the EES. On top of EES data, border guards should also have access to issued visa as well as, if applicable, RTP related data. In addition to data necessary for the entry/exit processes, border guards can sometimes also be in charge of the visa and RTP application/ enrolment process¹³⁶.

- ***EES/RTP System outputs – information to be provided to the travellers***

With the implementation of the EES, stamp(s) on visas and passports will no longer be available. As a consequence, travellers will need to be reminded about their entry and exit date to be in a position to calculate the remaining number of days of the authorised stay. Such information could be useful to the traveller, for instance for booking his flight tickets.

The Study has identified a number of options to access this information varying in terms of breadth of content and channels of access.

- > ***Information to be provided to the travellers at the borders***

On the one hand, as stated in the article 9 of the current EES legislative proposal, the automated calculator shall inform the competent authorities and the third-country national of the authorised length of stay on border entry and identify third country nationals upon exit who have overstayed. On the other hand, the legislative proposal amending the Schengen Border Code, proposes to amend Article 7 thereof by providing that – *“upon request, the border guard shall inform the third country national of the maximum number of days of authorised stay. The third country national may also request a written record containing the date and place of entry or exit.”* Currently the SBC does not impose any legal obligation on border guards to deliver an hand written paper indicating the remaining number of authorised days of stay. In light of this, there seems to be an apparent contradiction between the proposed amendment to the SBC and Article 9 of the EES proposal in the sense that Article 9 imposes an obligation to inform the TCN while the amendment to the SBC imposes it only on request of the TCN.

¹³⁶ Article 4(3) of Regulation(EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13/8/2008; Article 1 of Council Regulation (EC) No 415/2003 of 27 February 2003 on the issue of visas at the border, OJ L 64, 7/3/2003 and Articles 4 and 5 of Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, COM(2013) 97 final, 28/2/2013.

The Study assessed the impact of different technical options, analysing different locations and communication channels, going from more to less restrictive solutions in terms of compliance with data protection requirements.

Table 62 Assessment of the channels of information to be provided to the travellers at the borders

Option	Channel of information to be provided to the travellers at the borders	Location	Analysis criteria			
			Duration of the border crossing	Cost	Infrastructure	Implementation complexity
Option A	Systematic display	ABC gates	+	-	++	-
Option B	On demand print	ABC gates	-	N	-	-
Option C	Systematic display	Border guards booth and mobile equipment	++	-	+	-
Option D	On demand print	Border guards booth	-	N	-	+
Option E	Systematic print	Border guards booth	--	N	--	+
Option F	On demand oral	Border guards booth	+	++	++	++

Explanation of the scoring scale:

(--) highly negative impact

(-) limited negative impact

(N) neutral impact

(+) limited positive impact

(++) highly positive impact

Based on the above analysis, the following can be outlined:

- The display or printing of the information for TCN at the border guard's booth will request additional equipment;
- While the provided information is critical for MEV and RT, it is not relevant for TCNVH with a single or 2-entry visa. So the on-demand options should be preferred to the systematic options with the exception of the systematic display;
- The option F (on demand oral) has many positive impacts on the analysis criteria and no negative impact. Contrarily to printing and display, this option is also convenient for all types of borders.

•

• **Main findings**

To conclude, the preferred option recommended by the Study is a systematic display of at least the maximum number of days at ABC gates (option A) combined with at least one other option B, C, D, E or F. The EES legislative proposal establishes a legal obligation for border guards to inform the TCN on the authorised length of stay. On the other hand the legislative proposal amending the Schengen Border Code establishes that TCN may request a written record containing the date and place of entry or exit.¹³⁷ Article 9 of the EES legislative proposal provides that the automated

¹³⁷ COM(2013) 96 final, Article 7 paragraph 8

calculator shall inform the competent authorities and the third-country national of the authorised length of stay on border entry and identify third country nationals upon exit who have overstayed. Therefore, the systematic display of this information would require a change in the current legislative proposals to make it explicit that this information will be displayed at ABC gates or at manual gates.

> ***Information to be provided to travellers on demand within and outside borders***

This section of the Study examines information to be provided to travellers on demand within and outside borders. It addresses the questions on when (at entry or at exit, or both) and how the traveller could be informed on the remaining number of days he/she is allowed to stay in the Schengen area.

The current EES legislative proposal foresees in Article 9 as we have seen in point 5.5.2.1 that the automated calculator shall inform the traveller on of the authorised length of stay **at entry**. It also provides in Article 34 for the right of TCNs to obtain communication of the data relating to him or her recorded in the EES from any Member State¹³⁸. However, this obligation only concerns data related to him or her **already recorded in the EES** and would not cover an obligation to reply to questions on the remaining period of stay in the Schengen area at any given time.

An automatic calculator has been developed for the general public and for the Member States authorities and is currently available via a website to all travellers who would like to consult it. The calculator deals with the 90/180 day rule. In case of visa obliged third-country nationals, the length of authorised stay is clearly stated in the visa sticker and often differs from 90 days (which is the maximum that can be granted). The calculator does not support the calculation of stay against the authorised stay indicated on the visa sticker if this period is shorter than 90 days within 180 days and against the validity of the visa. On the basis of the previous entry and exit **dates the software can “only” calculate whether the third country national fulfils the general 90/180 days rule or not** and it can give projections for maximum lengths of stays in the future in the future from the intended date of entry on basis of previous entry and exit dates. Holders of short-stay (C-type) visas should therefore also check the validity of the visa and the number of days as indicated on the visa sticker.¹³⁹

The Study also identified alternative options for channels of the information to be provided to travellers. The options are described further below.

Option A (email) and option B (phone): Provide information to the travellers upon request (by email/phone) sent to the competent authorities. The scope of retrieved information should be agreed in the information request.

This option brings additional data protection risks because this requires prior authentication of the requester. Regarding phone requests, additional checks could be performed by the competent authorities to verify the identity of the requester. Regarding requests made by email, identity verification is considered to be more complex. In fact this option could be used only for those cases for which the contact details of the requesters are already known and have been collected for a specific and limited purpose compatible with this one. In addition, the option could highly

¹³⁸ Article 34. COM (2013) 95 final

¹³⁹ User manual for the short-stay “Schengen” calculator http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/docs/short_stay_schengen_calculator_user_manual_en.pdf

increase the workload for authorities and accordingly operational costs, therefore it is not recommended by the Study.

Option C (OK/NOK return message depending if one remaining day of stay left) and option D (OK/NOK return message depending on the foreseen date of return): provide minimal information to the travellers.

The granting of an internet connection to the travellers will not be done through a secured channel. As a consequence, anyone could access and query the system from anywhere without being identified and authenticated.

This option greatly increases IT security risks as well as the complexity of the system architecture.

Travellers should use their unique identifier as search criterion.

Search criteria (as defined in the MRZ)

Passport number

Code of the country which issued the travel documents

The minimum information that the query should return is an OK/NOK message depending if the traveller has at least one remaining day of stay left. Alternatively, the foreseen return-date should be entered so that only OK/NOK could be returned. It should be made clear to the travellers that OK/NOK does not mean that the person is allowed to enter as there are other entry requirements that the travellers need to comply with.

As passport is a sequential number in most of the countries, additional information could be requested in order to increase the authentication level (i.e. names, date-of-birth, data of last exit or entry).

Option E (provide information on remaining number of days + date of the limit of stay) and option F (provide information on remaining number of days + date of the limit of stay + travel document validity date): provide extended information to the travellers

To use the same search criteria as those envisaged in Option D and E. Based on this, the extended information provided to the travellers would include:

Information to be provided to the travellers

Visa validity date (for VH only)

Travel document validity date

Remaining number of days

Stay validity date (for VE, RTP and MEV only)

Table 63 Assessment of the options for the communication requests and return of information

Options	Communication	Return information	Analysis criteria
---------	---------------	--------------------	-------------------

	request		Level of service delivered to the travellers	Cost	Data protection	implementation complexity
Option A	Email request sent to the competent authorities	Remaining number of days + Date of the limit of stay	--	--	-	++
Option B	Phone request sent to the competent authorities	Remaining number of days + Date of the limit of stay	+	--	- *	++
Option C	Self Web-service	OK/NOK return message depending if one remaining day of stay left	+	-	-	-
Option D	Self Web-service	OK/NOK return message depending on the foreseen date of return	++	-	-	-
Option E	Self Web-service	Remaining number of days + Date of the limit of stay	++	-	--	-
Option F	Self Web-service	Remaining number of days + Date of the limit of stay + Travel document validity date	++	-	--	-

Explanation of the scoring scale:

(--) highly negative impact

(-) limited negative impact

(N) neutral impact

(+) limited positive impact

(++) highly positive impact

* provided that the person can be identified with certainty

Granting a direct access to the central IT system would bring additional data protection and IT security risks and would increase the complexity of the system architecture. Indeed, anybody would be able to query the application provided that he has the passport number and the issuing country (i.e. especially the case when a passport is stolen). Additional security measures should be implemented in order to mitigate those risks, such as:

- Implement an access through a dedicated interface to a replicated server with a minimum set of duplicated information;
- Ask an additional piece of information which is not on the passport (e.g. place of last exit).

•

• **Main findings**

Option A and B are not recommended by the Study because of high operational costs of relevant authorities. In case **it is considered that TCN will know their own entry and exit dates and that the calculator is made available to them**, granting a direct access to TCN (options C, D, E and F) could be also avoided given the associated negative impacts.

- **EES and RTP system(s) outputs – information to be provided to the carriers**

Under Article 26 of the Schengen Convention¹⁴⁰, carriers are obliged to ensure that an alien is in possession of the travel documents required for entry into the territories of the MS. They are not obliged to check the stamps in the passport of visa holders or non-visa holders to ensure that the aliens they transport still have the right to enter the Union as regards the authorised period of stay. However they do check in the case of a single entry visa holder that a stamp has not been entered in the passport in the page facing the one on which the visa is affixed to ensure that it is still valid.

Annex V Part A of the Schengen Borders Code further provides that “if a third country national who has been refused entry is brought to the border by a carrier, the authority responsible locally shall:

- a) order the carrier to take charge of the third country national and transport him or her without delay to the third country from which he or she was brought, to the third country which issued the document authorising him or her to cross the border, or to any third country where he or she is guaranteed admittance, or to find means of onward transportation in accordance with Article 26 of the Schengen Convention and Council Directive 2001/51/EC of 28 June supplementing the provisions of Article 26 of the Convention implementing the Schengen agreement of 14 June 1985¹⁴¹.”

With the adoption of the EES system, the stamp(s) will no longer be available. Therefore, alternative solutions could be considered in order to enable carriers to comply with their obligations to establish whether a single-entry visa or MEV has already been used by the traveller.

In light of the above considerations a number of potential options that could be taken in order to help carriers meet their control obligations, have been listed.

Option A: Relieve carriers from their obligation to verify whether the single-entry visa or MEV has already been used by the travellers. This option would reduce the number of actors accessing the

¹⁴⁰ Article 26 of the Schengen Convention provides as follows:

“1. The contracting parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967, to incorporate the following rules into their national law:

a) If aliens are refused access into the territory of one of the Contracting Parties, the carrier which brought them to the external border by air, sea or land shall be obliged immediately to assume responsibility for them again. At the request of the border surveillance authorities the carrier shall be obliged to return the aliens to the third State from which they were transported and or to the third State which issued the travel document on which they travelled or to any other third State to which they are certain to be admitted.

b) The carrier shall be obliged to take all the necessary measures to ensure that an alien carried by air or sea is in possession of the travel documents required for entry into the territories of the Contracting Parties.

2. The Contracting Parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967, and in accordance with their constitutional law, to impose penalties on carriers which transport aliens who do not possess the necessary travel documents by air or sea from a third State to their territories.

3. Paragraphs 1(b) and 2 shall also apply to international carriers transporting groups overland by coach, with the exception of border traffic.

¹⁴¹ OJ L 187, 10.7.2001 p. 45.

personal data of travellers. This solution is considered to be less restrictive in terms of data protection compliance as it would not require access to personal data.

Such an option would in principle not require a modification of the current carriers' liability legislation. Carriers are only legally obliged to ensure that an alien is in possession of the travel documents required for entry into the territories of the MS. Since the stamp in the visa will not be longer there they cannot be required to check it. On the other hand they will remain obliged to assume responsibility for refused aliens.

Option B: Provide a restricted and secured access (please refer to section 4.4 for further information) to carriers

This option would enable them to fulfil their current obligations. Carriers could query the EES using the unique identifier of the primary key of the travellers, i.e. passport number and issuer country code taken from the MRZ.

Search criteria (as defined in the MRZ)

Passport number

Issuer country code

In order to be compliant with data minimisation principles, the result of the query should return exclusively an OK/NOK reply on the validity of the travel document. Alternatively, the foreseen return-date should be entered so that only OK/NOK could be returned.

This option would require an amendment of the EES legislative proposal.

As an illustration, Australia's ETA system allows users to perform a fast and simple check to verify whether a passenger has a valid visa for Australia. This ETA system is available worldwide to travel agents and airlines through the SITA communications network. Airlines must have access to a SITA communications link before they can communicate with the ETA system.

Option C: Extend carriers' obligation to check remaining authorised days of stay

This option entails the extension of carriers' obligations by including checks on the remaining authorised days of stay, taking into account the overall duration of the stay and the return date.

If this option were to be retained, the information that carriers may access would include:

Information to be accessed by the carriers

Visa type (Single, MEV)

Visa validity used (for VH only)

Travel document validity date

Remaining number of days

Stay validity date (for VE, RTP and MEV only)

- **Main findings**

Option C is the one with the greatest legal implications both in terms of impact on the legislative proposal and on data protection compliance. It would put on carriers the obligation to check the remaining authorised period of stay which is not within their obligations under Article 26 of the Schengen Convention.

Indeed Article 27 of the current EES legislative proposal explicitly excludes the possibility of transferring EES data or of making them available to third countries, international organisations or any private party. By way of derogation from this rule specific data may be transferred to a third country or an international organisation if necessary in individual cases and under strict conditions (Article 27(2)). In case access is granted to carriers, under either options B or C as a minimum, this article should be modified.

– ***Data protection considerations on the options brought forward by the Study***

The different options analysed in the aforementioned section should be assessed against data protection principles adopted or incorporated within the legal framework of the EU, notably with regard to:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;¹⁴²
- Regulation (EC) No. 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions bodies and on the free movement of such data.¹⁴³

In addition, since the Study looked into the possibility of providing EES access to law enforcement authorities, the following source of law is also relevant:

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.¹⁴⁴

◦ ***Minimum dataset***

According to Article 6 (c) of Directive 95/46/EC, data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The EES legislative proposal lists a certain number of data items to be inserted in the individual file and in the entry exit record, both for TCNVHs (art. 11) and for TCNVEs (art.12). Similarly, the RTP legislative proposal provides for the insertion of a certain number of data items in the application file as foreseen under Articles 25 and 26 of the proposal.

The Study investigated to which extent these data are “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed” as provided for by

¹⁴² OJ L 281, 23/11/1995, p. 31–50

¹⁴³ OJ L 8, 12/01/2001, p. 1–22

¹⁴⁴ OJ L 350, 30/12/2008, p. 60–71

article 6 (c) of Directive 45/96 and whether less intrusive options can be implemented to achieve the policy objectives.

In light of this, the Study identified the minimum dataset necessary to achieve the objectives as spelled out in the EES and RTP legislative proposals.

Such an option would guarantee a certain degree of data minimisation, limiting the collection of data to only what is strictly necessary for the purpose of the systems (for further details please refer to chapter 5.2).

The Study also investigated the possibility of including optional data that are currently collected by Member States in the national EES. These data are not currently envisaged in the legislative proposal and since they are not considered necessary to achieve the EES objectives, their inclusion would go against the principle of data minimisation.

◦ ***Further processing of data***

According to Article 6(b) of Directive 95/46, data must not be further processed in a way incompatible with the purposes for which they were collected in the first place. As an alternative to collect a second time the data related to the visa that are necessary to provide the link with the VIS, the Study identified the need for further use of a limited number of data items initially collected in the context of VIS, notably:

- The visa sticker number: which represents the unique link in VIS to identify on which grounds the entry into the Schengen territory is granted;
- Authorised period of stay, because visa expiry date does not always correspond to the authorised period of stay;
- The number of permitted entries: whether the visa provides for a single, two or multiple entries.

According to EU legislation, further processing of data can be envisaged only if the purpose for which data are further processed is compatible with the initial purpose and there is a reasonable expectation of the data subject as to the further use of the data collected. As regards the first requirement, the further processing of the aforementioned VIS data is considered to be compatible with the original purpose for which VIS data were collected, since both VIS and EES are instruments supporting the management of external borders and more specifically instruments that collect data to grant TCNs access to the Schengen area. With regard to the second requirement, the Study recommends including necessary steps to meet the reasonable expectations of the data subjects as to the further use of the visa sticker number and the number of permitted entries at the time of collection. This could be achieved for example by informing the data subject at the time of collection of the data. If such an option would be retained it would require a modification of the VIS legislation.

◦ ***Balance between system integration and data protection***

The analysis brought forward by this Study highlighted the need, on the one hand, to create the necessary conditions to reduce - to the extent possible - process and data duplication. On the other hand, it stressed the need to adopt a solution that is fully compliant with data protection requirements.

The need to limit data duplication is derived from the fact that EES and RTP share certain steps in the border process management and the need to process a common set of data. While it may appear that these two systems can exist in parallel and independently of each other, they are in fact closely related. A person that applies for RTP status would need at some point to cross the EU Schengen Border, and when doing so this individual would need to resubmit for EES a subset of data that were already submitted in the context of the RTP. In another scenario a person who has already crossed the EU Schengen Border and who would apply for RTP would have to re-submit data (and in particular the biometrics collected in the EES).

This duplication seems to be mainly related to the principle of purpose limitation according to which data collected for a specific purpose should not be further processed for incompatible purposes. This would for example be the case if data collected to grant RTP status were then used for commercial purposes. In line with data protection legislation, in order to be able to legally have a common database storing the common data needed for both systems, it is necessary to show that this information would be used for the same purpose or at least for purposes that are compatible with each other.

The collection and processing of data in the context of EES and RTP should be interpreted as serving the common purpose of an integrated border management, characterised by different phases going from data collection and processing to storage.

By looking at the systems as different modules part of an integrated border management process, it would be possible to envisage a solution whereby a limited set of common core data items are shared and can be used for the same purpose, be it for registration, storage or verification.

This approach would require extensive modifications to the Smart Borders Package as it stands today and it is not the purpose of this Study to review the scope and objectives of the two legislative proposals. Rather, the objective is to identify possible options for a pilot.

- ***Law enforcement access***

If the option to provide access to law enforcement authorities is retained, the Study recommends ensuring that data are handled only by the designated competent authorities to the extent necessary for the performance of their tasks. To reach this objective, access to the data should be **strictly defined based on the “need to know” principle**. Differentiated logging in according to the user’s role should therefore be planned, thereby entailing that accesses to the systems, or part of the systems, are managed according to the user’s profile and role.

In order to guarantee secure processing, the Study also recommends keeping a record of who has requested access for what purpose to which data and ensuring a regular review of those logs. The logging messages should be limited to the structure and the meta-data (which type of data – a first name for example) and thus would not contain the exchanged data.

- ***Impact on legislative proposals and relevant legislation in force***

The majority of the deviations from the legislative proposal which are related to data have been already enlisted in section 3.8. Thus this table only enlist the additional deviations from the legislative proposals that have been discussed into details in the Data chapter.

Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of TCN crossing the external borders of the Member States of the European Union¹⁴⁵.

Option	Instrument and articles	Impact ¹⁴⁶	Impact on legislative proposal
LEA	EES: new specific articles to be drafted	Limited	The EES legislative proposal establishes that the access to EES by law enforcement authorities should be evaluated two years after the system is brought into operation. Therefore, enabling LEA from the very beginning would require a modification of the legislative proposal.
Access provided to carriers	EES: Chapter III; 27; new provisions	Limited	The EES legislative proposal does not foresee to provide access to the system to carriers. If this option would be retained, then the EES legislative proposal would need to be modified.
Checks on remaining number of days by carriers (option C)	EES: no Article exists; Schengen Convention: 26	Extensive	Currently the EES legislative proposal does not establish whether and how carriers should have access to information related to the entry and exit records of TCNs and which type of checks they should carry out. If carriers would be requested to check the remaining number of stays, then it would require a change to the relevant legislation, notably Article 26 of the Schengen Convention.
Information to travellers	Proposal to amend the SBC: (new) Article 7 paragraph 8 EES: 9	Limited	Currently the legislative proposal amending the SBC establishes as only obligation for border guards to inform third country nationals on their request about the maximum number of days they are still allowed to stay within the Schengen area. If information will be systematically displayed, then a change to this legislative proposal is requested. However, the EES proposal in Article 9 foresees that the calculator shall inform the competent authorities and the TCN of the authorised length of stay on border entry.
Data retention	EES: 20	Limited	Currently the EES legislative proposal establishes a general data retention period of 181 days, with exception of 91 days (if the TCNs has not accessed the EU territory during the previous 90 days) and a data retention period of 5 years for overstayers. If alternative rules to the data retention period will be chosen instead, then the EES legislative proposal would need to

¹⁴⁵ COM (2013) 95 final.

¹⁴⁶ **Limited impact:** only one legislative proposal of the Smart Borders Package is impacted **Extensive impact:** at least two legislative proposals are impacted **Very extensive impact:** at least one legislative proposal and at least one piece of current are impacted.

be modified.

Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme.¹⁴⁷

Option	Instrument and articles	Impact¹⁴⁸	Impact on legislative proposal
RTP 10 fingerprints	RTP: 8	Limited	Currently, the RTP legislative proposal provides for the enrolment and processing of four fingerprints. Any modification to this number would require an amendment to the RTP legislative proposal.

¹⁴⁷ COM (2013) 97.

¹⁴⁸ **Limited impact:** only one legislative proposal of the Smart Borders Package is impacted **Extensive impact:** at least two legislative proposals are impacted **Very extensive impact:** at least one legislative proposal and at least one piece of current legislation are impacted.

– Summary

The table highlights when options are to be included in the **pilot**, when they require **further Study** or when it a **policy choice** has to be made.

Table 64 Summary of the options /findings

Subject	Options / findings	EES	RTP	Category	Comments
Minimum data set	Dataset as outlined in the RTP legislative proposal.	N/A	√	Policy choice	The Study identified that the RTP dataset as per the legislative proposal is sufficient to meet RTP objectives . However the minimum dataset considered necessary to fulfil the objective of the EES could be reduced to 26 data from 36 which is defined in the EES legislative proposal.
	While the EES legislative proposal suggests storing a set of 36 data, the EES minimum dataset considered necessary to fulfil the objective of the EES while maximising automation is composed of 26 data grouped as follows: <ul style="list-style-type: none"> • Individual file data (first names, surnames, date of birth, current nationalities, sex and fingerprints (facial image)); • Travel document data (travel document number, travel document type, travel document country code); • Visa-related data (visa sticker number, visa expiry date, number of authorised entries, authorised period of stay); • Stay changes data (the revised expiry date of the authorisation to stay, authority responsible for changing the limit to stay, date of change of limit of stay, place of change of limit of stay, ground for change or revocation); • Entry / exit records (date and time of entry, entry authoriser authority, entry BCP, date and time of exit, exit BCP); • RTP-related data (RTP application number, RT status information). 	√	N/A	Policy choice	
Data management models	Distributed model: implemented as in the VIS, i.e.: <ul style="list-style-type: none"> • Duplicating the individual file data per each entry/ exit record in case of the EES. • Duplicating the individual file 	√	√	Further study	The options should be further analysed and evaluated, once the

	data per each application in case of the RTP.				architectural options would be determined.
	<i>Federated model</i> : if an update of an individual file data field is needed, the update is recorded, however the former record is retained.	√	√	Further study	
Data retention period	Data retention as outlined in the RTP legislative proposal.	N/A	√	Policy choice	The Study has not identified any disadvantages derived from the data retention period as set up by the RTP legislative proposal.
	Option A - Data retention of entry/exit records: maintaining the data retention rules as laid down in the current EES legislative proposal for non-RT TCNs (for 181 days, 91 days or 5 years in the case of overstay) Data retention of individual file and entry/exit records of RTP members: the data retention period for RTP members as long as their RT status, or 181 days from the last exit, whichever is longer.	√	N/A	Policy choice	Data retention rules established by the EES legislative proposal present a series of disadvantages. The choice of the option is the policy decision on the balance between data protection and border crossing facilitation.
	Option B - Data retention of EES records is a uniform 5 year retention period	√	N/A	Policy choice	
	Option C - Data retention of entry/exit records: each entry/exit record shall be stored for a maximum of 365 days or 5 years in the case of overstay. Data retention of individual file: each individual file shall be stored in the EES for a maximum of 366 days after the last exit record, if there is no entry record within the 365 days following that last exit record.	√	N/A	Policy choice	
Provide access to law enforcement authorities	Option A - Provide access to law enforcement authorities, based on the VIS model. National authorities and Europol could access EES for consultation searching via a limited set of biometric and alphanumeric data.	√	N/A	Policy choice	The Study does not take any stand on one preferred option.

	<p>Option B - Provide access to law enforcement authorities, based on the Eurodac model. Searches by national authorities and Europol would be limited to the use of fingerprints.</p>	√	N/A	Policy choice	
	<p>Option C - No access provided to law enforcement authorities.</p>	√	N/A	Policy choice	
<p>Information to be provided to the travellers at the border</p>	<p>Information to be provided to the travellers at the border:</p> <p><i>Option A</i> -systematic display at ABC gates</p> <p><i>Option B</i> - on demand print at ABC gates</p> <p><i>Option C</i>- systematic display at border guards booth and mobile equipment</p> <p><i>Option D</i> - on demand print at border guards booth</p> <p><i>Option E</i>- systematic display at border guards booth</p> <p><i>Option F</i> - on demand oral at border guards booth</p>	√	√	Policy choice	<p>Preferred option:</p> <p>-Systematic display of at least the maximum number of days at ABC gates (option A) combined with at least another option.</p>
<p>Information to be provided to the travellers on demand within and outside borders</p>	<p>Information to be provided to the travellers on demand within and outside borders. An automatic calculator has been developed for the general public and for the Member States authorities and is currently available via a website to all travellers who would like to consult it. However the Study has identified the following alternatives:</p> <p><i>Option A</i> -SMS</p> <p><i>Option B</i> - e-mail (data protection risk)</p> <p><i>Options C, D, E, F</i> - self-web service + additional security measures to mitigate risks.</p>	√	√	Further study	<p>Preferred option:</p> <p>- Further use of automatic calculator.</p>
<p>Information to be provided to</p>	<p>Information to be provided to the carriers :</p>	√	√	Pilot	<p>The Study does not take any stand on one</p>

<p>the carriers</p>	<p><i>Option A</i> - relieve carriers from their obligation to verify whether the single-entry visa or MEV has already been used by the travellers</p> <p><i>Option B</i> - provide a restricted and secured access to carriers</p> <p><i>Option C</i> - extend carriers' obligations to check entry requirements</p>				<p>preferred option</p>
----------------------------	---	--	--	--	-------------------------

2. Architecture

Objectives

This section of the Study aims to provide a qualitative overview of the main architectural possibilities for the EES and the RTP and of potential impacts on related applications such as the **VIS and the Member States' national systems connecting to it, including the entry-exit systems** already in operation in some Member States. The main focus is on the applications domain, but consideration will also be given to the business and data domains, which are covered in more detail in Border Control Processes chapter (section 3.2) and in the Data chapter (sections 5.2 and 5.5). However, this section should not in any way be considered as an architecture requirements specification, which would aim to provide a quantitative overview of the solution.

This section provides an analysis of architectural design options for the EES and the RTP in order to identify possible synergies among these two systems (EES and RTP), and other existing large scale IT systems. The communication from the EC to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs¹⁴⁹ **states that "Synergy" encompasses technical, economical and organisational elements**. Therefore, the aim will be to analyse the potential synergies of the various architectural options from a technical, economical and organisational perspective.

The following Thematic files are covered by this section:

- EES and RTP: single or separate systems (TF 15);
- EES, RTP and VIS: independent or integrated (TF 16);
- Interaction with other IT systems (TF 17);
- Re-utilisation and integration of existing national systems (TF 18);

Minimising the various databases to be searched or verified by creating a trust chain based on a single trustable relation (TF 9.4).

Approach

Based on the analysis of the proposed business processes, the relevant actors are identified in the various architectural options for the EES and the RTP, including human and computer actors. An analysis of the needs and capabilities of such actors helps in defining the high level business requirements and general architectural principles. Also, by linking the general EES and RTP process descriptions and flows to the architecture, all relevant EES and RTP business services are identified with certainty, which allows the definition of the architectural building blocks.

Once the building blocks have been outlined, the various options for the logical target architecture can be examined. The options are assessed based on technical, economical and organisational aspects (such as maintenance complexity, operational complexity, availability and information security), but the final assessment is done according to specific criteria. The main specific criteria for architecture-related TFs are:

- Cost;
- Data protection;
- Complexity of implementation.

¹⁴⁹ COM (2005)597

These criteria are found to have the highest importance for the assessment of the architectural options, as they mostly reflect the needs, expectations and considerations of the Member States' authorities, TCNs and other stakeholders. Duration of the border crossing is also considered to be highly important, yet it is assumed to be a requirement for all architectural options rather than an assessment criterion.

The section is structured in the following way:

- **Context** - provides an overview of architectural baseline, i.e. presents the needs, link to EES and RTP processes, high level requirements, architectural assumptions and architectural building blocks;
- **General architecture** – describes general architectural artefacts which are independent of the choices that are described in the different TFs;
- **EES and RTP: 1 or 2 systems** – examines advantages and disadvantages of EES and RTP integration options;
- **EES, RTP and VIS: independent or integrated** – discusses advantages and disadvantages of integration with VIS;
- **Interaction with other IT systems** – provides an overview of advantages and disadvantages of interaction with other IT systems;
- **Reuse of existing systems** – propose the interface that will allow existing national systems to integrate into the EES architecture.

– **Context**

◦ **Expectations, needs and capabilities**

The architectural baseline of the EES and the RTP is first of all determined by the business needs and capabilities of its prospective users and related actors. This section provides an overview of the actors falling within the scope of the target architecture. System actors are considered as users who will interact with EES and RTP, so they are classified into human and computer actors.

There are two main groups of human actors, namely TCNs and MS authorities (LEA access is a special case and is discussed in detail in section 6.1, while carrier access is described in section 6.2). Both of those groups, TCNs and MS authorities, are involved in business activities falling within the scope of the target architecture, so their expectations and needs are the key drivers underlying RTP and EES options. The following expectations, needs and concerns, are assumed, among others:

- **TCNs:**
 - short border crossing procedures, including non-duplication of procedures such as capturing of fingerprints;
 - data protection,;
 - effective and timely exceptions handling;
 - no erroneous decisions.

- **Member States' Authorities:**
 - short border crossing procedures;
 - effective border control, which would detect irregular immigrants, passport fraud and other kinds of violations;
 - synergies with existing systems;
 - smooth operations, including timely procedures;
 - effective exceptions handling;
 - data protection.

The following main computer actors were identified:

- *EES*;
- *RTP*;
- *VIS*;
- *SIS II*;
- *National end-user systems*;
- *National databases*;
- *INTERPOL*.

Table 65 Role of key human actors falling within the scope of the target architecture

Activity	TCN		Member States				
	TCNVE	TCNVH	Consulate / dedicated services responsible for RTP enrolment ¹⁵⁰	Authorities responsible for carrying out checks at external borders	Authorities responsible for carrying out checks within the national territories	Immigration authorities	Law enforcement authorities
EES check and registration at entry / exit	✓	✓		✓	✓	✓	✓
RTP application/enrolment	✓	✓	✓			✓	
RTP entry / exit	✓	✓		✓	✓	✓	

¹⁵⁰ In the case the RTP enrolment is performed at the consulate

Computer actors that represent capabilities within the scope of the target architecture are listed in the table below, along with their roles in EES and RTP related activities.

Table 66 Role of key computer actors falling within the scope of the target architecture

Activity	EES	RTP	VIS	SIS II	National end-user systems	National databases	INTERPOL
EES check and registration at entry	✓		✓	✓	✓	✓	✓*
EES check and registration at exit	✓		✓*	✓*	✓	✓	
RTP application/ enrolment		✓	✓	✓	✓	✓	✓*
RTP entry	✓	✓	✓	✓	✓	✓	
RTP exit	✓	✓	✓*	✓*	✓	✓	
Visa application	✓	✓	✓	✓	✓	✓	✓*
Stay duration information	✓*						

* - not mandatory

o **Link to the EES and RTP processes**

To clearly define the scope for the architecture and ensure an integrated view on the EES and RTP, the general process descriptions and flows (see sections 3.2 and 3.3) will be analysed in terms of their relevance to the architecture; the business services which will implement them will also be described. Where relevant, a link to the section where this architectural artefact is discussed is also provided.

> **EES process flows**

The flows and the different process steps of the EES are taken from section 3.2 and their potential impact on the architecture for the EES and the RTP is discussed below.

The process flows for entry and exit are reproduced below.

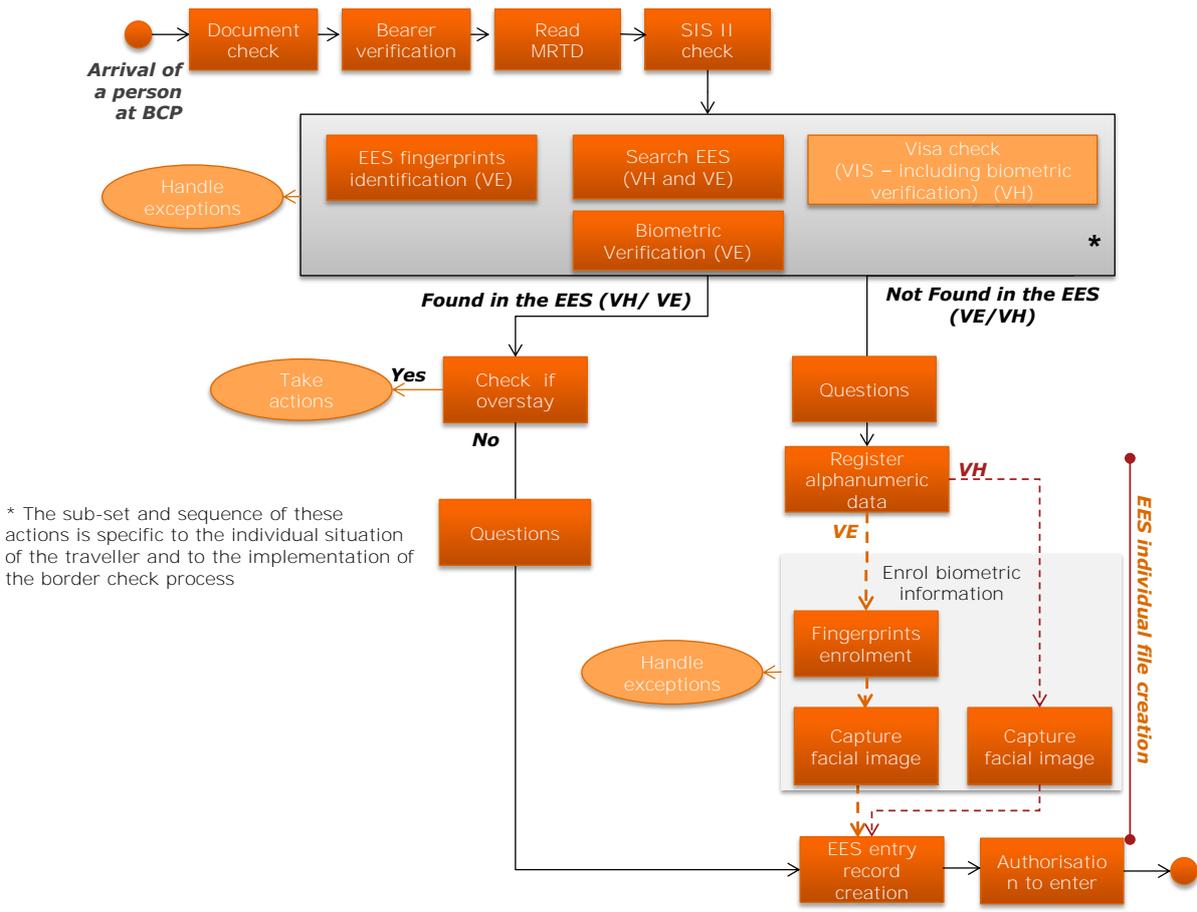


Figure 36 EES – check and registration process flow at entry

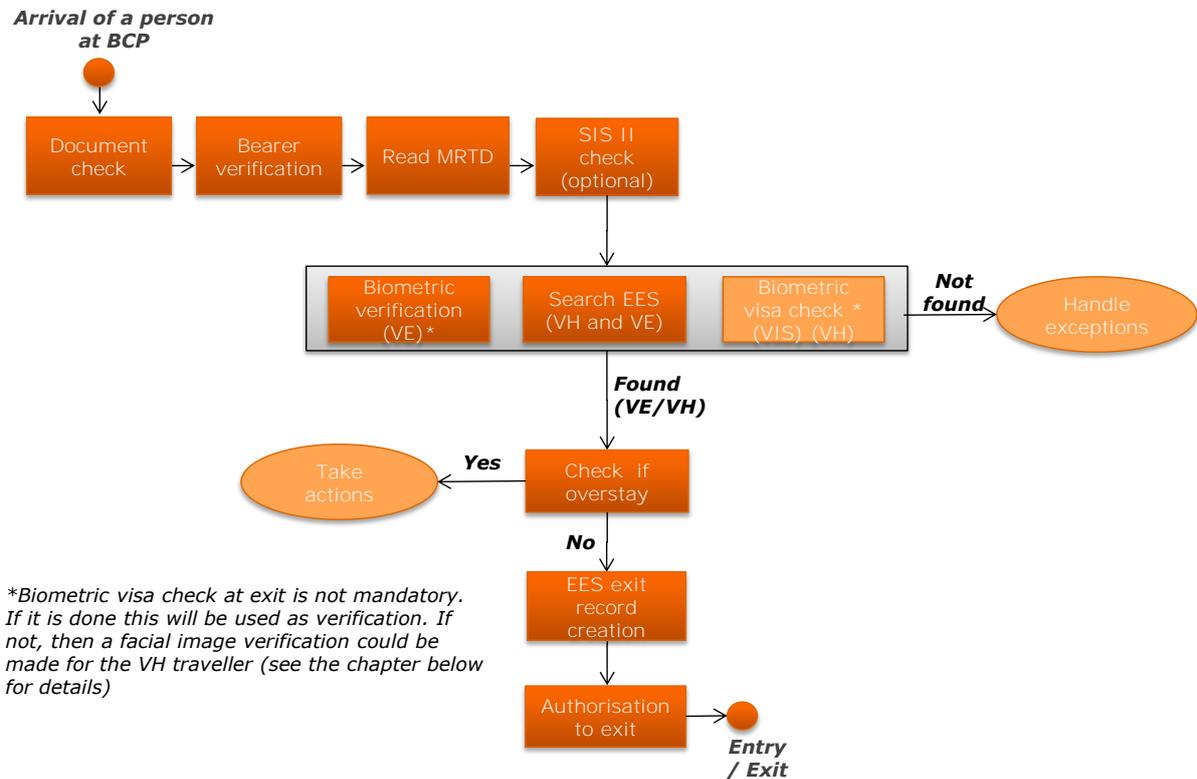


Figure 37 EES – check and registration process flow at exit

Which translate to the following process steps:

Table 67 Process steps for EES and their impact on the architecture

	In scope architecture	Comment
Document check	✗	The verification of the validity of the travel documents, including the Passive Authentication (PA) and the discretionary Active Authentication (AA) are out of scope of this architecture study and their implementation is the sole responsibility of the Member States.
Bearer verification	✗	The verification of whether the holder of the MRTD is its lawful owner is out of scope of Architecture chapter, because it is a functionality covered by border control equipment.
SIS II (and other databases)	✓	The impact on the architecture of the consultation of SIS II and other relevant databases is discussed in section 6.5.2.
Visa check (VIS)	✓	Visas will be checked against the VIS in the same manner as they are today. The possible synergies with EES and RTP will be analysed in section 6.4.1.
Questions	✗	The questions that are asked by the border guard to the TCN are out of scope for the target architecture.
EES fingerprint identification	✓	Fingerprint identification is performed using an AFIS (possibly the BMS) which is discussed in section 6.4.5.
EES search	✓	Search is one of the services to be provided by the EES (see Table 68).
EES biometric verification	✓	Biometric verification is one of the services to be provided by the EES (see Table 68).
EES individual file creation	✓	The EES individual file creation is in scope for the architecture.
EES entry/exit record creation	✓	The EES registration is in scope for the architecture.
Authorisation to enter/exit	✓	The authorisation for entry/exit will entail the creation of a corresponding entry/exit record in the EES.
Second line/	✗	Second line activities include more detailed searches and

In scope architecture	Comment
Internal actions	therefore bring their requirements on the architecture. In fact, queries on a high number of criteria combinations and inexact searches can prove to be very taxing systems using conventional databases.
Internal checks	 The EES will be consulted during the checks in the national territories.

The table below describes a possible EES service catalogue, which is based on the EES process analysis provided in section 3.2 of the Study.

Table 68 Possible EES service catalogue

Service	Description of the service
Entry / Exit registration	<p>The entry registration service enables the authority responsible for carrying out checks at external borders and within the national territories to register the entry, including the person’s data, the document data (MRZ) and the visa related data into the EES.</p> <p>The exit registration service enables the authority to register the exit from the Schengen area into the EES.</p>
Biometrics enrolment – registration of biographic and biometric data	The authority can register the person’s alphanumeric and biometric data.
Identification	At first entry the authority can perform an 1:N search using FP, or 1:few search using FI, for checking that no duplication exist.
Biometric verification	The authority checks the EES to verify that the bearer of the MRTD is the same person arriving at an entry or exit as the person registered upon the first entry.
Search and retrieval	<p>The authorities can search the EES, select records based on search criteria of the TCN, and then retrieve the information needed to fulfil the border checking tasks (first and second lines).</p> <p>Depending on the choice concerning the possible share of some of RTP data, this could also consist in retrieving from the RTP the limited subset of information necessary and sufficient to support the border checking activities</p> <p>This service also encapsulates the VIS services available to border check authorities (first and second lines). The possible interrogation of the RTP or of VIS services <u>will be hidden from the MS by the NUI, as it will provide a uniform query interface that abstracts away where certain data are kept</u>. The synergies between the VIS and RTP are described in more detail in section 6.4.1.</p>

<i>Service</i>	<i>Description of the service</i>
Stay Duration calculator	The authority can calculate the authorised stay duration for a TCN and based on these results detect if the TCN has not stayed 90 days or more over the last 180-day period.
Reporting / statistics	The authorities can create, deploy, and manage e.g. statistical reports about overstayers and TCNs' entries and exits.
Access Rights Management	Access Right Management services will provide differentiated access to remote directories and authentication mechanisms for different authorities.
Logging	The logging service would retain information on all activities performed by different authorities in the EES.
Monitoring	The service would enable the performance monitoring of the EES hardware and software services, as well as applications.

> *RTP process flows*

The different steps of the RTP process are taken from sections 3.3.2 (application / enrolment) and 3.3.3 (entry / exit) and their impact on the architecture for EES / RTP is described below.

Table 69 *Process steps for RTP and their impact on the architecture*

	In scope architecture	Comment
RTP application / enrolment process		
Application	✓	The application for RTP status (including the possibility to apply on-line for TCNVE) is in the scope of the architecture.
Documentation check	✗	Unless otherwise, the verification of the validity of the travel documents, including the Passive Authentication (PA) and the discretionary Active Authentication (AA) are out of scope of this architecture study and their implementation is the sole responsibility of the Member States.
Bearer verification	✗	The verification of whether the holder of the MRTD is its lawful owner is out of scope Architecture chapter, because it is the functionality of ABC gates and other border control equipment.
RTP identification (1:n)	✓	Fingerprint identification taking place at RTP application is performed using an AFIS (possibly the BMS) which is discussed in section 6.4.5.
Questions	✗	The questions that are asked are out of scope for the architecture.
SIS II check	✓	The impact on the architecture of the consultation of SIS II and other relevant databases is discussed in section 6.5.2.
VIS check	✓	The impact on the architecture of the consultation of the VIS is discussed in section 6.4.
Vetting	✓	The vetting procedure – which is to be defined – could include consultation with other Member States. The consultation mechanism is discussed in section 6.5.4.
RTP registration	✓	The RTP registration is in scope for the architecture.

	In scope architecture	Comment
<i>RTP application / enrolment process</i>		
RTP online application	✓	The possibility to submit the RTP application online or even register online to the RTP (see Alternative RTP process section) would have an impact on the architecture. Enabling the input of data from a public website raises additional security concerns (depending on the implementation of this service) that will need to be addressed in an exhaustive risk analysis.
EES individual file creation	✓	The EES individual file creation is in scope for the architecture.
<i>RTP process upon entry and exit</i>		
RTP Retrieval	✓	The retrieval of the RTP record is one of the business services of RTP.
RTP Biometric verification	✓	Fingerprint matching against the central system is in scope of the architecture.
VIS check	✓	Visas will be checked against the existing VIS in the same manner as they are today. The possible synergies with EES and RTP will be analysed in section 6.4.1.
SIS II check	✓	The impact on the architecture of the consultation of SIS II and other relevant databases is discussed in section 6.5.2.
EES search	✓	Running a search in EES is one of the business services of EES.
EES entry/exit record creation	✓	The EES registration is in scope for the architecture.
Authorisation to enter/exit	✓	The authorisation for entry / exit will entail the creation of a corresponding entry / exit record in the EES.

The RTP service catalogue could comprise the services that are listed in the table below. Section 3.3 of the Study provides a detailed description of the processes related to RTP services.

Table 70 Possible RTP service catalogue

Service	Description of the service
Registration, extension, repeal or revocation of RTP application	The authority can register RTP membership based on information provided in the RTP application. The authority can also register additional information if it decides to extend, annul or revoke RTP membership, or to shorten the RTP's validity period . The service also comprises on-line registration and the subsequent support functionalities
Identification of applicant	The authority at the enrolment in the RTP of a new traveller can search the relevant database(s) (depending on the implementation) to ensure that the applicant has not applied before under another name or with different travel document (RTP "shopping") . This service will support the RTP identification (1:n) step as described in 3.3.
Biometrics enrolment – registration of biographic and biometric data	The authority can register the applicant's alphanumeric and biometric data.
Search	The authority can search the relevant database(s) to examine applications.
Biometric verification	The authorities responsible for carrying out checks at external borders and within the national territories search the RTP to verify the identity of the RTP holder against the RTP.
Reporting / statistics	The authorities can e.g. create, deploy, and manage statistical reports about RTP members.
Access Rights Management	Access Rights Management services will provide differentiated access to remote directories and authentication mechanisms for different authorities.
Logging	The logging service would retain information on all activities performed by different authorities in the RTP.
Monitoring	The service would enable the performance monitoring of the RTP hardware, software services, and applications.

◦ **Broader issues to be taken into account**

The Study and assessment of the architectural options and of the relevant TFs has been carried out taking into account the existence of broader issues and high-level requirements that guide and limit the technical choices. This involves a number of legal, financial and organisational constraints, as listed below.

- **Costs:** the allocated budget poses constraints for the proposal of the solutions and will ultimately guide which options can be chosen;
- **Availability objectives:** requirements for high availability have a significant effect on the design of EES and RTP services. They might limit interaction possibilities with each other and other systems which have totally different availability requirements. Although these requirements have not been defined in this phase of the project, it is assumed that these requirements will be comparable with or more stringent than those for comparable systems e.g. VIS;
- **Data protection:** this constraint encompasses how data can be handled, accessed and stored. This constraint is particularly relevant for any option that would involve the merging or accessing of data collected for different purposes;
- **Data retention:** the requirements for data retention determine and put constraints on the storage and handling of the databases and also encompass additional operations;
- **Regulation of existing systems (e.g. VIS):** access, integration or changes to existing systems would require, in most cases, amendments to the relevant underlying regulations beforehand. In order not to delay and add uncertainty to the implementation of the project, there is a need to allocate time for these amendments;
- **Operational maintenance:** the maintainability of the system(s) has a direct impact on the maintenance costs and on the availability of the systems themselves. This aspect will be of importance at later phases of the project, influencing the possible technical choices for the systems (e.g. whether to opt for the virtualisation of the servers, who will operate certain components);
- **Support to end user:** the importance to provide a timely and quick support to the end users of the systems is in line with the high availability requirements for these systems. The EES and RTP must be equipped with tools for the identification and resolutions of the issues affecting the end-users of the system.

◦ **High-level requirements**

Taking into account the high level business requirements for the architectural options of the EES and RTP, and based on the needs and capabilities of the users/actors, the following architectural assumptions have been retained:

- EES and RTP operations shall be maintained with a minimum of interruptions, according to their different availability requirement profiles (see section 6.1.4.3);
- EES and RTP related processes and their supporting systems need to comply with all relevant laws, policies, and regulations;
- Personal data shall be processed fairly and lawfully;

- EES and RTP shall be designed to be viable in the long-term;
- Technical simplicity of EES and RTP architecture shall be achieved;
- The same concepts and technologies (e.g. web services) as used in other related systems such as VIS and SIS II shall be reused if possible;
- Appropriate logging and traceability shall be ensured;
- Operational management of EES and RTP shall be integrated in eu-LISA's common management infrastructure and processes;
- Interactions with other IT systems that are used in relation with the EES/RTP processes (such as VIS-BMS / SIS II) should be optimized with a view to maximizing response times while guaranteeing an adequate data protection regime.

All of the above assumptions are taken into account when analysing the different architectural options for the TFs where appropriate. The first one ("operation with a minimum of interruptions") is not included explicitly but may have a significant impact on the overall logical architecture. Therefore it is discussed in more detail in the next section.

> *Availability*

From a preliminary analysis it becomes clear that the respective availability of EES, and, to a certain extent of RTP, will need to be comparable with or better than that of SIS-II and VIS. Although not specifically discussed in an answer to any of the TFs, it is important to highlight this here and discuss some of the possible safeguards. These will need to be investigated and elaborated on in more detail when establishing the Business Continuity and Disaster Recovery Plan.

The first and most important safeguard would be the use of **fall-back processes** which are to be defined and made available to the relevant stakeholders (e.g. border guard at BCP).

All Member States are connected to the central sites via the TESTA¹⁵¹ network which is offered by an outsourced provider and under a single control. Despite the availability measures that are taken **and the stringent SLA's, an outage of this central TESTA network can occur. To protect against this type of outages the duplication of the network** operated by an independent provider could be envisioned as a safeguard. However, given the uncertainty on the feasibility at the level of the network providers and given significant cost implications, envisaging this option is not desirable.

Another option would be to work with a **national copy** of the data (such as is the case for SIS II). This would neither be a preferable solution for multiple reasons:

- It is contrary to the overall architectural concept of having a centralised system;
- The synchronisation of the data between all Member States, given the large number of border crossings (more than 700.000 per day, see section 2);
- The need to provide the required business services to the different Member States;
- The storage/processing power/ BMS capability that would be needed in each Member State. An intermediate solution with only a copy of the alphanumeric data would only marginally improve availability.

¹⁵¹ sTESTA until 2015 and then Testa-ng

A limited set of functionality (reliable message transport, flow control, multiple call-back support, logging) could be provided by the **National Uniform Interface (NUI)**¹⁵², which is to be seen as an evolution of the current National Interface. The technical details of the NUI are described in more detail in section 6.6.4.

- **Architecture building blocks**

Architecture building blocks are perceived in this Study as the components of the logical model that define the structure and behaviour of the EES and RTP as systems. The building blocks also include the components which are needed to represent interaction alternatives with other systems.

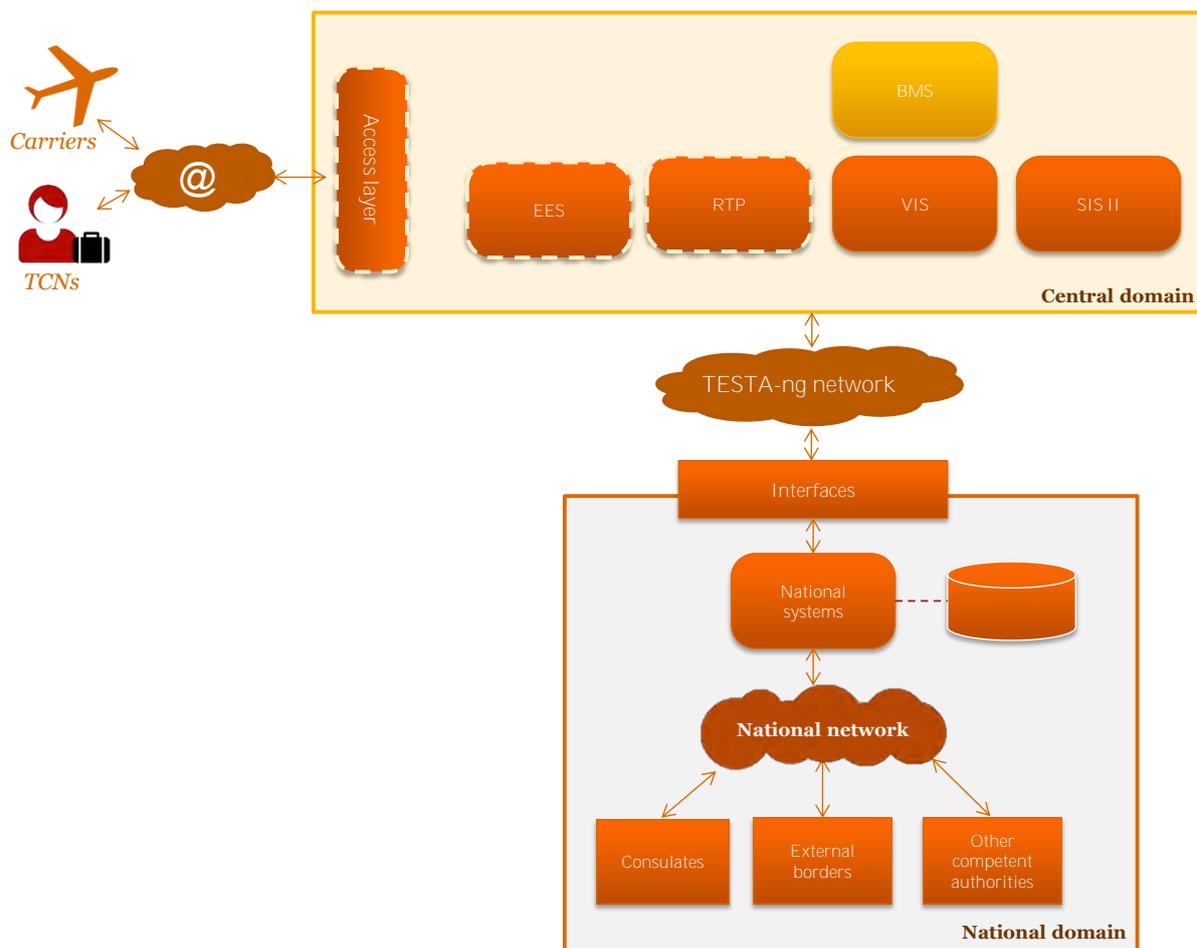


Figure 38 Overview of the main building blocks within the scope of the target architecture

It has to be stressed that the access via a public network (depicted as "@" in the figure above) for Carriers and TCNs should not be construed that these actors have direct access to all systems that

¹⁵² The National Uniform Interface is foreseen by the Legal proposal

are available in the Central domain. They would of course only have (a very limited) access to the EES and/or RTP. This is discussed in more detail in section □□.

Also, it should be noted that the building blocks presented at Member State level in the National domain are only a general representation. This should not be interpreted as meaning that a Member State is using such architecture or is expected to use it.

6.1.5.1. Current building blocks

The Trans European Services for Telematics between Administrations (TESTA)¹⁵³ provides a European backbone network for data. The network uses the standard Internet Protocols (TCP/IP), but operates separately from the internet. It provides guaranteed performance and high levels of security.

VIS, SIS II – some of the architectural options include other IT systems that are currently used for the border crossing processes, including VIS and SIS II. Those systems are described in Oof the Study.

Biometric Matching System (BMS) is a biometric database and search engine, currently working as back-end of the VIS. It provides a range of services related to the handling of biometric data (identification, verification, update, deletion, quality checks, etc.). An evolved system (BMS-2) with more transactional capacity will be implemented by March 2015. The BMS is described in more detail in section 6.4.5.

National Interface (NI) is a generic representation for the interfaces that are deployed by the Central systems. It also provides a unified access (encapsulating network complexity) for the National Systems to these Central systems.

National System (NS) provides access for the different systems of a Member State to the features offered by the Central Systems. The NS is the only system communicating with the Central Systems, and complying with an ICD, via the NI and is designed and operated solely by the Member State. The level of sophistication and functionalities for the NS differs between Member States.

¹⁵³ s-TESTA will be changed to the upcoming **Trans-European services for telematics between administrations – new generation (Testa-ng)**. Testa-ng will provide secured and highly available network services to sensitive and important applications. On the basis of the information that is available, it is assumed that the change of network will not have significant impact on the architectural options.

6.1.5.2. Future building blocks

Entry-Exit System (EES) is an application for the recording and storage of information on the time and place of entry and exit of TCNs crossing the external borders. Based on the process analysis and identification of business services catalogue, the need for the following EES components is considered:

- **Entry-Exit Database (EEDB)** would contain data related to the TCNs individual files and the entry and exit records. Please refer to section 3.2.2 where the whole dataset that would be stored in the EEDB is explained;
- **Facial matcher** is an optional component which depends on the choice of the TOM. The component could enable TCN's verification (and possibly identification) based on facial-images (combined with alphanumeric data). Facial matcher could also complement BMS capabilities in cases when fingerprint enrolment would not be possible or deemed to provide insufficient accuracy. These cases are discussed in detail in the section on Biometrics;
- **Stay duration calculator** – the component that would assess the eligibility of the TCNs entry and stay as foreseen in Article 5 of the SBC (90 days in any 180-day period). The calculator would provide information on the authorised length of stay and flag cases of expired visas, etc. The stay duration calculator would also support functionality of overstayers' extraction engine by indicating overstayers;
- **Overstayers' extraction engine** – the component would check EEDB regularly and indicate overstayers by creating an alert list;
- **Search engine** – a component which would enable searches in the EEDB based on a combination of alphanumeric and biometric criteria. The search engine would also enable the retrieval of statistical data related to the border crossings or overstays of the TCNs;
- **Supporting functions** – such as (statistical) reporting, logging, monitoring, security, interfacing with other systems (where appropriate).

EES Interface would deliver the services provided by the EES to the Member States. The business services are described in detail in section 6.1.4.1.

Registered Traveller Programme (RTP) is an application which will provide, as one of its components, a central database for third-country nationals registered in the Registered Travellers Programme (RTP).

- **Registered Traveller database (RTDB)** - would contain data related to RTP applications and membership. Section 3.3.2 describes the dataset that will be used and stored in the RTP system;
- **Search engine** – a component which would enable searches in the RTDB based on a combination of alphanumeric and biometric criteria. The search engine would also enable the retrieval of statistical data related to RTP applications and membership;
- **Facial matcher** could enable verification (and possibly identification) of RTP members based on facial-images (combined with alphanumeric data);
- **Supporting functions** – such as reporting, logging, monitoring, security, interfacing with other systems (where appropriate).

RTP Interface would deliver the services provided by the RTP to the Member States. The business services are described in detail in section 6.1.1.

National Uniform Interface (NUI) should be seen as an evolution of the current NI which would provide additional services making it possible to offer a higher level of service to the Member States. For the Member States this NUI would make very little difference in the type of business services that are offered and in how they are accessed. The NUI is described in more detail in section 6.6.4.

Internet access – it is foreseen in this Study that carriers and TCNs would have access via a public network (i.e. the internet or similar). The details of this access and proposed safeguards are described in section 6.6.4.

The combinations of future building blocks together with current building blocks are further discussed in sections 6.6.4, 6.6.5, 6.6.6 and 6.6.7 to show the structure and behaviour of the EES and the RTP, as well as their interactions with other systems.

– **General architecture**

A number of general architectural artefacts will be described first; they are independent of the choices that are described in the different TFs. These artefacts can be seen as the building blocks on which the different TOMs (see chapter 2) are built.

Central site

The availability needs that were identified in section 6.6.4 have a significant impact on the architecture of the Central Site (CS) of the EES and RTP. For the VIS the CS is implemented in a datacentre in Strasbourg (France), while a Backup Central Site (BCS) exists in Sankt Johann im Pongau (Austria). These sites operate in an active/passive setup. A study is carried out by eu-LISA to examine the migration towards an active-active setup for VIS and the impact it will have on the infrastructure. The active-active setup means that both data centres are active and requests are distributed over all available nodes.

At the moment load balancing inside the active central unit data centre is done in a static way. VIS load balancing is done on the basis of the set of connected Member States, i.e. each of the two servers receives the requests from one half of the Member States. A project is underway to migrate towards a more dynamic type of load balancing which would make it possible to distribute the load evenly and dynamically over the different servers. It is foreseen that this could be implemented by the year 2016.

The current VIS and other applications are implemented on dedicated hardware, i.e. specific servers, storage, networking. A study is carried out to migrate towards a setup based on virtualised hardware, which would allow a more flexible setup and better use of resources. This study also includes the offering of a single set of supporting services, such as backup and monitoring across the different applications, in contrast with the current silo approach.

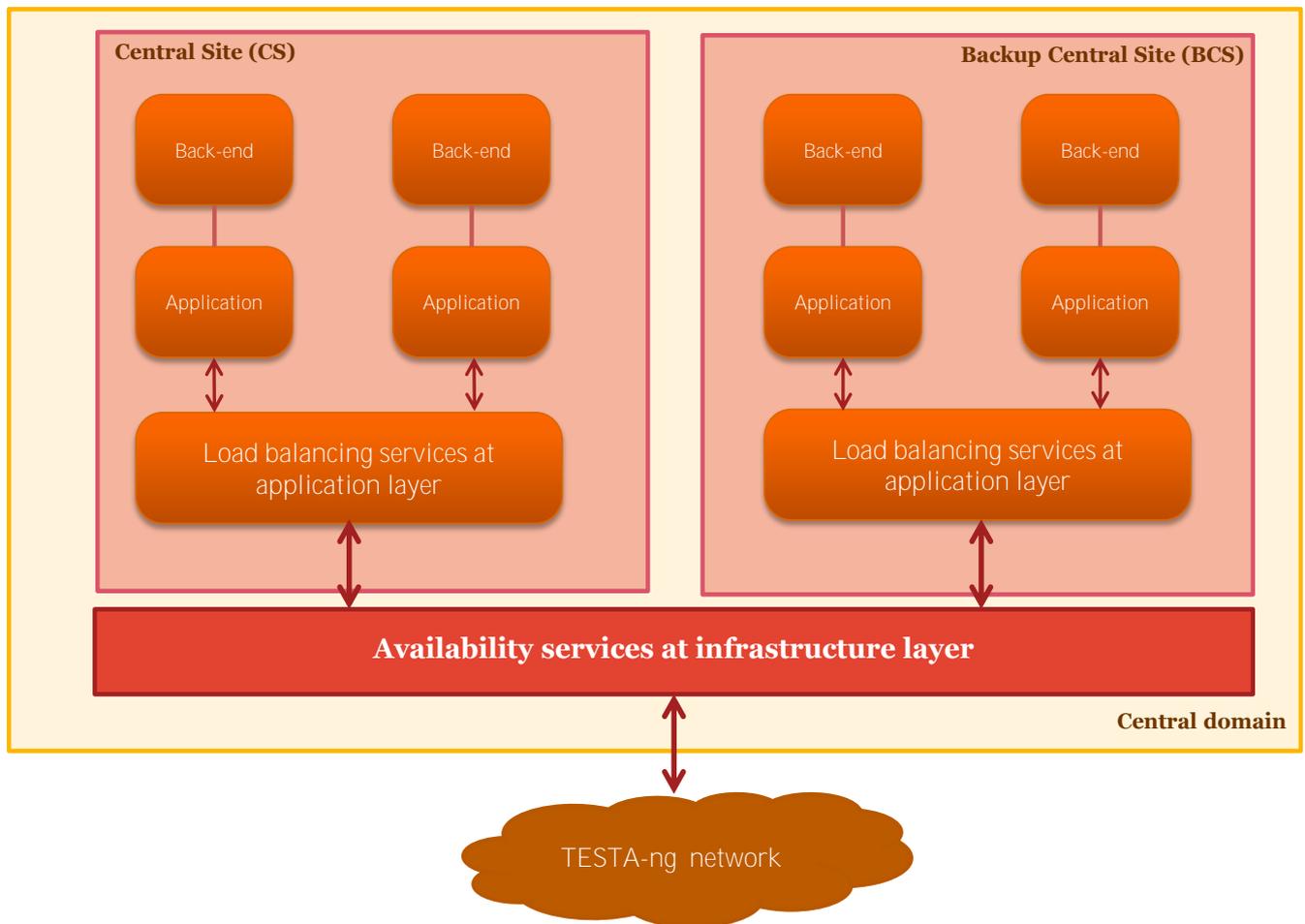


Figure 39 Overview of logical architecture for the central site

Access via the internet to EES / RTP

It is foreseen that different stakeholders could have access from a public network (i.e. the internet) to a limited set of services offered by EES / RTP. The following were identified:

- A TCN pre-registering for RTP status;
- (air) carrier checking the EES status of TCNs;
- A TCN needing to consult the remaining stay duration.

Given the sensitive personal information that will be stored in EES / RTP, and the business critical services offered, it is of utmost importance that adequate security safeguards would be put in place. The exact nature of these controls will follow from an exhaustive risk analysis. The ones that follow from best practices are presented in the sections below.

Pre-registration for RTP status by TCN

To speed up the processes at the border crossing, it is foreseen that a TCN could pre-register his/her application for RTP status. A web site will be set up for this pre-registration. As this site is

open to the general public, very strict security checks are to be performed on the input that is provided by the TCN.

A standard set of guidelines to protect against common threats can be found in the Owasp Top 10 (https://www.owasp.org/index.php/Top_10_2013-Introduction).

Carrier checking EES status of TCN

Carrier checking EES status of TCNs would be a very restricted and strictly controlled web service. The service could be provided via a public network (i.e. the internet) or SITA communication link such as described in section □□°.

Consultation of remaining stay duration and RTP status by TCN

In case no information was printed upon entry or information was lost, this service would enable a TCN to check the remaining duration of his/her stay and his/her RTP status. The different options for this service are discussed in chapter 3. When access via a website is envisioned, the TCN would only have access to a read-only copy containing only the required subset of EES data. Only the data needed for the identification of the TCN, the information about his/her stay duration and his/her RTP status would be extracted. Filtering would also be performed to only extract data on active travellers, i.e. having an entry record but no matching exit record.

To ensure that data only flows from the central EEDB to the read-only copy (and not in the reverse direction) or to prevent this channel from being used by an attacker strict procedural controls must first be put in place. But also the use of a unidirectional network (or data diode) should be foreseen.

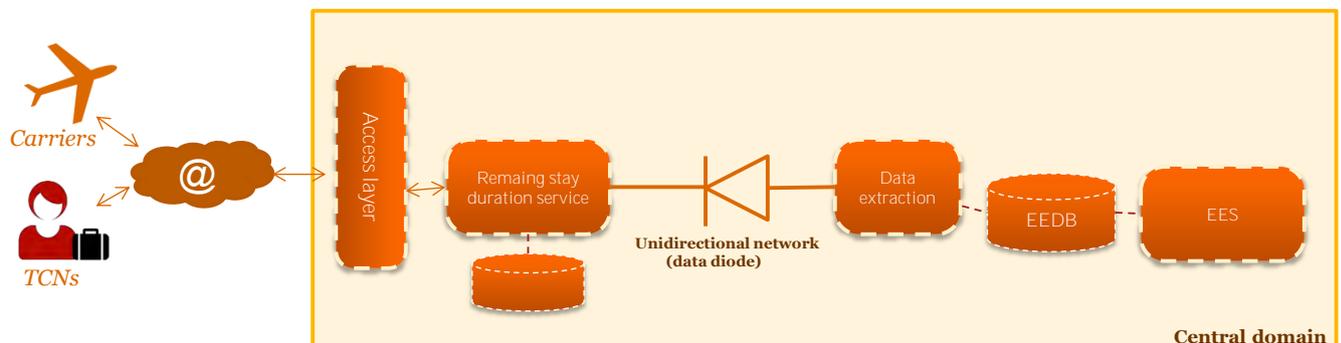


Figure 40 Logical architecture for the "remaining stay duration" service

This would be comparable to the service that is offered by the Australian government via the Electronic Travel Authority (see ETA at <https://www.eta.immi.gov.au/ETA/etas.jsp>).

– ***EES and RTP: single or separate systems (TF11.2, TF15)***

The current legal proposal for the Smart Borders provides for the establishment of two separate systems: the EES with the main objective of monitoring entries and exits of TCNs admitted for a short stay (with the exclusion of family members of EU citizens and the holders of residence permits referred to in the Schengen Borders Code), while the RTP should facilitate crossing the border for pre-vetted frequent travellers, including TCNs holding a residence permit. EES and RTP serve two separate yet closely related purposes: they both contribute to the functioning of an integrated border.

This section provides the comparison of EES and RTP data sets and examines the advantages and disadvantages of the available options in implementing EES and RTP functionalities as separate systems or as a single system. The comparison of the data sets identifies the different types of access needed, while the options show the different possibilities in the design and operation of the systems. The EES and RTP functionalities and the corresponding business service catalogues, which were described in the previous section of the Study, are the same for all options and their variations.

Please note that the options described in this section do not entail the possible interaction of EES and RTP with VIS and other systems. The alternatives for these interactions are discussed in detail in the sections □□ and □□ of the Study.

6.3.1. Comparison of EES and RTP data sets (TF11.2)

The comparison of EES and RTP data sets takes into account technical considerations such as data integrity and security as well as legal requirements to comply with data protection legislation, notably with regard to the principle of purpose limitation and the question of further processing.

The minimum dataset that was studied in chapter □□ on TF11.1 and the large amount of data shared between EES and RTP is represented in the following architectural figure:

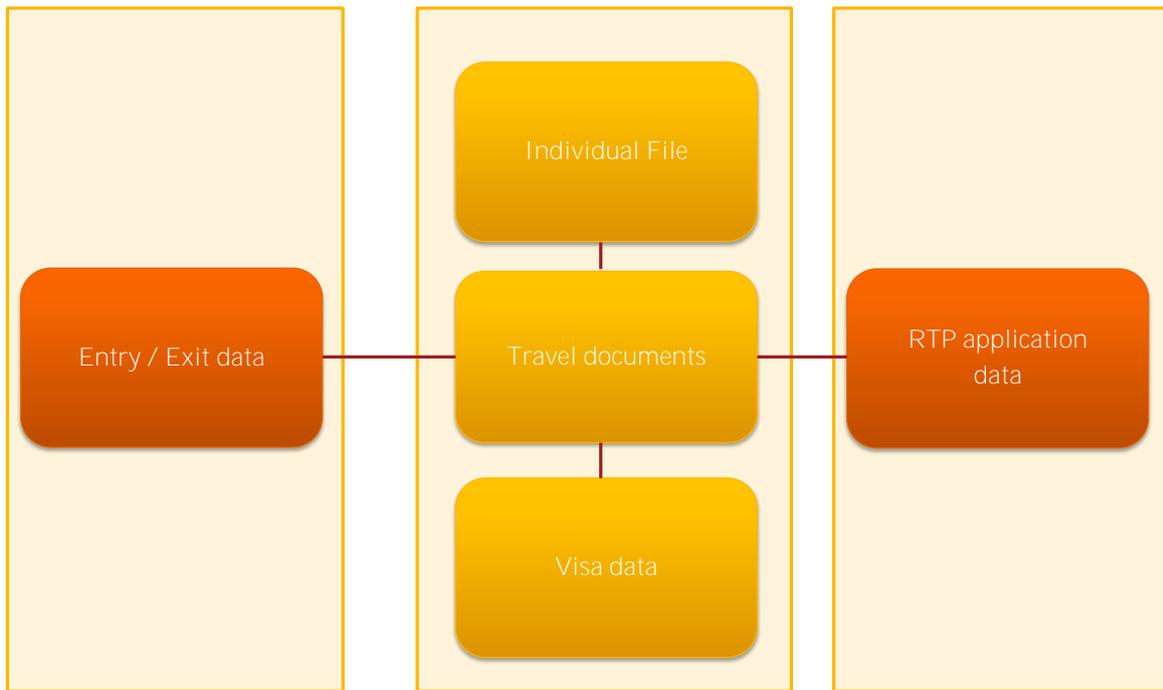


Figure 41 Overview of the data shared between EES and RTP and the links with application-specific data

The following factors have been taken into account when comparing EES and RTP data sets and assessing the various options:

- Categories of travellers;
- Type of data stored;
- The number and type of access to the system.

The approach taken was to first analyse similarities and differences that exist for the above-mentioned factors with regard to each system considered separately. They are summarised in the table below (a tick means that this specific factor is in scope for the application (EES or RTP), whereas a cross means not in scope for this application). Then the impact that the implementation of one single system would have on each of the above-mentioned factors was assessed.

Categories of Travellers	EES	RTP
TCN with non-admitted RT application (TCNVE and TCNVH)	✗	✓
TCN with issued RT application (TCNVE and TCNVH)	✓	✓
TCNVE (non RTP)	✓	✗
TCNVH (non RTP)	✓	✗
LBT permit holder ¹⁵⁴	✗	✓

¹⁵⁴ To be finally decided by the MS.

Residence permit holder¹⁵⁵

✗ ✓

Type of data	EES	RTP
Individual file data	✓	✓
Biometrics data	✓ ¹⁵⁶	✓ ¹⁵⁷
Entry/Exit records	✓	✗
Authorised stay status and validity information	✓	✗
RTP status and validity information	✗	✓
RTP application	✗	✓
Visa status and validity information	✓	✗

Competent authorities access	EES	RTP
Border guards	✓	(✓) ¹⁵⁸
Authorities in charge of RTP acceptance	✗	✓
Law Enforcement Access	✓	✗

While it is clear that certain authorities will have access to both EES and RTP data, the one-system **option might have an impact on the protection of the individuals' data**. In general terms a physical separation in the case of two systems is thought to be more secure than a logical separation in the case of one system, however a practical equilibrium is to be found and the same level of data protection ensured using advanced Access Management Tool. Another aspect that should be taken into account is collection of redundancy data, which might be the case if EES and RTP were implemented as two separate systems.

Given the above mentioned considerations regarding potential data protection risks and collection of redundancy data, alternative option could be envisaged as well, in order to simplify the procedure and avoid the submission of the same data twice while guaranteeing a high level of data protection. An option could entail the maintenance of two separate systems that will store separately data that are collected for the specific purpose of EES and RTP, respectively as foreseen in the existing proposals. At the same time, those data that are common to the two systems could be stored in a single system. If this option was retained and LEA was to be granted, then the

¹⁵⁵ To be finally decided by the MS.

¹⁵⁶ For TCNVE with no RTP status only, as biometrics of TCNVH are stored in the VIS and biometrics of TCNVE with RTP status are stored in the RTP.

¹⁵⁷ Duplication of biometrics stored in the VIS (article 8 of the current RTP legislative proposal).

¹⁵⁸ Depending on the specific solution chosen for RTP. If self-service is chosen, then there will be no need for access to RTP for the Border Guard.

technical solution envisaged should guarantee that law enforcement authorities do not have access to data that they are not supposed to access.

Regardless of the selected option, the Study considers it necessary to include additional safeguards and mitigating actions to reduce the impact that any of the options retained would **have on the protection of the individuals' personal data if law enforcement access were to be granted**. These safeguards refer to those that are already in place in the context of the VIS and include: a central access point, well defined access rights, data logging and other data security measures.

Main findings

The comparison takes into account technical considerations including data integrity and security as well as legal requirements imposed by the data protection legislation. Different data sets, such as categories of travellers, type of data to be stored and number and type of access to the system have been analysed in order to identify similarities and differences. It is clear that since both options of combined or separate systems provide advantages and disadvantages, a practical equilibrium is to be found with respect to ease of use and sharing of data. Regardless of the selected option, the Study considers it necessary to include additional safeguards and mitigating actions to reduce the impact on the protection of personal data, in the context a central access, logging and other measures.

6.3.2. Option 1: two separate systems (TF15.1.1)

This option implies that EES and RTP would be implemented as two completely separate systems with two separate databases (the data interaction and management is described in section □□). Each of these systems would be accessed by the national information systems through an independent interface. Although the interfaces would be independent, it is foreseen that these would be nonetheless very comparable and owing to the business needs (e.g. RTP would need access to EES during application, EES would need to check RTP during entry/exit) each would need to access both systems for the strict information needed in the accomplishment of the supported border checking activities.

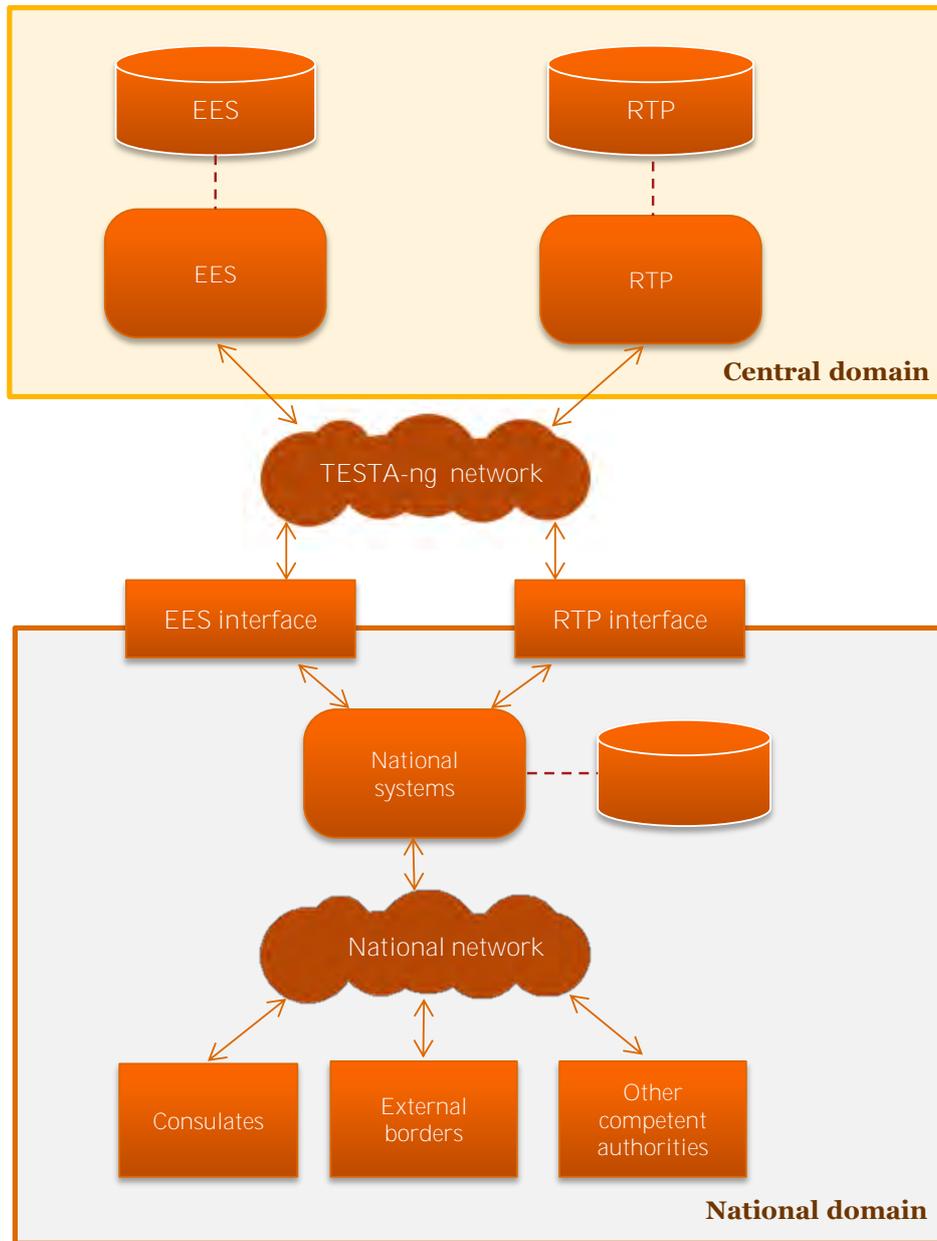


Figure 42 High level overview of the EES and RTP architecture as separate and independent systems

The table below summarises the advantages and disadvantages of having the EES and RTP as separate and independent systems.

Table 71 Advantages and disadvantages of EES and RTP as separate and independent systems

	Advantages	Disadvantages
Onetime	<ul style="list-style-type: none"> The benefit of this model is that each implementation would be targeted to a specific solution, so it would allow tailoring the system for its specific usage and type of users. The implementation of data retention requirements, which might be different for EES and RTP, would possibly be made easier. This benefit is modest as the activity would be simpler as compared to a situation where only one system would be used. 	<ul style="list-style-type: none"> Assuming the overlapping functionalities indicated above, the costs of implementation of two separate systems would be higher. Please refer to the section of contractor development costs in the Cost Report for detailed analysis. A higher number of databases, a higher number of transactions, and duplication of data would imply not only the need for additional hardware and software, but also the need for additional human resources. Please refer to the section of administration costs in the Cost Report for detailed analysis; The services facilitating the interaction between EES and RTP will need to be build.
Recurrent	<ul style="list-style-type: none"> There would be a clear distinction between EES and RTP data; therefore the EES and RTP databases could be more easily protected from the unwanted actions of unauthorized users because the specific access needs and the lesser impact if one of the databases is compromised. Yet, given that all of the data lies behind a secure Testing network, adding system separations would only offer marginal extra security; Data protection would be more easily assured due to differential access control for different databases; Housekeeping of the databases, i.e. freeing up storage space, improving and optimizing run-time performance would be simpler. This benefit is modest as the activity would be simpler as compared to a situation where only one system would be used; The independence of the two systems allows them to adapt to regulatory changes much more easily. 	<ul style="list-style-type: none"> The space requirements and the maintenance costs for two separate networks terminal access points and systems would also be higher. Please refer to the section of office space in the Cost Report for more information; The same personal data would be stored twice, which would increase the risk of data leakage; This approach is in contrast with the data minimisation principle and might also lead to inconsistencies in the data

Main findings

This option implies that EES and RTP would be implemented as two completely separate systems with two separate databases, accessed through independent interfaces, although interactions are anticipated.

Having the EES and RTP as two separate and independent systems would be advantageous from a complexity and implementation perspective for the separate systems.

However, given the large overlap between the two systems in functionality and certainly in data, this would result in a huge development effort and a duplication of hardware and software leading to significantly higher investment and maintenance costs (*please refer to the section "Cost difference between single EES/RTP and two separate systems" in the Cost Report for detailed findings*). Integrating two separate systems would also have an impact at national level.

6.3.3. Option 2: a single system (TF15.1.2)

The option implies that the EES and RTP would be designed and implemented as a single system with a single database. However EES and RTP data would be logically separated although physically located on same servers. EES and RTP related business services would be provided via a single interface. It should be noted that a single interface would not mean single access control but would allow to have separate access mechanisms and profiles.

This option is in agreement with the minimal dataset that is discussed above and depicted in Figure 41. It also has the best alignment with the process approach.

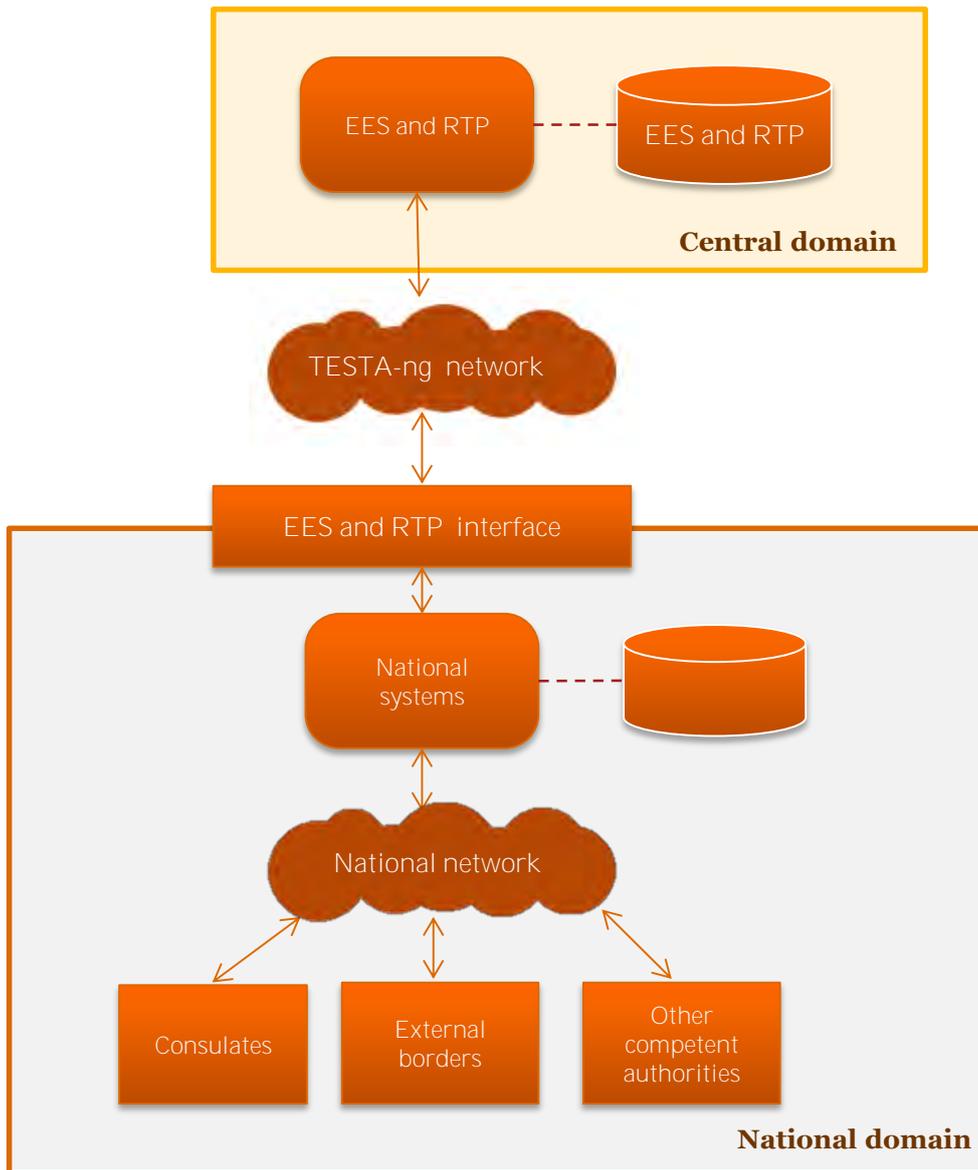


Figure 43 High level overview of the EES and RTP architecture as a single system

The advantages and disadvantages of uniting the EES and RTP under a single system are described in the table below.

Table 72 Advantages and disadvantages of EES and RTP as a single system

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> • A lowering of the infrastructure costs could be achieved, because of shared hardware (servers, connections, etc.), shared database and service layer infrastructure. <i>Please refer to the section of hardware costs in the Cost Report for detailed analysis;</i> • Only one network would be used for EES and RTP processes while the existence of two separate systems gives an argument for having two separate networks. This advantage does not apply in case the same network is used even when two systems are implemented; • There would be fewer transactions, so database storage could be optimised. 	<ul style="list-style-type: none"> • EES and RTP would be designed and implemented as a single project, so it would be more complicated to ensure the timeliness of their realisation given the larger number of stakeholders involved; • Possible lower availability and adaptability to regulatory changes.
<i>Recurrent</i>	<ul style="list-style-type: none"> • Potential inconsistencies of CRUD (create, read, update or delete) operations would be avoided and data synchronisation efforts would not be needed; • If RTP and EES were developed as a single system, database operations accessing data from both systems could be performed in-process, which would have a positive impact on performance; • Greater synergies at hardware level increase the use of the system processing power for each of the EES and RTP sub-systems, when only one does require so. 	

Main findings

This option implies that the EES and RTP would be designed and implemented as a single system with a single database, accessed through a single interface, although separate access mechanisms and profiles would be used. EES and RTP data would retain their logical separation, although they would be physically located on the same servers.

Having a single, integrated system for EES and RTP would have multiple benefits. It aligns best with the process approach and the minimal dataset for EES and RTP which show the interweaving between them. There would also be a lowering of the infrastructure and development cost when choosing this option (*please refer to the sections "Synergies for developing one single system" in the Cost Report for detailed analysis*). On the other hand the possible added complexity of the implementation and possible issues with different retention times need to be carefully managed.

6.3.4. Comparison of the two options (TF15.2)

The first option, whereby EES and RTP would be developed as two independent systems, has advantages with regard to: segregation of data, reduced level of complexity at application level. However, it presents significant overlaps in terms of functionalities and data to be enrolled and stored between EES and RTP, which would lead to higher development efforts and duplication of systems in addition managing the development and roll out of two systems in parallel will be more complex than having to handle only one project, in particular when the stakeholders are the same. The ultimate result will be higher costs as well as greater risks from a data integrity perspective, because by duplicating the same data there is a greater risks for a-synchronisation and storage of inaccurate data.

The second option, whereby EES and RTP would be developed as a single system does not present the disadvantage of having overlapping functionalities and, as such, is more cost-efficient (*please refer to the section "Cost difference between single EES/RTP and two separate systems" in the Cost Report for detailed findings*). It is also more in line with EES and RTP processes and is best suited to implement the proposed minimal data model. In addition, it is aligned with data minimisation principle.

Table 73 Comparison of EES and RTP design options

Option	Costs	Data protection	Complexity of implementation
EES and RTP as separate and independent systems	--	N	-
EES and RTP as a single system	N	-	--

– EES, RTP and VIS: independent or integrated (TF 16)

This section of the Study examines EES, RTP and VIS in order to identify and highlight their possible synergies and interactions. As the EES and RTP information flows and related processes have been thoroughly covered in sections 3.2 and 3.3 respectively, this section will focus on the business services and processes of VIS.

6.4.1. Comparison and synergies of EES, RTP and VIS (TF16.1, TF16.2)

The possible synergies between EES, RTP and VIS are examined in this section, comparing the processes, actors, business services, data and possible web services of the systems.

Processes

From a high level perspective, VIS and RTP related processes are very much alike. Process flows of both systems involve elements of application, checks, creation of new records, capturing of biometric information and verification of an individual according to the biometric information entered.

The EES-related processes are conceptually different from VIS and RTP processes, though the processing of travellers at the border under the EES would nonetheless encompass the current processing of passengers according to VIS. The individual is not applying for entry/exit, no

document is issued, there is identification and verification, which is the same as in VIS and RTP processes.

Actors and business services

The VIS mainly provides services to visa authorities and to the authorities responsible for carrying out checks at external borders and within the national territories, so the main process actors of VIS-related process flows and EES- and RTP-related processes are somewhat identical. The VIS business service catalogue, described in the table below, is similar to the one of the RTP (and partly to EES), as they have similar actors and they are involved in the same business processes.

Table 74 VIS business service catalogue

Service	Description of the service
Receiving and processing of visa application	The visa authority receives the visa application and searches the VIS for the purpose of examining the request. All data from the application form, including the photograph, is entered into the VIS.
Biometrics enrolment and check to prevent visa shopping	The visa authority collects the alphanumeric and biometric data from the visa applicant and searches the VIS with both alphanumeric and FP to prevent visa shopping.
Visa decision and issue of the visa sticker if applicable	The visa authority enters information related to the decision to issue or refuse a visa.
Visa extension, annulment or revocation	The visa authority enters information related to the decision to extend, annul or revoke a visa.
Visa and traveller verification	The authorities responsible for carrying out checks at external borders and within the national territories search the VIS for the purpose of verifying the person's identity (also with the use of FPs) and/or the visa's authenticity.
Identification of the TCNVH or applicant	The authorities responsible for carrying out checks at external borders and within the national territories can identify TCNVHs or visa applicants by searching the VIS database.

Data and web services

The similarities in processes and business services of EES (to a lesser extent), RTP and VIS determine the similarities in data collected and stored at each process step. Those similarities are examined in section □.

The similarities between VIS RTP and EES (to a lesser extent) data flows and business services and the fact that these systems are involved in the same business processes show that synergies could be achieved in terms of hardware, software, documentation, facilities, manual procedures, or roles played by organisations or people. The table below summarises the high-level identification of synergies.

Table 75 Identification of synergies between EES, RTP and VIS

System	Processes	Actors	Services	Data
RTP	✓	✓	✓	✓
EES	✓	✓	✓	✓

The synergies could be exploited in different ways:

- By upgrading VIS for the purposes of the EES and RTP;
- By taking a progressive approach, i.e. initially using VIS artefacts of the development of the EES and RTP (such as descriptions of processes, elements of code etc.) and afterwards examining the possibility to make the VIS as a sub-set of the EES and RTP;
- By using VIS-BMS.
-

The aforementioned options and their variations are described and discussed in more detail in the following sections (6.4.2, 6.4.3, 6.4.4 and 6.4.5) of this Study.

Main findings

The possible synergies between EES, RTP and VIS are examined in terms of processes, actors, business services, data and possible web services of the systems. Regarding processes, the VIS and RTP processes are very much alike, while the EES shares a limited number of processes with VIS. Regarding actors and business services, since the systems serve similar services, the main process actors are mostly identical for VIS, EES and RTP, while the business services of VIS are also similar to those of RTP and partly to those of EES. The similarities above determine equal similarities in the data collected and stored. Finally, the similarities in data flows denote that synergies can be achieved at different levels (hardware, documentation, facilities, manual procedures or people).

It should also be noted that EES will manage all the TCNs crossing a Schengen external border while VIS and RTP will be involved in the management of subsets of these TCNs. The subsets of TCNs managed by VIS and RTP will overlap as some of the TCNs will be Visa Holders and Registered Travellers. This means that all the TCNs crossing a Schengen external border will be **managed through the EES "standard" process (creation of an individual file and/or creation of an entry/exit record)** while a limited number of these TCNs will be also managed through the VIS and/or the RTP processes.

6.4.2. Option 1: EES and RTP independent from VIS

If EES and RTP were completely independent from VIS, the data (including the biometric data) stored in VIS would not be shared with EES and RTP. The functions of EES, RTP and VIS would be totally decoupled. The information available in different databases would need to be accessed via multiple individual calls or via concurrent calls from a higher level interface (if this exists).

The National information systems would coordinate the actions of border crossing processes and also the concentration of the calls to the different central systems. EES, RTP and VIS would interact with national systems via separate interfaces. Alternatively, MSs could decide to re-do their VIS system to have a uniform interface between EES, RTP and VIS. However, the latter option could mean a major overhaul of the National visa system. If MSs built new systems in addition to the ones they already have, it would have very limited impact on the operations of the existing systems, but could have a negative effect on existing business processes at national level and travellers entering the Schengen Area.

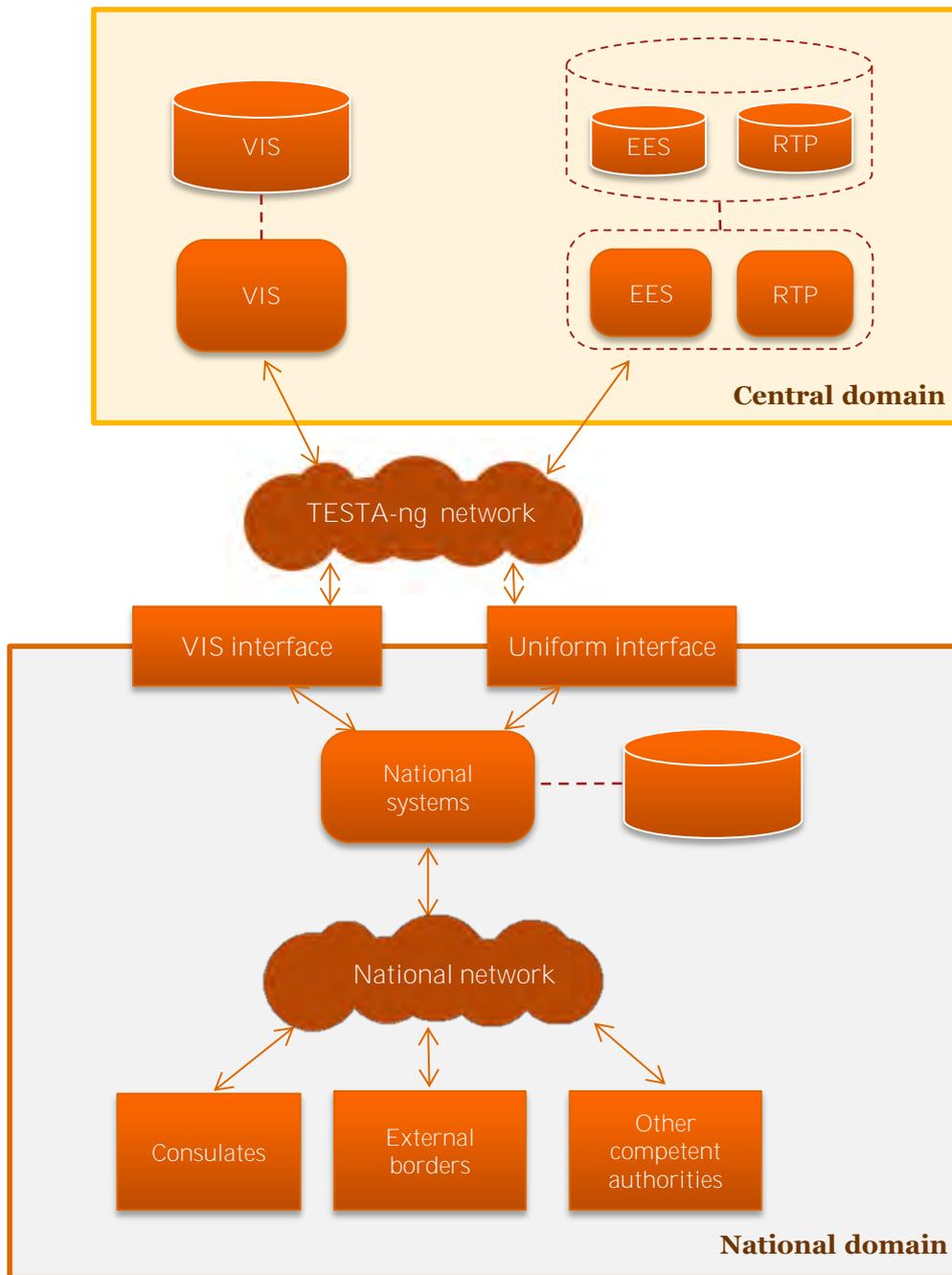


Figure 44 High level overview of the EES and RTP architecture, decoupled from VIS

The advantages and disadvantages of decoupling the EES and RTP architecture from the VIS are presented in the table below.

Table 76 Advantages and disadvantages of decoupling the EES and RTP architecture from VIS

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none">• EES and RTP would be developed independently with limited impact on VIS. Architectural changes may be needed only to the extent that the biometric and alphanumeric data is utilised in VIS for VH travellers and there would be an increase in calls/transactions on the VIS once EES is introduced;• Management of EES and RTP development independently from VIS would be less complex due to the introduction of a new platform. There would be a lower number of stakeholders involved, a lower number of various development teams, companies and technologies embraced. It would also make it possible to: begin with a clean slate, without having to embrace the previous technical choices, most of which having been made a decade ago and avoid any kind of migration phase and a complex testing phase, necessary when performing a major update of a live system (management of legacy systems).	<ul style="list-style-type: none">• RTP and VIS, as separate systems, would have duplicative capability in marginally different ways. Technical and organisational synergies would be neglected, therefore leading to additional costs.

Recurrent

- The VIS would be further used as originally intended and in accordance with its legal framework, so (from the architectural point) no substantial legislative changes regarding VIS would be needed;
- It would be possible to change EES, RTP and VIS at any time with no impact on other systems;
- In the case of independent systems, the RTP enrolment process would be the same for TCNVHs and TCNVEs, so the logical architecture of the systems would be simpler.
- From the MS point of view, there is a potential risk that having a VIS separated from EES and RTP (implemented as one or two systems) increases the complexity for querying these different systems from border crossing points and thus potentially increasing response times. The risk of querying multiple systems is already addressed nowadays, as the national system used for supporting border controls accesses different systems and hides the underlying complexity from border guards.
- The data flows in RTP would duplicate some of the VIS data flows, depending on the RTP scenario retained.
- Coordination/orchestration of the transactions towards each system that take place in a business process. The precise ordering of the interaction with the different systems and the output of these transactions needs to be re-combined in the end, for the purpose of the actual business process.

Main findings

Having the EES and RTP independent from the VIS would allow for a simpler build and operate phase while not relying on a legacy system that will be more than ten years old when the development of EES/RTP is initiated. It would also have little impact on the current VIS setup (at both MS and Central domain), if compared to the option of VIS upgrade for the purpose of EES and RTP (please refer to section 6.4.3). In addition, testing and entry into operation would be facilitated if the management of legacy systems can be avoided (lessons drawn from the SIS II experience). There would however be duplicated capabilities and missed opportunities of synergies at central level. Those synergies would help simplify the design of the National Uniform Interface while simultaneously improving response times.

6.4.3. Option 2: EES and RTP integrated with VIS

The main points underlying the option of upgrading the VIS for EES and RTP purposes is the hosting of alphanumeric and biometric data in the same, but logically separate system as well as facilitating an integrated process approach. An upgrade of all national VIS will be required, thus making the testing and entry into operation much more complex and risky (lessons drawn from the SIS II experience).

It should however be noted that it is erroneous to consider that the border control processes can only be streamlined for the benefit of the traveller and the border guard if and only if VIS, EES and RTP functionalities and data are in one system. The experiences of the SIS II and the VIS have

shown that MSs are able to hide the architecture of national systems behind an integration layer: as such, with one swipe of the passport on the MRZ reader, usually a whole set of pre-formatted queries are launched to both national databases and central systems. Alternatively, an integration layer can be created at the level of the National Interface (see further section 6.6). The general pattern is that the more central applications are integrated at central level, the less integration at national level is required. By simply considering that if 1 man-month development of such an integration layer is saved for each MS, a total of 30 man-month effort is saved overall.

Having these EES, RTP and VIS applications integrated would have in addition a serious impact on the VIS legal instrument, which shall be amended. A high-level overview can be found in the figure below.

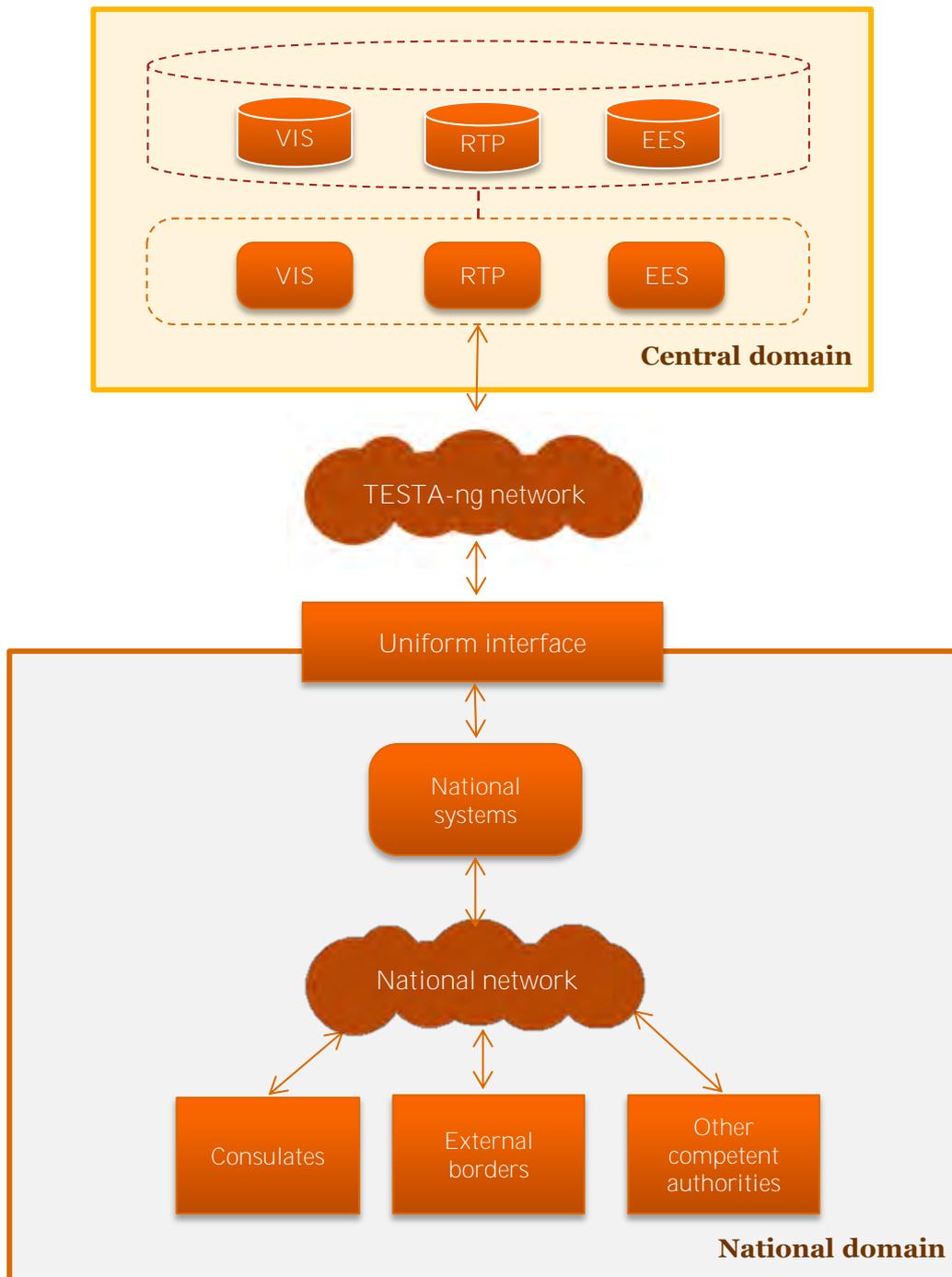


Figure 45 High level overview of the EES and RTP architecture, integrated with VIS

Among the disadvantages are the risks such a project involves: the EES and RTP functionalities impact the VIS significantly, which means that what is called a "VIS upgrade" is almost a new system, as EES will manage all the TCNs crossing a Schengen external border while VIS and RTP will be involved in the management of subsets of these TCNs. This "upgrade" will then have to be re-tested for all VIS, EES and RTP functionalities and performance. From the **MSs' standpoint, the decision to "upgrade" the N-VIS to include EES and RTP is not necessarily the same, but in any event a complete development and testing of VIS, EES and RTP needs to be done.**

After the testing, both the VIS and the national systems then need to be migrated to the integrated solution, which would be highly complex and risky.

The assumption will be made here that the national interface remains the same and is not replaced by a National User Interface in the sense explained in section 6.6. The "VIS upgrade" scenario does not exclude this as a later evolution but it seems logical that the interface with the VIS is kept and that only EES and RTP functionality are added.

The assumption is also kept that a single BMS would be used. Section 6.4.4 demonstrates the economic value of this choice.

The advantages and disadvantages of having the EES and RTP architectures integrated with the VIS are provided in Table 77.

Table 77 Advantages and disadvantages of EES and RTP integrated with VIS

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> • Artefacts of VIS architecture could be reused, including the reuse of VIS logical components and, in the case of full integration, the reuse of physical infrastructure (including the network). This could possibly shorten the systems design and implementation processes, yielding advantages in terms of costs. <i>Please refer to the section "Costs of the system if the EES and RTP systems are upgraded from the VIS" in the Cost Report for detailed findings;</i> • By having a single system, it would be possible for the MS to facilitate border processing (e.g. one enrolment, check) without having to hide this complexity behind an integration software layer, as is currently the case in similar situations; • The development and operational complexity for the MS could be slightly lower, as a single interface will be used and most complexity will be at central level to coordinate services. 	<ul style="list-style-type: none"> • The option of including the entry/exit functionality in the VIS has been discarded by the EES impact assessment due to significant data protection implications and the need to adhere to the principle of purpose limitation;¹⁵⁹ • In the case of full VIS integration with RTP and EES as a single system or integration with RTP only, the originally intended use of VIS would change, so major changes in the VIS legal framework might be needed. This might have a severe impact on the timeliness of implementation and on when the systems would be available; • Coordination of the EES and RTP development integrated into VIS would be a complex task. As a first estimate, the project for building EES and RTP integrated with VIS would be at least of the same magnitude, both centrally as for MS, as the project that led to the implementation of VIS; • The evolution of a complex system, already operational across 30 countries, with high requirements of availability could entail risks of delays leading to higher costs (see SIS II experience where testing and migration of legacy data proved to be significantly more complex in

¹⁵⁹ European Commission, Impact Assessment: Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council Establishing entry/exit system, SWD(2013) 47 final, 28.2.2013, p. 20.

Advantages

Disadvantages

Recurrent

- All of the sub-options of EES and RTP integration with VIS would offer the advantage of a reduced number of transactions related to RTP enrolment, as additional biometric data would not be captured and entered in RTP for TCNVH. This depends however on the RTP scenario retained;
- A cost advantage could also be achieved on systems maintenance, as VIS procedures such as backups, and business continuity plans could be reused. The above is applicable from the MS perspective as well, as the existing infrastructure can be reused. This however depends on the high-availability architecture retained for EES transactions. *Please refer to the section "Costs of the system if the EES and RTP systems are upgraded from the VIS" in the Cost Report for detailed findings;*
- Improvements to VIS may be envisaged, e.g. changing VIS to an active/active configuration may provide availability benefits for the system;
- Even though in case of VIS full integration, changes in EES, RTP and VIS would become more complicated to carry out, the changes would benefit all 3 systems simultaneously, thus diminishing the costs. *Please refer to the section "Costs of the system if the EES and RTP systems are upgraded from the VIS" in the Cost Report for detailed findings.*

comparison to the VIS development where there was no legacy to manage and which entered into operation much more smoothly).

Please refer to the section "Costs of the system if the EES and RTP systems are upgraded from the VIS" in the Cost Report for detailed findings.

- The question of upgrading VIS for the purposes of the EES and RTP follows the chronology of implementation of the systems considered. However, logically, EES is the generic system as it includes the identification of all TCNs – whether VH or VE – while VIS only contains data about VHs.

Main findings

Upgrading VIS to integrate EES and RTP functionalities makes sense at first sight from a

Advantages**Disadvantages**

capabilities, business processes and data perspective. With a single system development, more streamlined maintenance and development efforts might be achieved and more cost effective developments may arise based on the fact that such developments benefit three systems rather than a single system at a time.

However, it would have a significant impact on the existing VIS, at national level in particular: The evolution of a complex system, already operational across 30 countries, with high requirements of availability will lead to a much more complex testing phase and entry into operation, compared to the development of stand-alone systems. In addition, such an implementation of the EES / RTP starting from the existing VIS platform would also lead to a complex legislative process since the VIS legal framework would need to be adapted accordingly. *Please refer to the section "Costs of the system if the EES and RTP systems are upgraded from the VIS" in the Cost Report for detailed findings of the costs of longer development phase.*

6.4.4. Option 3: Progressive approach: re-using VIS artefacts allowing further synergies

In addition to option 1 (EES and RTP independent from VIS) and 2 (VIS upgraded for EES and RTP), a progressive approach could be considered, which would not necessarily seek full integration of three systems but simplify the build of the EES/RTP systems by re-using the VIS components and thus facilitating the development and operational acceptance testing and minimising the impact on MS while allowing synergies (service calls) between systems at central level.

In this option, initially the EES and RTP would be built independently of the VIS; yet, the EES/RTP legal proposal should provide for further VIS integration. Numerous VIS artefacts could be re-used for RTP development, as their target population and system functionality have substantial overlaps (e. g. definitions of processes and tasks (*please refer to 6.4.1 for EES, RTP and VIS synergies*), requirements, data models, user credentials, authentication method and access rights design, technical specifications, source codes and other system documentation). As such, a maximum number of existing VIS technical modules would be re-used.

The EES and RTP should be built in the perspective of possible future integration of the VIS processes that synergies could be achieved. Also, the EES and RTP should be built according to a modular design envisaging and allowing future expansions and integrations to achieve the maximum extent of synergies. In addition, the BMS would be a unique SOA-BMS serving all three systems (*for further details please refer to section 6.4.5*).

- In the Central domain, an abstraction layer would be added before the VIS, EES and RTP (i.e. between the network connections with the MS and the applications themselves). This layer would link the different systems and shield the complexity of the implementation of the different systems, alleviating the need for the MS systems to know which service is implemented on which (sub)system. This layer would also be an orchestrator, by directing the calls to the proper backend application and in the correct sequence. Furthermore, this abstraction layer would – at a later stage – make it easier to integrate or migrate the backend applications or database.

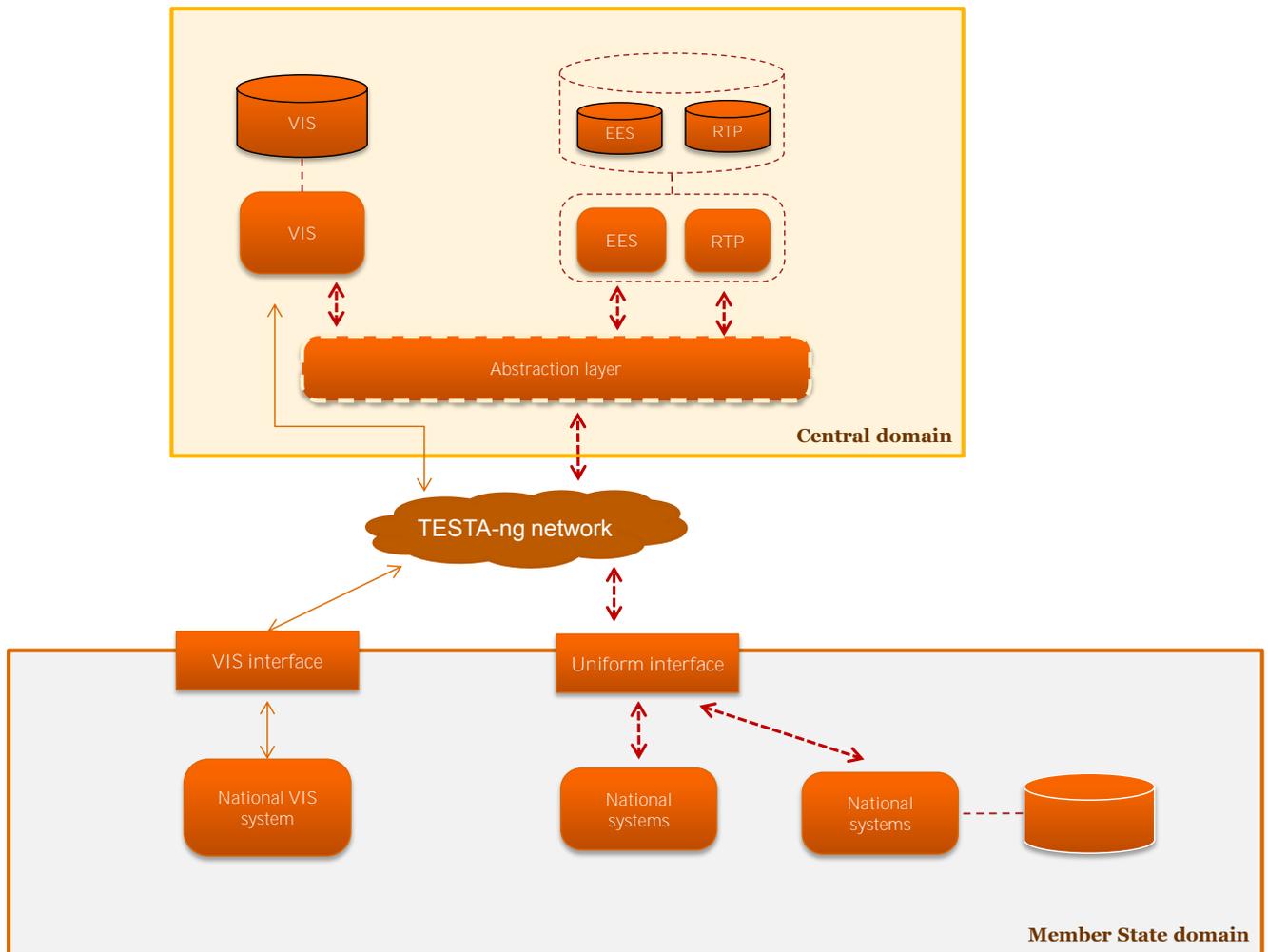


Figure 46 High level overview of the EES, RTP and VIS architecture, with abstraction layer

- At the **national level**, there would be no impact on the national VIS. In the initial phase, the EES /RTP NUI would be used. This NUI should be designed in such a way that it would allow for an easy future VIS integration, which can then happen in a transparent way as the complexity and the details of the implementation are abstracted away.
-
- Synergies could also be achieved in the operational phase by having the new platform partly managed by the existing VIS operators.
-
- If in the future the EES/RTP and VIS legislative instruments provide for additional synergies between three systems, further integration could be envisaged. For instance, one single network could be used and the next generation VIS could be integrated to the EES/RTP platform, possibly further decreasing operational costs. *Please refer to the section "Costs of the system if VIS artefacts are re-used for the EES and RTP" in the Cost Report for detailed findings.*

After the development phase of EES and RTP and a stabilisation period into operations (2021-2022), the VIS will be reaching the end of its lifecycle and a new major overhaul would be required, providing the opportunity to implement the necessary changes to the VIS, which could become a sub-system of the integrated solution.

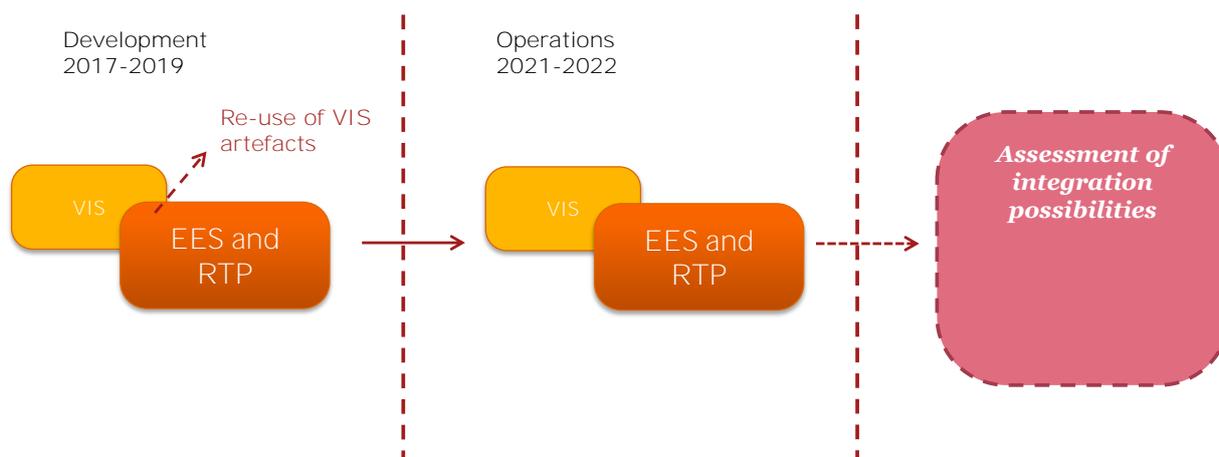


Figure 47 Phases in the progressive approach

If EES and RTP were initially built independently of the VIS, the complexity and risks of the projects would be reduced significantly. The SIS II experience shows that complex project management (not complex testing) leads to substantial delays and under-budgeting. There would be fewer stakeholders involved as well as fewer development teams, companies and technologies embraced. It would also make it possible to begin with a clean slate, without having to embrace **the previous technical choices and vendors’** solutions and without a migration phase or a complex testing phase, necessary when performing a major update of a live system. There would also be fewer legal issues, i.e. no major change of VIS legal basis required in the coming years because of RTP and EES.

-
- The table below provides considerations of advantages and disadvantages of a progressive integration between the EES/RTP and the VIS in comparison with having VIS upgraded for the purposes of the EES and RTP.
-

Table 78 Advantages and disadvantages of a progressive integration in comparison to the option of VIS upgrade for the purposes of the EES and RTP

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> • By building EES and RTP and integrating VIS afterwards, the complexity of the projects and associated risks would be reduced. VIS would initially be impacted only by requests from the EES; • If moving to an active-active set-up is considered, it could be possible to develop EES and RTP with an active-active set-up first, then change VIS to an active-active set-up, and integrate both systems once they are in the same configuration. This option is less complex than implementing EES and RTP in active-passive set-up, integrating with VIS and afterwards moving to an active- 	<ul style="list-style-type: none"> • Until a full integration is achieved, synergies will not be fully exploited; • The integration decision would be postponed, with no guarantee that it will ever take place; • It would take longer to develop the EES/RTP central system and then integrate it with VIS than upgrading VIS for the purposes of the EES and RTP.

- active configuration;
- The amendment of the VIS legal basis would not cause delays in the development of the EES and RTP and could be carried out in parallel;
- The components of the VIS could be re-used without the need to intervene in a live system;
- Testing duration would be shorter, as all MSs would use the same National Uniform Interface. For more information about the National Uniform Interface, please refer to section 6.6.4 of the Study. Once the EES and RTP were rolled-out, a more precise assessment of the integration effort could be carried out as the system was live and stabilised.

Main findings

The option of a progressive approach yields the advantages of re-using VIS artefacts and at the same time mitigates the risks of complex project management.

-

6.4.5. Common SOA-based BMS (TF16.4)

This section of the Study assesses the available options regarding the use of existing BMS services in a Services Oriented Architecture (SOA) - type of setup by EES and RTP. From a high level perspective, there are two options:

- Creating a new RTP and EES – BMS;
- Further developing a common SOA based BMS (preferably an upgraded version of the VIS-BMS), which would be accessed by RTP, EES and VIS.

The VIS-BMS is a biometric matching system currently providing services to VIS. The services include verification and identification of fingerprint images, search, quality controls, insertion, deletion and updates of BMS records. However, biometric verification from a facial image is not provided by VIS-BMS. Facial images are currently matched locally at ABC gates. Member States communicate with BMS only through VIS. From an architectural point of view it would be feasible for VIS-BMS to provide services to EES and RTP.

At the time of writing, a project is underway to deliver a BMS-2 in March 2015. The objective of this project is to deliver a higher performance system in terms of transactional capacity.

BMS-2 will be very much like the current BMS, as the interface to the VIS or the way it is used by a MS is not supposed to change. To mitigate the performance problems, the number of servers in the grid and the number of processors supported have grown to a much higher number. This makes it possible to cater for future scalability.

The frontend service bus is implemented by a DAON product at the moment, but will be replaced in BMS-2 by a Morpho product that is better tuned for multimodal matching.

The table below summarises the main advantages and disadvantages of the first option, i.e. developing a new BMS which would provide services to RTP and EES, besides the existing VIS-BMS.

Table 79 Advantages and disadvantages of developing a new BMS specific to EES and RTP

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> The architecture of a new system would be less complex; The launch of a new BMS would possibly involve fewer stakeholders, which might mitigate some of the project implementation risks. 	<ul style="list-style-type: none"> The software and hardware of the existing VIS-BMS might be under-exploited at certain times (night/weekend), which would have a negative impact on costs.
<i>Recurrent</i>		<ul style="list-style-type: none"> There would be a functional overlap between the new BMS and VIS-BMS, as the services provided for TCNVEs would basically be the same; There would be two distinct searches in the new BMS and VIS-BMS for un-documented persons (people carrying no documents); The software and hardware of the existing VIS-BMS would be under-exploited during their operational phase, which would have a negative impact on costs.

Main findings

A less complex architecture could be envisioned, but there would be a negative impact on costs and the new BMS and the VIS-BMS would have a very large overlap of functionality.

The advantages and disadvantages of the second option, i.e. further developing a common SOA-based BMS, are listed in the table below.

Table 80 Advantages and disadvantages of linking RTP and EES with a SOA-based VIS-BMS

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> Technologies and expertise gained while developing VIS-BMS would be leveraged. Although further investments would be needed, the previous investments that have been made into VIS-BMS and BMS-2 would be utilised; In the BMS-2 architecture, additional modules (essentially capacity extension) and modes (e.g. facial image) should be able to be added easily. 	<ul style="list-style-type: none"> Unless facial recognition is done locally (for instance at ABC gates), the expansion of VIS-BMS for the use of facial recognition would be needed, especially if the number of fingerprints were reduced to less than 8.
<i>Recurrent</i>	<ul style="list-style-type: none"> Operational and maintenance costs for a single VIS-BMS would be lower; The processing capacity is made available to <u>all</u> systems so that unused activity on one system benefits the others – synergy on the processing capacity. 	<ul style="list-style-type: none"> The processing time of the queries might increase (needing corrective actions from capacity management). The same is true for hardware demand at the central system level; Integrating the EES/RTP data to the existing BMS might increase complexity when it comes to testing

and operations.

Main findings

Reutilising the technology and expertise gained from VIS-BMS would help achieve significant cost savings (*please refer to the Cost Report for detailed estimation of the costs*). BMS-2 is expected to cater for the changes required, but might need to be extended.

During consultations with the various MS, the second option (i.e. further developing an SOA-based BMS) emerged as a clear favourite.

6.4.6. Comparison of the options

The table below provides an assessment of BMS options within the scope of the target architecture based on the predefined criteria, the main findings can be found in the separate preceding tables.

Table 81 Comparison of architectural options

Option	Costs	Data protection	Complexity of implementation
EES and RTP independent of VIS	-	N	-
EES and RTP integrated with VIS	-	-	--
Development of a new BMS	-	N	N
Linking of RTP and EES with VIS-BMS	+	-	-

– Interaction with other IT systems (TF17)

Regarding the RTP and EES interaction with other IT systems, within the scope of this Study we consider only the frontline systems. This sub-chapter provides a brief description of such systems for the BCP and examines potential interactions with EES and RTP, also taking into account potential implementation solutions.

6.5.1. Other IT systems used for the Border Control Processes (TF17.1)

An overview of the IT systems used for the border control processes is provided in the table below. The main focus of the descriptions of the IT systems is on their functional requirements.

Table 82 Description of other IT systems used for border crossing processes

IT systems	Description
VIS	A description of VIS purpose, technical aspects and architecture is provided in OThe analysis of VIS related processes and possible interaction with EES and RTP is provided in TF 16.1 and TF 16.2.
SIS II	A description of SIS II purpose, technical aspects and architecture is provided in O The main business functions of SIS II are listed below: <ul style="list-style-type: none"> • Create alert: this process is initiated when an appropriate user requests to the central SIS II to create an alert; • Update/delete/link alert: the goal of this process is to keep an alert up-to-

date, to amend or delete existing information, or to provide additional data that would allow better processing of an alert in case of a hit;

- Check person, vehicle or object: this process aims to identify persons, vehicles, and objects for which an alert exists in the system and to perform the action indicated in the alert;
- Flag alert: this is a function whereby the issuing country, upon request from another country, can set a flag to the alert. This flag is then used in the “other” country to take alternative actions, or no action if the country’s legislation does not allow the action indicated by the alert;
- Broadcast and notification: broadcasting is a mechanism that enables the MS to maintain a copy, in full or in part, of the central database. The notification mechanism enables the MS to subscribe to events, such as the creation or the deletion of an alert of a certain type about which they would like to be automatically informed.

I-24/7

The I-24/7 is a global police communications system, developed by INTERPOL. The system enables authorised users to share sensitive and urgent police information with their counterparts around the globe, 24 hours a day, 365 days a year. It operates as the network that enables investigators to access INTERPOL's range of criminal databases.

Authorised users can search and cross-check data in a matter of seconds, with direct access to databases on suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art.

The I-24/7 provides two functional alternatives MIND and FIND. FIND is used for queries directly in the central system.

MIND offers the same functionality, but the queries are done in the national copy.

National end-user systems and databases

National end-user systems and databases are described in section 3.5.1.1. Section 3.5.1.1 also discusses possibilities to re-use or integrate the existing system (including national EES) with the EES and RTP.

The table below gives descriptions of the EES and RTP related data sets. Those data sets are taken into account considering potential interaction and dependencies between the systems (see also section 3.5.1.1 and 3.5.1.2 for a more detailed description and the proposed use in EES and RTP).

Table 83 Description of related data sets

Data set	Description
API (Advanced Passenger Information)	API data are the biographical information taken from the machine-readable part of a passport and contains the name, place of birth and nationality of the person, the passport number and expiry date.
PNR (Passenger Name Record)	PNR data is information provided by passengers during the reservation and booking of tickets and when checking in on flights, as well as collected by air carriers for their own commercial purposes. It contains data such as: travel dates, itinerary, travel information, seat number, baggage information.
Passenger lists from ships	Passenger lists from ships are very similar to the information collected by APIS. They serve very similar purposes as APIS.

Main findings

There are several international IT systems used for the border control processes, including VIS, SIS II and I-24/7 (developed by Interpol) in addition to national end-used systems and databases. Moreover, there are datasets such as API, PNR and ships' passengers lists that are closely related to the EES and RTP.

6.5.2. Potential interaction and dependencies between the systems (TF17.2, TF17.3)

"Interaction between the systems" in this section is understood as basic application functions, which are the following:

- Search of existing entries;
- Creation or addition of new entries;
- Reading, retrieval, or view of existing entries;
- Update or editing of existing entries;
- Deletion/deactivation of existing entries.

"Dependency between the systems" is understood as a broader term than interaction involving not only technical, but also organisational dependencies.

SIS II

From a high level perspective the intended use of EES, RTP and SIS II are very complementary in the field of border control enforcement. According to feedback by some of the Member States, the border control officials are common for all of the systems under review.

However the SIS II related processes and business services are different from EES and RTP. SIS II, on the one hand, is an alert system for certain categories of persons and objects, so it provides business services such as issue of alert, check of a person, vehicle or object etc. EES and RTP, on the other hand, are identification and verification systems for TCNs, so their business services catalogue comprises services such as biometrics enrolment, travellers' identification, verification, registration etc. Furthermore the data obtained in these systems is different, SIS II obtains the **data for certain categories of persons and property, whereas EES and RTP obtain TCNs' biometric and biographic data, travel document data, entry/ exit records, RTP related data etc.** Also it has to be noted that in most MS these are under a different ministry; EES and RTP are typically under the Ministry of Foreign Affairs, while SIS II is under the Ministry of the Interior. The summary of EES and RTP comparison with SIS II is provided in the table below, a tick indicating a substantial synergy between the systems, while a cross indicates the absence of it.

Table 84 High-level identification of synergies between EES, RTP and SIS II

System	Processes	Actors	Business services	Data	Web-services
RTP vs. SIS II	✘	✔	✘	✘	✘
EES vs. SIS II	✘	✔	✘	✘	✘

The architecture of SIS II, a centralised system with distributed and locally cached databases at the MS, is not in line with the current vision of having a fully centralised system.

Taking into consideration the legal framework of SIS II, it shall remain a separate system from EES and RTP with strictly separated data and access.

I-24/7

I-24/7 is a similar system to SIS II. Some of its users, such as border control officials are the same as of EES and RTP. Some of the data obtained such as facial image, fingerprints is the same; however the related processes and business services are different from EES and RTP. Systems differences are highlighted in the table below, a tick indicating a substantial synergy between the systems, while a cross indicates the absence of it.

Table 85 High-level identification of synergies between EES, RTP and I-24/7

System	Processes	Actors	Business services	Data	Web-services
RTP vs. I-24/7	✗	✓	✗	✗	✗
EES vs. I-24/7	✗	✓	✗	✗	✗

It is also important to mention that I-24/7 is most often only implemented centrally at national level and further expansion is focused on extending access to I-24/7 services beyond the national central bureaus, i.e. it is intended to provide access to frontline officers such as immigration and customs officials. Therefore the decisions of potential interactions and dependences of EES and RTP with I-24/7 should be made at national level.

API (Advanced Passenger Information) and Passenger lists from ships

API and passenger lists from ships enables authorities responsible for border checks to receive information on passengers arriving at the border crossing before it takes place, these are also discussed in section 4.4. The stay duration calculator, an EES component to be used for the verification that the return travel (the exit) is within the boundaries of the allowed stay, could use API and passenger lists from ships. At this moment most of this data is received at a specific MS (foreseen port of entry) and used there in the border control process.

Main findings

Even though on a high level perspective the intended use of EES, RTP and SIS II is the same, the actual interaction of the systems remain in terms of actors, while the processes, the business services, the collected data as well as the architecture of the SIS II significantly differ from EES and RTP. Taking into consideration also the legal framework of SIS II, it shall remain a **separate system from EES and RTP with strictly separated data and access.**

I-24/7 is a similar system to SIS II, indicating that similarities are presented only in terms of actors. Moreover, since I-24/7 is implemented at national level, all decisions of **potential interactions and dependences with EES and RTP should be made at national level.**

With regard to API and Ships' Passenger lists, the stay duration calculator, an EES component, intended to be used to verify that the return travel (the exit) is within the boundaries of the allowed stay, could use them.

6.5.3. Legal considerations on system integration and personal data protection interoperability (TF 17.5)

The Study explored EES and RTP interaction with other IT systems notably: VIS, SIS II, I-24/7, APIs, passenger list from ships.

EES and RTP interaction with VIS

With regard to the integration of EES and RTP with VIS the Study concluded that such an integration makes sense from a capabilities and data point of view.

Therefore, the remainder of this section will analyse the legal considerations related to such an integration.

The first legal challenge posed by the integration of EES and RTP with VIS relates to the principle of purpose limitation stemming from EU data protection legislation. According to Article 6 of Directive 95/46/EC, **personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”** Based on this principle, this Study recommended to further use only the strict minimum data necessary to achieve the EES and RTP objectives and provided an analysis demonstrating that this further use is compatible with the purpose for which they were initially collected.

As they stand today, VIS, EES and RTP have been conceived as three separate systems aiming at achieving three different main objectives, as outlined by the respective legal instruments and legislative proposals:

- VIS has the primary objective of improving the implementation of the common visa policy, consular cooperation and consultation between central visa authorities. In addition, with regard to TCNVH, VIS aims to facilitate checks at external border crossing points and within the territory of the Member States, assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the member States, facilitate the application of Council regulation (EC No 343/2003 of 18 February 2003 establishing the criteria and mechanism for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national and contribute to the prevention of threats to the internal security of any of the Member States;¹⁶⁰
- EES, contrary to VIS, targets both TCNVH and TCNVE and has the purpose of improving the management of the external borders and the fight against irregular immigration, the implementation of the integrated border management policy, the cooperation and consultation between border and immigration authorities by providing access by Member States to the information of the time and place of the entry and exit of third country nationals at the external borders and facilitating decisions relating thereto;¹⁶¹

¹⁶⁰ Article 2 of Regulation (EC) No 767/2008.

¹⁶¹ Article 4 COM(2013)95 final.

- RTP, like EES targets both TCNVH and TCNVE and has the purpose of enabling pre-vetted TCNs to benefit from facilitation of border checks at the Union external border.¹⁶²

All three instruments share the same legal basis, i.e. Articles 74 (former Article 66) and Article 77 (former Article 62) of the Treaty on the Functioning of the European Union. The latter establishes in paragraph 1 that the European Union shall develop a policy with a view to:

- **“(a) ensuring the absence of any controls on persons, whatever their nationality, when crossing internal borders;**
- (b) carrying out checks on persons and efficient monitoring of the crossing of external borders;
- **(c) the gradual introduction of an integrated management system for external borders.”**

Article 77 paragraph 2 then enlists the measures that shall be adopted for the purpose of paragraph 1 and these include:

- **“(a) the common policy on visas and other short-stay residence permits;**
- (b) the checks to which persons crossing external borders are subject;
- (c) the conditions under which nationals of third countries shall have the freedom to travel within the Union for a short period;
- (d) any measure necessary for the gradual establishment of an integrated management system for external borders;
- **(e) the absence of any controls on persons, whatever their nationality, when crossing internal borders.”**

These are therefore separate measures with specific purposes all contributing to the achievement of the more general objectives established in paragraph 1 of Article 77.

Therefore, the merging of the three systems could take place only following a revision of the scope of the current VIS legislation together with a revision of the EES and RTP legislative proposals.

When considering the merging of VIS with EES and RTP it is also relevant to take into account the analysis brought forward by the EES Impact Assessment. In particular, on page 20 of the EES Impact Assessment, it is explained that:

“The main purpose of the VIS is to permit the verification of the visa application history and, at entry, to verify whether the person presenting the visa at the border is the same person to whom the visa has been issued. It concerns only those third-country nationals who are required to hold a visa. **The VIS was not developed to keep track of entries and exits of third-country nationals nor is it meant to allow checking whether a person, after entering the EU legally, has or has not complied with the authorised stay according to the visa. [emphasis added] The VIS feasibility study, carried out in 2003 before the development of the VIS, suggested that it would not be beneficial to develop several large-scale IT systems as one, nor to use VIS to record entry and exit data. It would need substantial changes to the nature and capacity of the VIS if entry/exit data were also to be recorded in it. The workflow of the VIS is optimised to deal with 10 million visa applications per year. Adding around 200 million records of entries and exits would require significant investments especially in hardware, software, data storage and communication infrastructure.**

¹⁶² Article 3(1) COM(2013)97 final.

Moreover, there would be significant data protection implications if the system were to include both visa holders and visa-exempt persons. The principle of purpose limitation needs to be adhered to and the risk of function creep has to be prevented as highlighted by the EDPS in his opinion on the Communication on Migration. Therefore the possibility of including entry/exit functionality in the VIS itself and the storage related to non-visa holders in the VIS can be **discarded.**"

In addition, VIS can be accessed by law enforcement authorities, as established by Council Decision 2008/633¹⁶³ while the RTP legislative proposal does not include such an access and the EES legislative proposal states that such a possibility should be assessed after two years from the entry into operation of the system. As a result, the merging of the systems would require reviewing the current rules on LEA in line with the EU data protection legislation clearly establishing differentiated access for different categories of data. Depending on the result of discussions regarding LEA in the EES and RTP, this issue may not be relevant going forward.

A possible merging of VIS, EES and RTP would also need to take into account the fact that currently the three systems have different data retention period rules.

Based on Article 23 of the VIS Regulation the calculation of the data retention period may start counting as of:

"(a) on the expiry date of the visa, if a visa has been issued;

(b) on the new expiry date of the visa, if a visa has been extended;

on the date of the creation of the application file in the VIS, if the application has been withdrawn, closed or discontinued;

on the date of the decision of the visa authority if a visa has been refused, annulled, shortened **or revoked."**

Based on Article 20 of the EES legislative proposal:

"1. Each entry/exit record shall be stored for a maximum of 181 days.

2. Each individual file together with the linked entry/exit record(s) shall be stored in the EES for a maximum of 91 days after the last exit record, if there is no entry record within 90 days following that last exit record.

3. By way of derogation from paragraph 1, if there is no exit record following the date of expiry of the authorised period of stay, the data shall be stored for a maximum period of five years following the last day of the authorised stay.

Finally, Article 21 of the RTP legislative proposal establishes that:

"1. Each individual application file shall be stored in the Central Repository for a maximum of five years, without prejudice to the deletion referred to in Articles 16(7), 26(2) and 35 and to the keeping of records referred to in Article 45.

That period shall start:

(a) on the date of expiry date of granted or extended access to the RTP;

¹⁶³ OJ L 218, 13.8.2008.

(b) on the date of the creation of the application file in the Central Repository, if the application has been withdrawn;

(c) on the date of the decision of the competent authority if access to the RTP has been refused or revoked.

2. Upon expiry of the period referred to in paragraph 1, the Central Repository shall automatically delete the individual application file.

3. The registered traveller may keep the token.”

The merging of the three systems would require carefully assessing what is the necessary data retention period for each data category taking into account the purpose for which it is collected. The study associated with the report puts forward a variety of arguments for the harmonisation of these retention times. If VIS/RTP/EES integration was chosen as an appropriate approach, then such harmonisation becomes even more crucial to avoid the legal issues alluded to in this paragraph.

Finally, the merging of the systems will lead to a database containing data of TCNs subject to different rights as regard the free movement of individuals within the EU territory. In particular, TCNs that are family members of EU citizens and TCNs in possession of an EU resident permit should be subject to minimum checks at both entry and exit of EU external borders nor should their data be accessed by law enforcement authorities. In the associated study report, the pros and cons of including these classes of TCN in the various databases are discussed; in the case of VIS/EES/RTP integration, then the arguments for rendering their enrolment in the EES/RTP are increased. However, experiences with existing large-scale IT systems indicate that suitable access controls and separation of data logically can achieve the necessary categorisation of individuals and control of appropriate data access as required. By merging VIS, EES and RTP the safeguards granted by the existing physical separation would be greatly reduced and alternative measures **would need to be implemented in order to guarantee the full protection of TCNs’ rights.**

EES and RTP interaction with other IT systems

The Study concluded that SIS II and I-24/7 should remain separate systems from EES and RTP and therefore no analysis is carried out as regard the appropriate balance on system integration and personal data protection.

The study also concluded that APIs and passenger lists from ships will only be used for management of the queues at the border by Member States and should not be used as input for EES or RTP and therefore no analysis is carried out as regard the appropriate balance on system integration and personal data protection.

As regard the possibilities to re-use or integrate existing national systems, since such an option only includes the re-use of the architecture, no data protection concerns have been identified.

Main findings

With regard to the integration of EES and RTP with VIS, the main legal challenge relates to the principle of purpose limitation stemming from EU data protection legislation. The integration of the systems would thus require an amendment of the VIS legislation currently in force and the amendment of both EES and RTP legislative proposals to reflect such integration.

The Study concluded that SIS II and I-24/7 should remain separate systems from EES and RTP and therefore no analysis is carried out as regard the appropriate balance on system integration and personal data protection.

6.5.4. Consultation mechanism between authorities (TF17.4)

This sub-section of the Study discusses the addition of consultation mechanism between authorities. A consultation mechanism (e.g. which would be used during the RTP vetting) will be present, the question is how it will be implemented (in a similar way as to the VIS or using another, integrated technology).

In the workshop of 26 March 2014, MS authorities expressed diversified interest in having consultation mechanism. Some of the authorities were satisfied with the case of VIS and a specific consultation mechanism using the VIS infrastructure (the so-called VIS Mail solution). Based on MSs feedback it seems that given the required efforts and the complexity of its implementation as a separate solution, some MSs are in favour of a simpler, central-based messaging system.

VIS Mail has been developed in two steps, VIS Mail-1 currently running and VIS2, which will take-over both VIS Mail-1 and VISION services. VIS Mail-1 was developed as a specific communication network for the transmission of information for consular cooperation and for requests for supporting documents, for correction of data and for advance data deletion¹⁶⁴. It was designed after the VIS contract signature, and went live together with the VIS in 2011. VIS Mail-2 integrates VISION functionality, a consultation mechanism between MS authorities for visa purposes.

The end-users using this new consultation mechanism for e.g. TCNVE would be typically different (and may have separate budgets) from the ones who use VIS Mail.

A new consultation mechanism could be built based on notification features that would be available in the central system for any asynchronous call-back (such as the ones present in the VIS). The consultation mechanism would thus be easier to implement and maintain by MS and the Management authority. Having a separate system would bring additional expenses and effort in the implementation, the operation and the maintenance through a separate operation and release management scheme.

Main findings

The consultation mechanism shall be implemented; however, a decision still needs to be made as regards how this mechanism would be created in practice. A new consultation mechanism could be built based on notification features that would be available in the central system for any asynchronous call-back, making it easier to implement and maintain. A separate system would bring additional expenses and effort in the implementation, the operation and the maintenance through a separate operation and release management scheme.

– Re-use and integration of existing national systems (TF18)

This sub-section of the Study analyses the possibilities to reuse or integrate existing national systems and proposes the interface that will allow the existing national systems to integrate into

¹⁶⁴ EC implementing decision of 6.9.2013 amending the Annex to Commission Implementing Decision adopting the technical specifications for the VIS Mail Communication Mechanism.

the EES and / or RTP architecture. The question of national systems reuse is addressed generically and not in a Member State specific way.

6.6.2. Possibilities to re-use or integrate the existing systems with EES and RTP (TF18.1, TF18.3)

Some Member States have national Entry-Exit systems (NEES) and biometric border control systems. From a high level perspective those systems serve similar purposes (however identifying overstay is not the main reason for some) as EES, so their functional requirements are often similar, yet the information flows, data structures, architectural design can vary. The map of EU/ Schengen Member States recording of entries and exits is provided in the figure below.

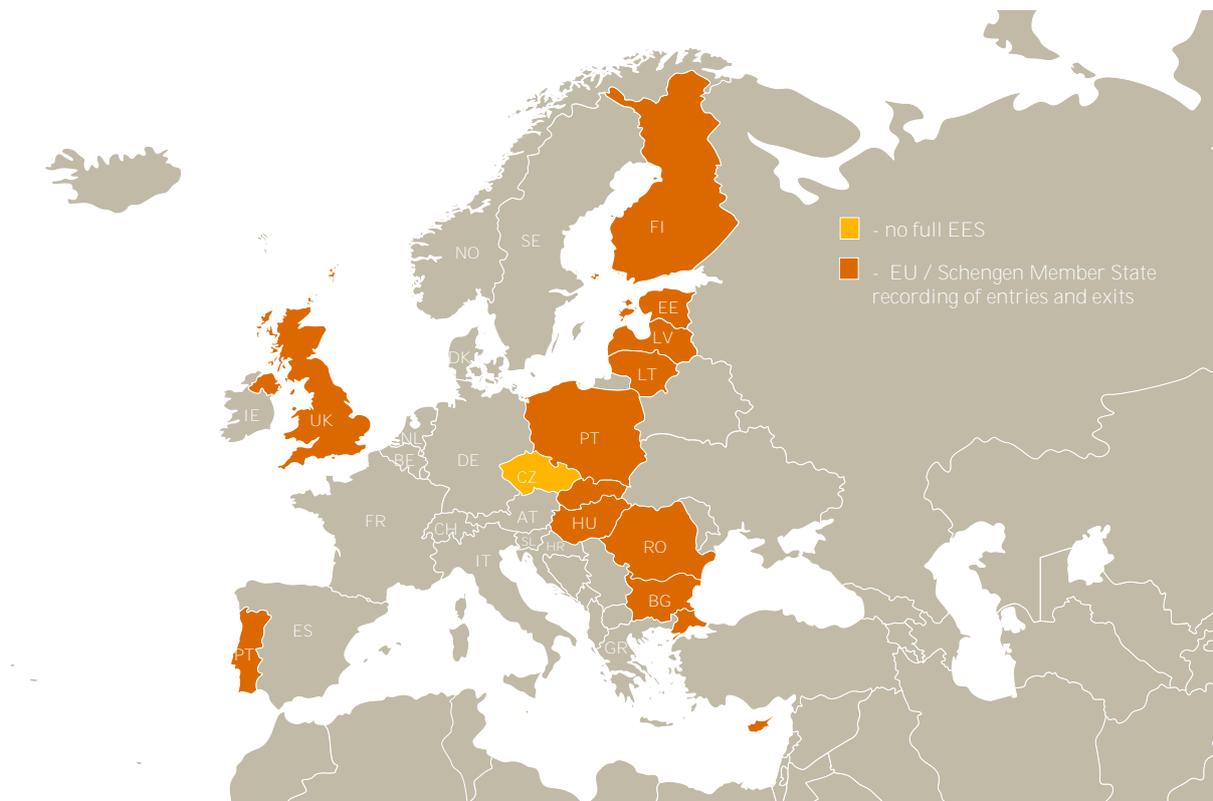


Figure 48 The map of EU/ Schengen Member States recording of entries and exits

There are also attempts to establish Registered Traveller Programmes that aim to facilitate the border-crossing duration for certain categories of travellers. The RTPs most often relies on the use of traveller's biographic or biometric data, such as fingerprints or an iris scan. However, RTPs are typically the result of private initiatives of the airports that intend to provide portfolios of commercial services for frequent-flyers.

The description, which illustrates the variety of national systems used for Registered Traveller Programmes and biometric border control, is provided in 0.

The leverage of investments made in EES, RTP and ABC gates at national level was one of the key concerns during the Workshop of 26 March 2014. Using and building on existing solutions is often the more cost-effective option and reduces risks. This also helps prevent a continuous increase in the number of systems with the increasing complexity.

There are several possibilities to re-use or integrate the existing systems with EES and RTP:

- The use of a common interface, in case a national system is capturing entry and exit data;
- The use of an MS-tailored interface;
- The standardisation of a national system for the benefit of other MS.

The use of a **common interface** for the existing systems towards the central application is discussed in the following section.

Given previous negative experiences, the implementation of an **MS-tailored interface** towards existing National Systems is not preferred. Recent history (VIS, SIS-II) has shown that developing a separate interface per MS can lead to a very divergent set of interfaces which are difficult to keep in sync, operate and maintain. This diversity has also been noted to be a hindrance for further evolution.

For MS that do not yet have any systems, **reuse of a National System** that has been proven comprehensive and satisfying in one MS could be viable option. This system could be implemented in multiple MS after having been made reusable. This approach was applied in the SIS II projects under an initiative of the Contractor and on a bilateral basis with interested MS. It is similarly the case of the contract just signed by eu-LISA with the Eurodac provider, whereby MS could sign specific contracts with the Contractor for the delivery of a kind of standardised national platform. During the analysis it became clear that an MS does not specifically need a separate National System, but can have its border management system interface directly with the National Uniform Interface (NUI) (see section 6.6.4) or via the MSs own service bus. As such this option was not retained.

The MS that already have an **existing NEES** will keep the system (with their data) for national purposes and the MS must implement the interface within their NEES to the interface defined by the National Uniform Interface (NUI) (see section 6.6.4). The wide variety of technical implementations in the MS makes it impossible for this study to analyse in detail. The NUI is meant to facilitate interfacing for these existing systems.

Main findings

Some Member States have national Entry-Exit systems (NEES) and biometric border control systems which, despite their similarities in terms of functional requirements, can vary as regards information flows, data structures and architectural design. There are also attempts to establish **RTPs, mostly using travellers' biographic or biometric data. However, they are** typically the result of private initiatives by airports. There are several possibilities of re-using or integrating the existing systems with EES and RTP, including the use of a common interface, the use of an MS-tailored interface or the standardisation of a national system for the benefit of other MS.

6.6.3. Data aggregation (TF18.4)

This subsection addresses the TF question of data aggregation, i.e. whether central system holds all data or that the data is distributed about multiple (national) systems and is merely aggregated in the central system.

There will be no data aggregation as all data will be stored on the central system. The existing national systems will insert / modify their data in the central systems. For the central system there will be no difference and as such this will have no impact on data aggregation.

Main findings

There will be no specific data aggregation as all data will be stored on the central system. The existing national systems will insert/modify their data as in the other systems.

6.6.4. Definition of the common interface (TF18.2)

This subsection of the Study provides the definition of the common interface between national systems and the central system particularly where a national system capturing entry and exit data already might exist and the connection to a central system should induce as little changes as possible. Regardless of the back-end implementation of a national EES (NEES) or border management system, there is a case for a **unified interface layer**, namely the **National Uniform Interface (NUI)**.

This is in particular described in the COM legislative proposal on the EES¹⁶⁵ (COM(2013) 95). This NUI, together with a possible abstraction layer at the central site, would also help shielding the implementation details of the different components of this central system.

This NUI would also help alleviate some of the problems encountered within the context of some of the large-scale information systems in the field of Home affairs, such as:

- The lack of a reliable messaging solution at the Member States premises, meaning that the MS need to implement an in-house solution aiming at offering reliable messaging, such as a retry mechanism;
- The absence of a flow control mechanism at message level.

The NUI could be designed to offer the following features, which will be described in more detail in the following section:

- *Reliable Message Transport (RMT);*
- *Flow Control (FC);*
- *Pass Through;*
- *Multiple Callback Capability;*
- *Message orchestration;*
- *Logging Services on behalf of the National System;*
- *Technical monitoring and reporting.*

The NUI should be seen as a further evolution of the current concept of a generalised National Interface which would provide additional features to the network delivery. For the Member States this NUI would make no difference in the business services that are offered by the Central System and in how they are accessed. The NUI brings additional features that do not affect the message structure and content.

In the following sections the NUI will be looked at in more detail, in the first section the possible location of the NUI will be discussed together with the impact this has on the services offered by

¹⁶⁵ The EES shall be composed of:

- a Central System comprising a Central Unit and a Back-up Central Unit, capable of ensuring all the functionalities of the Central Unit in the event of the failure of the system;
- a National System comprising the required hardware, software and national communication infrastructure to connect the end user devices of the competent authorities as defined in Article 7(2) with the Network Entry Points in each Member State;
- a Uniform Interface in each Member State based **on common technical specifications and identical for all Member States**;
- the Network Entry Points, which are part of the Uniform Interface and are the national points of access connecting the National System of each Member State to the Central System; and
- the Communication Infrastructure between the Central System and the Network Entry Points.

the Central System. Afterwards the architecture is looked at in detail and the possible operational management is discussed.

6.6.3.1. Impact of placement of the NUI features

The NUI is foreseen by the legal basis in the Member State domain. Current experience has shown that there are possible challenges for the Management authority with a partial de-centralised mode of operations shared with Member States, i.e. when some logic is supported by devices located in each Member States geographical area, thus requiring at least a partial support from the MS.

Most notably the impact is on operational management, but also on cost, security and organisation, and the concern lies with maintenance at remote locations as an option in which the features of the NUI are located in the Central domain is also examined.

NUI in Member State domain

When the NUI would be placed in the Member State domain its features are described in the table below

Table 86 Features supported by the NUI in Member State domain

Feature	Description
Reliable Message Transport (RMT)	RMT ensures that once an asynchronous message is delivered to the NUI, the sender is guaranteed to get a response back from the Central System, even if it is temporarily impossible to be reached at a given time. RMT caters for buffering (in input queues) that hides transmission problem and applies transmission retry logic as long as necessary with the Central System. RMT requires as well its counterpart in the Central System that implements corresponding output queues. The impact is very limited in the Central System, which already implements these queues for example in VIS and SIS II. The sole difference is that the messages are not sent by an in-house national web service but by the queue manager of the NUI.
Pass through	For synchronous messages the NUI will act as a pass through towards the central systems, as there is no need to queue them: synchronous messages have to be processed immediately after their submission and in parallel by the Central System. Having a Pass through service allows having a generic architecture.
Flow Control (FC)	FC will make sure that the Central System is not swamped with messages by performing traffic shaping at the message layer. It ensures that the number of messages does not exceed a specific ceiling per unit of time.
Multiple Call-back Capability (MCBC) for asynchronous calls	MCBC will make it possible to register multiple Call back addresses and as such will enable multiple National Systems to perform asynchronous calls.

Feature	Description
Message orchestration	<p>Message orchestration would perform de/multiplexing of messages. For example, a unique search message from a NS with a passport number and the issuing country could be split in 3 messages for EES, RTP and VIS respectively. Then the feature will combine the results before sending back to the NS.</p> <p>This feature is the logical consequence of data minimisation (absence of duplication) where the data has to be retrieved from each of the underlying systems.</p>
Logging service (LoS)	LoS will create a logging of all requests, traffic, etc. It would complement the National System(s) logging services, as far as the exchanges with the central System are concerned.
Technical monitoring and reporting	Technical monitoring and reporting provides information about the workings of the NUI, such as the availability, number of accepted and rejected messages, enforcement of data protection rules and other technical monitoring related information especially useful in case of local or remote diagnosis for example following an incident.

NUI in Central domain

When placing the NUI features in the Central domain, this implies that some of these features are useless (such as the RMT that is supposed to encompass the Testa-ng network) or offer very little added value.

Technically, this means that in the Member State domain there is no centrally-managed device/solution present that operates at the application layer (layer 7 in the OSI model) but only devices which operate at the network layer (layers 3-4 of the OSI model) as in the current VIS National Interface (i.e. precisely Network Entry Point). The situation is described in the table below.

Table 87 Features to be performed by NUI in Central domain

Feature	Description
Reliable Message Transport (RMT)	<p>As RMT operates at the layer of business messages (i.e. application layer) this implies that RMT is not possible at the Member State when the features of the NUI are placed in the Central domain. A RMT located centrally would have no interest as it would not hide the network interruptions of service.</p> <p>Each MS would have to implement a separate solution in their National System. This would lead to a situation where the implementation would be left up to the MS choice, with no guarantee of (uniform) implementation. Which would also imply that MS may have problems when managing their systems if a messaging system is used which is not standardized across all MS. This could require more intervention of the Management authority in terms of support.</p>

Feature	Description
Pass through	For synchronous messages the NUI will act as a pass through. This feature would be useless as it would mean that the National System liaises directly with the Central System such as with the VIS today
Flow Control (FC)	It is best practice to enforce the FC as close as possible to the sender, but this could also happen in the Central domain. This might have a negative impact on bandwidth however as the connection requests towards the central site are made before FC policing takes place at the central site.
Multiple Call-back Capability (MCBC) for asynchronous calls	Given the current setup in which, the choice has been made to have only a single IP address per MS, it would not be possible to have multiple call back addresses if this feature is located in the Central domain. This implies that multiple IP addresses per MS would need to be provided or that this functionality would need to be implemented by the MS in their National System. If implemented by the MS this would mean an additional cost per MS and add complexity.
Logging service (LoS)	This will not be impacted by the location of the NUI, but at a first sight it would appear illogical presenting this as a service specific to the National System but located centrally.
Technical monitoring and reporting	This will not be impacted by the location of the NUI, but would have a more limited interest for stakeholders such as the MS as the data would be predominantly about the central working.

6.6.3.2. Architecture of the NUI

The logical architecture for the NUI is described in the figures below, indicating where the different services would be offered. Although only a single site is shown in the picture of the architecture (for reasons of readability), it has to be inferred that the exact same solution is also deployed in the backup site. As such "(B)CEP" means the CEP in the Central Unit and the BCEP in the Backup Central Unit and thus the "Central domain" encompasses both sites. The terms used in the architecture are taken from the current VIS setup and from the legal proposal; they are summarised in the table below.

Please note that the Legal proposal considers the NUI as also comprising the National End Point (NEP), which is purely a network component. For the sake of simplicity only, the NEP appears as separate in the following drawing.

Table 88 Terms, abbreviations and acronyms used to describe the NUI logical architecture

Term/abbreviation/acronym	Meaning
Border management system	The (existing) system used by a MS to operate the border processes
(B)CEP	(Backup) Central End-Point
ICD	Interface Control Document
LNI	Local National Interface
National System	An (existing) national system operated by the MS (e.g. a national EES)
National visa system	The system that is used by the MS to operate the visa process.
(B)NEP	(Backup) National End Point
NUI	National Uniform Interface
Testa-ng network	A European backbone network for data, it connects the MS with the Central Site.

The NUI offers “supporting” features, the business services being defined in an ICD for each central system. So depending on whether or not EES and RTP will be integrated there will be 2 or 3 separate and different ICDs to describe the EES, RTP and VIS. Given the potential economy of scale, some of these ICDs may however be offered via the same component (LNI, NEP), but in such a case additional measures will need to be taken to ensure that traffic flows are separated.

NUI features in Member State domain

The figure below shows the logical architecture for the NUI and its relation to the VIS setup in the Member State domain. The existing VIS components are not impacted by the introduction of the NUI. Only where the National visa system wants to access functionality from the EES or RTP, is a message sent via the NUI.

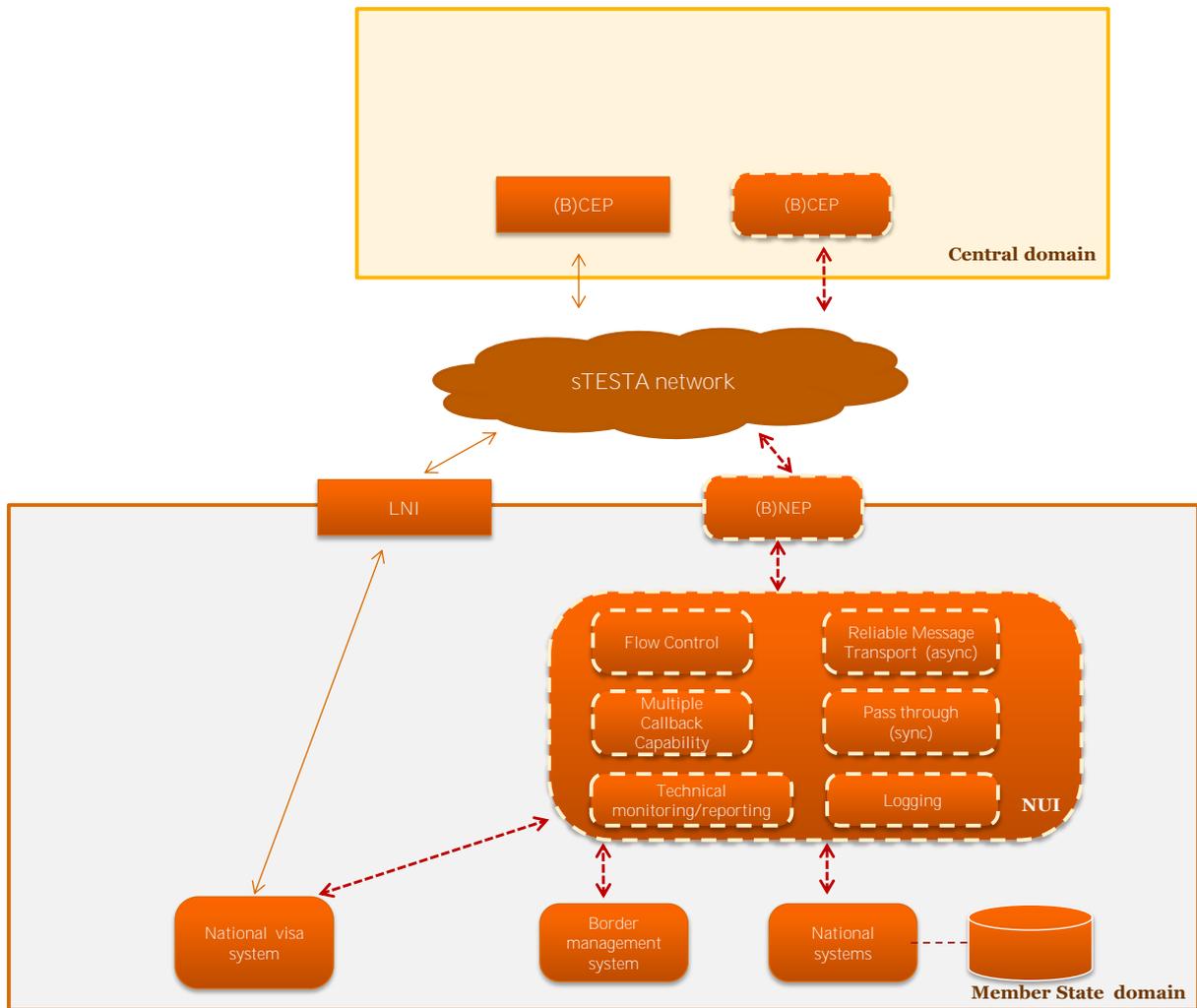


Figure 49 Logical architecture for the NUI separated from VIS components

NUI features in Central domain

When the features of the NUI would be placed in the Central domain, the following architecture would be foreseen. As an RMT component has to be present in the Member State domain, there are different possibilities (MS implements the RMT functionality centrally, or it has this functionality spread out over multiple applications). The architecture below is therefore only indicative in this respect.

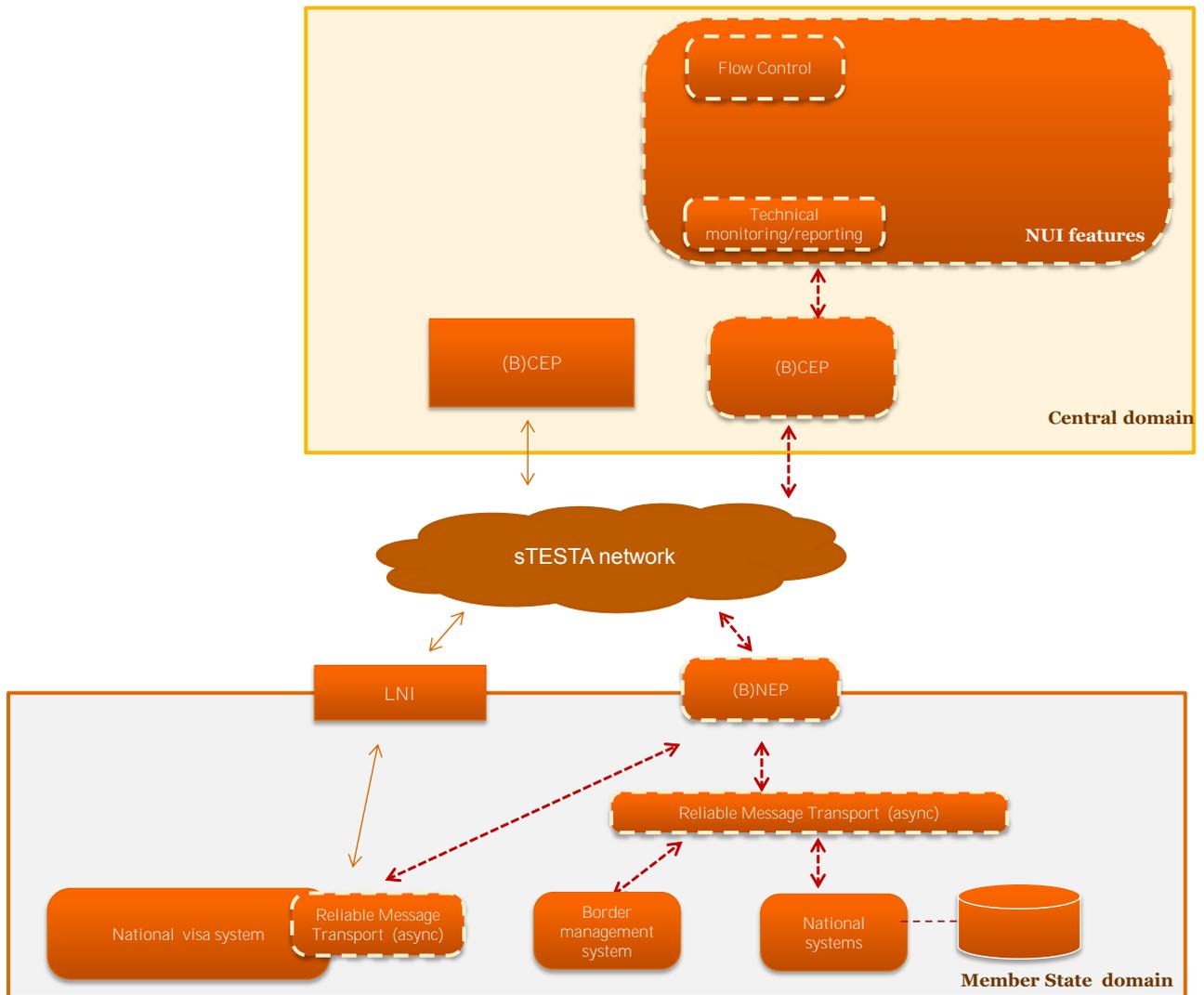


Figure 50 Logical architecture with the NUI features implemented in the Central domain

The advantages and disadvantages of having the **NUI** in the **Member State domain** are listed in the table below.

Table 89 Advantages and disadvantages of placing the NUI in the Member State domain

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> • Better recovery after network outages. • One common solution for all MS • Comparable to the current SIS II solution, as regards RMT. • Lighter integration of national system in the European framework or easier implementation of national system solution: no need to implement flow control, RMT and logging mechanism in the national system. 	<ul style="list-style-type: none"> • Complex deployment and implementation.

	Advantages	Disadvantages
<i>Recurrent</i>	<ul style="list-style-type: none"> • Increase national service resilience: higher data quality (strong data consistency between national and central systems), less technical errors, and thus less operational and maintenance efforts needed. • Better control over network usage. • Features perform their task as designed. 	<ul style="list-style-type: none"> • Maintenance in Member States domain might be a problem (e.g. remote hands), although mitigation measures are possible. • Operational management impacted by MS (partial shift from the national system to the NUI). • Potential cost and <u>security impact</u>.

Main findings

The setup of the NUI in the Member States domain has multiple advantages and allows the features to be performed in the most effective way. The impact on operational management would be overall positive with potentially slightly more involvement on the NUI but less intricacies on the national system and the data exchanges.

The advantages and disadvantages of placing the **NUI** features in the **Central domain** are listed in the table below.

Table 90 Advantages and disadvantages of placing the NUI features in the Central domain

	Advantages	Disadvantages
<i>Onetime</i>	<ul style="list-style-type: none"> • This setup would be in line with the vision of having a fully centralised architecture. 	<ul style="list-style-type: none"> • Each MS would need to implement the RMT itself. This would mean that there would be a need to interface with all the different queuing systems at the MS, which would lead to additional complexity; • It would be strange to have a Logging feature specific to the National System but located centrally.
<i>Recurrent</i>	<ul style="list-style-type: none"> • Maintenance of this setup would be well controlled and the change management would be fully under control of the central site. 	<ul style="list-style-type: none"> • Additional resources to manage the exchanges with the central system and the potential data discrepancies; recovery procedure to be established and applied in case of outages; • No RMT in the Member State would mean that this would not hide the network unavailability from the MS; • By not having the Flow Control near the sender this would be less effective; • The technical monitoring and reporting would have a more limited interest.

Main findings

Although the setup with the NUI features placed in the Central domain is in line with the vision of a fully centralised architecture and have benefits from an operational management perspective, the impact on the features is huge. A number of features offered cannot be well (or only partially) implemented on the Central domain, which would lead to more complicated and divergent architectures in the MS.

6.6.3.3. Operational management of the NUI

The operational management of the NUI is an important aspect of the analysis of the architecture and the placement of the supporting features has an impact on it. Irrespective of their limited interest, if the features offered by the NUI were placed in the Central domain it is clear that it falls under the responsibility of the central site.

When the NUI is placed in the National domain however there are two main possibilities: a) the NUI is built and operated by the central site, b) the NUI is built by the central site, but its operation is shared with the MS. **In the figures below the “demarcation of responsibility” is shown, indicating that everything “above” the line falls under the responsibility of, and is operated by, the central site.** The components below this line fall under the responsibility of, and are operated by, the MS.

The first option shows the case in which the **NUI is built and operated by the central site**. This has the operational impact that a (rather) complex system is to be operated by the central site, while it has little control over the physical operation of the system, as well as difficulty in monitoring the system and ensuring the continued integrity of the installation.

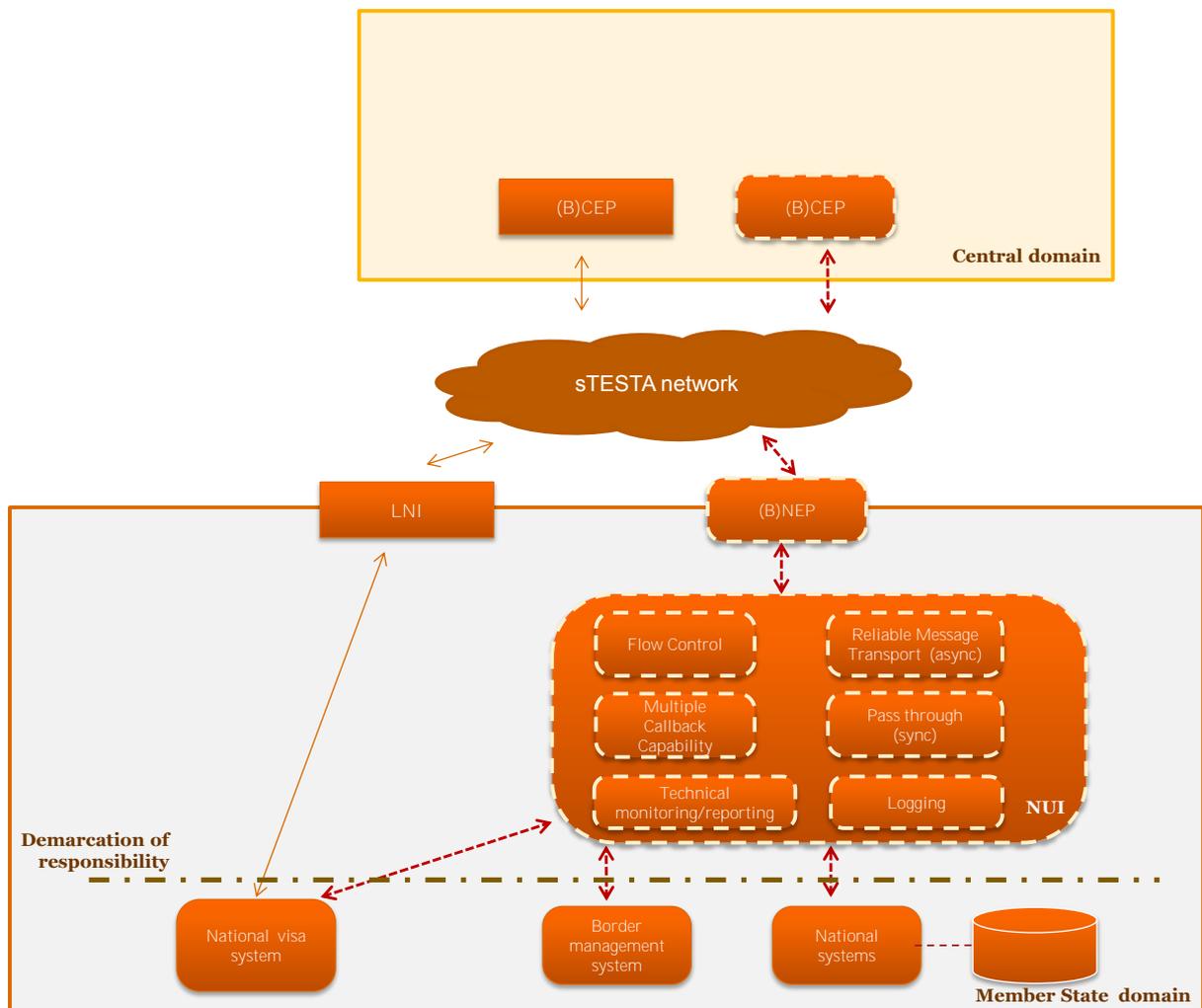


Figure 51 Demarcation of responsibility when NUI build and operated by central site

In the second option the **NUI is built by the central site, but operated by the MS**. As such it falls under the responsibility of the MS. This has the advantage that the MS has easy access to the NUI and can integrate the change (and other operational) management with that of the other systems it operates. However, it implies that the MS has the resources and the knowledge to operate the NUI.

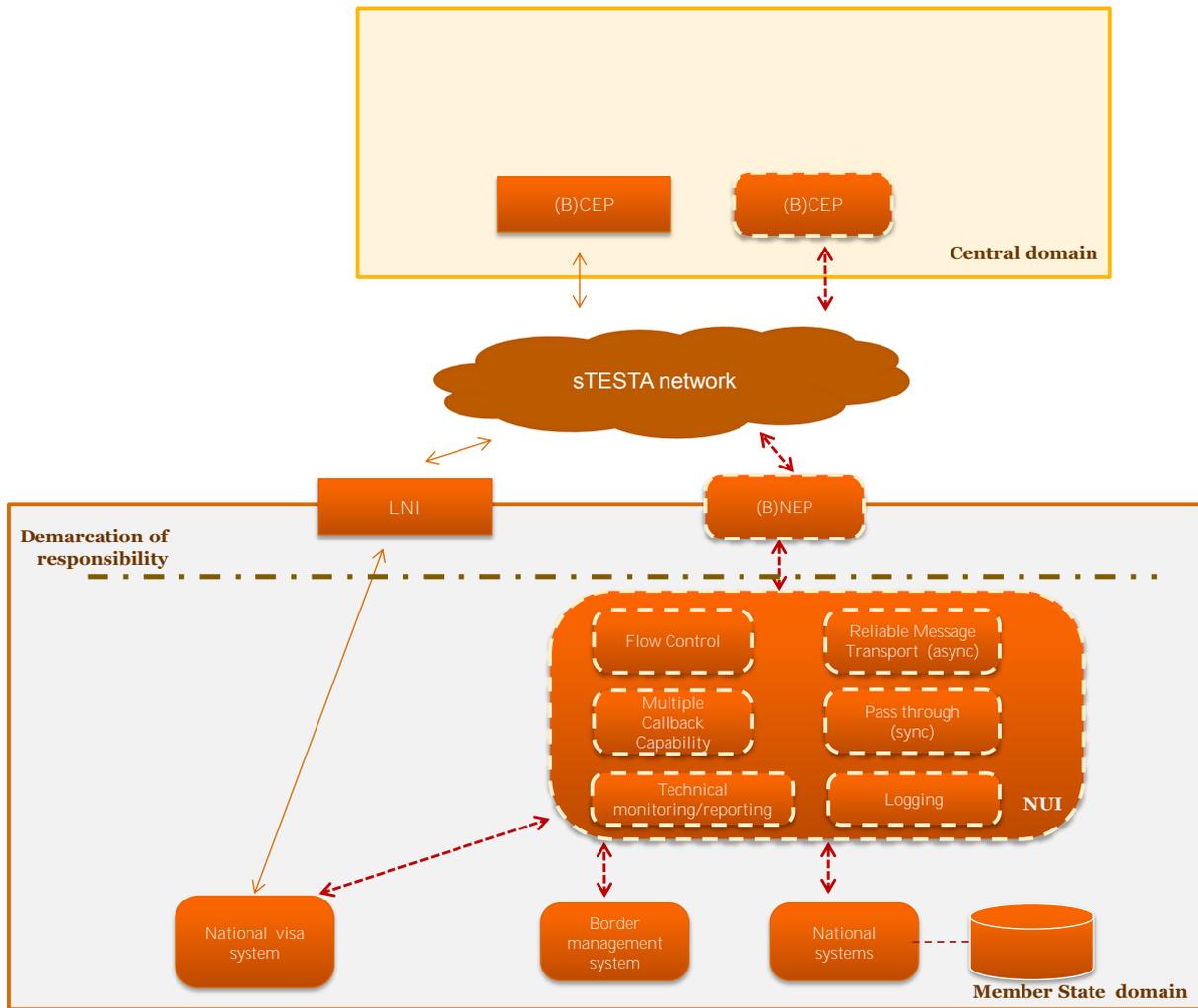


Figure 52 Demarcation of responsibility when NUI build by central site and operated by MS

The advantages and disadvantages of having the **NUI built** and **operated** by **the central site** are listed in the table below.

Table 91 Advantages and disadvantages of having the NUI built and operated by the central site

	Advantages	Disadvantages
Onetime	<ul style="list-style-type: none"> A uniform NUI is built and is deployed in all the MS. 	
Recurrent	<ul style="list-style-type: none"> Processes can be fully integrated in standard operational management. 	<ul style="list-style-type: none"> Maintenance and operation to be performed by central site, which can be difficult and costly when physical access is needed (e.g. installing machine, power cycling, patching cable); Working of the NUI may be impacted by changes or events at MS location.

Main findings

Having the NUI built and operated by the central site has the advantage of being able to have a fully integrated approach in which a standardised operational management can be used. There are however problems when physical access to the machines is needed or when the working is affected by events at MS location

The advantages and disadvantages of having the **NUI built** by the **central site** and **operated** by **the MS** are listed in the table below.

Table 92 *Advantages and disadvantages of having the NUI built by the central site and operated by the MS*

	Advantages	Disadvantages
Onetime	<ul style="list-style-type: none">• A uniform NUI is built and is deployed in all the MS in the context of the central system implementation.	<ul style="list-style-type: none">• MS might not have the resources or the competencies to operate the NUI.
Recurrent	<ul style="list-style-type: none">• Maintenance and operation performed by MS, which have easy access to the NUI;• MS has full control over events or changes that might impact the working of the NUI.	<ul style="list-style-type: none">• Possible impact of change management by the MS on the central site;• Change management would need to be strictly synchronised as otherwise multiple different versions of the NUI might be around.

Main findings

Having the NUI built by the central site and operated by the MS has many advantages: the maintenance and operation is performed by the MS which has easy access to the NUI and it can also be well integrated in the standard change management by the MS. The possible impact of changes at MS level might have a knock-on effect on the central site. Therefore these would need to be synchronised.

For the operational management of the NUI the following distribution of tasks could be envisioned:

- Daily monitoring (central);
- Local interventions in case of incident – outage, first level investigation (local but under central coordination);
- Technical maintenance - hardware & software upgrades (central, with local support if needed);
- Business evolution - implementation of new features (central).

6.6.3.4. Possible future evolutions

During the Study on the NUI a number of possible future evolutions were identified. These ought to be taken into account when defining the detailed technical solution for Smart Borders. Below these are represented for reference only.

Integration of LNI – NEP at MS

Because of economies of scale and ease of management, it might make sense to merge the network end points (LNI – NEP) in the Member State domain of EES, RTP and VIS in one (two for those member states opting for a business continuity point). The following figure describes this evolution of the standard architecture in which the functionality of the VIS– LNI is extended to support the EES and RTP communications. Consequently the different CEPs in the central domain would also be merged. This means that messages from the national visa system for the VIS would go via the NEP, through which all messages from the NUI would also flow. It is obvious that strict measures need to be employed at the NEP and CEP to ensure the segregation of the different traffic flows.

One of the advantages of a set up in which the LNI is integrated in the NEP is that it reduces the number of components in the Member State domain by a factor 3: 1 NEP and maximum 1 BNEP versus 3 NEPs and maximum 3 BNEP. Similarly there is the reduction in number of CEP's at the Central domain which would lead to an administrative simplification and better maintainability.

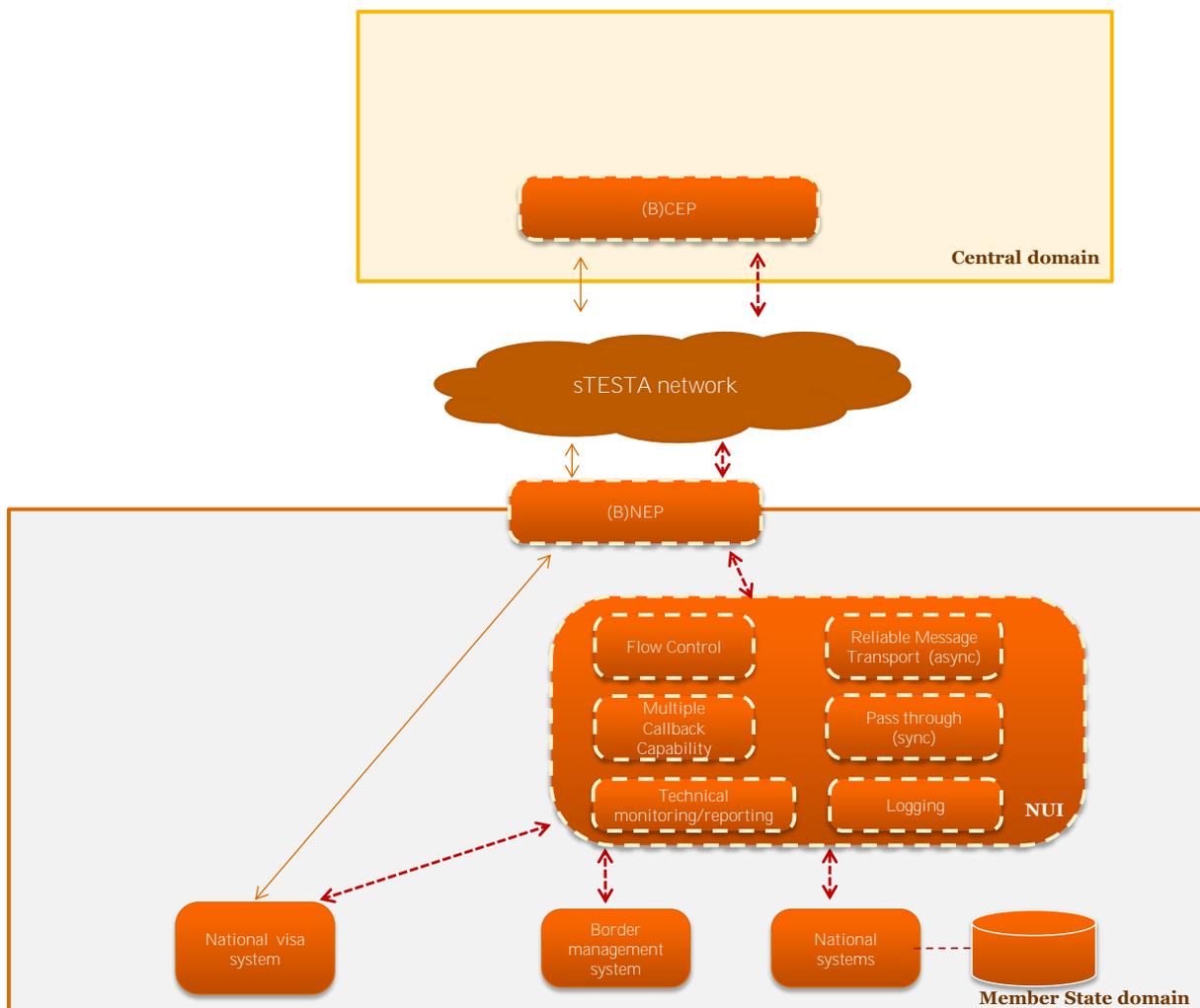


Figure 53 Logical architecture for the NUI with integrated LNI and NEP functionality

Additional features of the NUI

The following are additional features that the NUI might offer. They were mentioned during discussions, but are not fully elaborated at this moment. They are only mentioned here for future reference.

- Possible routing to both CU and BCU: it could be envisioned that the NUI plays an active role in making the routing decisions between CU and BCU. How this would integrate with existing fail-over mechanisms would need further research;
- NIST file creation and validation: In VIS there are various problems where NS are not always formatting a valid, correct or complete NIST file (the fingerprint container definition). The NUI could make sure that the MS send fingerprint images and facial-images that are coded by the NUI;
- Gateway to VIS: Although all MS have by now implemented the VIS in their national border management system, the EES and RTP will again 'mess-up' this user-interface and BC-application. The NUI could function as a 'concentrator' for sending data to EES/RTP and VIS in parallel and waiting for a response from both to continue the workflow. This will already be partially implemented because of the data minimisation that is described above, while the orchestration between the different applications (EES / VIS / RTP) is also described above. This could also have a positive impact on the synergies of between EES / RTP and VIS (see section 6.4);
- Publish and subscribe interface for daily overstayer data: the list of actual overstayers will be generated on a daily basis. Somehow it needs to be shared with the MS; it is foreseen that this will at least be made available as a static, flat file via FTP. Each entity may want a different form and frequency and layout. The NUI could store the overstayers in a generic XML file which various entities can 'manipulate in an automated way';
- National register of border-crossing point codification: surely, in each MS, the various border-crossing points will be identified in a very different way. At the central level, there need to be a coherent codification. The NUI could contain a translation table between the national codification and the SB codification (e.g.: Germany uses a numerical identifier: 113700 is Hamburg airport while Netherlands uses the ICAO codes: EHAM is Schiphol airport. At the EES level we would probably want an ISO 3166 coding: DE/HH/HAM and NL/NH/AMS). This would however require message inspection, but by performing the translation at the MS side this would allow working with a single, coherent ICD;
- XML translation: it could be envisioned that various national systems (BC, Police, Immigration, MFA) would want (or need) to talk a different 'ICD dialect' with the NUI than the actual Smart Borders ICD. By acting as a translator the NUI could ensure that these different systems can all talk to the Central System. This however could lead to a way of NUI customisation; a balance would have to be found between a uniform and customised national interface;
- Gateway to other IT systems: the NUI could be a generic gateway for MS systems to other central IT systems (such as SIS II or I-24/7). As such it could provide a single interface for the MS systems that need to interact with external systems.

• **Statistics and forecasts**

Objectives

Quantitative data are fundamental for assessing the size and structure of the EES and RTP population, as well as the impact that the new processes will have on the current situation.

The aim of this chapter is to present the statistics and data gathered, mainly from the MS and the VIS, addressing TF20. These data were used to forecast the magnitude of the flows of passengers in 2020 and in 2025 (as presented in section □□), which led to the estimation of the number of travellers registered in the EES, as well as of the potential demand for the RTP.

The scope of the statistical analysis presented in this chapter is defined in TF20:

- Collection and analysis of counts of travellers crossing external borders performed by MS during an agreed period of time;
- Analysis of visa statistics.

Approach

The Study's approach consists of the following steps:

1. **Statistics on visas issued:** breakdown per type and trends over the period of time (section 7.1).
2. **One-week data collection by the MS¹⁶⁶:** all entries and exits at the external borders of the Schengen Area (with the addition of Bulgaria, Croatia, Cyprus and Romania) were recorded during one week, from 12 to 18 May 2014 (section □□).
3. **Extrapolation of border crossings for the entire year 2014:** border crossings for 2014 were calculated by multiplying the data collected during one week by a factor estimated by using the historical data from the VIS (first line checks per week during one year ¹⁶⁷) as benchmark (section □□•).
4. **Estimation of average yearly growth rates:** estimation made on the basis of a review of relevant documentary sources, such as ICAO¹⁶⁸, CLIA¹⁶⁹, Frontex¹⁷⁰, Boeing¹⁷¹, IATA and Airbus¹⁷² (section □□•).

¹⁶⁶ Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland (note: Liechtenstein was also invited, but has no BCPs).

¹⁶⁷ The quality of the data within the VIS depends on the MS's implementation of the first line VIS check (with or without FPs)

¹⁶⁸ ICAO – Aviation Data – http://cfapp.icao.int/tools/38thAssyikit/story_content/external_files/EconomicDevelopment_AviationDataAndIndicators.ppsx - last accessed June 2014

¹⁶⁹ http://www.irn-research.com/files/9913/9480/6948/CLIA_Europe_Stats_and_marts_2013.pdf, last accessed in June 2014

¹⁷⁰ 2011 – Frontex – “Future of Borders” – http://frontex.europa.eu/assets/Publications/Research/Futures_of_Borders.pdf

5. **Projection of the border crossings to 2020-2025:** estimation of future flows of passengers by applying the average growth rate to the figures for 2014 (section □□◦).
6. **Estimation of the number of individual files stored for EES and RTP:** number of people whose data would be captured in the systems, calculated by using the number of visas issued in one year as benchmark and the estimations of returning travellers among VE travellers (section □□◦).
7. **Estimation of potential RTP demand:** calculation of the potential demand for the RTP among VH and VE travellers (section □□◦), based on the number of multiple entry visas (MEV) issued, on the adoption rates in other comparable programmes and on the usage of ABC gates.

Assumptions

- No radical changes in the international traffic of travellers;
- No significant changes in the distribution of border crossings across the various border types and passenger types;
- No changes in the current list of visa-exempt countries that would have a significant impact in the composition of travellers entering and exiting the Schengen Area;
- No significant changes in the rules for granting Schengen visas;
- A new data collection would be performed should any additional MS join the Schengen Area, in order to assess the impact on border traffic.

– *Statistics on visas issued*

This section presents the data from the statistics collected by DG Home Affairs¹⁷³ from the Schengen countries regarding short-stay visas issued over the years, their breakdown by type, and the number of first-line checks. The VIS statistics have been instrumental in gaining a better understanding of the current situation for VHs, which have been used as reference to estimate the border crossings in 2014 (see section □□◦) and to estimate the number of unique travellers (see section □□◦).

The statistics collected are on airport transit visas ('A visas') and uniform short-stay visas ('C visas') both for single entry and multiple entries ('MEV'). Short stay visas can also be of limited territorial validity ('LTV'). Most of the short-stay visas issued in 2013 were either C single entry visas (≈54%) or C MEV (≈45%), while C LTV visas represented only 1% of the total number of visas issued. A visas were only marginal and accounted for only 0.1% of the visas issued.

The number of short-stay visas issued has increased steadily over the last few years, growing from 11 million in 2010 to more than 16 million in 2013, with a yearly growth rate of 13% to 15%. MEVs accounted for most of this growth, almost doubling in number and reaching more than 7

¹⁷¹ <http://www.boeing.com/boeing/commercial/cmo/index.page> - last accessed June 2014.

¹⁷² <http://www.airbus.com/company/market/forecast/> - last accessed June 2014.

¹⁷³ Statistics available on http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-policy/index_en.htm - last accessed. July 2014

million, representing 45 % of all the A and C visas issued in 2013 vs. 34% in 2010 (see Figure 54).

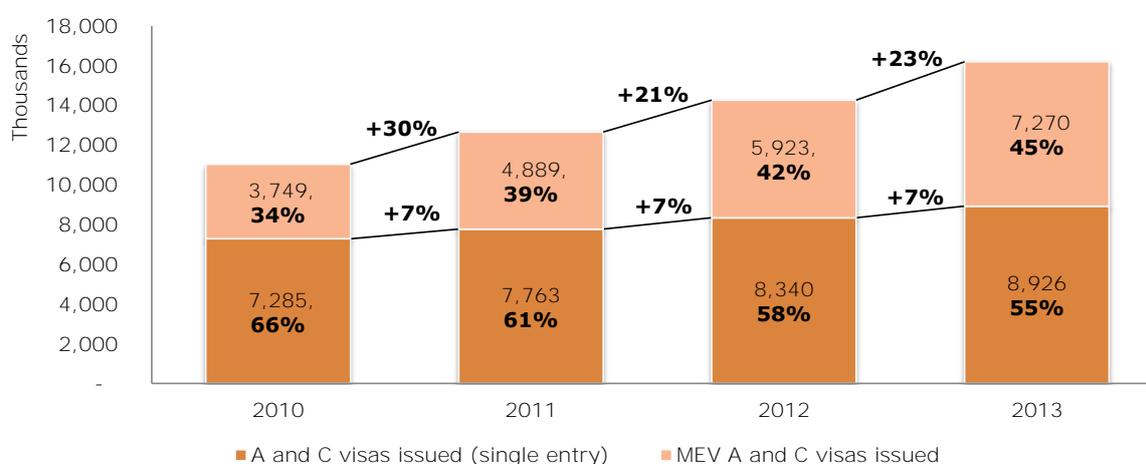


Figure 54 Number of visas issued per year by the Schengen Area MS with a breakdown between MEVs and single entry visas (in thousands) - Source: DG Home Affairs

The number of visas issued can be read as an approximation of the number of VH that travelled to the Schengen Area in 2013, which has been instrumental in estimating the number of people that could be registered in the EES in the future (see section □□).

– Data collection from the MS in 2014

◦ Overview of data collection exercise

From 12 to 18 May 2014, MS carried out a sampling exercise to obtain statistical data regarding border crossings at the external borders. In total, 30 countries¹⁷⁴ were invited to count both entry and exit border crossings per border type (air, land and sea) and for each category of travellers (EU citizens, visa-exempt and visa-required TCNs). The table below presents the data collected during the exercise.

Further investigations took place over the course of the Study to improve and refine the understanding of the situation at the various borders across Europe. Among the additional information collected, four MS provided indications on the likelihood that the same VE passenger would cross the border again over a certain period of time. This indication was then used to support the computation of the number of individual files that will be stored in the Smart Borders system(s).

¹⁷⁴ Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland (note: Liechtenstein was also invited, but has no BCPs).

Table 93 Data collection exercise carried out by MS in 2014

Data collected	Sample size
Entry and exit border crossings for air, sea and land borders: <ul style="list-style-type: none"> • For TCNVEs; • For TCNVHs; • For EU citizens. 	28 MS (24 Schengen countries out of 26, plus Bulgaria, Cyprus, Croatia and Romania) out of the 30 invited.
Entry and exit border crossings for air, sea and land borders through ABC gates.	10 MS (9 Schengen countries plus Bulgaria) out of 12 ¹⁷⁵ with ABC gates installed.
Estimation of differences in traffic between peak and off-peak periods	20 MS (17 Schengen countries, plus Bulgaria, Croatia and Romania).
Additional data requested	
Border crossings of TCN-VE due to the same traveller in a given period of time	5 MS (4 Schengen countries, plus Romania).
Number of border crossings with Local Border Traffic (LBT) permits	4 MS (3 Schengen countries, plus Romania).

Schengen countries and MS yet to join the Schengen Area.

Data from Bulgaria, Cyprus, Croatia and Romania were collected to enable a better assessment of the magnitude and complexity that the Smart Borders system(s) will have to address when these countries join the Schengen Area. However, the Study focuses on the current list of Schengen countries. In fact, adding the values collected for the MS yet to join the Schengen Area would introduce a significant bias, as their external borders would change once they have joined. For these reasons, these MS are presented as a separate group in the following sections.

Outcome of the one-week data collection

During the data collection week, 24 Schengen countries registered more than 10 million border crossings at the external Schengen borders (52% at entry and 48% at exit). An additional 3.6 million crossings were recorded in the four countries that are not yet part of the Schengen Area.

The number of crossings by EU citizens (6.7 million) is almost twice as high as the sum of crossings by TCNVE and TCNVH (3.4 million), representing 14% and 20% of crossings respectively (see Figure 55) in the Schengen Area.

¹⁷⁵ Austria (test unit), Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Netherlands, Norway, Portugal, Spain, United Kingdom. Source: MS answers to questionnaire (February 2014).

As regards Bulgaria, Cyprus, Croatia and Romania, the distribution per type of passengers is different as the weight of EU citizens is higher (86% vs. 66% in the Schengen Area). This could be explained by the exchanges these nations have with bordering Schengen countries.

Moreover, the share of border crossings by TCNVHs is considerably lower than in the Schengen countries, and is even lower than the share of crossings by TCNVE (see Figure 59).

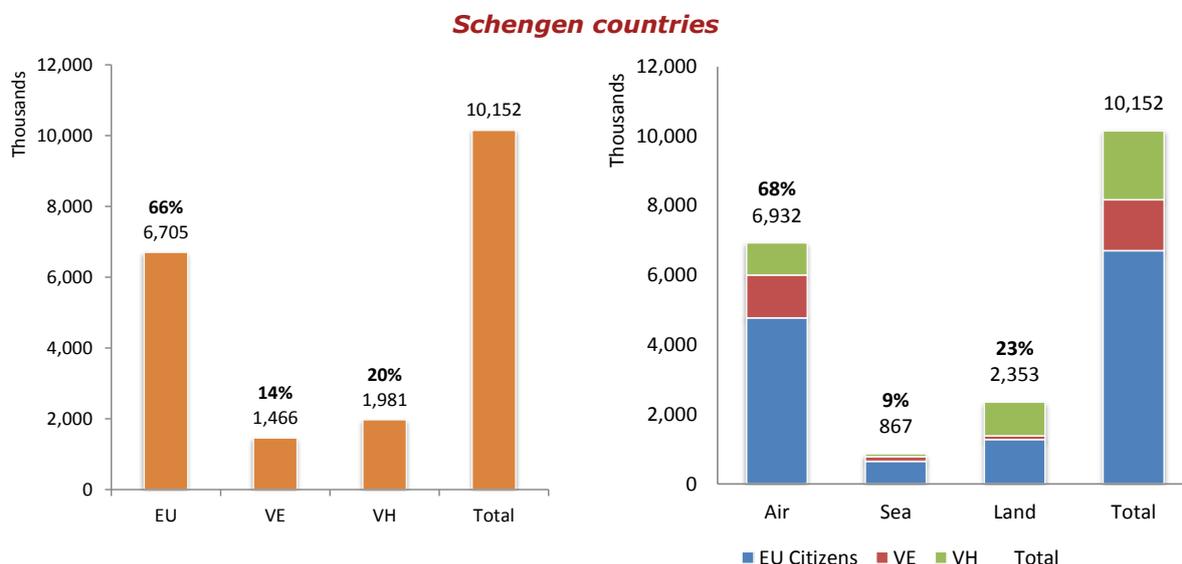


Figure 55 Breakdown of entry and exit border crossings per passenger type (for 24 Schengen countries) – Source: data collected by MS during week 20 of 2014.

Figure 56 Breakdown entry and exit border crossings per border type (for 24 Schengen countries) – Source: data collected by MS during week 20 of 2014.

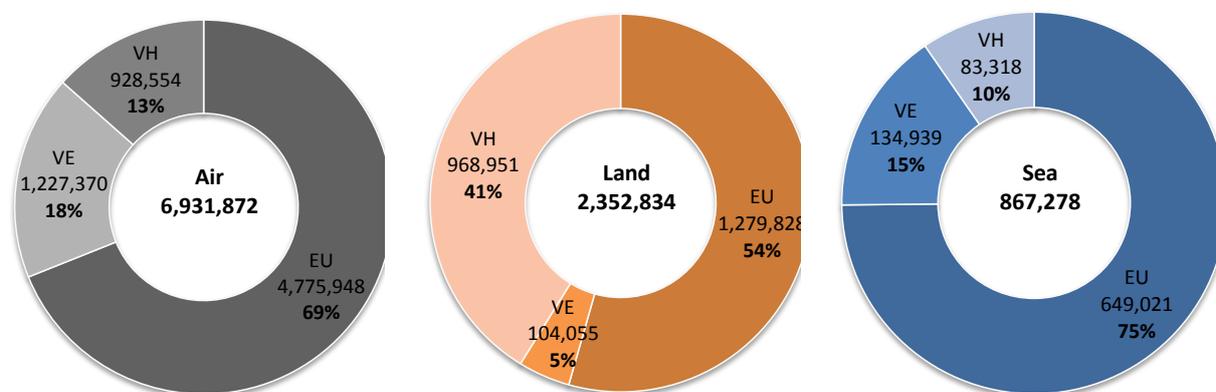


Figure 57 Breakdown of the entry and exit border crossings for the Schengen countries per type of passenger across the various types of borders – Source: data collected by MS during week 20 of 2014.

Air borders represent by far the largest share of external border crossings (68%), before land borders (23%) and sea borders (9%) (see Figure 56). However, the number of crossings by VHs is slightly higher in absolute number at land borders (968,951, but 41% of total land border crossings) than at air borders (928,554, but 13% of total air border crossings) (see Figure 57). The distribution per category of traveller indeed varies significantly across the different types of border. This is also the case for MS that are not yet part of the Schengen Area, where the relative weight of VHs ranges from 3% at land borders to 11% at air borders.

Bulgaria, Croatia, Cyprus and Romania

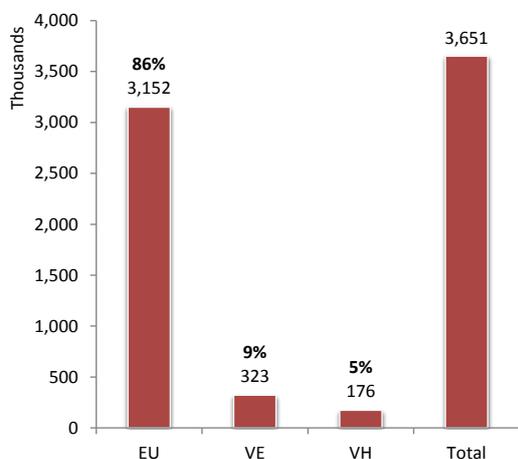


Figure 58 Breakdown of entry and exit border crossings per border type (for **BG, CY, HR, and RO**) – Source: data collected by MS during week 20 of 2014.

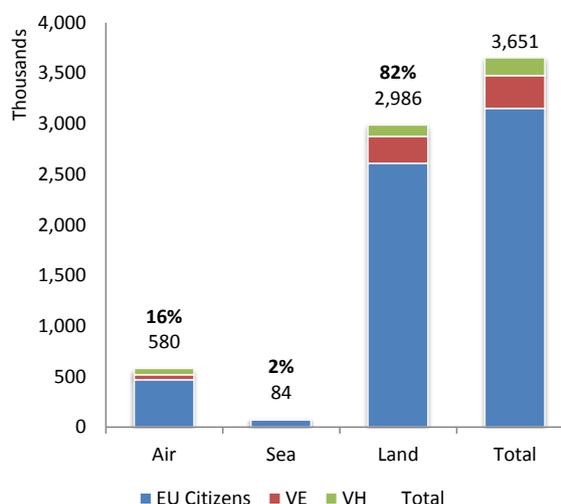


Figure 59 Breakdown of entry and exit border crossings per passenger type (for **BG, CY, HR, and RO**) – Source: data collected by MS during week 20 of 2014.

> **Peak vs. off-peak values**

Border crossings vary significantly during the year due to seasonal and other external factors. Therefore, the data of the sampling week, considered to be off-peak, needs to be contextualised against peak periods to provide an indication for the sizing of the IT infrastructure needed to sustain such peak periods.

The volumes of crossings during peak periods were calculated using the estimations of the variation between off-peak and peak periods provided by the MS (17¹⁷⁶ Schengen countries out of 20 which provided estimates). Figure 60 shows how the number of crossings during the sampling week compares to that of peak periods, which is approximately double.

For consistency and to avoid introducing any bias, the graph only includes data from the Schengen countries that provided data.

Table 94 below summarises the range of variations between peak and off-peak periods by providing the minimum, maximum and median values. There are significant differences from country to country, and peak values for some countries may be up to several times the off-peak values.

¹⁷⁶ Out of the 20 MS that answered, this section only takes into consideration the MS that are part of the Schengen Area.

Table 94 Overview of the variations between off-peak and peak values. Source: MS¹⁷⁷

	Min	Max	Median ¹⁷⁸
Air	30% (Switzerland)	386% (Italy)	79%
Land	33% (Belgium)	264% (Hungary)	103%
Sea	48% (Belgium)	2585.7% (Norway)	156%

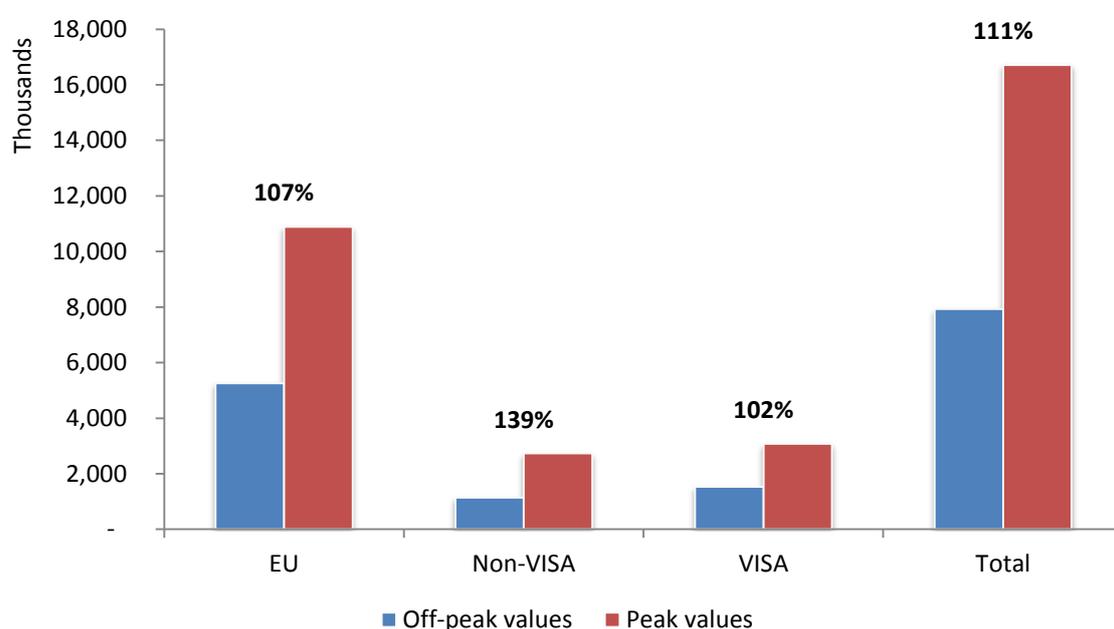


Figure 60 Off-peak vs. peak crossings: breakdown per category of traveller (one week's worth of values for: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland (land borders only), Germany, Greece, Hungary, Italy, the Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland) - Source: data collected by MS during week 20 of 2014.

> Crossings through ABC gates

Border crossings through ABC gates are still marginal compared to the total number of border crossings. Their aggregate value is just 1% of all border crossings and they are mostly used at air borders.

¹⁷⁷ Austria, Belgium, Czech Republic, Denmark, Estonia, Finland (land borders only), Germany, Greece, Hungary, Italy, Netherlands, Norway, Poland, Spain, Sweden, Switzerland.

¹⁷⁸ The median is the numerical value separating the higher half of a data sample from the lower half. The median has been used as it provides an indication more robust to extreme values.

Among the countries with ABC gates¹⁷⁹, Finland is the only one using ABC gates at land and sea borders, which amounted only to 427 border crossings while in the same period (week 20 of 2014) Finland recorded 17 310 border crossings through ABC gates at air borders.

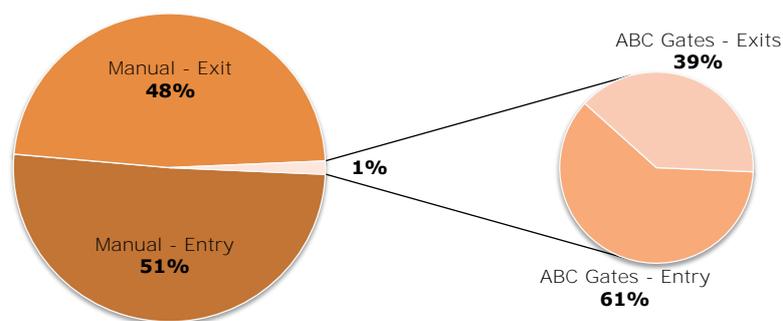


Figure 61 Total entry and exit crossings (24 Schengen countries) (in 9 Schengen countries¹⁸⁰) – Source: data collected by MS during week 20 of 2014.

– **Extrapolations and forecasts**

◦ **Extrapolation from one-week values to yearly values**

Based on the one-week data collected by MS, an estimation of the number of crossings at the external borders of the Schengen Area was made for the whole year 2014. To take into account any seasonal effects, the estimation also used VIS statistics (i.e. the number of first line checks during the same week in 2013¹⁸¹ – see Figure 62) as reference.

¹⁷⁹ As of May 2014.

¹⁸⁰ Austria (test unit – not operational), Czech Republic, Estonia, Finland, Germany, Netherlands, Norway, Portugal, Spain.

¹⁸¹ The data for the full year 2014 is not yet available, for this reason the data for year 2013 was used instead, for the comparison between the number of first line checks performed in week 20 and the number of first line checks performed during the entire year.

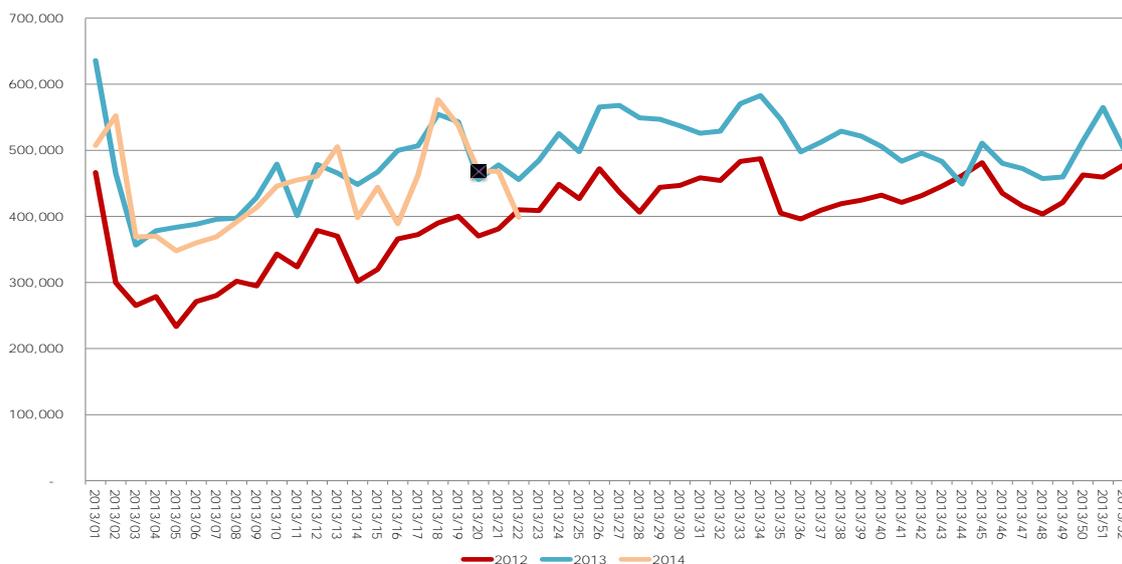


Figure 62 First line checks in VIS per week¹⁸² in 2012, 2013 and 2014 (up to week 22)¹⁸³ – Source: the VIS.

Week 20 represented 1.8% of first line checks in the VIS for the year 2013 (and also for 2012). Under the assumption that the 2014 distribution would not change significantly (which seems to be confirmed by data for the first four months of 2014), and that other categories of travellers such as VEs have similar dynamics to VHs, this percentage has been used to calculate full-year border-crossing values (see Table 95). This approach provided an evidence-based multiplication factor for the extrapolation.

Estimated weight of week 20 = First line checks performed in week 20 / total number of first line checks performed in 2013

Yearly values = One-week values (MS count) / Estimated weight of week 20 (= 1.8%)

Table 95 Summary of the extrapolation for border crossings at the external borders of the Schengen Area for 2014 (in millions).

	Air	Sea	Land	Total
	<i>Entry and exit</i>	<i>Entry and exit</i>	<i>Entry and exit</i>	
EU	265	36	71	372
VE	68	7	6	81
VH	52	5	54	110
Total	385	48	131	564

¹⁸² The quality of the data within the VIS depends on the MS's implementation of the first line VIS check (with or without FPs).

¹⁸³ For reference, week 20, during which of the data collection exercise was done, is marked with a black dot in the graph.

The addition of Bulgaria, Cyprus, Croatia and Romania would increase the number of border crossings for VE and VH respectively of 22% and 9% according to the data collected from the MS¹⁸⁴.

◦ **Estimation of growth rate for the forecasts**

Long-term forecasts of future passenger traffic are influenced by factors such as natural events, geo-political changes, changes in oil prices and GDP trends (among other things).. An overview of estimated growth rates for the different types of borders is provided below.

For the purpose of this Study, the selection of a growth rate to project 2014 flows to the period 2020/2025 was based on a documentary review of forecasts available from different sources (ICAO¹⁸⁵, Frontex¹⁸⁶, Boeing¹⁸⁷, Airbus¹⁸⁸, CLIA¹⁸⁹). European aggregate values have been calculated, as predictions per MS cannot be made with any precision.

In addition to the sources presented below, the World Tourism Organization (WTO), in its 2014 Tourism Highlights publication¹⁹⁰, forecasts a 2.7% growth rate for tourism for the period 2010-2020 and 1.8% for the period 2020-2030, with an overall average of 2.3%. However, the WTO estimations focus only on tourists, a subpopulation of travellers, without distinguishing between air, sea and land borders, which makes its forecasts not suitable for estimating the changes to the numbers of border crossings.

AIR

Most of the information available regards air borders and air passengers, for which the sources available (see Table 96) are aligned in forecasting around 4% annual growth in the coming years.

Table 96 Forecast growth rates from the documentary review

Source	Estimated yearly growth rate	Scope
--------	------------------------------	-------

¹⁸⁴ The figures do not take into account the future reduction of external borders once Bulgaria, Cyprus, Croatia and Romania will be fully into the Schengen Area. It is therefore considered the maximum value of the increase.

¹⁸⁵ ICAO – Aviation Data
http://cfapp.icao.int/tools/38thAssyikit/story_content/external_files/EconomicDevelopment_AviationDataAndIndicators.pptx - last accessed June 2014.

¹⁸⁶ 2011 – Frontex – “Future of Borders” -
http://frontex.europa.eu/assets/Publications/Research/Futures_of_Borders.pdf

¹⁸⁷ <http://www.boeing.com/boeing/commercial/cmo/index.page> - last accessed June 2014.

¹⁸⁸ <http://www.airbus.com/company/market/forecast/> - last accessed June 2014.

¹⁸⁹ http://www.irn-research.com/files/9913/9480/6948/CLIA_Europe_Stats_and_marts_2013.pdf, last accessed in June 2014.

¹⁹⁰ UNWTO Tourism Highlights, 2014 Edition - <http://mkt.unwto.org/publication/unwto-tourism-highlights-2014-edition> - last accessed June 2014.

IATA (2014)	3.9%	AIR only - Europe (2012 - 2016)
AIRBUS GROUP - Global Market Forecast 2012-2031	4.1%	AIR only - Europe (2011 - 2031)
Boeing - Long-Term Market - Current Market Outlook 2013 -2032	4.2%	AIR only - Europe (2013 - 2032)
ICAO (2010) - as reported in FRONTEX's "Futures of Borders"	4.3%	AIR only - Europe (2010 - 2030)
	Median¹⁹¹	4.2%

SEA

Limited information is available regarding the trends at sea borders and projections for the number of passengers in the upcoming years.

According to a report of the Cruise Lines International Association (CLIA)¹⁹², the number of passengers grew on average by 7.1% per year in Europe between 2009 and 2013, and in particular by 4% between 2012 and 2013.

LAND

The availability of forecast data for land borders is very limited. In addition, these data are characterised by a high level of variance with regard to traffic volumes and conditions, making difficult any comparison between countries and even between BCPs of the same country.

Four MS (Bulgaria, Latvia, Poland and Romania) provided some indications concerning their expected growth rate, which are presented in Table 97. The growth rates range from 1% to 13% per year depending on the country, underlining the necessity to work with aggregate values for the entire Schengen Area.

Table 97 Estimations of growth rates for land borders – Source: MS, March 2014

Country	Annual growth estimation
Bulgaria	4 - 6%
Latvia	5 - 10%
Poland	11 - 13%
Romania	1 %

Conclusion

For the purposes of this Study, the value used for projections is the median value of the figures for Europe from ICAO, IATA, Airbus and Boeing, i.e. 4.2%. In light of the scarcity of data for land borders and of forecasts for sea borders, this estimated growth rate was applied to all types of

¹⁹¹ The median is the numerical value separating the higher half of a data sample from the lower half. The median has been used as it provides an indication more robust to extreme values, however, in this case, the use of the mean would yield similar results.

¹⁹² http://www.irn-research.com/files/9913/9480/6948/CLIA_Europe_Stats_and_marts_2013.pdf, last accessed in June 2014.

borders. The error margin introduced by adopting the same growth rate for all types of borders is limited by the fact that air borders account for a large majority (68%) of total border crossings.

◦ **Outcome and summary of key forecasts for 2020/2025**

The forecasts presented below are intended to provide indications of the expected order of magnitude of the traffic at the external borders in 2020 and 2025. They have been calculated by applying the estimated yearly growth rate (as defined in section 4.4) to the figures extrapolated for the entire year 2014.

The results predict an increase of border crossings for the Schengen countries of approximately 28% by 2020 and 57% by 2025 (please refer to Figure 63, Figure 64 and Figure 65).

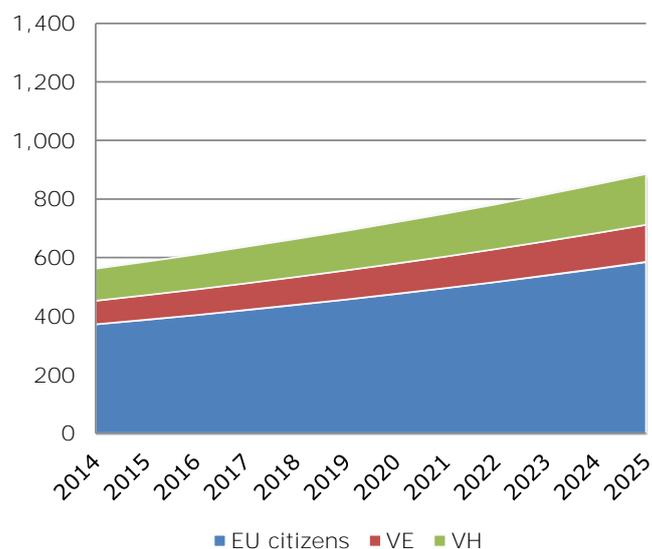


Figure 63 Forecast for 2025 of the number of border crossings (in millions) for **Schengen countries** per category of traveller.

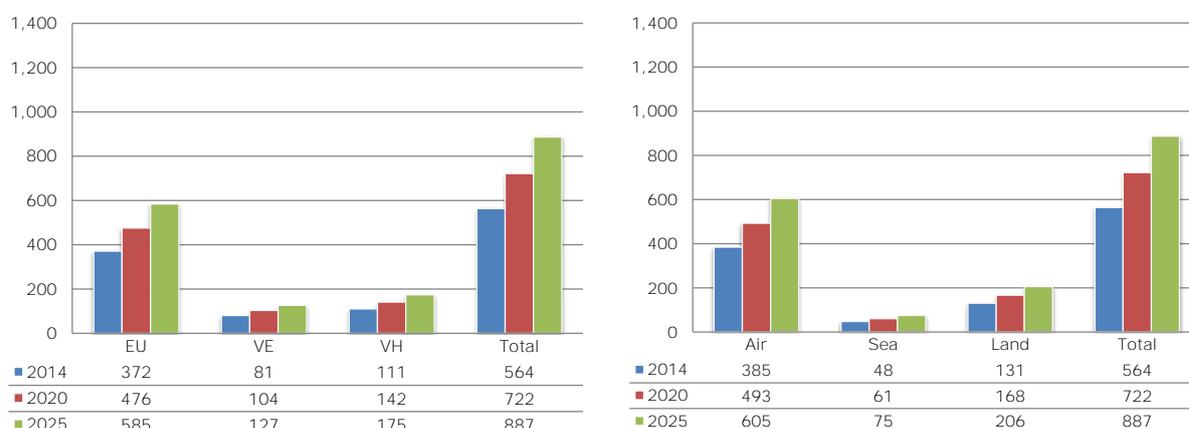


Figure 64 Estimate for 2014 and forecast for 2020 and 2025 of the number of border crossings (in millions) per category of traveller for **Schengen countries**.

Figure 65 Estimate for 2014 and forecast for 2020 and 2025 of the number of border crossings (in millions) per type of border for **Schengen countries**.

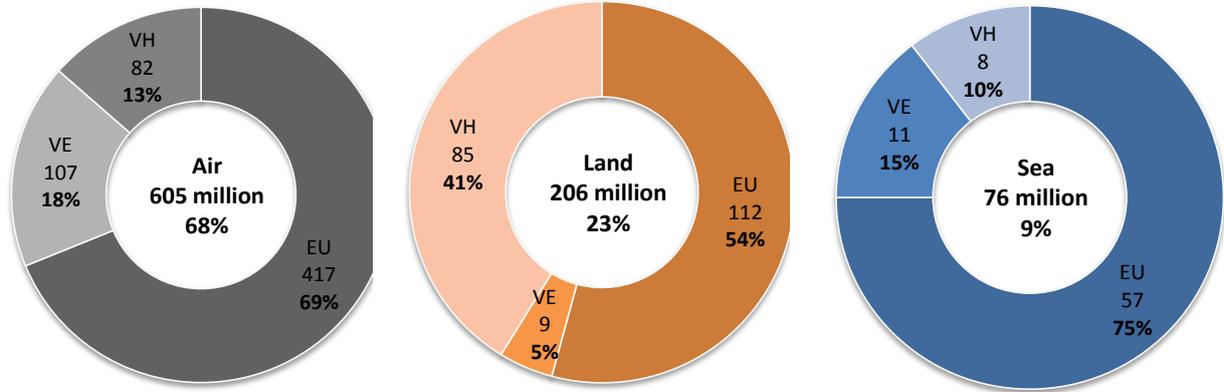


Figure 66 Breakdown of the projected number of entry and exit border crossings for **Schengen countries in 2025** per type of passenger across the various types of borders (figures in millions)

Figure 67, Figure 68, and Figure 69 below present the same forecasts with the addition of the border crossings projected to 2020/2025 for Bulgaria, Croatia, Cyprus and Romania.

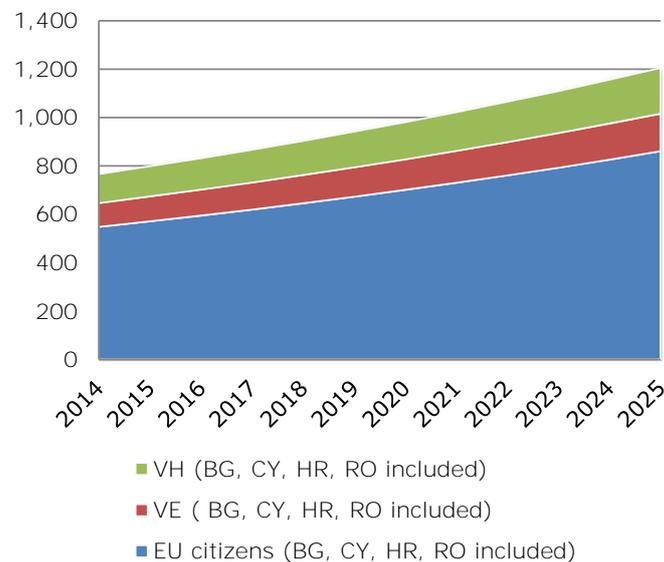


Figure 67 Forecast for 2025 of the number of border crossings (in millions) for **Schengen countries plus BG, CY, HR and RO** per category of traveller.

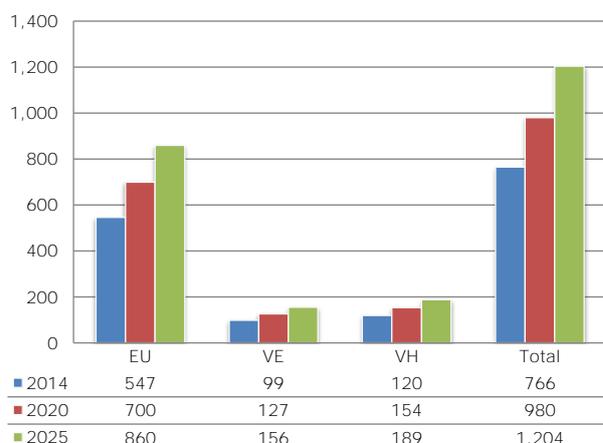


Figure 68 Estimate for 2014 and forecast for 2020 and 2025 of the number of border crossings (in millions) per category of traveller for **Schengen countries plus BG, CY, HR and RO**.

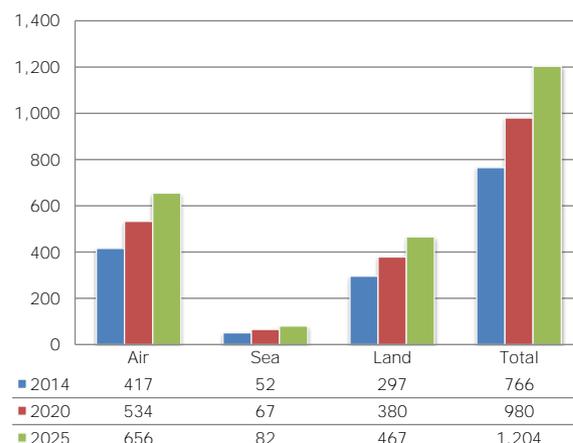


Figure 69 Estimate for 2014 and forecast for 2020 and 2025 of the number of border crossings (in millions) per type of border for **Schengen countries plus BG, CY, HR and RO**.

The reference figures for the Study, based on the calculation described in □□*, are the estimations for 2020 for the Schengen countries, as illustrated previously in Figure 64 and Figure 65 and summarised in the table below:

Table 98 Reference figures for border crossings at the external borders of the Schengen Area used in the Study.

2020 (in millions)				
	Air	Sea	Land	Total
EU	340	46	91	477
VE	87	10	7	104
VH	66	6	69	141
Total	493	62	167	722

As previously indicated, the addition of Bulgaria, Cyprus, Croatia and Romania would increase the number of border crossings shown in the table above of 22% and 9% for VE and VH respectively, according to the data collected from the MS.

◦ **Estimation of the number of individual files**

In addition to the total number of border crossings, it is important to estimate the number of travellers that will have their data stored within the EES and RTP system(s).

It is assumed that each traveller, being recorded at entry and exit, corresponds to at least two border crossings. Therefore, it is possible to obtain an initial estimation of the maximum number of individual persons that would need to be recorded in the EES, by dividing in half the estimated number of border crossings, as if each traveller was to have only one trip per year.

To avoid overestimating the number of individual files that will be stored, the total number of border crossings, after being divided by two, has been multiplied by a correction factor, whose estimation is presented below.

As regards VHs, this factor was estimated by reconciling the number of border crossings during one year for VHs (approximately 110 million in 2014, see Table 95) and the number of visas issued projected to 2014 (i.e. approximately 19 million).

The estimation of the number of visas that are expected to be issued in 2014 has been calculated by applying the historical average growth rate in the last few years (14% according to the visa statistics, see section 7.1) to the 2013 figures (approximately 16 million, see Figure 54).

The assumption behind this approach is that people would, on average, apply for only one visa per year, taking advantage of the MEV if they needed to travel frequently into the Schengen Area.

Projected visas issued in 2014 = 2014 border crossings for VHs * 0.5 (entry/exit adjustment) * Correction factor

Correction factor for VHs = Projected visas issued in 2014 (≈19 million) / (2014 border crossings for VHs (≈110 million) * 0.5) = 0.34

Number of VH travellers = Border crossings * 0.5 * Correction factor (0.34)

As regards VE travellers, the correction factor has been adjusted taking into account the estimations provided by five MS¹⁹³ for the proportion of border crossings due to the same traveller. The results showed a lower percentage of recurrent travellers among VE travellers in comparison with the estimation for VHs.

Number of VE travellers = Border crossings * 0.5 * Correction factor (0.74)

Finally, the estimated number of travellers was increased to take into account overstayers, whose individual files are retained longer. Due to the scarcity of data that would enable an accurate estimate of the percentage of overstayers, the Study worked on the assumption that they represent up to 5% of the total population of travellers each year. This value also provides a buffer if the number of frequent travellers is overestimated (Table 99 below summarises the results).

The estimation of the number of EU citizens is not needed, as they would not be captured within the EES/RTP or the AFIS.

Table 99 Summary of estimations for the size of the individual file database

	2014 (in millions)	2020 (in millions)	2025 (in millions)
VE			
Border crossings (entry + exit)	81	104	128
Number of travellers	30	39	47
Number of individual files (1 yr. data retention + 5% overstayers and buffer) ¹⁹⁴	32	41	50

¹⁹³ Greece, Latvia, Norway, Romania and Slovakia provided estimations. The resulting value is the median of the indications.

¹⁹⁴ Assuming that the system was fully operational since one year.

VH	Border crossings (entry + exit)	110	141	173
	Number of travellers	19	24	29
	Number of individual files (1 yr. data retention + 5% overstayers and buffer) ¹⁹⁵	20	25	31

The reference values for the Study are the values estimated for 2020 for the Schengen countries (highlighted column in Table 99). The addition of the countries yet to join the Schengen Area would increase the border crossing for VE and VH of approximately 17% combined and the number of travellers up to 22%.

Five years data retention – calculation of the number of individual files

In the case of a data retention period of five years, calculated from the last exit, to calculate the number of individual files stored, it is necessary to take into account the dynamic over the time.

During the first five years there would be a stronger growth per year as no individual file would be deleted. Only after this initial period, the automatic deletion of the travellers, who have not returned into the Schengen Area in the last five years, would begin. The deletions would in fact reduce the growth rate of the number of individual files stored in the system.

In light of indications provided by the MS regarding the number of re-entries over the years, it can be assumed that, in average, the system will add 60% of the individual travelling each year to the database and will delete 45% of the travellers of five years earlier. However, the actual values will depend on the evolution of the volumes and dynamics of travellers flows in future years.

The below table shows the number of individual files stored in the EES per year, calculated considering 2020 as first year of operations.

Table 100 *Estimation of the number of individual files over the years in case of five years data retention period (in million)*

	2020		2021		2022		2023		2024		2025	
	VE	VH										
Number of travellers	38	24	62	39	87	54	114	70	141	87	152	94
Total (+5% overstayers and buffer)	65		106		149		193		239		258	

¹⁹⁵ Assuming that the system was fully operational since one year.

◦ **RTP demand estimation**

To arrive at a rough estimate of potential RTP demand, VH and VE are first analysed separately and then added up. Finally the number of resident permit and card holders interested in an RT status are added.

As regards VHs, MEVs are considered to be a proxy of the maximum number of people that may be interested in the RTP. According to the visa statistics for 2013, 45% of visas issued were MEVs (see section 7.1). Out of the number of MEVs, assuming that the interest for RTP would be concentrated on those that are mainly aimed at using ABC gates (available mostly at air borders), the RTP demand can be estimated based on the following:

- MEVs represent 45% of visas issued. The assumption is that 45% of VHs are MEVs;
- 66% of VHs access the Schengen Area via air borders;
- A maximum of 70% of travellers who are entitled to use an ABC gate actually use it.

Therefore the maximum RTP demand of VH is estimated as $0.45 * 0.66 * 0.7 * VH = 0.21 * VH$

As regards VE travellers, the percentage of frequent travellers – and potential RTP subscribers – is much harder to forecast. A five per cent estimation is used in this Study, which is based on expert discussions with the Commission and benchmarking figures from other existing RTP programmes. For instance:

- The Dutch PRIVIUM programme at Schiphol airport has 48,000 members, which accounts for approximately 0.5% of the total targeted number of travellers¹⁹⁶ (2014);
- The Australian SmartGate programme in Brisbane airport has around 6% registered travellers (2007);
- The US Global Entry programme has, on average, around 3% of trusted travellers entering through airport entry kiosks (2013). The NEXUS programme¹⁹⁷ has, on average, around 19% trusted travellers entering the United States through dedicated NEXUS lanes (2013).

The estimate of demand for RT status for Resident permit and card holders is estimated as 20% of the total number of long term resident permits issued in 2025. To reach this value, it is estimated that the demand would grow from 10% in 2014 and 2020 to 20% in 2025. These values are based on the assumption of a significant interest for RT status from this population to facilitate regular travels but is not supported by any clear evidence.

The total estimated demand for the RTP is the sum of the potential maximum demand for VH, VE and Resident permit and card holders, which is calculated as follows:

Total estimated demand for the RTP = 0.21* VH + 0.05 * VE + 0,25 * Resident permit/card holders

The results of these calculations are presented in Table 101 below

¹⁹⁶ PRIVIUM is Schiphol Airport's automated border crossing programme for frequent fliers who want to enjoy trouble-free travel. The passport holders of all EU countries as well as Norway, Iceland, Liechtenstein and Switzerland are eligible to apply for the membership of the PRIVIUM programme. The majority are business travellers, flying an average of 16 times a year through Amsterdam Airport Schiphol.

¹⁹⁷ United States Government Accountability Office, "TRUSTED TRAVELERS: Programs Provide Benefits, but Enrollment Processes Could Be Strengthened", May 2014, <https://www.hsdl.org/?view&did=754130>

Table 101 RTP potential demand estimations

	2014 (in millions)	2020 (in millions)	2025 (in millions)
VE – Number of travellers	30	39	47
Maximum potential demand for RTP	1,5	2	2
VH – Number of travellers	19	24	29
Maximum potential demand for RTP	4	5	6
Resident permit/card holders	5	5,5	6
Maximum potential demand for RTP	0,5	0,6	1,2
RTP maximum of potential demand	6,0	7,6	9,2

The actual demand for the programme would probably be only part of the potential demand indicated above. It will depend on several aspects, such as:

- The rate of adoption over time;
- The final cost of the programme for the traveller;
- The real advantages that the RTP will bring over the regular TCN lanes at the various BCPs;
- The visibility of the programme to TCNs, including possible cooperation with other existing trusted traveller programmes;
- The enrolment procedure (e.g. the adoption of an easy-to-use website for the enrolment is likely to have a positive impact on actual demand);
- The existence of similar services provided by airports and airlines (such as preferential lanes for business/ first class passengers).

On the basis of expert consultations within the Commission and Frontex, the Study assumed that actual demand will ultimately be between 5% (approximately 50% of the potential demand by 2025) and 8% (approximately 80% of the potential demand by 2025) of the total border crossings. The same percentages have been used during the simulation carried out to assess the impact of the RTP on the other categories of travellers (see annex J for further details).

For the first three years, the expected subscriptions and traffic have been further reduced to take into account the progressive growth of the adoption rate over time. The table below summarises the estimated demand (note that these figures are the reference values used throughout this Study):

Table 102 Estimations for expected demand of RTP¹⁹⁸

	2020 (in millions)	2021 (in millions)	2022 (in millions)	2023 (in millions)	2024 (in millions)	2025 (in millions)
<i>Growth adjustment for the RTP demand</i>	<i>0.25</i>	<i>0.50</i>	<i>0.75</i>	<i>1</i>	<i>1</i>	<i>1</i>
RTP border crossings (5% of the total with growth adjustment applied)	9	19	29	41	43	44
Estimated number of frequent travellers (VH and VE equivalent to 5% of the border crossings)	0.8	1.8	2.7	3.8	4.0	4.1
RTP border crossings (8% of the total with growth adjustment applied)	14	30	47	65	68	71
Estimated number of frequent travellers (VH and VE equivalent to 8% of the border crossings)	1.3	2.8	4.4	6.1	6.4	6.6

The addition of Bulgaria, Cyprus, Croatia and Romania could increase the RTP membership up to approximately 15% of values estimated taking into consideration only Schengen countries.

For comparison, the US Global Entry programme came into operation in 2008 and reached 1 million subscribers by 2013; however, the price for this programme is USD 100 (approximately EUR 73), making it significantly more expensive than the RTP membership, whose price, according to the current legislative proposal, would be EUR 20 EUR, or EUR 10 in the case of people also applying for an MEV.

When the Smart Borders Pilot is implemented, a survey could be carried out among TCNs (VH and VE) travelling to Europe, to help identify actual RTP demand more precisely.

Estimating the actual demand for the RTP is of fundamental importance in determining the resources to be allocated to the programme (such as the number of lanes at BCPs).

For the purposes of the cost estimation, the Study took as reference figures the maximum demand (i.e. 7,6 million of potential subscribers for 2020). This cautious approach is closer to the figures adopted during the impact assessment (which envisaged 5 million of subscribers) and is meant to reduce the risk of underestimating the necessary infrastructure to support the RTP.

¹⁹⁸ These estimations do not take into consideration the demand from resident permit/card holders

• **Conclusions**

– **Introduction**

The purpose of this section is to outline the key elements and findings from the TF analysis performed in chapters 3 through 6 and to bring together the different items into workable solutions for the EES and RTP.

As the study has shown, whether in processes, biometrics, data and architecture, different choices can be made but they are going to yield different results in terms of facilitation, security and complexity

The concept of potential Target Operating Model (TOM) was introduced in the Study to combine and describe all the activities required to effectively operate EES and RTP, namely to assemble **one unique set of choices** for each activity where different possibilities exist.

As a starting point, the TOMs for EES and RTP can be defined separately, as the choices that impact EES differ from the ones for RTP. The structure for each TOM contains five main building blocks:

1. **Common features:** the features that do not vary from one TOM to the other. This study still shows options that are open (such as minimum dataset or retention period) but once a choice would be made, it will apply to all TOMs.
2. **Differentiators:** the features that distinguish the different TOMs. From the process descriptions and the impact on duration, security and complexity, it appears that biometrics are the key differentiator for EES. For RTP, the differentiator is the way the enrolment is performed. The border crossing of the RTP is, however, not impacted.
3. **Additional discussion elements:** the features that are not directly related to the processes of EES or RTP but that could have an impact on EES and RTP operations. For instance including optional fields in the EES or only the MRZ data. The option can be chosen for each TOM; the latter would not shape the solution but it would have an impact on the border crossing duration.
4. **Process accelerators:** elements that may mitigate the potential negative impact of implementing the EES and RT according to a specific TOM.
5. **Architecture:** architecture choices to be made which do not directly impact the TOMs because end-user services are delivered independently of these. The architecture choices only impact the means used for delivering the services and therefore their cost.

Three TOM's for EES and two for RTP were built.

Each TOM was defined around the main process steps and their sub-processes represented in the table below. The guiding principles for data protection were taken into account from the design of the solution.

EES	RTP
<p>Search in the EES</p> <ul style="list-style-type: none"> if the person is not found = first entry, if the person is found = subsequent entry <p>First entry</p> <ul style="list-style-type: none"> Identification Individual file creation Entry record <p>Subsequent entry</p> <ul style="list-style-type: none"> Search in the EES Verification if a person is found in EES Entry record <p>Exit</p> <ul style="list-style-type: none"> Search in the EES Verification Exit record 	<p>Enrolment</p> <ul style="list-style-type: none"> Identification <p>Entry</p> <ul style="list-style-type: none"> RTP status check Verification Entry record <p>Exit</p> <ul style="list-style-type: none"> RTP status check Verification Exit record

Each TOM was assessed against the criteria of **duration**¹⁹⁹, **security**²⁰⁰ and **complexity**²⁰¹ as well as constraints due to the operational environment and costs whereas exceptions and degraded mode scenarios are presented in Annex F.

Manual document checks as well as the manual check of whether the document holder is the rightful document owner are not always addressed here, as they are part of the existing border control processes.

The analysis of TOM options is further described in the following sections 8.2 and 8.3.

Common features

The common features, different for EES and RTP, are presented in the two tables below. The specific descriptions and assessments of these options can be found in chapters 3.2 and 3.4.

EES

Items	Description
1. Primary search	- Search using issuing country and document number of the MRZ, from the passport (e-MRTD or MRTD)
2. Individual file	- Data: MRZ data are taken for all travellers (from MRTD/e-MRTD) and used as the minimum dataset for the file. Visa number is added for VHs.

¹⁹⁹ Assessment based on the impact on border crossing times for travellers, including check and waiting time as well as rejections and exception handling.

²⁰⁰ Compliance with the Schengen Borders Code and related best practices, and added value of the biometric functionality (including biometric reliability) to support the Border Control Processes.

²⁰¹ Assessment based on the difficulties that can be anticipated during implementation. Solutions that are too cumbersome to implement could lead to issues, delays and cost overruns.

- The photo is stored for verification and enrolment. The sources for the picture would be, in order of preference, e-MRTD, live photo or scan of the passport picture.
- VHS:
 - Biometric data from the VIS are re-used to avoid a new enrolment in the EES.

3. Data retention

The following options are suggested by the Study:

- Option A: alignment of the EES data retention period of the individual file of TCN with the length of the RTP status and maintaining entry / exit records as per the legislative proposal (181 days/91 days or 5 years for overstayers)
- Option B: 5-year retention period for entry/ exit records and alignment of individual file data retention with the one of entry/exit records or RTP application data, whichever is longer
- Option C: a maximum of 366 days (after the last exit record, if there is no entry record within the 365 days following that last exit record) for entry/ exit records and alignment of individual file data retention with the one of entry/exit records or RTP application data, whichever is longer

4. VHS

- VIS verifications are trusted, i.e. there is no need to register the fingerprints of VHS in EES

5. Bearer verification

- VES: it is recommended to introduce an automatic bearer verification using the photo in the e-MRTD (where available) compared to a live photo

6. Document verification

- e-MRTD (when used) - Passive authentication (PA) is strongly recommended to ensure that the content of the chip has not been tampered with
- Where possible, Active Authentication (AA) should be used also, to identify cloning and copying of the chip

RTP

Items	Description
1. Record retrieval	- e-MRTD issuing country and document number are used to check the RTP status in the border process. No other data is required from the RTP individual file.
2. Data retention	- Maximum length of 5 years, from the expiration of the RTP status.
3. Status	<ul style="list-style-type: none"> - Can be granted for a maximum of 5 years. - The period cannot have a longer duration than the validity of MRTD/e-MRTD or the visa validity (or if applicable, the residence card or residence permit), whichever expires first. - The competent authority granting RTP status could decide to grant the status for a shorter period.
4. Token	- e-MRTD is used as a token for the automated verification of RTP status.

- 5. VHs**
 - VHs: having a MEV is a prerequisite to RTP membership.
 - VIS verifications are trusted in the RTP process, i.e. there is no need to register fingerprints of VHs (further details can be found in section 3.3)²⁰².

- 6. Application data**
 - In line with the legal proposal (art.25).

- 7. Online application**
 - VEs: recommended in TOM M and mandatory in TOM N
 - VHs: recommended but RTP request can still be introduced at consular post at the moment of the visa request.

Differentiators

From the analysis performed, it appears that for EES the type of biometrics used (FI or FP) and the number of FPs used are the key differentiator for the entry/exit process definition and duration.

For EES, there are three combinations of biometrics which differ significantly one from the other:

- FI without FP (TOM A)
- FI and 4 FPs(TOM B)
- FI and 8 FPs²⁰³ (TOM C).

By assuming a re-use of biometrics already captured earlier for visa or passport issuance, (i.e. the VIS verification in the border control process is used as a trusted action for EES also and the photo stored in e-MRTD is used whenever this is possible) the impacts of the introduction of FP are lowered and are differentiated for VEs and VHs.

The main differentiation of the TOMs M & N is the way the enrolment would be performed.

In TOM M, the enrolment is performed as described in chapter 3.3. This includes a visit to a consular post or a border crossing point to lodge an application. The application can be sent online beforehand.

In TOM N, the whole RTP application process can be handled via the internet (please refer to chapter 3.6 for further details) and the enrolment is performed after the requestor has a track record in the EES. The past record of entries/exits can therefore be used for the assessment and the biometrics stored in the EES is used in subsequent verifications of the RT. For persons with residence permits/cards, there is a specific way to handle them within TOM N, which implies passing a manual gate at some point in time after the application is made, to have an individual file created in EES, before the status is granted.

Process accelerators

The approaches that could speed up border crossing times²⁰⁴ include:

- **Making the enrolment of biometrics faster but still reliable.** The enrolment of biometrics for TCNVEs is a step introduced by EES and which is by definition more time-

²⁰² Depending on the final implementation, an amendment of the VIS legal basis might be necessary to allow the use of the VIS for RTP purposes.

²⁰³ The impact of using the FI and 10 FPs is very similar to the TOM built on the basis of an FI and 8 FPs; as a result, it could be considered essentially a variation of TOM C

²⁰⁴ See section 3.5.

consuming than the existing process where this is not happening. Accelerators can be looked at for making this step as short as possible.

- Two ideas are proposed: the capturing of fingerprints on the fly and capturing the iris rather than fingerprints.
- **Data gathering** from carriers before arrival (e.g. API, PNR, passenger list from ships, crew lists, trains) in order to enable each MS to improve queue and lane management.
- **Self-pre-registration** before the border check (e.g. recording of MRZ data, EES search, biometric verification, full alphanumeric dataset registration, enrolling fingerprints for registration, capturing a live photo for registration, preliminary creation of the individual file).
- **Organisational measures**, such as separate TCNVE and TCNVH lanes, flexible use of lanes, waiting areas at land borders.
- **Minimising the number of documents used** e.g. maximise the use of the e-MRTD, use the (e-)MRTD as a token for RTP, use document number to search the VIS and use ABC gates.
- **Process automation**, i.e. allowing TCNs to use ABC-gates at exit.

The benefits of the process accelerators vary depending on the options for using data and biometrics.

Additional discussion topics

The table below addresses the additional cross-cutting topics for all the TOMs. These topics are subject to further discussions and decisions, in parallel with the Pilot and could potentially be impacted by the results of the Pilot.

Items	Description
1. LBT permits	<ul style="list-style-type: none"> - EES: It is suggested not to register LBT permit holders in the EES. This is in line with the current process where no stamping is necessary for these travellers. - RTP: Registration of persons with LBT permits in RTP would follow the normal RTP application process.
2. Residence permits (RP)	<ul style="list-style-type: none"> - EES: It is suggested not to register persons with residence permits in the EES. This is in line with the current process where stamping is made for the purpose of controlling the days needed to keep a residence permit and not for calculating the days related to the stay in the territory. The registration would therefore not serve any purpose relevant to the EES, as it is now defined. - RTP: Registration of resident permit holders in RTP would either follow the normal RTP application process (TOM M), a specialised process would be implemented in case of TOM N or alternatively, RTP status would not be possible for this category.
3. Additional, optional fields	<ul style="list-style-type: none"> - Additional, optional fields are fields that are captured in the current national systems, similar to EES. It is suggested not to include these fields as part of the entry/exit record in EES. This would require a manual registration, which would add time to the border check and the data quality would be difficult to be established on a uniform level.

- 4. **Transition period** - TOMs are described disregarding any transitional period for the use of biometrics. This does not mean that no transitional period is possible rather simply that the TOMs focus on the target situation.

- 5. **NEES (national Entry Exit Systems)**
 - Can continue to exist, including their national data store, if the MS decides so.
 - **National Uniform Interface (NUI):**
 - will ensure the integration between NEES and EES by providing services such as queuing and logging.
 - defines the subset of data to be exchanged from NEES to EES e.g. the minimal dataset for the individual file registrations

- 6. **Data to external actors** (e.g. carriers)
 - A choice should be made on what can be exposed to external actors:
 - Data will be readable e.g. number of days left, or
 - Data will not be readable, but only key information e.g. the person has x days left.

- 7. **LEA**
 - Biometric data can be used to search against EES for identification purposes
 - All data is accessible (variants are to be identified)
 - Latent can be used for searches, with varying degree of accuracy depending on the number of fingerprints enrolled
 - Specific searching capabilities need to be developed for LEA, in line with stringent access control procedures

- 8. **Immigration authorities**
 - Checks of undocumented VE people in the territory is possible by doing either:
 - 10 FPs, 8 or 4 FPs - 1:N searches, or
 - Facial image searches together with basic identity attributes such as date of birth, name and/or gender

- 9. **Self-service kiosk**
 - **Border control at entry:** To reduce the pressure, self-service kiosks will be used, where appropriate, to capture and enrol the EES minimum dataset. The (biometric) verification against the EES/VIS should be supervised by a border guard.

Architecture for TOMs

One or two systems

EES and RTP would be included in one central system (i.e. sharing the same technological platform), which would not be integrated with the VIS. The biometric information would be processed by the same AFIS as for VIS if fingerprints were used.

National uniform interface (NUI)

The development by the Agency and use of a National Uniform Interface (NUI) by all Member States is recommended, containing functionalities like: services for EES and RTP, Reliable Message Transfer (including queuing and temporary buffering), flow control, multiple call-back addresses for national systems.

A detailed overview of the main architectural options for the EES and the RTP and the potential impacts on related applications such as the VIS and the MS's entry and exit systems already in operation is provided in Chapter 6. Also, the technical feasibility of implementing EES and RTP as separate systems or as a single system, possible synergies and interactions between EES, RTP and

VIS are further explored²⁰⁵, together with possibilities of reusing or integrating existing national systems.

²⁰⁵ The VIS integration is further discussed under section 6.4.

– EES TOMs A, B and C

Below is an overview of **TOMs A, B and C** in relation to data and biometrics. It should be noted that verifications, in degraded mode, are not mentioned in the table. Detailed descriptions of the activities can be found in chapter 3.2 and 3.3. A transitional period is not taken into account.

Border check	TOM A	TOM B	TOM C
Document authenticity and validity	MRTD/e-MRTD: Physical/optical document safeguards e-MRTD: Passive and Active Authentication		
Bearer verification at each border crossing	VEs: MRTD: visual check of picture vs bearer e-MRTD manual lane: FI from e-MRTD vs live photo or bearer e-MRTD in ABC: FI from e-MRTD against live photo VHs: bearer verification considered to be part of the VIS framework		
Biometric enrolment at first entry ²⁰⁶	VEs/VHs: FI from e-MRTD ²⁰⁷ stored in EES VHs: no FP enrolment (10 FP's are stored in VIS)		
	VEs: No FPs are stored	VEs: 4 FPs are stored in EES	VEs: 8 FPs are stored in EES
Biometric verification at subsequent entries/exits (holder vs. travel doc and holder vs. database)	VEs: verification of FI from e-MRTD against photo in EES VHs: live FP (1,2 or 4) against VIS	VEs: live FP (1,2, or 4) against EES VHs: live FP (1,2, or 4) against VIS Verification of FI in ABC-gates using FI	
Biometric identification at first entry ²⁰⁸	VEs: Discretionary 1:few using FI and alphanumerical data VHs: Systematic identification was done at the moment of the visa application	VEs: Systematic 1:N identification using FPs VHs: Systematic identification was done at the moment of the visa application	

²⁰⁶ EES search is made using issuing country and document number but an individual file in EES is not found.

²⁰⁷ If the e-MRTD is not available, then a live picture or the scan of the travel document could be used instead.

²⁰⁸ At first entry or in case a new passport is used, to avoid duplicates and to increase security.

Entry/Exit record creation	Data recording of border crossing, e.g. day, time, BCP
-----------------------------------	--

All TOMs allow the identification of non-documented persons, although with different levels of performance (i.e. speed or accuracy).

o **Overview**

TOM A
Using only FI and no systematic 1:N identification

First Entry: Registration of the individual file

Items	Description
1. MRZ data	- use the minimum dataset (from MRTD/e-MRTD), including the visa-sticker number (with the country code) for VHs (potentially automatically retrieved from VIS based on MRZ of the MRTD)
2. Photo	Storage of photo in EES for VE/VH from: <ul style="list-style-type: none"> - e-MRTD (VE/VH), if available in a secure way - live photo - scanned photo from MRTD. The latter can only be useful for manual (ocular) verifications at a later time.
3. Existence of duplicates	- A 1: few search is made in the EES, using FI, to reduce the risk of the existence of duplicates – on a sub-set based on name, dob, gender.

Entry / Exit: Search and Verification

Items	Description
1. EES search	- Individual file is retrieved using issuing country and document number
2. Verify	- VEs: verification is made by using a live photo that is compared to the e-MRTD photo (ABC-gates) or to the photo in the EES, where possible - VHs: the verifications made against the VIS, using FPs as is the case today, are trusted
3. ABC gates at exit	- Verification: the photo from e-MRTD is compared to a live photo
4. Manual verification	- In case the automated verification is not available or possible, the border guard makes a manual verification by using a printed or displayed photo

Entry / Exit: Recording - The data recorded at entry/exit would be in accordance with the legal proposal (e.g. date, time, BCP).

TOM B

Using FI, 4 FPs and systematic 1:N identification at first entry

First Entry²⁰⁹: Registration of the individual file

Items	Description
1. MRZ data	- Same as in TOM A
2. FP	- VEs: 4 FPs are enrolled
3. Photo	- Same as in TOM A
4. Existence of duplicates	- De-duplication search by using alphanumerical data and supplementing it by a 1:N search in the EES, using FPs and FI , to eliminate the existence of duplicates

Entry / Exit: Search and Verification

Items	Description
1. EES search	- Same as in TOM A
2. Verify	- VEs: identity is verified by using 1, 2 or 4 FPs that are compared against the EES file - VHs: the verifications made against the VIS are trusted - Live photo: It is recommended to verify the bearer by using a live photo that is compared to the e-MRTD photo, where possible
3. ABC gates at exit	- Verification: could be made by using FPs or by using the e-MRTD photo and comparing it to a live photo.
4. Manual verification	- Same as in TOM A

Entry / Exit: Recording - The data recorded at entry/exit would be in accordance with the legal proposal (e.g. date, time, BCP).

TOM C

Using FI, 8 FPs and systematic 1:N identification at first entry

As regards TOM C, the main difference with TOM B is that an e-MRTD photo would be used together with 8 FPs as biometric identifiers instead of 4 FPs.

◦ **Estimated durations, security and complexity by each TOMs**

In order to obtain further information on the biometrics and data options chosen for the TOMs, that could have an impact on the duration of border crossings, a simulation exercise was performed at air and land borders crossing points based on real patterns of travellers.

²⁰⁹ Search in the EES is made but person not found.

- For air borders: the simulations were performed for entries into and exits from the Schengen Area taking as a basis of computation the entries and exits on an average day in a busy period for an airport with a high volume of travellers²¹⁰. Volumes of travellers were increased to correspond to projections by 2020.
- For land borders: the simulations were performed only for exits from the Schengen Area as the queues for entry to the Schengen Area are not on Schengen territory and observations were therefore not possible. The computations were done for a land border crossing point between Estonia and Russia operating 24/7. Volumes of travellers were increased to correspond to projections by 2020. Computations were only done for the queues of individual cars and buses, not for pedestrians or lorries. The chosen period of analysis also has above-average volumes of border crossings.

For air borders, the effect of adding a so-called "Smart Borders overhead" to current border control practices makes it possible to have results for the additional durations for controls implied by TOMs A, B and C.

The impact was measured on the following performance parameters:

- Service Level Compliance: the service level is expressed as a percentage of travellers serviced within a given time span. For the air border these time spans were 2, 5 and 10 minutes. The service levels included dwelling time and actual time for the border check.
- The dwelling time represents the time the traveller has to use to complete the border check clearance including the queuing time.
- The impact on workload, for border guards, is measured by computing the additional number of minutes worked for executing the additional controls implied by EES at entry or exit. It should be clear that the workload presented could not automatically be translated into additional required manpower. The real need for added manpower depends on the individual BCP, its organisation, infrastructure, peak pattern, etc. The result of the simulation can be seen as an indication. See Annex J for more details on the measurement when simulating the workload.

The following performance parameters were used for land borders:

- Service Level Compliance: same as for air borders but the levels are set for time spans 10, 30 and 60 minutes.
- The average dwelling time is defined in the same way as for air borders.
- The impact on the border guards' work effort is computed using the "usage factor". The usage factor is the percentage of the available time where activity (i.e. when checks are being done) is performed.

In the following tables, **security** and **complexity** aspects are added as well, in comparison with the "as-is" situation.

Scoring	Definition
----------------	-------------------

²¹⁰ The computations were also done for a mid-range airport but are not used for these conclusions, as the impact is systematically less visible than for a larger airport

- - Highly negative impact on the border control processes, in relation to the specific criteria

- Limited negative impact on the border control processes, in relation to the specific criteria

- N** Neutral impact on the border control processes, in relation to the specific criteria

- +** Limited positive impact on the border control processes in relation to the specific criteria

- ++** Highly positive impact on the border control processes, in relation to the specific criteria

A five-level scoring scale is used as described below. The first entry, subsequent entries and exits are presented in three separate tables.

First entry

Options		TOM A	TOM B	TOM C	Duration (sec)	Security	Complexity
1.	e-MRTD: Retrieve photo (if available and chip can be read securely); otherwise use a live photo	✓	✓	✓	5	+	+
	A scanned photo from MRTD	✓	✓	✓	(10)*	--	N
2.	4 FPs Enrolment		✓		20-30	+	-
	8 FPs Enrolment			✓	40-60	++	--
3.	1:N identification: Systematic (only VEs)		✓	✓	20-30	+	-
	Duration (sec)	5	45 -65	65-95			

* The printed photo would only be scanned in the case of a traveller with MRTD; those travellers are likely to be few when EES is introduced. The added time is therefore not factored in here.

Subsequent entries

	Options	TOM A	TOM B	TOM C	Duration (sec)	Security	Complexity
1.	Verification: Use a photo	✓	✓	✓	15-20	+	+
	Verification: number of FPs			1-4	15-20	+	-
2.	1:N Identification: systematic (only VEs) ²¹¹		✓	✓	20-30	+	-
	Duration (sec)	15-20	35-50	35-50			

Exit

Options	TOM A	TOM B	TOM C	Duration (sec)	Security	Complexity
1. Verification: Use a photo	✓	✓	✓	15-20	+	+
Verification: number of FPs (only VEs)		1-4	1-4	15-20	+	-
Duration (sec)	15-20	15-20	15-20			

Note: for TOM B and C, fingerprints or photo could be used for verification (e.g. photo at ABC-gates at exit and fingerprints at entry).

Conclusions of simulations in relation to TOM A-C

The durations added to the current border control processes for TOM A, B and C are:

Steps	TOM A	TOM B	TOM C
	Added duration in seconds		
1. First entry	5	45-65	65-95
2. Subsequent entries	15-20	35-50	35-50

²¹¹ The systematic identification for VEs is recommended at first entry only, however, it was included in the simulation at subsequent entries for completeness and to consider to a more cautious estimate, already accommodating the option of identification not only at first entry.

3. Exit	15-20	15-20	15-20
----------------	--------------	--------------	--------------

- Legend: e.g. 15-20 depends on the choice made.

These estimated added time is set in relation to the outcome of the simulations of border checks (see Annex J for details) to make an assessment of the impact. The following observations of Annex J (Simulation results) are worth highlighting:

Air borders

Steps	Added duration description
<ul style="list-style-type: none"> • First entry 	<ul style="list-style-type: none"> - EES registration: <ul style="list-style-type: none"> - Service Level: an added duration of less than 60 seconds on average, using 30 seconds for verifications, shows quite a limited impact on the relevant service levels (5 and 10 minutes) - Dwelling time: when in combination with existing border formalities including verification, 60 seconds are added, the average dwelling time increases by 16 seconds, from 1 min 50 seconds to 2 minutes 6 seconds. These changes can be qualified as modest. - Workload: under the same circumstances, border guard workload increases by less than 9.4% (at 40 seconds, the increase is around 4.5%). - Duplications: A 1:N search is made, using FPs, to eliminate the existence of duplicates. - As a comparison to the simulation results, the added duration of TOM B is between 45 and 65 seconds. It seems to have a very limited impact on service levels and dwelling time and a rather low impact on the workload.
<ul style="list-style-type: none"> • Subsequent entries and exits 	<ul style="list-style-type: none"> - An added duration of 30 seconds or less has in principle no impact on service levels, dwelling time or workload. - TOM B and C entail an additional processing time that is potentially higher than 30 seconds. However, on the basis of the results of the simulation, this should have a limited impact on the service levels and on the dwelling time (please refer to Annex J for further details).
<ul style="list-style-type: none"> • Exit 	<ul style="list-style-type: none"> - The added duration for TOM B is between 15 and 20 seconds; it has in principle no impact on service levels, dwelling time or workload.

Land borders

- The added duration for TOM B is between 15 and 20 seconds and it has to be calculated differently since the simulation is made for each vehicle.
- Given the average number of occupants in the vehicles and the fact that, in practice, several persons can be checked at the same time, the added duration would correspond to around 30-40 seconds per vehicle.
-

Steps	Added duration description
<ul style="list-style-type: none"> • Exit (land borders) 	<ul style="list-style-type: none"> - An added duration of 60 seconds per car, at exit, has the following impact: (i) the service level of 30 minutes decreases by around 2%, which represents around 35 seconds of added time for the total time of queuing and being checked. (ii) The dwelling time increases by around 3%. (iii) The usage factor increases by 12%, but this still leaves some margin to handle peak situations.

◦ **Evaluation of the TOMs for the EES (A, B and C)**

TOM A

TOM A, when compared to the “as-is” situation, would have a neutral impact on security (i.e. VEs would be better authenticated), little impact on duration on the first entry and subsequent entries and would not add any complexity.

The attention points of TOM A are as follows:

Attention points	Description
<ul style="list-style-type: none"> • Undocumented TCNVEs 	- Limited use after border crossing, the process/procedure/technology of trying to identify these persons is more complex and time-consuming with a residual risk of not finding the person back.
<ul style="list-style-type: none"> • Identifying undocumented TCNVEs 	- Will rely on reducing a candidate list by using generic filtering information such as gender, entry record without an exit record, age groups and language affinity. On this reduced candidate list, an automated facial recognition will be performed using the live image from the undocumented person.
<ul style="list-style-type: none"> • Risk of not performing a fingerprint-based identification 	- Where persons carrying multiple e-MRTDs/MRTDs with slightly different names (or dates of birth) would go undetected, cases of fraud would not be found and travellers would be able to stay for longer periods in the Schengen Area.
<ul style="list-style-type: none"> • Use of EES data 	- If the data in the EES were used to support analysis of irregular immigration or criminal activities, the added value would be limited.
<ul style="list-style-type: none"> • LEA 	- Latent searches are not possible.

The risks that need to be reduced by running the Pilot would be:

Items	Description
<ul style="list-style-type: none"> • Facial image comparison 	- Limited experience in existing processes to use photo as biometric identifier, in particular the issues relating to matching the e-MRTD photo to the photo stored in a database (duration, complexity).
<ul style="list-style-type: none"> • Enrol facial image 	- The time it takes to capture a picture from a passport and problems should be checked.

TOM B

TOM B would have an impact of 45 to 65 seconds on the first entry and 35-50 seconds extra on subsequent entries for an individual traveller, and the simulations made show a very modest impact on performance parameters for air and land borders. It would **increase security** (i.e. good authentication of VEs), however, and add medium complexity.

The attention points of TOM B are as follows:

Attention points	Description
• Duration	- Longer individual border crossing duration than with TOM A
• Complexity	- Increased complexity in relation to TOM A
• LEA	- LEA latent searches (except thumbs) are possible but with limited results since only 4 FPs are used

The risks that need to be reduced by running the Pilot would be:

Items	Description
• Enrol 4 FPs at first line border check	- Feasibility and performance of enrolling 4 FPs at the borders (impact on process, equipment and quality)

TOM C

TOM C would add 65 to 95 seconds on the first entry and would have a more limited impact on subsequent entries (35-50 seconds). The simulation showed that going beyond the 60 seconds at first entry has

The simulation showed that additional time required for the enrolment of the 8 FPs would have a negative impact on the likelihood of serving the traveller within two minutes, consequently increasing the average dwelling time. However, service levels of 5 and 10 minutes per traveller would not be affected. For subsequent entries and exits the TOM C would have the same impact as TOM B.

TOM C would **increase security** (i.e. good authentication of VEs) but add more complexity.

The attention points of TOM C are as follows:

Attention points	Description
• Duration	- Longer individual border crossing duration than with TOM A
• Complexity	- Increased complexity in relation to TOM A and B - Difficult (if not impossible) to implement for certain land and sea borders without changes to the process or other technological solutions
• LEA	- Full LEA latent searches (except thumbs) are possible with good results

The risks that need to be reduced by running the Pilot would be:

Items	Description
• Enrol 8 FPs	- 8 FPs is at present cumbersome to enrol using handheld equipment. Constraints related to time and space would be even more of a problem than when enrolling 4 FPs. - Check technological alternatives for enrolling 8 FPs from VEs in all situations at land and sea borders - Check the use of kiosks for enrolling 8 FPs from VEs in particular situations at land and sea borders

When comparing the impact (on SLA, dwelling time and workload) to the estimated added duration of the TOMs (e.g. to TOM B), the impact may appear surprisingly modest.

It should however be re-called that the highest impact on border crossing time occurs for **VEs** and they represent **about 15%** of the total number of travellers. Within this group, the impact is more

noticeable for first entries than for subsequent entries, although the percentage of first entries vs the total plays only a secondary role. Since less than 15% of all travellers incur a longer border crossing time, the performance parameters (SL compliance, dwelling time, workload) for all travellers on average **are affected modestly**.

The **overall conclusion** is that the implementation of EES by 2020 with TOM B at air and land borders would have a **limited negative impact** on **service level, dwelling time** and **workload**.

The simultaneous implementation of RTP at air borders always has a positive effect on the same parameters. The positive effect becomes noticeable for travellers once the percentage of **RTs exceeds 5%**. As long as the ABC gates currently installed are not saturated, the increased use of ABC gates by TCNs subscribing to RTP should not impact EU travellers.

– RTP TOMs M and N

This section presents an overview of the TOMs for the RTP: TOM M and N. While the process steps of TOM M and N would not vary at entry and exit, yet the source of biometrics verification would be different, namely:

TOM M would rely on fingerprints and photo being part of the registration in the RTP application process (VE).

TOM N would rely on the existing biometrics of the EES (VE). No enrolment of biometrics would be made in the RTP application process. Identifications and verifications in the border control process would be made using the EES. Therefore, the use of biometrics for these actions is not explicitly presented in the table below.

All three TOMs analysed for the EES (TOM A, B and C) can be combined with both TOMs M and N. Moreover, both TOMs would rely on VIS for the verification of VH.

Neither of the TOMs would use a separate token. For common features, architecture choices, process accelerators and additional discussion elements please refer to section 8.1.

The process for TOM M is described in chapter 3.2 and the process for TOM N is described in chapter 3.6.

◦ Overview

Options		TOM M	TOM N
<ul style="list-style-type: none"> RTP enrolment procedure based on EES data. 		No	Yes
<ul style="list-style-type: none"> EES individual file created at the end of the application process 		✓	EES individual file is a pre-requisite
<ul style="list-style-type: none"> 1:N identification using FPs against the RTP (in the RTP application process – to prevent RTP shopping) 	<ul style="list-style-type: none"> VEs: 	✓	Relies on 1:N identification at 1 st entry in EES
	<ul style="list-style-type: none"> VHs: 	Not necessary – person already identified within the VIS	Not necessary – person already identified within the VIS
<ul style="list-style-type: none"> Number of FPs enrolled for RTP application 	<ul style="list-style-type: none"> VEs: 	Same as for the EES (i.e. 4 for TOM B)	0 FPs, relies on the EES for the biometric verification
	<ul style="list-style-type: none"> VHs: 	0 FPs, the VIS FP verification is trusted.	0 FPs, the VIS FP verification is trusted.
<ul style="list-style-type: none"> Verification using photo (ABC)²¹², FPs (ABC or manual) 		✓	✓ (EES process is used)

²¹² Applicable only for VE, unless the VIS regulation is revised, as it currently mandate the verification through FPs.

RTP application process

Steps	TOM M	TOM N
1. Application	<ul style="list-style-type: none"> - Applications: made at consular posts or at border crossing points - VH: need to have a MEV to apply for RTP 	<ul style="list-style-type: none"> - The RTP application (VH/VE) is made on-line on the condition that the <u>traveller already exists in the EES</u> (individual file, entry and exit). The verification of the traveller is made as part of the EES process. - No enrolment of FPs needed since the FPs stored in the EES will be used. - For residence permits, residence card and D-visa holders, it is proposed to have an individual file created, before the RTP status is granted. However, for persons with residence permits/cards or with D-visas, there would not be any entry/exit record created.
2. Identification	<ul style="list-style-type: none"> - VE: 1:N identification against RTP - VH: 1:N identification occurred when applying for the visa 	<ul style="list-style-type: none"> - N/A – the RTP application relies on the existence of an individual file in the EES. The identification (if retained) would be part of the EES process and is described as an option in section 3.2.
3. Enrol	<ul style="list-style-type: none"> - VE: 4 FPs captured and stored in RTP - VH: The FPs stored in the VIS application process are used as the basis for verification. - VE/VH: Photo captured and stored in RTP. - EES individual file: created at the end of the application process 	<ul style="list-style-type: none"> - FPs: already exist in the EES. No enrolment. The number of FPs in RTP is then de facto the same as in the EES: - Photo: already exists in EES. No enrolment - EES individual file: N/A – there is no need for this option as the EES file exists from the start.

Border check

Steps	TOM M	TOM N
1. Status control	<ul style="list-style-type: none"> - RTP record is retrieved– using issuing country and document number 	<ul style="list-style-type: none"> - Same as TOM M

2. Verification²¹³	Depending on the border crossing, verification is made using either: <ul style="list-style-type: none"> - Facial recognition based on the e-MRTD photo and a live photo or using the photo stored in RTP, or - VE: FP comparison against the central RTP, using 4-1 FPs captured - VH: VIS check is trusted - Manual (ocular) verification, using the photo – used in degraded mode 	<ul style="list-style-type: none"> - Same as TOM M - except VE: FP comparison against the central EES, using 4-1 FPs captured, or live picture compared against the FI stored within the EES.
3. Entry / Exit	<ul style="list-style-type: none"> - Entry-exit record created 	<ul style="list-style-type: none"> - Same as TOM M

◦ **Simulations results related to RTP**

- The RTP positive impact becomes noticeable for travellers once the percentage of RTs exceeds 5%. Simulations of RTP travelling show improvements in service times, dwelling times and workload in correlation with an increase in the expected number of RTP travellers using ABC gates. As long as the ABC gates currently installed are not saturated, the increased use of ABC gates by TCNs subscribing to RTP should not impact EU travellers.

◦ **Summary of the TOMs for the RTP (M and N)**

TOM M

TOM M, despite the joint technical architecture with the EES, would be the closest to the legislative proposal of the two TOMs proposed for the RTP. It would, in fact, retain its own database of biometric identifiers (at least for VE) and would not provide for any dependency from the EES, besides the anticipated consultation of EES in the application process and in border control processes.

The attention points of TOM M are as follows:

Attention points	Description
<ul style="list-style-type: none"> • Redundancy of the information stored 	<ul style="list-style-type: none"> • VEs would have their biometric data stored in the EES and in the RTP. • The IT infrastructure would have to accommodate two different databases of biometric identifiers, although the RTP database is a sub-set of the EES one. • Possible issues of inconsistency for the data stored in the different systems (i.e. EES and RTP) yet belonging to the same person.
<ul style="list-style-type: none"> • Online application / pre-registration 	<ul style="list-style-type: none"> • The possibility of an online pre-registration is recommended for this TOM, however, it would be difficult to implement without

²¹³ In the case of a combination with TOM A, for the EES, the FI would be used for the identification of the RTP member.

	<p>any link to the EES (e.g. to verify the correctness of the information provided by the TCN performing the online procedure).</p> <ul style="list-style-type: none"> • Even after the online pre-registration the TCN would still have to enrol his/her biometric data in the RTP database at a consular post or at a border crossing point.
<ul style="list-style-type: none"> • Reception capabilities of consulates and RTP registration points at the BCP 	<ul style="list-style-type: none"> • It is expected that RTP will largely re-use the resources already in place (i.e. the release of visas (in VIS), consulates and RTP registration points at the BCPs) thus it is important to ensure the allocation of sufficient resources to handle the flow of prospective RTP members that complete the registration and enrol FPs in place. <ul style="list-style-type: none"> • The estimation and fluctuations in RTP demand over time will be a critical factor

TOM N

TOM N proposes a streamlined RTP system that would rely on the EES. The EES would be the sole repository of biometric data and would take care of the verification of TCNs for VE. The enrolment into the RTP would be possible through a website, provided that the TCN already exists in the EES, which would be likely, as the target audience of the RTP is composed of frequent travellers. This TOM reduces the burden of the registration centres at BCPs and at the consulates and is more convenient for travellers that use the website for the application and do not have to enrol FPs in person again.

TOM N is a step further in conceiving RTP and EES as a single system.

The attention points of TOM N are as follows:

Attention points	Description
<ul style="list-style-type: none"> • Online application procedure 	<ul style="list-style-type: none"> • The link with the EES and the opening of a window onto the data stored within a secure environment raises concerns that should be addressed in a risk analysis. • The IT infrastructure would have to be adapted and reviewed to ensure insulation from any risks and attacks coming from the online website²¹⁴. • The online procedure would be advantageous mostly for VE as, VH are likely to register into the RTP while applying for an MEV.
<ul style="list-style-type: none"> • Data protection 	<ul style="list-style-type: none"> • The link of EES and RTP has implications with regard to data retention. The data within the EES would not be deleted until either the expiration of the RTP status or of its own data retention period. <ul style="list-style-type: none"> • However, in a real-life situation, RTP members are by definition frequent travellers, therefore the individual file within the EES would not have been deleted as long the person continues travelling.

²¹⁴ Safeguards similar to those described under section 6.2 would have to be put in place for the consultation of remaining stay duration and RTP status by TCNs.

	<ul style="list-style-type: none">• The link of two systems could create some concerns regarding the data protection aspects that should be assessed in light of the specific implementation that will be adopted. However, it is important to observe that both EES and RTP intervene in the same business processes and have the same overall purpose of allowing and monitoring the entry into and exit from the Schengen Area by TCNs.• The two systems could even be conceived as a single system conceptually and technically, simplifying, thus, data protection compliance (in terms of storage and usage of the data across EES and RTP).
--	---

Given the numerous new elements and possibilities introduced by TOM N, further analysis should be undertaken to assess the risks and to determine which would be the best technical and legal implementation.

• **Options for the Pilot**

The Pilot's objective is to test the potential options in operational and relevant environments in order to decrease the risks related to the development and full implementation of EES and RTP in the Schengen Area. For instance the checks should be made on accuracy, effectiveness, and quality of the solution as well as on the impact on the border crossing duration.

From the point of view of mitigation of implementations risks, the Pilot should not cover a full end-to-end test of EES and RTP because none of these systems introduces requirements to the central system or the network that are completely different from the ones used in existing large-scale IT systems. Finally the time and budget earmarked for the Pilot do not correspond to the ones required for such an end-to-end Pilot. Hence, the objective would be to test significant parts or components of the solution and conclude on the results.

The results for the Pilot would provide a greater degree of certainty on the feasibility of the options chosen for designing future system(s) and processes.

The criteria to be considered when selecting options for the Pilot as a means to reduce the EES and RTP implementation risk are:

5. additional evidence is needed to verify the expected impact;
6. need to test possible process changes;
7. requirements for specific technical solutions and need to test related constraints or possibilities;
8. analysis results from TOMs indicating the options that add duration and/or complexity.

The following table lists proposed options for the Pilot. It is structured by:

1. Border control processes and use of biometrics
2. Process accelerators
3. Other relevant items

For each option, where applicable, type of technology to be used, type of border and environmental conditions to be tested are identified and marked as 'x' in the following table.

The cost of the Pilot is estimated in the separate Cost report (see Cost report section 7). It should be noted that the main cost drivers of the final budget of the Pilot will depend heavily on (i) specifications of the Pilot, (ii) sample size for test items and (iii) inclusion or exclusion of AFIS vendors, e.g. to borrow or buy their equipment.

The expected timeline of the Pilot is the following

Phase	Duration
Design	Sep'14 – Feb'15
Execution	March'14 – Sep'15
Reporting	Oct'15 – Dec'15

During the design phase the following actions should be undertaken:

- Define testing strategy to ensure the common understanding and approach between key stakeholders for achieving the expected outcome.
- Draft testing roadmap to further precise overall approach and magnitude. Also include more detailed project planning.
- Provide detailed test instructions (test cases) on what to be tested, under which conditions, on which population, with which device, with what outcome, etc.

During execution phase following assumptions can be made:

- The Pilot should be carried out in waterfall method, i.e. as many items as possible should be tested in one BCP in order to proactively adapt the execution of the testing and minimise additional effort required to set-up and monitor the testing.
- Minimum six border control points should be included to the Pilot (e.g. two airports, two land and two seaports).
- The number of MS, where test will be carried out, should be kept as low as possible. There should be a good balance between different MS and BCPs to cover the whole of the EU. For example MS with higher capacity – the ones who can provide more BCPs for testing, who have higher traveller flows or who already have relevant suppliers/contracts in place - should be preferred.
- The results of the test will be saved only locally.

In addition to the pilot, the annex K provides a list of additional items to be studied that would further explicit the processes, descriptions of data, and systems for EES and RTP. These additional items for study would also allow an additional refinement of the cost computation.

Options for the Pilot (reference to TF)	Specific Objective	New technology					Border type					Environmental factors ²¹⁵	
		Existing technology	Finger on the fly scanner	Hand-held scanner	ABC gates	Manual gates	Air	Land					Sea
								Train	Bus	Road	People in vehicle		
Border control processes and use of biometrics													
1. Enrol 4 fingerprints at first-line border check (for EES) (TF1, TF4, TF5)	<p>Check the feasibility of this solution</p> <p>1. Process:</p> <p>1.1 the potential gain in terms of time</p> <p>1.2 enrolment process reader operation, environmental conditions</p> <p>1.3 size of the scanning area</p> <p>2. Reader/ ease to collect.</p> <p>2.1. reader: functional and technical specs</p> <p>2.2. reader: qualifications/user-friendliness</p> <p>3. Enrolled result (quality)</p> <p>3.1. FTE/FTA/FAR/FRR etc.</p> <p>3.2. results further usage in BCP</p>	x	x	x			x	x		x	x	x	x
2. Enrol 8 fingerprints at first-line border check (for EES) (TF1, TF4, TF5)	<p>In addition to the above (reader, process, enrolled result)</p> <p>- evaluate the enrolment time difference between 4FP and 8FP together with human factor</p> <p>- implement the maximum number of quality algorithms as provided by AFIS vendors and NIST</p>	x	x	x		x	x			x			

²¹⁵ Cold weather (<-10C), rain, snow, storm; limited space; limited Wi-Fi signal.

Options for the Pilot <i>(reference to TF)</i>	Specific Objective	New technology					Border type					Environ-mental factors ²¹⁶
		Existing technology	Finger on the fly scanner	Hand-held scanner	ABC gates	Manual gates	Air	Land			Sea	
								Train	Bus	Road		
3. Enrol facial image (live) <i>(TF1, TF4, TF5)</i>	<p>Check the feasibility of this solution</p> <p>1. Process:</p> <p>1.1 the potential gain i+B8n terms of time</p> <p>1.2 enrolment process reader operation, environmental conditions</p> <p>2. Reader/ ease to collect.</p> <p>2.1. reader: functional and technical specs</p> <p>2.2.reader: qualifications/user-friendliness</p> <p>3. Enrolled result</p> <p>3.1. FTE/FTA/FAR/FRR etc.</p> <p>3.2. results and further usage in border control processes (including multimodal use)</p> <p>4. Quality of the image you can obtain in the regular border control setting without specific measures (e.g. light or background)</p>	x		x			x	x			x	

²¹⁶ Cold weather (<-10C), rain, snow, storm; limited space; limited Wi-Fi signal.

4. Capture photo from e-MRTD and verify it against another source (e.g. live photo or photo in a database) (TF1, TF4, TF5)	Check the feasibility of this solution - check against image taken in the regular border control setting without specific measures (see 3.4) - confirm the speed - occurrence of difficulties - number of broken chip, non-connectivity etc. Passive Authentication should be included as a security mechanism.	x					x	x			x	x	x
--	---	---	--	--	--	--	---	---	--	--	---	---	---

Options for the Pilot (reference to TF)	Specific Objective	New technology					Border type					Environ-mental factors ²¹⁷	
		Existing technology	Finger on the fly scanner	Hand-held scanner	ABC gates	Manual gates	Air	Land					Sea
								Train	Bus	Road	People in vehicle		
5. Searching VIS based on document number, not using the visa-sticker number (TF 5)	Test whether this will yield the appropriate match, which would allow to avoid reading the visa sticker and assess the impact on the border control process						x	x	x	x	x	x	
6. Web-interface to the carriers as a technical pilot (TF 14)	Reduce the risk of security in the functionality as it would be the first time when large scale IT system will be exposed to outside world (e.g. eu-LISA link to carriers). Study how carriers can retrieve the information from EES.												

²¹⁷ Cold weather (<-10C), rain, snow, storm; limited space; limited Wi-Fi signal.

Options for the Pilot (reference to TF)	Specific Objective	New technology					Border type					Environmental factors ²¹⁸	
		Existing technology	Finger on the fly scanner	Hand-held scanner	ABC gates	Manual gates	Air	Land					Sea
								Train	Bus	Road	People in vehicle		
Process accelerators (TF 9)													
Enrol iris	Does iris provide the means to speed-up the enrolment? Is it applicable at all the borders?						x			x		x	
Use of self-service kiosks	Validate the usefulness, usability and security in relation to using self-service kiosks for registering, checking and enrolling biometrics	x			x		x			x			
Reading e-MRTD/MRTD													
Verify document using PA (and possibly AA)													
Capturing fingerprints (4 and/or 8)													
Capture photo from MRTD and verify bearer against a live photo													
Use of assistance													
Make initial checks (or simulate these)													
Using time efficiently in the waiting areas	- Validate the feasibility of introducing pre-border checks in the waiting areas of land borders (where such areas exist today). - Possibility to include self-service kiosks									x			
Exit checks	- Check the process of TCN using ABC gates at exit. - Check the time	x			x								

²¹⁸ Cold weather (<-10C), rain, snow, storm; limited space; limited Wi-Fi signal.

List of abbreviations

AA	Active Authentication
ABC	Automated Border Control. Also referred to as e-Gates or electronic gates
AFIS	Automated Fingerprint Identification System
ABIS	Automated Biometric Identification System
API	Advanced Passenger Information
APIS	Advanced Passenger Information System
BAC	Basic Access Control
BC	Border Check
BC-NS	Border Control National System
BCP	Schengen External Border Crossing Point
BG	Border Guard
BMS	Biometric Matching System
BSI	Bundesamt für Sicherheit in der Informationstechnik (in English: Federal Office for Information Security)
CDS	Country Document Signature
CISA	Convention implementing the Schengen Agreement
CLIA	Cruise Lines International Association
CRL	Certificate Revocation List
CP	Consular Post
CSCA	Country Signing Certificate Authority
CVCA	Country Verifying Certificate Authority
DOB	Date Of Birth
e-MRTD	Electronic MRTD
EAC	Extended Access Control
EAC-CA	Chip Authentication
EAC-TA	Terminal Authentication
EC	European Commission
EEA	European Economic Area
EEC	European Economic Community
EER	Equal Error Rate
EES	Entry-Exit System
EESDB	Entry-Exit System Database
EIO	Entry Into Operation

ETA	(Australian)Electronic Travel Authority
EU/EEA/CH	Persons of the EU, the European Economic Area and Switzerland
FAR	False Acceptance Rate
FI	Facial Image(s)
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False non-Match Rate
FOP	Form Of Payment
FP	Fingerprint(s)
FPIR	False Positive Identification Rate
FRR	False Rejection Rate
FTA	Failure to Acquire
FTE	Failure to Enrol
HR	Human Resources
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IRIS	Iris Recognition Immigration System
IS	Inspection System
LBT	Local Border Traffic
LEA	Law Enforcement Access
MEV	Multiple Entry Visa
MRTD	Machine Readable Travel Document
MRP	Machine Readable Passport
MRZ	Machine Readable Zone of a Machine Readable Travel Document
MS	EU Member State(s)
NUI	National Uniform Interface
PA	Passive Authentication
PKD	Public Key Directory
PKI	Public Key Infrastructure
PNR	Passenger Name Record
QOS	Quality of Service
RFID	Radio Frequency Identification
RT	Registered Traveller
RTP	Registered Traveller Programme
RTPDB	Registered Traveller Programme Database
SBC	Schengen Borders Code
SDLC	Software Development Lifecycle
SIS II	Schengen Information System of the 2 nd Generation
SOA	Service-Oriented Architecture
SOD	Document Security Object
TCN	Third Country National

TCNRT	Third Country National – Registered Traveller
TCNVE	Third Country National – Visa Exempt
TCNVH	Third Country National – Visa Holder
TF	Thematic File
TOM	Target Operating Model
VE	Visa Exempt
VH	Visa Holder
VIS	Visa Information System

Glossary

Automated Border Control (ABC) system	An automated system, which authenticates the e-MRTD, establishes that the passenger is the rightful holder of the document, queries relevant systems and automatically determines eligibility for border crossing according to predefined rules.
Biometrics	Automated recognition of individuals based on their biological and behavioural characteristics. In the context of EES and RTP the biometric characteristics considered are facial image and fingerprints.
Border check	The checks carried out at Border Crossing Points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorized to leave it. [Schengen Borders Code, Article 2.10].
Border Crossing Point (BCP)	Any crossing-point authorised by the competent authorities for the crossing of external borders. [Schengen Borders Code, Article 2.8].
Certificate	An electronic document establishing a digital identity by combining the identity name of identifier with the public key of the identifier, a validity period and an electronic signature by a third party.
De-duplication	Biometric identification check (1:N) that may be performed as a part of the enrolment process to ascertain existing enrolment status of biometric data subject.
e-MRTD	Machine Readable Travel Document (e.g. passport) containing a Contactless Integrated Circuit (IC) chip within which data from the MRTD data page, a biometric measure of the passport holder, and a security object to protect the data with PKI cryptographic technology is stored, and which conforms to the specifications of ICAO DOC 9303, Part 1.
Enrolment	Enrolment is the process of collecting biographic and biometric data from an individual for registration.
EU Long term resident permit holders	Any third-country national who has long-term resident status as provided for under Articles 4 to 7 of Directive 2003/109/EC
External borders	Schengen countries' land borders, including river and lake borders, sea borders and their airports, river ports and lake ports, provided they are not internal borders.
Persons enjoying the right of free movement under Union law	According to Article 2 §5 of the Schengen Borders Code: (a) Union citizens within the meaning of Article 17(1) of the Treaty, and third-country nationals who are members of the family of a Union citizen exercising his or her right to free movement to whom Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States (15) applies; (b) third-country nationals and their family members, whatever their nationality, who, under agreements between the Community and its Member States, on the one hand, and those third countries, on the other hand, enjoy rights of free

movement equivalent to those of Union citizens.

First Line Check	The border check conducted at the location at which all travellers are checked. See also "Second Line Check".
Identification (1:N)	In the context of EES and RTP, the following definition of identification (1:N) is used: the process of determining a person's identity through a database search against multiple templates. It is referred to as One-to-Many (1:N), in which "N" is a variable that corresponds to the database size.
Identification (N:N)	In the context of EES and RTP, the following definition of identification (N:N) is used: the process of attempting to match each template in the database against all others. In case of a positive match this would indicate a person is registered under different identities. It is referred to as Many-to-Many (N:N), in which "N" is a variable that corresponds to the database size. Such a N:N identification would not be part of an EES or RTP border control process, but could be used in the background to improve the quality of the data.
Local Border Traffic	The regular crossing of an external land border by border residents in order to stay in a border area, for example for social, cultural or substantiated economic reasons, or for family reasons, for a period not exceeding the time limit laid down in the Local Border Traffic Regulation. [Local Border Traffic Regulation, Article 3.3].
Local Border Traffic permit	A specific document, as introduced by Chapter III of the Local Border Traffic Regulation, entitling border residents to cross an external land border under the local border traffic regime. [Local Border Traffic Regulation, Article 3.7].
Long-term resident's EU residence permit'	A residence permit issued by the Member State concerned upon the acquisition of long-term resident status.
Manual verification	A manual verification is made by a person and includes, in most cases, ocular inspection of a picture, from the travel document or displayed from another source, and comparing this picture to the person being checked.
MRTD	Official document, conforming with the specifications contained in Doc 9303, issued by a State or organisation which is used by the holder of international travel (e.g. passport, visa,) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by a machine.
Multimodal biometrics	Combination of information from two or more biometric measurements. It is also known as "Fusion" and "multibiometrics".
Overstayer	A person who has entered the EU Schengen area legally (i.e. with a valid travel document and/ or a visa) but has remained in the territory beyond the time he/she was entitled to stay.
Privacy by Design	Privacy by design is a concept according to which "[...] the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default

mode of operation.

The objectives of Privacy by Design — ensuring privacy and gaining personal **control over one's** information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles. Privacy by Design is a concept that was first used in the report **“Privacy-enhancing technologies: the path to anonymity” published in 1995** and has been developed by the Information and Privacy Commissioner of Ontario Ann Cavoukian.

Residence permit

Any authorisation issued by the authorities of a Member State allowing a third-country national to stay legally on its territory. The residence permits can be short-term (ST) or long-term (LT).

Schengen visa

Uniform short stay visa that entitles the holder to stay in the territories of all Schengen States for a period of maximum of 90 out of 180days and that may be issued for the purpose of single or multiple entries.

Second line check

A further check that may be carried out in a special location away from the location where all travellers are checked (first line). [Schengen Borders Code, Article 2.12].

Third Country National (TCN)

Any person who is not a Union citizens within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union and who is not covered by the definition of persons enjoying the Community right of free movement outlined in Article 2.5 of the Schengen Borders Code. [Schengen Borders Code, Article 2.6].

Thematic Files

Set of key issues related to the EES and the RTP jointly agreed between the **Commission and the Member States participating to the workshop “Meeting of 7th February 2014 to establish the objectives of the study to identify options for the Entry Exit and the Registered Traveller Programme”**. The TFs define the scope of the present Study.

Verification (1:1)

One or more samples from one biometric data subject are captured, processed into a usable form and then compared against a biometric reference (1:1 comparison).

Reference documents

Title	Author	Date of the document
7 Foundational Principles, Implementation and Mapping of Fair Information Practices	Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada	
Annual Risk analysis 2013	Frontex	04/2013
Best Practice Operational Guidelines for Automated Border Control (ABC) Systems	Frontex	31/08/2008
Best Practice Technical Guidelines for Automated Border Control (ABC) Systems	Frontex	31/08/2008
Best Practices at EU land BCPs (draft version)	Frontex	2014
Biometrics Design Standards For UID Applications	Unique Identification Authority of India (UIDAI)	2009
Cost analysis of EES & RTP	Unisys	19/04/2010
Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 07/08/2007		07/08/2007
Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350,	European Union	30/12/2008
Crossmatch SEEK II Secure Electronic Enrolment Kit and Multimodal Identification Platform	Cross Match technologies	25/06/2008
Current Market Outlook 2013-2032	Boeing	
EES and RTP technical options	Directorate General Justice, Freedom and Security - 30th Immigration and Asylum Committee	14/10/2008
EES Feasibility Study	Unisys	06/02/2008
Entering the EU borders & visas (Infographic)	DG Home Affairs	02/11/2010
Futures of Borders	Frontex	12/2011
Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing a registered traveller programme, SWD(2013) 50 final	European Commission	28/02/2013
Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council	European Commission	28/02/2013

establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union, SWD(2013) 47 final

Schengen Handbook – Annex 4 - List of Border Crossing Points	European Commission	06/11/2006
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281	European Union	23/11/1995
Operational and Technical Security of Electronic Passports	Frontex	07/2011
Opinion on EES and RTP	European Data Protection Supervisor	18/07/2013
Policy study on an EU Electronic System for travel Authorisation	PwC	02/2011
Privacy by Design: delivering the promises	European Data Protection Supervisor	07/05/2010
Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection of prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.	European Commission	25/01/2012
Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.	European Commission	25/01/2012
Proposal for a Regulation of the European Parliament and of the Council on the Union Code on Visas (Visa Code) (recast), COM(2014) 164 final.	European Commission	11/04/2014
Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union. Brussels, COM(2013) 95 final, 28.2.2013	European Commission	28/02/2013
Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP). Brussels, COM(2013) 96 final.	European Commission	28/02/2013
Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme. Brussels, COM(2013) 97 final	European Commission	28/02/2013
Public Key Infra discussion paper	Frontex	14/06/2014
Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28/12/2006	European Commission	28/12/2006
Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105	European Commission	13/04/2006

Appendixes

Regulation (EC) No 767/2008, Concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), Official Journal L218, 13/08/2012	European Commission	13/08/2012
Technical Specifications for the Study on the Technical options and recommendations for a Smart Borders pilot and Revised Cost Analysis	DG Home Affairs	03/2013
The Commission's legislative proposals on Smart Borders: their feasibility and costs	European Parliament	10/2013
UID Enrolment Proof-of-Concept Report	Unique Identification Authority of India (UIDAI)	2011

Biometrics overview

Introduction to biometrics

Although similar in some aspects, human beings differ in appearance, behaviour and biological traits. Various recognition technologies can be used in order to create and maintain a reliable identity repository. For the purposes of EES/RTP, the most important ones are: Photographs, Fingerprints; Face, and potentially Iris. Other technologies exist, but are currently considered less relevant to EES/RTP: hand geometry, voice, vascular patterns, dynamic signature verification, keystroke dynamics, vein/palm scans and DNA. Other features such as gait (how a person walks) are subject to further study.

A typical system architecture is depicted below.

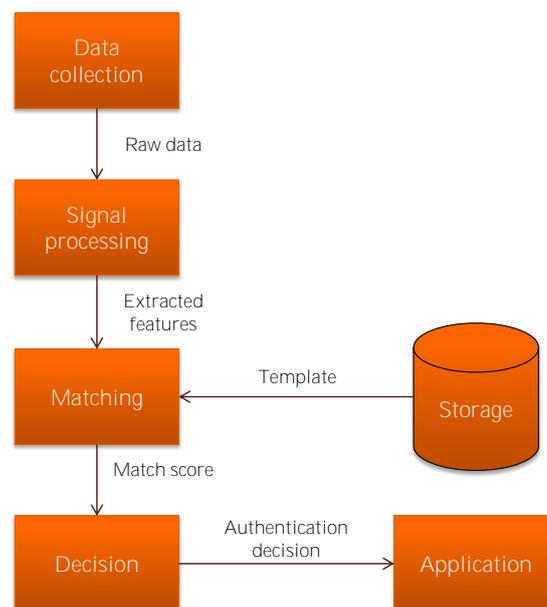


Figure 70 A typical biometric system architecture

Initially, raw data is collected and processed into features, which are stored in the form of a template in a database. Upon subsequent data collection at a later point in time, the newly collected data features can then be matched against the already stored template.

The key aspects of the different biometrics can be described as:

- Photographs are popular basic biometrics, due to their simplicity. However, individually they are not considered as sufficiently reliable e.g. for international travel purposes, as individuals may still bear sufficient resemblance to one another, making it impossible to distinguish them under operational conditions;
- Fingerprints are the oldest and most widely adopted biometric identifier used in automatic processing and matching. As a result, this is the most mature of all biometric technologies;
- Face recognition uses the structure and spatial geometry of landmarks such as the nose, eyes, lips and jaw line. It can be performed on 2-D and 3-D images. This technology has improved significantly over the last decades;
- Iris recognition uses the pattern that is formed by the muscle tissue and cell structure in the iris region of the eye. The iris image is captured using infrared illumination and a camera. It attracted a lot of attention in the last decade;

Appendixes

- Hand geometry recognition uses the contour of the hand, the length and thickness of the fingers, and the spatial distance between other landmarks of the hand. It is heavily favoured in physical access control applications;
- Voice recognition uses characteristics such as the pitch, intonation and vocal speed of an individual's voice. It has seen low adoption in the commercial sector;
- Vascular pattern recognition uses vein patterns. Veins carry deoxygenated blood back to the heart, and research indicates that the pattern formed by the vascular network is relatively unique and permanent;
- Dynamic signature verification uses velocity, direction, number of strokes, time of each stroke, and pressure applied by the user during the signing process;
- Keystroke dynamics uses the typing rhythm of a user on keyboards or other input devices;
- DNA has originally been used in forensic sciences, but is now pursued as a biometric technology. However, there are still issues to be addressed such as invasive data capture, processing time (hours rather than seconds) and price. The Study currently considers DNA to be out of scope for the secure eID Toolkit;
- Other biometric technologies such as retina, gait, ear lobe, scent, and knuckle recognition are also being actively researched.

The application to capture a traveller's information for enrolment takes the basic biographic information. In case biometric information is required, this is captured as well. With regard to capturing the citizen's basic information, it is common practice to use a breeder document or its electronic equivalent.

With regard to breeder documents, those are the fundamental physical evidence accepted by national authorities to establish a *prima facie* claim to an identity. They will capture basic identity attributes such as name and gender, and whatever attributes are required by the identity system. The latter may include name of the parents, address, date of birth etc. Typical enrolment steps are to establish identity (evidence that the claimed identity is valid, evidence that the claimer links to the claimed identity, and evidence that the claimer operates under the claimed identity), confirm citizenship or similar status, and assess entitlement. The ICAO provides commonly accepted guidance in these aspects, a.o. in their ICAO 9303 series of documents. In case of a positive outcome of the assessment, the breeder document is propagated to the next step in the issuance process, which may include error and duplication checking, and approval.

When enrolment of biometric features is required as well, a link between the breeder document and the biometric data needs to be established.

With regard to biometrics, enrolment is obviously dependent upon the type of biometric identifier selected. This may include a picture, fingerprints, iris scan etc.

Enrolment is the process of collecting biometric samples from a user and subsequent processing and storing of their biometric reference in the system database or portable token. A biometrics system must cope with changes in the data collection environment, and in the data being collected:

- The biometric feature may change;
- The presentation of the biometric feature at the sensor may change;
- The performance of the sensor itself may change;
- The surrounding environmental conditions may change.

Within the signal processing subsystem, the feature extraction module receives the raw biometric data from the data collection module and extracts the distinguishing features from the raw data, transforming it into the form required for storage and matching.

For the same biometric characteristic, there are various ways of extracting the distinguishing features. These may be proprietary or standardized. The module may perform a quality analysis of the raw data to determine if it is satisfactory for use. If the data fails the quality test, the user may need to supply the biometric characteristic again. The raw biometric data may be pre-processed prior to feature extraction in order to remove noise or to be normalised in some way. Typically, it is not possible to reconstruct the raw data from the extracted features.

The matching module receives the processed data from the feature extraction system and compares it with the biometric template from the storage module. It measures the similarity of the claimant sample with an enrolled template. Each comparison yields a score, which is a numeric value indicating how closely the sample and the template match. There are different methods for computing the score. Examples include distance metrics, probabilistic measures, and neural network-based methods.

The decision module receives a score from the matching module and, using a confidence value based on security risks and risk policy, interprets the result of the score. The decision module usually returns a binary yes or no. In the most common case, the decision is based on a single threshold. If the score is above the threshold, the module concludes that the user is indeed the individual owing the template. If not, the module indicates the user is not that individual. In more complicated cases, the decision is made based on more than one matches and a yes decision is taken if, for example, 2 out of 3 submitted samples match. Note that it is possible that a legitimate claimant is rejected by the biometric system due to the very nature of the biometric data. The data collection module does not collect exactly the same biometric information at every attempt to use the system and so it is possible that a legitimate user is rejected or an impostor is admitted by the biometric system.

The matching module rates the similarity between the collected biometric data and the reference template. If the match score is above the tolerance (or acceptance) threshold, the claimant is accepted. If it is below the threshold, the claimant is rejected. Biometric systems can therefore generate two types of errors:

- **Type I error: where the system fails to identify a valid user ('false non-match' or 'false rejection');**
- **Type II error: where the system accepts an impostor ('false match' or 'false acceptance').** The value of the acceptance threshold is crucial to the performance of the system and depends on the security requirements of the application. If the threshold is relatively high (i.e. it is tough to meet), more valid users will be rejected (hence the 'false non-match' rate will be high) but fewer impostors will be accepted ('false acceptance' rate will be low). On the other hand, if the threshold is relatively low (i.e. it is easy to meet), more impostors will be accepted ('false match' rate will be high) but fewer valid users will be rejected ('false non-match' rate will be low). There is thus a trade-off between these two types of errors. Such a threshold setting will depend on the security requirements of the application.

The storage module maintains the reference templates for enrolled (registered) users. It may contain a single template for each user or thousands of templates depending on the system architecture or intended use. The template may be physically stored in physically protected storage in the biometrics device, in a conventional database on a computer, or in a portable token such as a smartcard. Collateral information, such as name, identification number, etc., binding the owner to his/her reference template may also be stored together with the reference template.

It can be observed that the subsystems within the model are logically separate. Some subsystems may be physically integrated. However, usually there are separate physical entities in a biometric system. As a result, biometric data has to be transmitted between the different physical entities. Obviously, biometric data is vulnerable during transmission. Therefore it is often encrypted.

Introduction to electronic passports

The issuing process for e-passports starts with the application by a citizen for an e-passport at a passport office. Here the applicant offers the required (breeder) documentation to support his application. Based on the offered documentary evidence (optionally cross checked with independent sources and criminal records) the application is either accepted or rejected in the entitlement decision.

If positive, the e-passport is personalized with **the applicant's personal information, and supplied with cryptographic keys**. For personalization, a blank passport is used, which conforms to international standards such as from ICAO.

Subsequently the e-passport is delivered to the applicant, and older passports are typically invalidated. Once the applicant has received his e-passport, it can be used to prove identity e.g. in Border Control.

If the e-passport is stolen or lost the e-passport holder is expected to report this so the document can be invalidated.

Finally, Security Management is the process that allows the control of risks throughout the passport life cycle.

Security features to protect biometric data in e-Passports

Summary of e-passport logical security mechanisms

The table below present a summary of the logical security mechanisms of an ICAO 9303 electronic passport. This includes the protection of the various Data Groups containing a.o. the MRZ, facial image, fingerprints, eyes.

The table is followed by sections which describe these security mechanisms in more detail. However, in case of ambiguity, the texts in the official ICAO 9303 documents prevail.

Table 103 Summary of logical security mechanisms

Logical security mechanisms	What is protected	How is it protected	External cryptographic dependencies	Obvious features not protected by this mechanism
BAC (Basic Access Control)	Confidentiality and integrity of message exchange between e-MRTD and IS	<i>Symmetric keys derived from public domain information</i> At personalisation time , symmetric key derivation algorithm is included in both IS and e-MRTD. Key derivation data is encoded in e-MRTD's DG1 and Visual MRZ. At verification time , IS derives 2 symmetric keys (encryption and message authentication code-	None The masterkey from where the encryption and mac-ing keys are derived, are printed on the passport, it can be freely copied on a photo-copier	DG integrity on the chip Chip cloning DG 3 and 4 access

Logical security mechanisms	What is protected	How is it protected	External cryptographic dependencies	Obvious features not protected by this mechanism
.....		<p>generation) from the visible MRZ, e-MRTD derives the same key from DG1.</p> <p>The derived keys are used during exchange of messages between e-MRTD and IS</p>		
PA (Passive Authentication)	Integrity of the DG contents	<p><i>Document Signer has public/private key pair. DS' pubkey is certified by CSCA, and certificate is made available. DS signature over DG hashes is verified.</i></p> <p>At personalisation time:</p> <ul style="list-style-type: none"> • A Document Signer (DS) is a subscriber to the MS CSCA PKI, and • The Document Signer signs the hashes of the DGs and stores them in the SOD. <p>Subsequently, the CSCA makes the certificate chain available to relying parties.</p> <p>At verification time, the IS uses the public key of the Document Signer (DS) from the CSCA certificate chain for verification of the signature over the DG hashes.</p>	<p>Country Signing Certification Authority (CSCA) of the MS that issued the e-MRTD.</p> <p>CRL</p> <p>DS certificates can be taken from SOD.</p> <p>CSCA certificates have to be provided by a trusted external source.</p>	Chip cloning DG 3 and 4 access
AA (Active Authentication)	e-MRTD integrity. Distinguish between original and cloned e-MRTDs	<p><i>Document Signer and e-MRTD both have public/private key pairs. Both keys are certified by CSCA, and certificates are made available.</i></p> <p><i>DS signature over DG hashes is verified.</i></p> <p><i>Challenge/Response based on chip's private key/IS.</i></p> <p>At personalisation time, e-MRTD generates own key pair, certificate generated by CSCA and stored in DG 15. Integrity of DG contents is guaranteed by PA.</p> <p>At verification time,</p>	<p>Same as PA. No further external information required (since AA pub key resides in DG 15)</p>	<p>DG integrity on the chip DG 3 and 4 access</p>

Logical security mechanisms	What is protected	How is it protected	External cryptographic dependencies	Obvious features not protected by this mechanism
		verification of visual MRZ against DG1 (Challenge/Response based on chip's private key/IS).		
EAC-CA (Extended Access Control- Chip Authentication)	Confidentiality and integrity of the contactless communication between e-MRTD and IS (objective is to improve the BAC protection) Chip authenticity is also obtained	<p><i>Document Signer and e-MRTD both have public/private key pairs. Both pubkey are certified by CSCA, and certificates are made available.</i></p> <p>At personalisation time of e-MRTD, key generation and certification of public key of e-MRTD</p> <p>CA public key stored in DG 14, authenticity guaranteed by PA.</p> <p>Prior to or at activation time of IS, key generation and certification of public key of the IS by CSCA.</p> <p>At verification time, asymmetric-based authenticity and key exchange mechanism using key pairs of e-MRTD and the IS, followed by use of symmetric keys (stronger than BAC keys)</p>	Same as PA No further external information required (since CA pub key resides in DG 14)	DG integrity on the chip DG 3 and 4 access
EAC-TA (Extended Access Control- Terminal Authentication)	Access control on DG3 Fingerprints DG4 Iris	<p>Prior to or at activation time of IS, key generation and certification of public key of the IS by CVCA</p> <p>At terminal (IS) activation time, terminal loads CVCA-issued Terminal certificates, which contain access rights on DG3 and/or DG4</p> <p>Challenge/Response driven by e-MRTD to decide on access to DG3 and/or DG4 by terminal.</p>	Country Verifying Certification Authority (CVCA) of the MS that issued the e-MRTD. CRL	DG integrity on the chip Chip cloning

Logical security mechanisms of e-passports

E-passports come with a number of security mechanisms. These are classified into:

- Document security mechanisms (printing, ink, holographs, etc.), which are not addressed here; and
- Logical security mechanisms, to protect the confidentiality, integrity and authenticity of the e-passport chip and the data it contains.

The logical security mechanisms are now summarised in the following sections. They are all based on the ICAO 9303 definition of the e-passport (ICAO 9303 Part 1, volumes 1 and 2, the supplements and the additional Technical Reports) and from the Frontex's "**Operational and Technical Security of Electronic Passports**".

Data is stored on the chip in the Logical Data Structure (LDS), containing a number of Data Groups (DGs). The data visually stored in the MRZ is also present in the chip, in DG1. Further DGs contain e.g. the Encoded Face (DG2), Encoded Finger(s) (DG3), Encoded Eye (s) etc. As per ICAO, DGs 1-15 inclusive shall be write protected, and further protection stems from hashes and digital signature over the hashes.

The DG 15 contains the optional public key info of the individual e-MRTD, required for Active Authentication (AA).

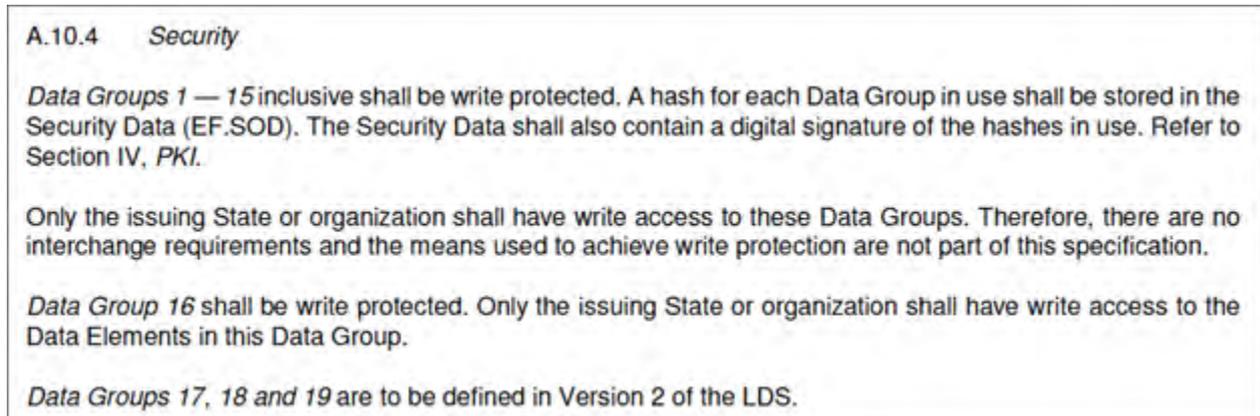


Figure 71 Quotes from ICAO 9303

The following logical security mechanisms can be implemented:

- Basic Access Control (BAC);
- Passive Authentication (PA);
- Active Authentication (AA);
- Extended Access Control (EAC) – Chip Authentication and Terminal Authentication.

Furthermore:

- DG 1 MRZ data during communication is protected by BAC, which secure the wireless communication channel;
- DG 2 FI is assumed not be privacy-sensitive, the holder's face is also printed in the MRTD and can be readily perceived (ICAO 9303 Part 1 Volume 2 2006);
- DG 3 FP and DG 4 Iris can be protected by EAC TA.

- 2.3 The digitally stored image of the face is assumed not to be privacy-sensitive information. The face of the MRTD holder is also printed in the MRTD and can be readily perceived.
- 2.4 The digitally stored image of the finger(s) and/or iris are additional biometric features which States MAY choose to apply for national use. They are generally considered to be privacy-sensitive and therefore need to be protected under the issuing State's national legislative framework.

Figure 72 Quotes from ICAO 9303

Basic Access Control (BAC)

- **What: protection of messages exchanged between e-MRTD and IS;**
- **How: symmetric key derived from MRZ, used to encrypt messages, external information: no further external information required.**

In the case of BAC, the Inspection System optically reads the MRZ (document number, date of birth of the holder, and the expiration date of the document), to derive the symmetric cryptographic keys which give access to data in the chip (access control) and ensure the confidentiality (encryption) of messages in the contactless communication between IS and the Machine Readable Travel Document (MRTD)²¹⁹.

Passive Authentication (PA)

- **What: guarantee the integrity of the DG contents;**
- **How: key pair of the Document Signer (DS) with CSCA certificate, verification of the SOd signature, verification of the certificate chain up to the CSCA certificate and verification of the DG hashes.**

In the case of PA, a Document Signer, which is a subscriber of a Country Signing Certification Authority (CSCA) of the Issuing Authority (IA) PKI, signs the hashes of the DGs and stores them in the SOd. The certificate to verify the signature can be obtained from the ICAO PKD or can be provided by the CDS in the SOd on the e-MRTD.

To guarantee the integrity of the DGs, the issuing authority calculated a hash-value over each DG separately and has placed these hashes in the document Security Object (SOd), digitally signed by the Document Signer, DS (the Issuing Authority). The authenticity of the CDS is guaranteed by the Country Signing Certification Authority (CSCA) of the Issuing Authority (IA). Therefore, in order to check the CDS, the IS needs the (root) certificate of the corresponding CSCA.²²⁰

Active Authentication (AA)

- **What: distinguish between original and cloned MRTDs;**
- **How: key pair of the e-MRTD, verification of MRZ against DG1 (Challenge/Response based on chip's private key/IS), e-MRTD certificate (stored in DG 15) guaranteed by PA.**

²¹⁹ Source: Frontex, Operational and Technical Security of Electronic Passports, 2011

²²⁰ Source: Frontex, Operational and Technical Security of Electronic Passports, 2011

AA enables the IS to distinguish between original and cloned MRTDs, by verifying that the electronic data belongs to the physical document and to the physical chip. This mechanism is optional and thus not present in all e-passports.

To verify that the data belongs to the physical document, ICAO requires that the *Machine Readable Zone* (MRZ) is compared to the MRZ-data from Data Group (DG) 1.

To verify that the data belongs to the physical chip, a challenge-response protocol is performed between the chip and the IS. Use is made of the document public key stored in DG 15 and the corresponding private key in the secure part of the chip. The public key is available to the IS, but the private key cannot be read. Only the original MRTD has knowledge of this private key. The inspection system sends a challenge to the MRTD. The MRTD signs this challenge with the private key and sends the response to the IS for inspection. The IS verifies the response by checking the signature with the public key from DG 15. Because of the uniqueness of the key pair, the IS can determine from the signature that the MRTD has the correct private key and is therefore original.

All information needed to perform the (optional) Active Authentication (AA) mechanism is present in the document. An IS does not require external additional information for AA. The authenticity of the AA public key stored in DG 15 is guaranteed by the PA mechanism²²¹.

Extended Access Control (EAC)

For EAC, a chip-individual EAC key set is defined by the implementing State. The key set may consist of either a symmetric key, e.g. derived from the MRZ and a National Master key, or an asymmetric key pair with a corresponding card verifiable certificate. Extended Access Control requires on-chip processing capability.

An EAC-mechanism is described by BSI. This EAC mechanism is required by the European Union as an additional security measure for the protection of fingerprint and iris stored in the passport. EAC ensures that only IS authorised by the issuing authority of a passport **can read that passport's fingerprint-** or iris information.

EAC adds functionality to establish the authenticity of both MRTD and IS. This enables the possibility to only provide access to authorised inspection systems. Besides, EAC provides stronger cryptographic mechanisms for securing the chip-reader communication than BAC²²².

EAC consists of two parts: Chip Authentication and Terminal Authentication.

Part 1 Chip Authentication

- **What: protect the contactless communication between MRTD and IS better than BAC does, chip authenticity also obtained;**
- **How: asymmetric-based authenticity and key exchange mechanism using key pairs of e-MRTD and the IS (CA public key stored in DG 14, authenticity guaranteed by PA), followed by use of symmetric keys (stronger than BAC keys) – no external information required.**

The Chip Authentication mechanism is performed to protect the contactless communication between MRTD and IS in a better way than BAC does. This is realised by exchanging stronger symmetric keys. The key exchange mechanism is based on asymmetric cryptography, involving private-public key pairs of both the MRTD and the IS. Since Chip Authentication uses the private key of the MRTD, stored in secure memory, it also implicitly establishes the authenticity of the chip.

This mechanism can therefore replace AA. The corresponding CA public key is stored in DG 14 and its authenticity is guaranteed by the earlier performed PA. Chip Authentication does not sign a challenge from the inspection system but is used to establish a secure channel between chip and inspection system. It therefore

²²¹ Source: Frontex, Operational and Technical Security of Electronic Passports, 2011

²²² Source: Frontex, Operational and Technical Security of Electronic Passports, 2011

does not leave a signature in the inspection system, i.e. a proof that the passport has been used at the inspection system, which enhances the privacy of the passport holder.

All information necessary to perform Chip Authentication is present in the document. An IS does not depend on external additional information²²³.

Part 2 Terminal Authentication

- **What: ensures only authorised terminals have access to the fingerprint (DG 3) / iris (DG 4) data in the MRTDs;**
- **How: access rights are indicated in Document Verifying certificates, before the MRTD provides access to these DGs, the IS must perform a proof of possession of the private key matching the presented certificate.**

The Terminal Authentication (TA) mechanism ensures only authorised terminals can have access to the biometric data in the MRTDs. A PKI for TA, also called Verifying PKI, is used for this. Performing TA consists of two steps:

- The MRTD checks the validity of a certificate chain offered by the IS;
- The MRTD checks whether the IS actually possesses the private key associated with the public key in the IS certificate it received in the first step²²⁴.

Member State Certification Authorities

Three different PKIs can be involved:

- Country Signing PKI for Passive Authentication – CSCA;
- Country Verifying PKI for Terminal Authentication – CVCA;
- PKI for communication security.

²²³ Source: Frontex, Operational and Technical Security of Electronic Passports, 2011

²²⁴ Source: Frontex, Operational and Technical Security of Electronic Passports, 2011

Method	Issuer	Insp. System	Benefits	Deficiencies
Passive Authentication (5.6.1)	M	M	Proves that the contents of the SO _D and the LDS are authentic and not changed.	Does not prevent an exact copy or chip substitution. Does not prevent unauthorized access. Does not prevent skimming.
ADVANCED SECURITY METHODS				
Comparison of conventional MRZ(OCR-B) and chip-based MRZ(LDS)	N/A	O	Proves that chip content and physical MRTD belong together	Adds (minor) complexity. Does not prevent an exact copy of chip and conventional document.
Active Authentication (5.6.2)	O	O	Prevents copying the SO _D and proves that it has been read from the authentic chip. Proves that the chip has not been substituted.	Adds complexity. Requires processor-chips.
Basic Access Control (5.7)	O	O	Prevents skimming and misuse. Prevents eavesdropping on the communications between MRTD and inspection system (when used to set up encrypted session channel).	Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Adds complexity. Requires processor-chips.
Extended Access Control (5.8.1)	O	O	Prevents unauthorized access to additional biometrics. Prevents skimming of additional biometrics.	Requires additional key management. Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Adds complexity. Requires processor-chips.
Data Encryption (5.8.2)	O	O	Secures additional biometrics. Does not require processor-chips.	Requires complex decryption key management. Does not prevent an exact copy or chip substitution. Adds complexity.

Figure 73: Original table of security mechanisms as per ICAO 9303 Part 1 Vol 2

As a summary of the previous review, here are the key principles for the protection of biometric information in an e-Passport.

Key principles:

- PA is mandatory for ICAO and guarantees the integrity and authenticity of the data stored in the chip. It requires validating the certificate chain of Document Signer and Country Signing CA;
- If PA fails, the check needs to rely much more on document security (particularly optical, e.g. OV – optically variable – safeguards);
- AA is discretionary, requires no further external certificates since DG15 provides the required public key. It does not protect against chip-cloning however. It is therefore recommended to follow Frontex best practices: if the passport supports AA, check it;
- The current PKD set-up is operational but not used by all countries (today approximately 20 countries publish), hence the most effective way to obtain certificates is a combination of PKD plus bilateral exchange;
- Certificate revocation is not actively used for certificates registered in the PKD, which puts responsibility on information exchanges to learn about certificate statuses. This is not likely to change over the next 3 – 5 years.

Security analysis

With regard to biometrics, the criteria used are Security (S), Duration of the border crossing (D), and **Implementation complexity (C)**. **'Security' is now addressed.**

Security has at least two major relevant domains in the EES/RTP context: added value of the biometric functionality, including biometric reliability, to support the border crossing processes, and system security (e.g. defence against hackers, malware, business continuity, etc.). There is limited security to the first domain. Security here is expressed in the form of individual performance rates and performance curves that combine such rates.

Security

Individual security performance rates

These are summarised in the table below:

Table 104 Summary of the various security performance rates

Performance metric	Definition	Remarks
Enrolment and Acquisition		
FTE – Failure to Enrol	Proportion of user enrolment transactions that cannot be completed according to the enrolment policy as per ISO ²²⁵	
FTA – Failure to Acquire	Probability of user attempts during verification or identification for which the system cannot acquire an appropriate sample as per ISO ²	An FTA may have the same root cause as an FTE, but they are differentiated by the process during which the error occurs
Verification		
FNMR – False Non-match Rate	Proportion of samples from genuine attempts that cannot be matched against enrolled templates of genuine users	Attempt-based
FMR – False Match Rate	Proportion of samples from imposter attempts that are successfully matched against enrolled templates of genuine users	Attempt-based
FRR – False Reject Rate	Proportion of verification transactions from genuine users that are incorrectly rejected.	Transaction-based (taking into account the number of failed attempts – there might be multiple false non-match errors resulting in one false rejection error) For single-attempt transactions, the FRR includes the FTA
FAR – False Accept Rate	Proportion of verification transactions from imposters that are incorrectly accepted.	Transaction-based
Identification		
FPIR – False Positive Identification Rate	Proportion of identification transactions performed by non-enrolled users that return a candidate list of which they are a member	FPIR is an open-set metric ²²⁶ , i.e. the input sample can potentially belong to a non-enrolled user
FNIR – False Negative Identification Rate	Proportion of identification transactions performed by enrolled users that return a candidate list of which they are not a member	FNIR is an open-set metric, i.e. the input sample can potentially belong to a non-enrolled user

Furthermore, to take all system errors into account:

²²⁵ ISO/IEC 19795-1 Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework

²²⁶ Open-set metrics equally exist but are used in performance curves rather than in individual metrics

Appendixes

- Total Error Rate (TER) is defined as $TER = FAR + FRR$;
- True Acceptance Rate (TAR) describes the probability that the system correctly matches a genuine user to the corresponding template stored within the system. **It** represents the degree to which the system is able to correctly match biometric information from the same person.

For a more exhaustive description of biometric metrics, refer to [BMR2012]

Security performance curves

A biometric system is designed to maximise the detection of imposters (for security we don't want imposters to be falsely accepted) and of genuine transactions (for convenience we don't want too many genuine users to be rejected). Evaluating the performance of such a system is done on the basis of statistical hypothesis testing. Assumptions or claims are tested by generating both a null hypothesis (e.g. different samples belong to the same individual) and an alternative hypothesis (where samples then belong to different individuals).

If two samples from the same person are then compared and determined to be from different persons, the null hypothesis is rejected, and an error is committed. Such error is called a Type I error. Alternatively, if the two samples belong to different persons but are determined to be from the same person, a Type II error is committed. A false rejection or false non-match are analogous to the Type I error. A false acceptance or false match error is analogous to the Type II error.

The genuine and imposter comparisons produce match scores that can be represented by score distributions. The ultimate goal of a biometric system is to have genuine and imposter distributions that do not overlap (because the area of overlap indicates the total proportion of system errors). The technical thresholds in the system define the proportion of errors categorised into false acceptances/rejections. Moving this threshold governs the trade-off between security and convenience. This is illustrated using curves, as summarised in the table below.

Table 105 Overview of the different security performance curves

Verification

DET – Detection Error Trade-off – FMR versus FNMR	Represents false match on the x-axis and the false non-match rate on the y-axis as a function of the threshold. For each possible threshold value, the two error rates are calculated and plotted.	The Equal Error Rate (EER) is the point where FMR and FNMR are equal. A lower EER indicates a better overall matching performance
---	--	---

DET – Detection Error Trade-off – FAR versus FRR	Represents false acceptance on the x-axis and the false rejection rate on the y-axis as a function of the threshold. For each possible threshold value, the two error rates are calculated and plotted.	The Equal Error Rate (EER) is the point where FAR and FRR are equal. A lower EER indicates a better overall matching performance.
--	---	---

Identification

CMC – Cumulative Match Characteristics	The x-axis of a CMC curve represents all possible rank values (the rank of a user is the smallest-sized candidate list of which a user is a member) and the y-axis represents the probability of correct identification at each possible rank value.
--	--

As a hypothetical system is discussed, security is provided on the basis of information available in the public domain as well as provided by vendors (as per the AFIS workshop of 30 April 2014 and the resulting White Papers).

Fingerprint security

Overview

Fingerprints are the oldest biometric technology, and are as a consequence considered the most mature technology. A normal person has 10 fingerprints which are all different. Even the prints from twins differ sufficiently to distinguish them.

Different numbers may be used for enrolment versus checking for verification/identification. For enrolment, it is preferable to perform a live capture of 10 fingerprints. For verification/identification, it is possible to use as little as one fingerprint, however, increasing the number of fingerprints increases security performance and matching speed. In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image.

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image must be captured one finger at a time. Rolled images require the operator to guide the rolling of each finger. The operational difficulty in capturing rolled image rules out its use in certain cases.

Plain images of 10 fingers are generally taken via 3 different slaps, 4 fingers right, 4 fingers left and 2 thumbs. This delivers the adequate levels of accuracy for border crossing processes and law enforcement. However it takes considerable time to acquire good quality prints, often needing re-scans of all or some fingers.

Taking such plain images of 10 fingers requires operational conditions as commonly found in airports, where slap readers can be installed on counters and supervised during operation. Device characteristics cover scan resolution, pixel depth and dynamic range. Handheld capturing devices are typically limited to capturing a single finger, and they achieve lower image quality.

Relationship to electronic passports

The relationship between fingerprints and electronic passports is characterized by the following observations:

- Electronic passports contain maximum 2 fingerprints;
- Fingerprints require the EAC certificates. Such certificates need to be obtained through the ICAO PKD or through bilateral exchange;
- Relying on the contents of the fingerprints provided by the chip requires successful use of PA.

Public domain security evaluations

The current state of the art of fingerprint technology is rooted in the FBI's interest in automating fingerprint processing in the 1960s. They prototyped fingerprint scanning in the 1970s and by 1980 established a database of 14 million records. Later in the 1980s the general deployment of AFIS systems in the US confirmed the continuing importance of the technology.

Today there are many different evaluation outcomes as well as fingerprint databases available in the public domain. As this information is available in the public domain, and copyright is typically rather permissive, we have occasionally inserted data or a table from such public sources. When we did so, we have systematically provided the original source.

Historically, NIST (National Institute of Standards and Technology in the United States of America) has been instrumental in performing global large scale evaluations, for fingerprints as well as for other biometrics. For fingerprints, the main evaluations are Fingerprint Vendor Technology Evaluation (FpVTE), Minutiae Interoperability Exchange (MINEX), Minutiae Template Interoperability Test (MTIT), Fingerprint Verification Competition (FVC, today on-going on the web), and Slap Fingerprint Segmentation Evaluations. For an overview of NIST evaluations, please refer to the appendix.

Appendixes

Furthermore, the CESG (Communications-Electronics Security Group in the United Kingdom) biometric report [CESG2001] is still often mentioned in literature as a foundation paper, since it was an early and relatively in-depth study (7 systems, 200 volunteers, reporting on FTE, FTA and DET curves).

However, recently, the UIDAI, (Unique Identification Authority of India) published their analysis and experiences with regard to enrolling the entire Indian population. Their analysis starts from the various NIST reports, but complements these with their own work. At the time of writing this EES/RTP report, they had enrolled approximately 600 million people, and aiming for 1.2 billion.

Guidance relevant for EES/RTP can be found in:

- Biometrics Design Standards for UID applications;²²⁷
- UID Enrolment Proof-of-Concept Report²²⁸.

Facial image security

Overview

Face images are historically used primarily for human visual inspection. However, automatic face recognition may be used as a secondary means of authentication/de-duplication.

For visual inspection by humans, a single face image of a person is sufficient. However, for the purposes of de-duplication and authentication of individuals who do not have fingerprints, automatic face recognition is recommended. To perform accurate authentication in such cases, the capture of multiple face images is strongly recommended during enrolment.

ICAO standards are typically applied and are widely used for the purposes capturing facial images. Such facial images are both printed on the passport page as well as stored in the chip. Those images stored in the chip are easy to obtain since there is no particular access control enforced. These images are currently in 2-D and are subject to spoofing.

For verification purposes, matching a live captured face image against the facial image provided by an e-Passport, without using any other biometric identifier, provides reasonable security. For identification, face image alone provides low accuracy rates.

Relationship to electronic passports

The relationship between facial images and electronic passports is characterized by the following observations:

- Electronic passports contain the facial image of the document owner;
- Reading this facial image can be done without access control limitations;
- Relying on the contents of the facial image provided by the chip requires successful use of PA.

Iris security

Overview

²²⁷ [BDS2009] "Biometrics Design Standards For UID Applications Version 1.0 (December 2009)", available at <http://uidai.gov.in/resource-center.html>

²²⁸ [POC2011] "UID Enrolment Proof-of-Concept Report (2011)", available at <http://uidai.gov.in/resource-center.html>

Iris imaging has been less studied and is less standardized than for example fingerprinting. For example, fingerprint scanners are tested and certified according to EFTS/F (Electronic Fingerprint Transmission Specification (Appendix F)) standards. An equivalent iris device certification is currently being discussed.

The irises of both eyes can be captured simultaneously, which is advantageous. The iris patterns of the eyes are not correlated, hence such capturing yields two independent biometric feature sets.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off the **enrollee's eyes, which makes it a less obvious candidate in some cases.**

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing the matching algorithm.

Relationship to electronic passports

The relationship between iris images and electronic passports is characterized by the following observations:

- Electronic passports may contain iris images of the document owner;
- Reading this iris information requires EAC certificates;
- Relying on the contents of the iris images provided by the chip requires successful use of PA.

Biometrics Design Standards for UID applications

The Indian UID projects aim to establish among others a biometrics-based identifier for the entire population of India. No experience is available regarding the number of entries (1.2 billion persons) or the specific Indian demographics of the data (e.g. including a significant portion of agricultural and manual workers). This report defines biometric standards, on the basis of estimating achievable accuracy from available evaluations, and then analyses what would be achievable.

With regard to estimating the achievable accuracy for fingerprints, the starting position is NISTIR 7110 (NISTIR -National Institute of Standards and Technology Interagency Report and NISTIR 7110 is the report on Matching Performance for the US-VISIT IDENT(ification) System Using Flat Fingerprints), which reports a FAR of 0,07% and a FRR of 4,4 % on a database of 6 million fingerprints of 2 plain fingers. As similar results were **reported for the FBI's IAFIS system (the Integrated Automated Fingerprint Identification System, or IAFIS, is a national fingerprint and criminal history system of the Federal Bureau of Investigation in the USA) of 46 million samples**, it may be concluded that a 99% TAR can be achieved for a database of 50 million.

Estimates regarding the scaling of these data for a larger gallery size and for 10 fingers are based on the assumptions that:

- FAR is linearly proportional to gallery size at a constant TAR;
- FRR does not vary over gallery size.

So for a system using 2 fingerprints, it can be expected that if the database size is increased by a factor of 200 (from 6 million to 1.2 billion), the same system will have a FAR of $0.07\% \times 200 = 14\%$. The FRR can be expected to remain unchanged at about 4%. Increasing the number of fingers from 2 to 10 is expected to yield an improvement of a factor of 1000 on the FAR (all other things remaining equal). This yields an estimated FAR of $14\% / 1000 = 0.14\%$, at a FRR of 4 %.

Based on an additional conversion factor of 10x change in FAR resulting in 2x change in FRR, the analysis yields a FAR of 1.4% at a FRR of 2%. This extrapolation of NIST data indicates that de-duplication accuracy (TAR) greater than 95 % is achievable for 10 finger matching against a database of 1 billion.

Based on the extrapolation of NIST reports, UIDAI arrives at the conclusion that using 10 finger matching against a database of 1 billion, it is possible to achieve a FAR of 1.4% at a FRR of 2%, and a de-duplication accuracy (TAR) greater than 95%.

Further analysis was then performed on the basis of three databases collected in India. These databases (DB1, DB2 and DB3) are of smaller size (respectively containing between 1,620 and 56,000 images). The conclusion arrived at is that UIDAI can achieve fingerprint accuracy of a quality similar to developed countries. The analysis of the processing of the images collected in the local databases concludes with 95 % confidence that

using images from DB2, lower accuracy can be expected when compared to the Western data, whereas DB3 (created with data collected using a four-finger slap sensor) is expected to achieve similar accuracy, i.e. a 99% TAR with about 1% FAR.

Based on additional research carried out by UIDAI on data captured locally from Indian citizens, it can be expected to achieve a 99% TAR with about 1% FAR, using a four-finger slap sensor.

UID Enrolment Proof-of-Concept Report

After establishing the Biometric Design Standards as described in the previous section, UIDAI conducted a Proof-of-Concept (PoC) on enrolment from March 2010 to June 2010. About 75,000 people in all were enrolled during the first phase of the PoC study, and 60,000 of them were re-enrolled during the second phase after a gap of three weeks.

In the PoC, fingerprints of all ten fingers, face photos, and iris images were captured. The ten fingerprints were captured in two different ways: first using a slap device, and then using a single finger device. Rural areas were emphasized in the study.

Enrolment

The total biometric enrolment time for each individual, on average, was a little over three minutes. Fingerprint enrolment took a little over half of this time.

Since enrolment was done for the 3 different biometrics at the same time, we have reproduced below the PoC report table for all enrolment times.

Table 106 'Enrolment times by age' from [POC2011], Annexure 2 p.29

Age	Under 20	20 to 30	30 to 40	40 to 50	50 to 60	60 to 70	70 to 80	Above 80
Face	0:00:31	0:00:31	0:00:33	0:00:35	0:00:37	0:00:38	0:00:40	0:00:45
Iris	0:00:42	0:00:42	0:00:49	0:00:54	0:00:58	0:01:07	0:01:15	0:01:24
Fingerprint	0:01:45	0:01:52	0:01:43	0:01:45	0:01:53	0:01:56	0:02:08	0:02:14

Identification matching

UIDAI reported that matching analysis was done on two sets of 20,000 biometrics, for a total of 40,000. However, the number of comparisons was several orders of magnitude more than 40,000, since each set of fingerprints would be matched against every other set of fingerprints in the data set. Similarly, the iris images from each person would be matched against that of every other person in the data set.

UIDAI compiled the data on the accuracy obtained by enrolling with only fingerprints, enrolling with only iris images, and by enrolling with both biometrics. The results can be found in Annexure 3 (p.30) of the UID Enrolment Proof-of-Concept Report (2011).

To compare the accuracies in these three cases, UIDAI focuses on the point where the FPIR (i.e. the possibility that a person is mistaken to be a different person) is 0.0025%.

Comparing the FNIR (False Negative Identification Rate) numbers achieved:

- by using ten fingers only is 0.25%;
- by using two irises only is 0.5%;
- by using ten fingers and two irises is 0.01%.

The conclusion we can draw is that the accuracy achievable using ten fingerprints is twice that of the accuracy achieved using iris images. Even more important, the accuracy achieved by using ten fingerprints and two irises is fifty times better than by using irises alone and twenty five times better than by using fingerprints alone. The accuracy level achieved was 99.99% in this case.

Role of biometrics in existing systems

Biometrics have always played an important role in binding a document owner to a document such as a passport. On that basis, 1:1 (verification) and 1:n (identification) checks can be done. Before there were machine-readable documents, a picture was already attached to a document for this 1:1 purpose.

Today, biometrics have been selected by ICAO as the primary mechanism to bind a document owner to a document such as a passport. For that purpose, within the Logical Data Structure (LDS) of an electronic passport, there are 3 Data Groups to store representations of face, fingerprints and eyes.

At personalisation time, some countries store biometrics both in a database (centralised or decentralised) and in the passport chip, while other countries only store it in the chip.

European systems making use of biometrics include:

- The Visa Information System (VIS), which allows Schengen countries to exchange visa data, in particular data on decisions relating to short-stay visa applications. Fingerprints of the applicant are taken and stored/processed in a biometric component of the VIS, the Biometric Matching System (BMS). All visas issued by a Schengen member state are registered in the VIS, with the application. Refused applications are also stored. 28 countries share this information. The data is owned by the country registering it. The visa information is sent from national systems via a specific interface (described by an ICD- Interface Control Document) and stored in the central VIS. There are no national copies and the Member States must submit queries to the central VIS. Furthermore:
 - As of October 2014, fingerprint matching must be carried out during border checks;
 - VIS registration is being rolled out worldwide and should to be finished before the summer of 2015 (pending a Council decision on planning).
- The EuroDAC system mandates fingerprint identification for asylum seekers and immigrants;
 - SIS II was established as a compensatory measure in relation to the abolishment of borders (Schengen) but also as an efficient tool for police cooperation. 30 countries share SIS II information. It allows Schengen countries to exchange data on suspected criminals, on people who may not have the right to enter into or stay in the EU, on missing persons and on stolen, misappropriated or lost property. The data is owned by the country registering it. The alerts are sent from national systems via a specific interface (also defined by a common SIS II ICD for Interface Control Document), stored in the central SIS II database, and distributed to those MS that have national copies of SIS II. **Common validation rules and codification of field values (e.g. a certain colour of a car is named "48")** ensures high quality and makes it possible for all countries to use the system. The legal basis stipulates not only what can be entered, but also what action to take when a hit is made. At the time of preparing this report, SIS II contained approximately 50 million alerts, including over 1 million alerts regarding persons and the rest regarding objects (documents, vehicles, weapons, etc.). SIS II records can contain facial images and/or fingerprints, however these are not used for identification purposes. If a person is registered in SIS II, fingerprints can be captured at the border and checked using the VIS or national databases. It is envisaged that the biometric capabilities of SIS II could be enhanced in the future; however, this would be separate from EES/RTP and does not fall within the scope of this study;
- Most Member States have one or more AFIS systems for Law Enforcement purposes. There is work on-going on the EU CCAFIS (Central Criminal AFIS, including fingerprints and DNA, as well as e.g. vehicle identification information), as authorised by the Prüm Treaty.

Furthermore it can be observed that today, the US has an ESTA (Electronic System for Travel Authorisation) in place. This is an automated system that determines the eligibility of visitors to travel to the U.S. under the Visa Waiver Program. The ESTA system registers and retains personal data of the visitor, much like a visa application does. There is no similar system in the EU²²⁹.

NIST biometric evaluations

Source: http://www.nist.gov/itl/iad/ig/biometric_evaluations.cfm

Fingerprint

[Fingerprint Vendor Technology 2012 \(FpVTE 2012\)](#)

[Evaluation of Latent Fingerprint Technologies - Extended Feature Sets \(ELFT-EFS 2009\)](#)

[Evaluation of Latent Fingerprint Technology 2007 \(ELFT07\)](#)

[MINEXII Match-on-Card Technology \(MINEX - 2007\)](#)

[Slap Fingerprint Segmentation Evaluations Overview](#)

[Proprietary Fingerprint Template Evaluations Overview](#)

[Fingerprint Vendor Technology \(FpVTE 2003\)](#)

[Ongoing MINEX Minutiae Interoperability Exchange Test \(OMINEX - 2005\)](#)

[Minutiae Interoperability Exchange Test \(MINEX04\)](#)

[Fast Tenprint Capture Devices Evaluation](#)

Face

[Face and Ocular Challenge Series \(FOCS\)](#)

[Face Recognition Grand Challenge \(FRGC - 2005\)](#)

[Face Recognition Vendor Test \(FRVT - 2000, 2002, 2006 & 2012\)](#)

Iris

[Iris Exchange Evaluation \(I, II IOCE, III, IV\)](#)

[Iris Challenge Evaluation \(ICE - 2005 & 2006\)](#)

Multiple Biometrics

[Multiple Biometric Evaluation \(MBE2009\)](#)

[Multiple Biometric Grand Challenge \(MBGC - 2007\)](#)

²²⁹ Electronic System of Travel Authorisation (ESTA) – such a system would apply to TCNs not subject to the visa requirement that would be requested to make an electronic application supplying, in advance of travelling, data identifying the traveller and specifying the passport and travel details. The data could be used for verifying that a person fulfils the entry conditions before travelling to the EU, while using a lighter and simpler procedure compared to a visa.

Further references

[BDS2009] "Biometrics Design Standards For UID Applications Version 1.0 (December 2009)", available at <http://uidai.gov.in/resource-center.html>

[BMR2012] "Biometrics Metrics Report v3.0" Prepared for: U.S. Military Academy (USMA) – West Point, available at <http://www.usma.edu/ietd/docs/BiometricsMetricsReport.pdf>

[CESG2001] "Biometric Product Testing Final Report", Issue 1.0, 19 March 2001, by Tony Mansfield, Gavin Kelly, David Chandler and Jan Kane. Available at the CESG website.

[ICSIP2006] "Fusion of Iris and Fingerprint Biometric for Recognition", proceedings of International Conference on Signal and Image Processing, ICSIP, 2006, Karnataka, India.

[NISTFUSION] NISTIR 7346 TR, "Studies of Biometric Fusion", 2007, available at the NIST website.

[NISTIRIS] IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST Interagency Report 7629

[POC2011] "UID Enrolment Proof-of-Concept Report (2011)", available at <http://uidai.gov.in/resource-center.html>

Case Law

Court of Justice of the European Union Case Law

C-290/98, *Commission v Austria* [2000] ECR I-07835

C-321/87, *Commission v. Belgium* ECR [1989] 997

C-257/01, *Commission v Council* [2005] ECR I-345

C-249/86, *Commission v Germany*

C-157/03, *Commission v Spain* [2005] ECR I-02911

C-503/03, *Commission v Spain* [2006] ECR I -1097

C-406/04, *De Cuyper* [2006] ECR I-06947

C-540/03, *European Parliament v the Council* [2006] ECR I-05769

Case C-524/06 *Heinz Huber v Bundesrepublik Deutschland* [2008] ECR I-09705

C-344/04, *IATA and ELFAA* [2006] ECR I- 00403

C-139/08, *Kqiku* [2009] ECR I-2887

C-101/01, *Lindqvist* [2003] ECR I-12971

C-482/01 and C-493/01, *Orfanopoulos and Olivieri* [2004] ECR I-8291

C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others* [2003] ECR I-4989

C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others*, Joint Affairs

C-30/77, *Regina v Boucherau* 27 October 1977, ECR [1977]

C-175/94, *The Queen v Secretary of State for the Home Department, ex parte Gallagher* [1995] ECR I-04253

C-65/95, *The Queen v Secretary of State for the Home Department, ex parte Shingara and Radiom* [1997] ECR I-03343

C-482/08, *United Kingdom v Council* [2010] ECR I-10413

C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* 8 April 2014

European Court of Human Rights Case Law

Amman v. Switzerland, Application no. 27798/95, judgment of 16 February 2000
Lupker v. the Netherlands, application no. 18395/91, judgment of 7 December 1992

Friedl v Austria, Application no. 15225/8931, judgment of 31 January 1995

Handyside v The United Kingdom, Application no. 5493/72, judgment of 7 December 1976

Kennedy v United Kingdom, Application no. 35394/97, judgment of 18 May 2010

Kruslin v France, Application no. 11801/85, judgment of 24 April 1990

Leander v Sweden, 26 March 1987, Application no. 9248/81, Series A, no.116.

Niemietz v Germany, Application no. 13710/8816, judgment of 16 September 1992

Appendixes

Peck v United Kingdom, Application no. 44647/98, judgment of 28 January 2003

P.G. and J.H. v the United Kingdom, Application no. 44787/98, judgment of 25 September 2001

Rotaru v Romania, Application no. 28341/95, judgment of 4 May 2000

Segerstedt-Wiberg and others v Sweden, Application no. 62332/00, judgment of 6 June 2006

S. and Marper v United Kingdom, Applications nos. 30562/04 and 30566/04, judgment of 4 December 2008

Exceptions

Handling exceptions at entry and exit

For all the steps of the EES processes exceptional cases could arise. These must be examined to be able to eventually adapt the solution and processes in order to mitigate, where possible, their occurrence and their impact and also to establish how they can be handled once encountered. The study is not entering into details as regards mitigations. The objective is to identify exceptions, also in view of what might be needed to further check, using the pilot.

Any need for a degraded mode, due to unavailability of components on central or national sides is here treated as an exception.

The table below presents a number of exceptions that are relevant to further study when designing processes and architecture.

EES Check

Cases	Causes	Measures
Changed document number/double citizenship		
	<p>A person having an individual file already registered in EES arrives with a new passport/a passport for his/her second citizenship.</p> <p>The situation can only arise for VE as VH can only use the passport corresponding to the visa sticker.</p>	<ul style="list-style-type: none">• An automated search using data of birth, name and gender could be made. This could be followed by an automatic biometric verification against the subset of data that the search provided (i.e. a 1:few identification);• The proposed identification using a 1:N search with fingerprints to the EES, for all VE arriving at the external border, would also be a solution to find any earlier individual file of the person;• If one of the above mitigations is not used, there would be a new individual file made for the person and subsequent entries/exits would be recorded to this or the older file, depending on the document used.
Children registered in the passport of their parent (no passport of their own)		
	<p>In some countries children under a certain age do not have their own MRTD/e-MRTD but are registered in the passport of their parent</p>	<p>Alternatives:</p> <p>(VH) All children that are visa holders must have their own visa and are registered in VIS. The visa sticker data can be used for registration in EES.</p> <p>(VE) The children's name, date of birth, country and the document number of the parents passport should be entered manually in the EES, as an individual file. The parent's individual file would be created as per the normal procedure.</p>
EES check not possible		
	<p>Central EES is not available (system or network not</p>	<ul style="list-style-type: none">• Data could be collected and stored locally. A check could be made later, if possible. See also

available/not working)	EES registration below; <ul style="list-style-type: none"> • Actions cannot be taken if the check shows that the traveller has overstayed.
National application for handling EES not available/not working	<ul style="list-style-type: none"> • Information could be kept (manually or in other data systems) locally and a check made later, if possible. See also EES registration below; • Actions cannot be taken if the check shows that the traveller has overstayed.
Biometric verification (after the person is found in EES) is not possible²³⁰	
<ul style="list-style-type: none"> • Central EES function for biometric verification not available/not working; • National application for handling EES biometrics not available/not working; • No biometric stored in EES due to transition or individual causes related to the person. • 	<ul style="list-style-type: none"> • No verification against EES using biometrics would be possible; • The only verification possible would be a manual verification, which leads to security risks.
Local equipment used for capturing biometrics not available/not working (e.g. broken, too low temperatures for mobile devices)	The verification to EES would not be made. Manual verification would have to be made. Alternatively, made by: <ul style="list-style-type: none"> • Using photo but not fingerprints; • Using fingerprints but not photo.
No photo stored at registration due to problems (see list under EES registration) or facial recognition not working.	Verification using photo impossible within EES
No fingerprints stored at registration due to problems (see list under EES registration) Fingerprint matching not working/no fingerprints stored in EES due to a possible transition period	Verification using fingerprints impossible

²³⁰ For VH the biometric verification would take place against the VIS database, however the considerations presented in this table would still apply.

EES Entry-exit

Cases	Causes	Measures
EES registration of individual file not possible		
	Central EES is not available (system or network not available/not working)	<ul style="list-style-type: none"> A registration could be made locally and queued for later registration; No central checks can be made in EES in the registration process. Manual verification has to be used.
	National application for handling EES not available/not working	<ul style="list-style-type: none"> No registration can be made in the central EES; Data could be captured manually or electronically in a back-up routine, for later registration.
EES registration of individual file with biometrics not possible/fully possible		
	Central EES function for biometric registration not available/not working	<ul style="list-style-type: none"> If possible biometrics could be captured locally and added to the registration later; If not, the registration will be without biometrics in the EES.
	National application for handling EES biometrics not available /not working	<p>The registration in EES would be without biometrics.</p> <p>Alternatively there could be a function to note this lack of biometrics in the EES and make a "first registration" at next crossing.</p>
	Local equipment used for capturing biometrics not available/not working (e.g. broken, too low temperatures for mobile devices)	<p>The registration in EES would be without biometrics.</p> <p>Alternatively:</p> <ul style="list-style-type: none"> Without photo but fingerprints are captured; Without fingerprints but with photo
	The concerned person does not have fingers, have fingerprints that cannot be captured or do not as many fingers as requested for registration	<p>The registration in EES would be without fingerprints or would have less than the required number of fingerprints.</p> <p>A mark that FP capturing is "not applicable" could be included, in a similar way as for VIS.</p>
	Local equipment and infrastructure used can only capture less than required number of fingerprints for the EES registration	<p>The registration in EES would have less than the required number of fingerprints.</p> <p>Note: This is an implementation choice, related (possibly) to costs, situation at the border crossing and other conditions. It could be that the legal regulations would not allow for this to happen.</p>
	Environment and circumstances makes it impossible to register biometrics or to register the amount of fingerprints	<p>The registration in EES would be without biometrics (photo and/or fingerprints) or would have less than the required number of fingerprints.</p> <p>Note: This is a temporary situation that could</p>

needed.

arise, not linked to availability central or national systems.

The person arriving for entry is recorded for an entry in the EES but has no earlier exit registration.

A number of situations can cause this, for example:

- Human error;
- System malfunction

Exit made without passing a BCP (e.g. in a leisure boat).

Manual procedures are needed to handle the exception. Since the person exited in the meantime, an exit should be recorded by default. This procedure could e.g. provide a conventional date on the presumed exit date to be entered.

The person arriving at entry is subject to a bilateral agreement between countries that affects the allowed maximally allowed stay

Alternatives:

- The registration is made as for any TCN;
- The registration is made in a specific way to distinguish it from other registrations.

This category of persons could be seen as overstayers by the EES system and should have been informed of the overstay when leaving the country. Therefore specific extension could have already been decided, at some point, but still within the persons' legal right as regards the stay.

EES recording not possible

Central EES is not available (system or network not available/not working)

- A recording of entry/exit could be made locally and queued for later registration.

National application for handling EES not available/not working

- Data could be captured manually or electronically in a back-up routine, for later recording of entry/exit.

At exit, massive influx of TCN freed from their obligation because of queues.

Preventive measures:
TCN's arriving in such countries should be informed of the risks and possibilities.

- QR code stickers could be distributed to be pasted in the passport for further regularisation. 1 QR code ⇔ 1 regular;
- Air and sea borders: use passenger's manifest of outgoing flights/ship departures to match entries.

EES shows that the person is an overstayer, but the person claims this is not correct, due to bilateral agreements.

Manual procedures are needed to handle this exception.

The person arriving for exit is not registered in the EES

The person arriving for exit is registered in the EES but last registration was also an exit

A number of situations can cause this, for example:

- Human error;
- System malfunction

Entry made without passing a BCP (e.g. in a leisure boat).

Manual procedures are needed to handle this exception.

Since the person entered in the meantime, an entry should be recorded by default. This procedure could e.g. provide a conventional date on the presumed entry date.

Handling exceptions – RTP enrolment

For all the steps of the RTP processes exceptional cases could arise. These must be examined to be able to eventually adapt the solution and processes in order to mitigate, where possible, their occurrence and their impact and also to establish how they can be handled once encountered. The study is not entering into details as regards mitigations. The objective is to identify exceptions, also in view of what might be needed to further check, using the pilot.

Any need for a degraded mode, due to unavailability of components on central or national sides is here treated as an exception.

The table below presents a number of exceptions that are relevant to further study when designing processes and architecture.

Cases	Causes	Measures
RTP 1:N check not possible.	Central RTP or VIS not available, biometric function not working, national system not working or national equipment for capturing biometrics not possible	<p>Alternatives:</p> <ol style="list-style-type: none">1. The fingerprints could be enrolled and the identification is performed later.2. In all cases the enrolment should be postponed until the check can be made.3. The enrolment is made without this identification. <p>The mitigation under point 1 is recommended. Postponing the enrolment could be possible in some cases and making the enrolment without the verification should be avoided since it adds a security risk.</p> <p><i>RTP enrolment is not time critical, but in this situation the person is at the premises for making the enrolment,</i></p>

which makes it more urgent to have a solution

The SIS II search cannot be made

Alternatives:

1. In all cases the enrolment should be postponed until the check can be made.
2. Data should be saved locally and the SIS II check made when it is possible. If this shows any uncertainty the RTP status could be revoked, if relevant.
3. The enrolment is made without this check. This option for mitigating the problem poses a security risk and should be avoided.

Enrolment of fingerprints cannot be made

•

The fingerprints of the person cannot be captured or the required number of fingerprints cannot be captured
System problem or problems with an equipment

Alternatives:

1. The enrolment should be postponed until fingerprints can be captured
2. As an exception a registration can be made if the photo can be taken
3. The RT status cannot be granted

Photo cannot be captured/registered

•

System problem, problems with an equipment, or any other problem

Alternatives:

1. The enrolment should be postponed until photo can be captured
2. As an exception a registration can be made if the fingerprints can be taken

RTP record cannot be created

System problem, problems with an equipment, or any other problem

In all cases the enrolment should be postponed

RTP entry-exit

Cases	Causes	Measures
RTP retrieval not possible		
	Central RTP is not available (system or network not available/not working)	<ul style="list-style-type: none"> The registered traveller would have to be treated as any TCN (VE or VH).
	National application for handling RTP not available/not working	<ul style="list-style-type: none"> The registered traveller would have to be treated as any TCN (VE or VH).
Biometric verification is not possible		
	<ul style="list-style-type: none"> Central RTP function for biometric verification not available/not working; National application for handling biometrics not available /not working. 	<ul style="list-style-type: none"> No verification using biometrics. Manual verification has to be made. RTP's cannot use the ABC gates and are handled manually as TCN's.
	Local equipment used for capturing biometrics not available/not working (e.g. broken, too low temperatures for mobile devices)	<p>The verification to EES would not be made. Manual verification would have to be made. Alternatively, made by:</p> <ul style="list-style-type: none"> Using photo but not fingerprints; Using fingerprints but not photo.
	No photo stored at registration due to problems (see list under EES registration) Facial recognition not working/no photo stored in EES due to transition period	Verification using photo impossible
	No fingerprints stored at registration due to problems (see list under EES registration) Fingerprint matching not working/no fingerprints stored in EES due to transition period	Verification using fingerprints impossible
The person arriving for exit is not registered in the EES		
The person arriving for exit is registered in the EES but last registration was also an exit		
	<p>A number of situations can cause this, for example:</p> <ul style="list-style-type: none"> Human error System malfunction <p>Exit made without passing a</p>	Manual procedures are needed to handle this exception.

BCP (e.g. in a leisure boat)

Assessment tables for the technical options for the Pilot

Technical options for the use of data and biometrics

	Cost (investment)	Security	Duration of border crossing	Complexity	Leverage on existing systems	Impact on infrastructure	Legal impact	Data protection	Quality of data	Usability
Impact on BCP										
Minimum data set needed for EES (registration and check)										
MRZ only + visa sticker number for VH	N	N	N	++	+	N	-	+	+	++
MRZ with optional fields	-	+	--	--	-	N	-	-	-	-
MRZ + all fields of the legal proposal	--	+	--	--	--	N	-	-	--	--
VIS can be checked using document number from MRZ	N	N	++	+	+	N	--	N	N	+
VIS checked using visa sticker number	N	N	N	N	N	N	N	N	N	N
Use of biometrics - EES										
8 fingerprints for EES registration	--	++	--	--	-	--	N	N	+	--
4 fingerprints for EES registration	-	+	-	-	+	+	-	N	-	-
Photo from e-MRTD used for EES registration	N	+	N	+	+	N	-	-	+	+
Live photo used for EES registration	-	+	-	-	-	-	-	-	+	+
Printed photo used for EES registration	N	--	N	N	N	N	-	-	--	--
Live fingerprints used for 1:N identification	N	+	-	-						
Live fingerprints used for EES verification	N	+	-	N	++	N	N	N	+	+
Photo from e-MRTD used for EES verification	N	+	N	+	+	N	-	-	+	+
Live photo used for EES verification	-	+	-	-	-	-	-	-	+	+
Use of biometrics - RTP										
Photo (e-MRTD to live photo) used for verification (ABC)	-	+	N	+	++	-	-	-	+	+

Appendixes

Photo (e-MRTD to live photo) used for verification (manual gate)	--	+	--	-	-	-	-	-	+	+
Photo (e-MRTD to RTP database) used for verification (manual gate)	N	+	N	+	+	N	-	-	+	+
Fingerprints (live capture to RTP database) used for RTP check (ABC)	--	+	N	+	--	-	N	N	+	+
Fingerprints (live capture to RTP database) used for RTP check (Manual)	-	+	N	-	-	-	N	N	+	+
Data set needed for recording EES entry/exit										
Date, time, place, BCP, authority, etc (all automated)	-	N	+	+						
MRZ with optional fields	-	+	--	--	-	N	-	-	-	-

Overview of the relevant existing systems

Visa Information System (VIS)

The Visa Information System (VIS)²³¹ allows Schengen countries to exchange and process data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. It consists of a central IT system, national systems in all participating states and of a communication infrastructure that links this central system to national systems. VIS is accessed at Schengen consulates, at central visa authorities and at all external BCP of Schengen countries²³².

The objective of the system is to support the common visa policy and the visa application procedures, and in particular:

- To identify visa applicants (and their visa history);
- To check and/or identify visa holders at borders, with the support of biometric identifiers (fingerprints);
- To prevent "visa shopping" and other types of fraud at consulates;
- To assist in the fight against irregular migration;
- To contribute to the prevention of threats to internal security of the Member States.

For each person applying for a Schengen visa, the VIS stores and retains for a period of maximum 5 years, both biographic and biometric information, including:

- Alphanumeric data (biographic information, visa information and additional information);
- **A photograph of the applicant's face;**
- Ten flat fingerprints, which are kept valid for 59 months from the enrolment in the system, in case of subsequent applications.

VIS started operations on 11 October 2011 and from 1 November 2011 all Schengen countries implemented mandatory checks of the VIS using the visa sticker number for queries. As of October 2014, the biometric verification at the border will also become mandatory. Each application file shall be stored in the VIS for a maximum of five years. The Member State responsible shall check the data concerned and, if necessary, correct or delete them immediately. Furthermore, when an applicant has acquired a nationality from one of the Member States the application files and the links relating to him or her shall be deleted without delay from the VIS by the Member State which created the respective application file(s) and links. The registration of applications and visas in the VIS, by consular postings, is being progressively rolled-out in predefined sets of world regions in accordance with Article 48 of the VIS Regulation No 767/2008. The roll-out is proposed to be completed during 2015. The VIS central system is operated by eu-LISA.²³³

²³¹ Regulation (EC) No 767/2008 of the European Parliament and of the Council

²³² http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm

²³³ Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60, 13.8.2008; Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286/1, 1.11.2011.

Technical aspects and architecture

The VIS architecture has the following characteristics and guiding principles:

- VIS is a central system with two physical locations, one of which is used as backup system;
- The VIS architecture includes a Biometric Matching System (BMS) for the fingerprint matching. Member States do not connect directly to the BMS, but only through VIS;
- 10 fingerprints are enrolled, however only 1 to 4 are necessary for the verification;
- Access is provided only to designated authorities of the Member States for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.²³⁴

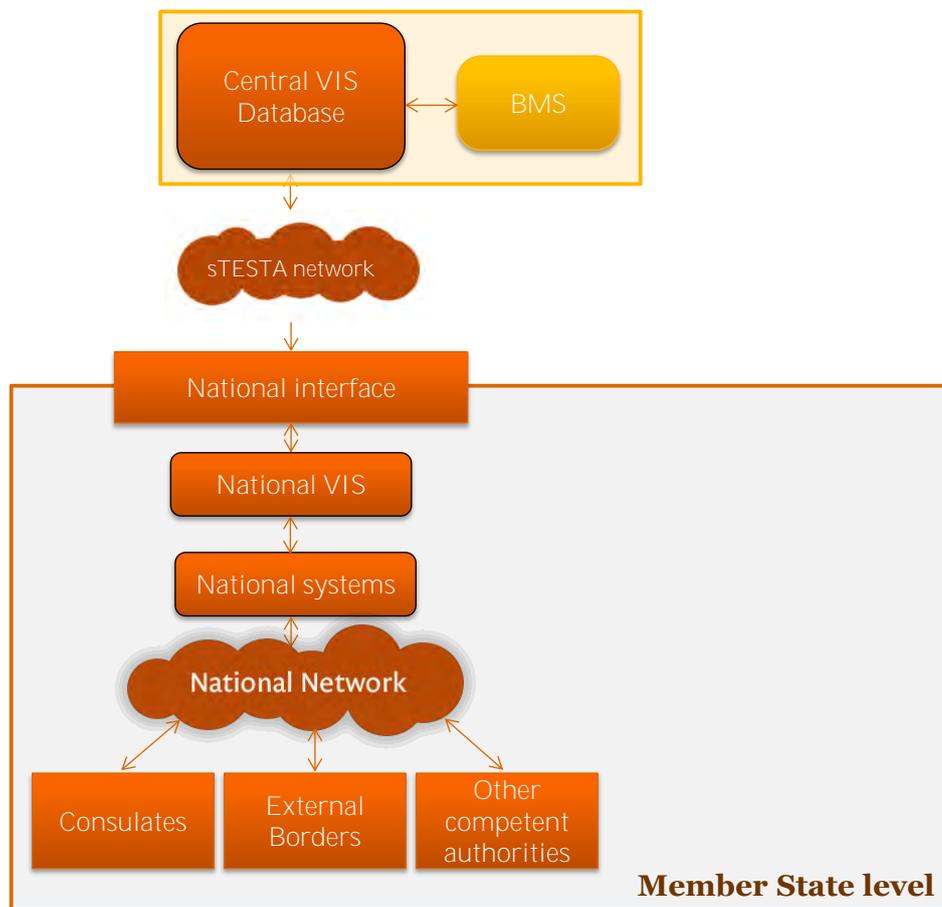


Figure 74 High-level overview of VIS

²³⁴ Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L218/129, 13.8.2008.

Schengen Information System (SIS II)

The second-generation Schengen Information System (SIS II)²³⁵ is a Europe-wide large-scale joint information system for public security that enables exchanges of information between national border control, police, customs and other competent authorities, ensuring that the free movement of people within the Schengen area can take place in a safe environment.

Competent authorities have access to alerts on persons and objects for the purposes of border checks, as well as police, customs and other checks carried out within the countries, and, to a certain extent, for the purpose of issuing visa and residence permits. At the external borders, it is mandatory to check a TCN in the SIS II before granting them access to the Schengen area.

SIS II replaced the former technical implementation of the Schengen Information System (SIS1). SIS II responds to the need of servicing an increasing number of users and handling an increasing number of queries.

SIS II provides the potential for additional functionalities, such as new categories of data and the use and storage of images and biometrics. The SIS II went live on 9 April 2013 and the central SIS II system is operated by eu-LISA.²³⁶

In each participating country, there is a dedicated office for handling supplementary information and bilateral or multilateral contacts with regard to the cases identified through the use of SIS II (e.g. providing supplementary information after a hit and managing the communication necessary for further police and legal actions). These offices are called SIRENE (Supplementary Information REquested at National Entry).

Technical aspects and architecture

The SIS II architecture is characterised by the following characteristics and guiding principles:

- SIS II is composed of a central database that is fully or partially replicated at national level for the countries that have chosen to have a national copy of the central database as part of their national architecture;
- The central system has two physical locations, one of which is used as backup system;
- SIS II allows the possibility to include fingerprints in an alert. While the storage of fingerprints as images is already being used by the participating countries, the option to use it for identification has not yet been implemented;
- The retention period of data stored varies on the basis of the type of alert and the specific situation.

²³⁵ Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28/12/2006 and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 07/08/2007.

²³⁶ REGULATION (EU) No 1077/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011.

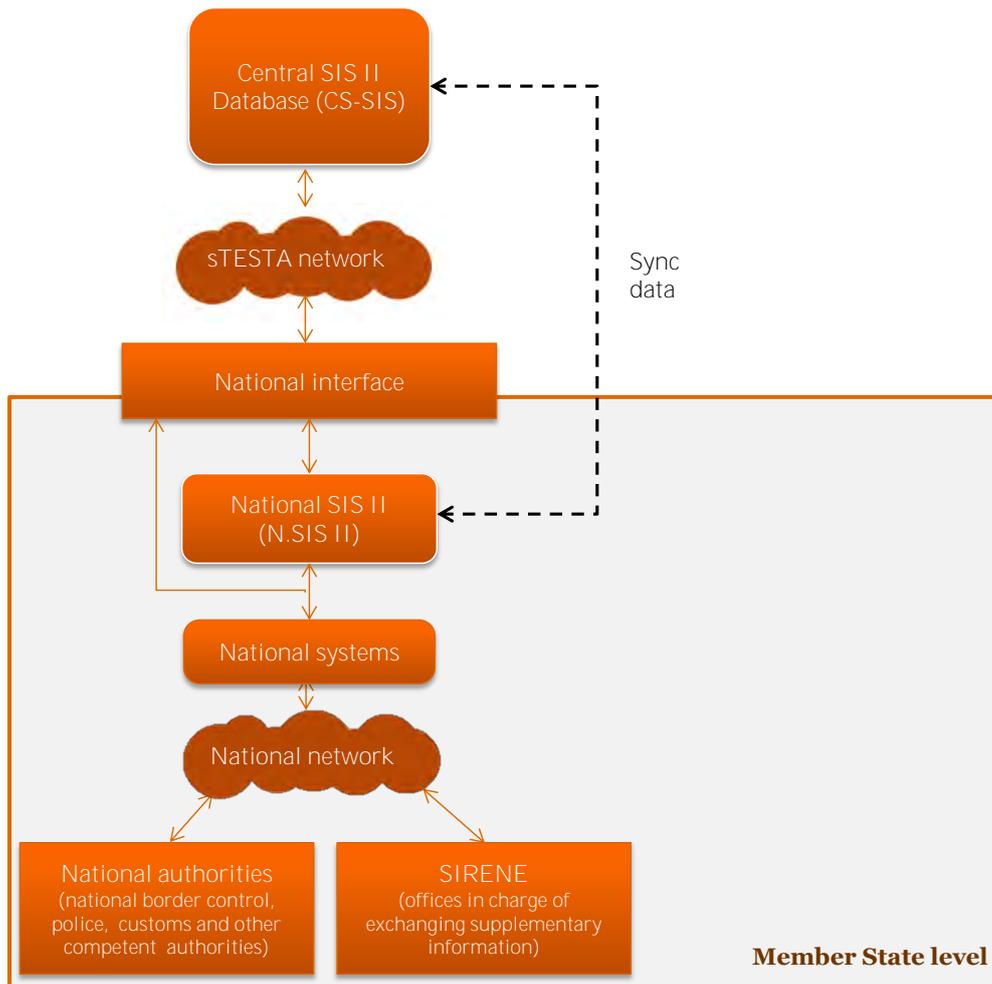


Figure 75 High-level overview of SIS II

National border control initiatives

This section provides the description of national border control initiatives and infrastructure.

Table 107 Description of national biometric border control initiatives

Biometric border control initiatives	Description
PRIVIUM programme	PRIVIUM is an automated border crossing programme for frequent fliers who want holdup-free travel at Schiphol Airport in Amsterdam, Netherlands. The passport holders of all EU countries as well as Norway, Iceland, Liechtenstein and Switzerland are eligible to apply for the membership of PRIVIUM programme, also US Global Entry members can use the PRIVIUM services. Member smartcards include the passport data, the PRIVIUM member number and two encrypted iris codes. During the pre-enrolment procedure the applicant has to fill in commercial database so that the smartcard would be prepared for the final enrolment. The final enrolment includes application processing, biometrics capturing, check of blacklist databases etc.

Biometric border control initiatives	Description
ABG pilot programme	ABG is a pilot of automated biometrics-supported border check service at Frankfurt Airport, Germany. This service is available to all citizens of the European Union (EU), European Economic Area (EEA) and Switzerland who have a valid machine-readable passport. Passengers who wish to use the ABG service must undergo an iris scan and register the resulting biometric data along with their passport data, which is used for biometric authentication during subsequent border crossings. The enrolment includes a query of the INPOL German police information system and SIS II among other procedures.
PARAFE (Automated Fast Track Crossing at External Borders)	PARAFE is an automated border control system at the Charles de Gaulle, Orly and Marseille airports, France. Any citizen of the EU and Switzerland are eligible to register to the PARAFE system, which is based on fingerprints. Prints of eight fingers are taken at enrolment. The templates, as well as data from the MRZ (Machine Readable Zone) of the passport and the biometric data are stored in a local database of the French Border Police at the Charles de Gaulle airport. At the time of automated border control the 1:1 verification is performed.

Infrastructure

The figures below show the numbers of ABC gates per country as of June 2014 and numbers of border crossings through ABC gates at entry and exit in 2013. It is expected that the number of border crossing through ABC gates for 2014 will change dramatically in Germany due to the rise in the number of ABC gates. For the period from the end of February to June 2014, there have been already 590 000 border crossings through ABC gates.

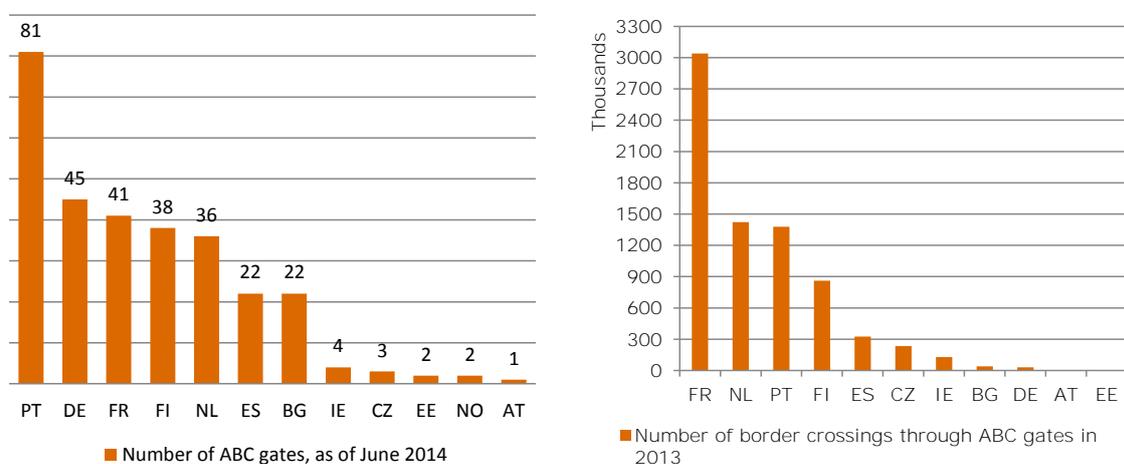


Figure 76 Number of ABC gates as of June 2014 and number of border crossings through ABC gates at exit and at entry in 2013 (in thousands); Source: Frontex

Thematic Files

DOMAIN		See chapter
BIOMETRICS		
TF1	Biometric identifiers for EES	
1.1	How many fingerprints are to be used (separated for enrolment and identification/verification)?	4.4.1
1.2	How and when to capture them (incl. preferably anti-spoofing measures)?	4.4.2
1.3	Synergies with other systems recording biometrics (Visa information System (VIS) and Registered Traveller Programme (RTP)) including for example the rationale for storage of the facial picture in EES (for visa holders, for visa exempt travellers)?	4.4.3
1.4	Impact of the use of the biometric identifier on the border control process as well as on enrolment time (incl. degraded mode).	4.4.4
1.5	Use of facial recognition (multi-modal). Is facial recognition in combination with the use of fingerprints (so-called multi-modal) a viable option for reducing the number of fingerprints to be captured?	4.4.5
1.6	Facial image/fingerprints possibly captured from the travel document (this question is linked to the exchange of Extended Access Control certificates, the implementation of which is not part of the Study).	4.4.6
TF2	Biometric identifiers for RTP	
2.1	Which biometric identifier(s) should be used for the RTP (separated for enrolment and identification/verification)?	4.5.1
2.2	Impact of the use of the biometric identifier(s) on border control processes	4.5.2
2.3	How and when to capture them (incl. preferably anti-spoofing measures)?	4.5.3
2.4	Synergies with other systems recording biometrics: Visa information System (VIS) and EES (for visa holders, for visa exemptions)?	4.5.4
2.5	Impact of the use of biometric identifiers on border control processes (ABC – automated border check - gates / manual process), including the degraded mode.	4.5.5
TF3	Biometric - Impact of a transition period on the functioning of the systems	
3.1	What are the advantages and disadvantages of not having (such) a transition period?	4.6.2
3.2	What would be the consequences for the travellers, for the border control process and (possibly) for LEA of a transition process without using the biometric identifier?	4.6.3
3.3	What are the advantages and disadvantages of a phased approach: in this approach each Member State would use biometrics once this is possible, before common implementation at a specified target date.	4.6.4
BORDER CONTROL PROCESSES		
TF4	Visa holders, visa exempt travellers, residence permits	
4.1	How will the border control process for the different categories of travellers be impacted by the introduction of the EES and RTP?	3.1 and 3.2
4.2	How different are these impacts for air, land and sea borders?	3.4.6
4.3	Is it possible or advisable to manage residence permits in RTP? TCNs who have a residence permit are not targeted by the EES.	3.4.5
4.4	What is the impact on local border traffic?	3.4.4.

TF5 Border processing time		
5.1	Impact of EES on border crossing time for the 1st visit and for the subsequent visits.	3.4.1.
5.2	Impact of the RTP on border crossing time (ABC and manual process).	3.4.1.
5.3	Impact on average border crossing time for TCNs at entry and exit.	3.4.2
5.4	Impact of the EES and RTP on traveller flows (queues), impact on EU citizen flows and border crossing time.	3.4.2
5.5	Impact on Border Crossing Points (organisation, resources).	3.4.3
TF6 EES process: 1st border crossing / subsequent crossings		
6.1	Formalisation of the EES process for the 1st entry (VH/ VE).	3.2
6.2	Formalisation of the EES process for subsequent border crossings occurring during the data retention period (VH/VE).	3.2
TF7 RTP enrolment process		
7.1	Formalisation of the RTP enrolment process (VH, VE, impact on Consular Posts / other enrolment centres.)	3.3.1-3.3.3 and MS toolbox
7.2	Formalisation of the RTP member border crossing process (VH/VE).	3.3.1-3.3.3
7.3	Identification of the consultation mechanism. This item addresses the way the RT database is consulted and also assesses the need, or not, to have the biometric data kept separate from the alphanumeric ones. In that case an identifier needs to link these two parts of the database.	3.3.4
7.4	Identification of interactions and dependencies between EES and RTP. This item deals with the way the entry-exit data will be updated for an RT and leads to an investigation on the location of data.	3.3.6
TF8 Process at exit		
8.1	Formalisation of the EES exit process (incl. degraded mode).	3.2
8.2	Formalisation of the RTP member exit process (incl. degraded mode).	3.3
8.3	Identification of the process variations at sea, land and air border.	3.4.6
8.4	Automation possibilities (use of ABC gates) for the different types of travellers.	3.5.4
TF9 Process accelerators		
9.1	Identification of measures decreasing the average time for border crossing at sea, land and air borders	3.5.1
9.2	Automation options for land borders. The way to organise the border crossing at land borders requires specific attention for cars with or without passengers and buses.	3.5.2
9.3	Minimizing the number of documents to be used when crossing a border.	3.5.3
9.4	Minimizing the various databases to be searched or verified by creating a trust chain based on a single trustable relation, possibly leading to changes in legal instruments.	6.3.2 and 6.3.3
TF10 Alternative options to the token		
10.1	Feasibility of using a Machine Readable Passport as token.	3.3.5
10.2	Identification of other options.	3.3.5
10.3	Advantages and disadvantages of the alternative options.	3.3.5
10.4	Impact on border control process (manual and automated).	3.3.5
10.5	Impact on the enrolment process.	3.3.5
LEGAL and DATA		
TF11 Privacy by Design		
11.1	Identification of the minimum Data set required (and sufficient) to fulfil the EES and RTP objectives while maximising automation.	5.2
11.2	Advantages and disadvantages of 1 or 2 systems (including safeguards and mitigating actions).	6.3.1
11.3	Identification of the biometric identifier(s) to be used considering the retention period, the size of the database and the objectives of the systems.	5.2.6
TF12 Retention period		

Appendixes

12.1	Impact of the duration of the retention period on the Border control process, Traveller and/or RTP member, System architecture and performance, Data protection, LEA	5.3
12.2	Extension of duration of the retention period in EES for the RTP members (alignment on the RTP membership duration). The retention period of RT data needs to be re-assessed in comparison to the outcome of the EES data retention period and the RTP membership duration.	5.3
TF13 Law Enforcement Access		
13.1	Analysis of statistics concerning LEA in VIS (Visa holders recorded in VIS will also appear in EES).	5.4.1
13.2	Identification of the business case for LEA. This item looks at the additional means and costs necessary for LEA.	5.4.3
13.3	Definition of the data required for LEA. LEA should not drive the definition of the data set. However, LEA can impact the retention period, the search patterns and can marginally influence the type of data kept.	5.4.2
13.4	Impact of LEA on the border control process.	5.4.4
13.5	Possible impact of LEA on the system architecture.	5.4.3
TF14 Output of EES and RTP systems		
14.1	Need to provide the traveller with information on the remaining number of days of authorised stay at entry as well as at exit (incl. impact on the infrastructure).	5.5.2
14.2	Need to provide the border guards and possibly carriers with information allowing the identification of Visa Holders with a single entry visa having already used their visa.	5.5.1 and 5.5.3
ARCHITECTURE		
TF15 EES and RTP: 1 or 2 systems		
15.1	Identification the advantages and disadvantages to develop:	
15.1.1	· 2 separate systems or	6.3.2
15.1.2	· 1 single system covering all EES and RTP functionalities.	6.3.3
15.2	Comparison of the 2 options and the various advantages/disadvantages, including data-protection issues.	6.3.4
TF16 EES, RTP and VIS (compatibility of processes / synergies)		
16.1	Comparison of EES, RTP processes and VIS processes. Compatibility analysis. Dependencies.	6.4.1
16.2	Identification of possible/potential synergies and options to implement these synergies.	6.4.1
16.3	Analysis of the possibility to fully integrate the systems.	6.4.2 and 6.4.3
16.4	Common SOA based BMS	6.4.4
TF17 Interaction with other IT systems / interoperability		
17.1	Identification of other IT systems used for the BCP.	6.5.1
17.2	Identification of possible/potential interaction between these systems and EES and RTP.	6.5.2
17.3	Identification of potential dependencies between systems.	6.5.2
17.4	Addition of consultation mechanism between authorities.	6.5.3
17.5	Identification of the appropriate balance between system integration and personal data protection	5 and 6
TF18 Existing national systems: re-use / integration		
18.1	Analysis of the possibility to reuse or integrate the existing system with EES and RTP including the opportunity of data migration.	6.6.2

18.2	Definition of the common interface between national systems and the central system in the case that a national system capturing entry and exit data already exists.	6.6.4
18.3	Potential need for adaptation of the existing infrastructures.	6.6.2
18.4	Data aggregation (central system specific data collected individually from the national systems versus central links).	6.6.3

COSTS

TF19 Cost Analysis of the Various Options

19.1	Update costs for EES and RTP (central + national).	Cost report
19.2	Cost analysis of the various options: changes in architecture, changes of data retention period, biometric identifiers (number of fingerprints, multimodal), LEA access, any other relevant option impacting significantly the costs.	Cost report

STATISTICS

TF20 Statistics on Border crossing

20.1	Update of the initial border crossing estimates for air, sea and land borders	7.1 - 7.3
20.1.1	Collection and analysis of counts of external border crossing travellers performed by Member States during an agreed period of time. This collection of statistics will be performed at the EC's request.	7.1 - 7.3
20.1.2	Analysis of statistics provided by VIS.	7.1 - 7.3
20.2	The Contractor is expected to search for statistics from reliable sources in order to substantiate quantitative information but is not expected to conduct the collection of counts at external border crossings. One of these sources of information are the statistics computed by the VIS system (example: number of visa applications, number of visas granted, refused, number of Multiple Entry Visas, ...)	7.1 - 7.3
20.3	The Contractor will receive the results of the counts of external border crossing travellers from 2009 and is expected to update its findings if more recent data becomes available.	7.1 - 7.3

Simulations border control processes

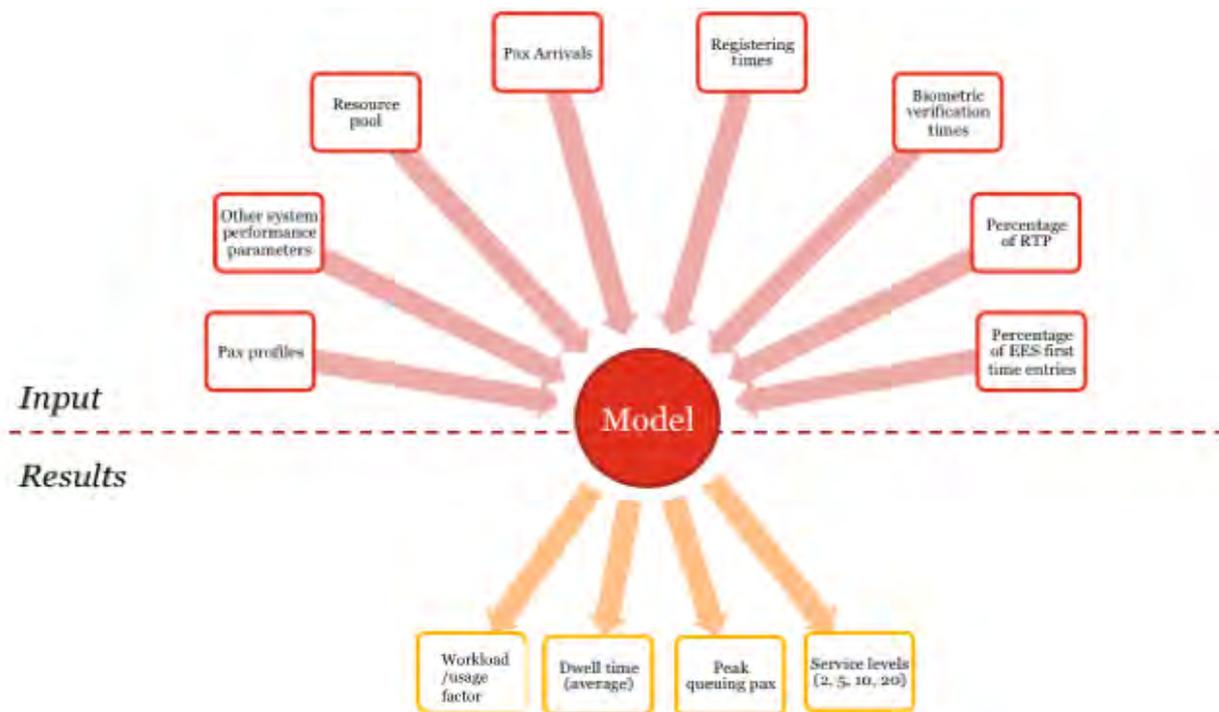
In the course of the Study, a series of simulations have been performed, in cooperation with Frontex and with support from them.

Method for simulation

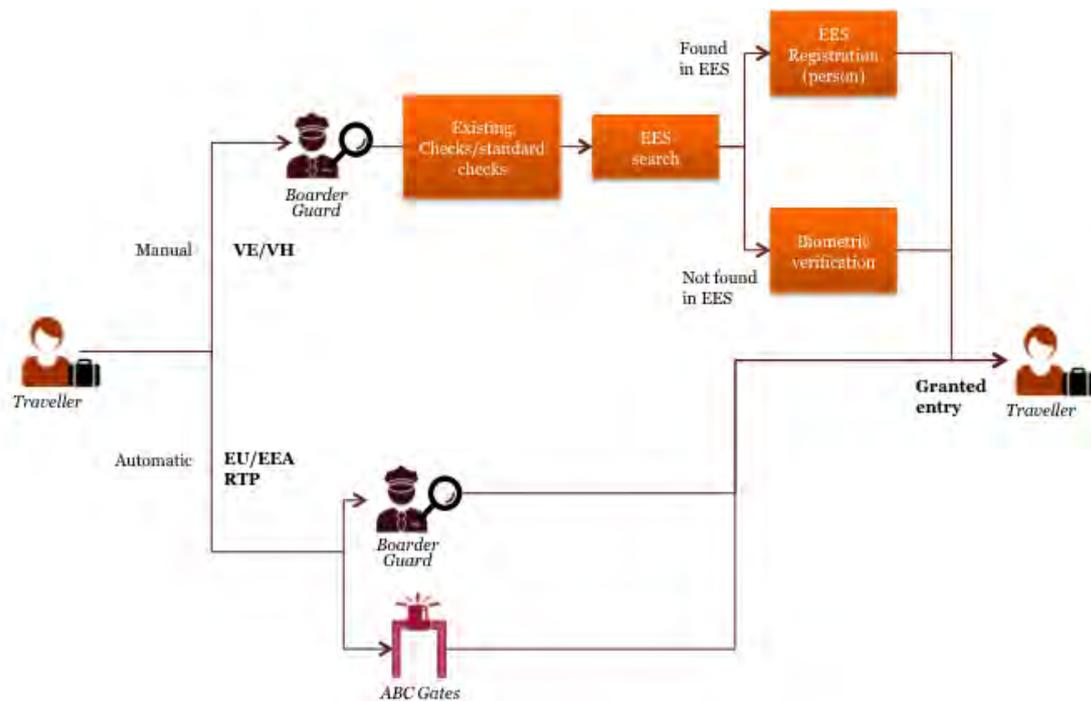
Discrete event simulation was used to assess the impact of any changes introduced in the border control process. The models used for air borders were customised versions of models previously used for simulations of actual air borders. The model for land borders was built from scratch.

Both models use real data from border crossing points that the concerned Member State authorities have provided. The focus of the simulations was the EES processes at entry and exit. RTP is seen as a sub-case of the simulations. In addition to the real data provided there were estimates inserted, including added time for registration, verification, etc.

The picture below shows the type of parameters used for running the tool and the type of results that would come out of the simulation.



The picture below shows the abstract model of the flow per category of traveller, including the EES and RTP in the flow. The picture shows the situation at entry. The only difference for the exit is that there is no registration in the EES – only biometric verification takes place at exit.



The simulations were made for two types of borders.

Air borders

Real data from four filters, two for arrival and two for departure, at a large airport within the Schengen area were put into the simulation tool. This data comes from an average day within the busiest month of the year.

Two filters (in the text named "Arrival filter B" and "Departure filter D") could be seen as very busy border crossing points comprising both manual booths and ABC gates; and the other filters (in the text named "Arrival filter A" and "Departure filter C") as border crossing points with more moderate volumes.

The simulation is performed for "incoming flows" at arrival (travellers entering the Schengen area) and "outgoing flows" at departure (travellers leaving the Schengen area).

Land borders

The real data that was used represents one month of border traffic and comes from a land border crossing point at the Schengen external borders. Only exit traffic was used in the simulation. Trucks and pedestrians are not included in the simulation for land borders. As regards trucks, the average checking time is around 30 minutes, mainly due to customs declarations and vehicle inspections, which makes it less relevant for the purposes of the simulation.

Three lanes with one booth per lane were used in the simulation and the vehicles were a combination of buses and private vehicles (motorbikes and private cars). Two lanes were used for private vehicles and one for combined buses and private vehicles. Checks take place while travellers stay in their vehicles (no need to step out). Most travellers are Russian citizens that are visa holders. It should be noted that neither the simulation nor the Study takes into account the potential change of this status, meaning the fact that a visa free agreement could be introduced for Russian citizens in the future. This is consistent with the assumption used throughout the Study that there are no (major) changes to the list of visa-exempt countries. The land border concerned uses both a pre-reservation scheme (a border crossing timeslot is reserved in advance prior to arrival at the BCP) and a live queue (for those who show up at the BCP without a pre-reservation) for all vehicles.

Simulation of air borders

Conditions

The real data used in the simulation are the following:

Volumes (traveller/day)		
Arrival filter A	3 000	The volumes are estimated to increase up to 3500 - 4000 in the coming 5 years. This was taken into account in the simulation
Arrival filter B	10 000	The volumes are estimated to increase up to 11-12000 in the coming 5 years. This was taken into account in the simulation
Departure filter C	11 000	The volumes are estimated to increase up to 12-13000 in the coming 5 years. This was taken into account in the simulation
Departure filter D	21 600	The volumes are estimated to increase up to 24-25000 in the coming 5 years. This was taken into account in the simulation

Configurations

Arrival filter A	No ABC gates, 5 manual booths
Arrival filter B	6 ABC gates, 6 manual booths
Departure filter C	No ABC gates, 6 manual booths
Departure filter D	6 ABC gates, 12 manual booths

Categories (traveller)

Arrival filter A	EU/EEA 69%
	VE 15 %
	VH 15 %
	Premium 1%
Arrival filter B	EU/EEA 74%
	VE 12.5 %
	VH 12.5 %
	Premium 1%
Departure filter C	EU/EEA 79%
	VE 10 %
	VH 10 %
	Premium 1%
Departure filter D	EU/EEA 69%
	VE 15 %
	VH 15 %
	Premium 1%

Note: The term "Premium" (travellers) refers to fast-tracked travellers; they still go through the same checks however. Practically, it mainly refers to airline crews.

The variables to be explored in order to assess the impact of EES and RTP are presented in the table below.

Variables

Percentage of border crossings of TCNs that require registration of the individual file in EES	0-50 %	<p>What is presented in the graph, in relation to this range are the values for 10 % and 50 %.</p> <p>10 % is indicated in the graphs, but this is not a realistic level of percentage and is only used to measure the importance of this parameter</p>
Percentage of border crossings of TCNs who are already registered in the RTP	0-10 %	The assumption is that RTP travellers are treated as EU/EEA travellers and that they use ABC gates when available
Time overhead for TCNs requiring registration of an individual file in the EES	Range of 0-180 sec	The values shown in the graphs are the average values of the potential additional time on top of the current border crossing time for performing the registration of the individual file in the EES.
Overhead for TCNs who need to be verified (not needing registration)	0-30 sec	This is the average value used for the potential added time to verify a TCN at entry/exit (the time for creating the entry/exit record is assumed to have a duration of 0 seconds)

The simulations are run for an extensive number of scenarios, exploring different values of the variants in the table above, to simulate what a day at an air border crossing point could look like after EES and RTP are implemented.

As an example, 1 400 simulations were run to obtain the data for airport filter A at arrival (entry). Up to 7000 simulations were run, 5 times, in other cases, to capture the statistic variations.

Below are the values used for the time the border check takes today, not taking into account the implementation of EES and RTP:

EU/EEA = 15 sec (manual)

EU/EEA = 20 sec (ABC-gate)

VE = 30 sec

VH = 45 sec

These values are realistic values for the given airport. The simulation tool in addition attributes a duration to each border crossing that is stochastically distributed so that the mean value equals the values mentioned above for each category of traveller. This brings the simulation closer to the reality.

Note: The benefit for persons using the ABC gates is mainly related to the dwelling time (the total time for queuing and performing the checks).

The results presented in the graphs relate to the following areas:

Service levels

The service level is in itself a time factor and service level compliance is the percentage of travellers for whom each service level is fulfilled. What is calculated in the simulations is service level compliance. The simulation shows how compliance changes, for a range of added durations to the border checks. The graph also shows results for different volumes of travellers (today – 2020).

It should be noted that the service level time includes the total average dwelling time for the travellers, not only the time for the border check.

The service levels are the following:

SL 2 = 2 minutes. This is a very challenging service level that is only used for ABC gates.

SL 5 = 5 minutes. This is a very high requirement for manual lanes.

SL 10 = 10 minutes. This is the most frequently used service level: having 85 or 90% of travellers served within 10 minutes is considered as a very good achievement.

Average dwelling time

The dwelling time represents the amount of time the traveller has to use to complete the border check clearance including the queuing time. It is computed from the moment the traveller arrives at the border check area, till the completion of the border check. The results are presented in relation to the same values as the service levels. It is the measurement that represents what the traveller experiences as "waiting for crossing the border".

Workload (air borders)

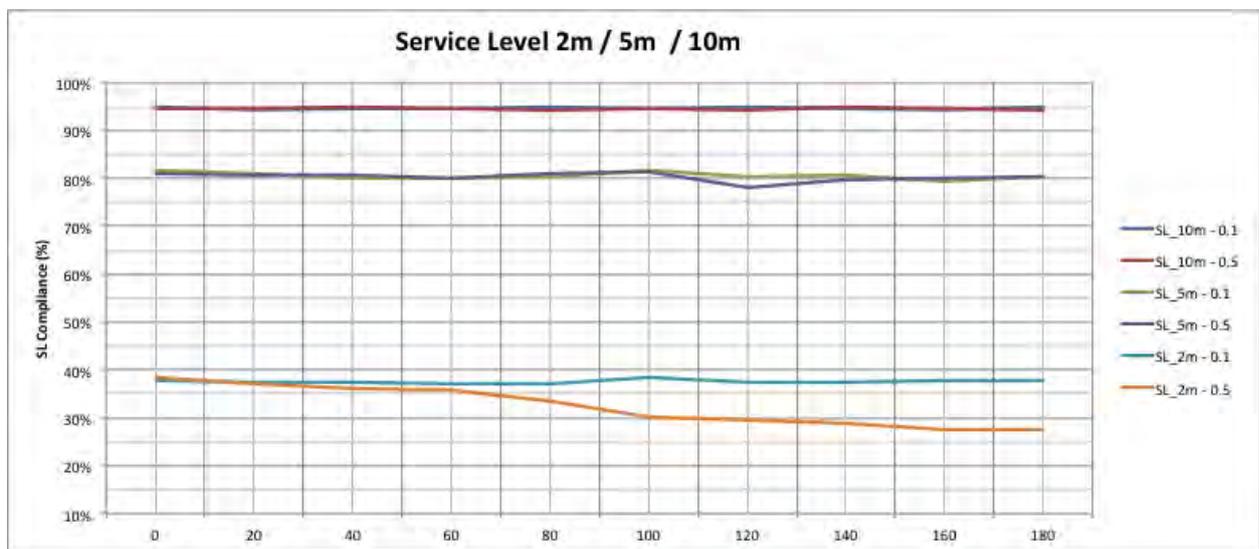
The workload included represents the total number of minutes of officer time required to perform border checks at the manual booths in one natural day. The graph shows the computed workload related to the added time for the actual check. For arrival checks, the result shows 2 alternatives, related to the percentage of TCNs for which an individual file needs to be registered.

Summary of the results – air borders

The summary takes into account the results at the four filters included in the simulation. The graphs shown are related to service level fulfilment, dwelling time and workload. The curves in the three types of graphs represent the results for all travellers passing through the specific border check. The simulation does not take into account travellers using the ABC gates. This is presented in a separate simulation (see section 0).

At entry

Service level fulfilment (Arrival filter A)

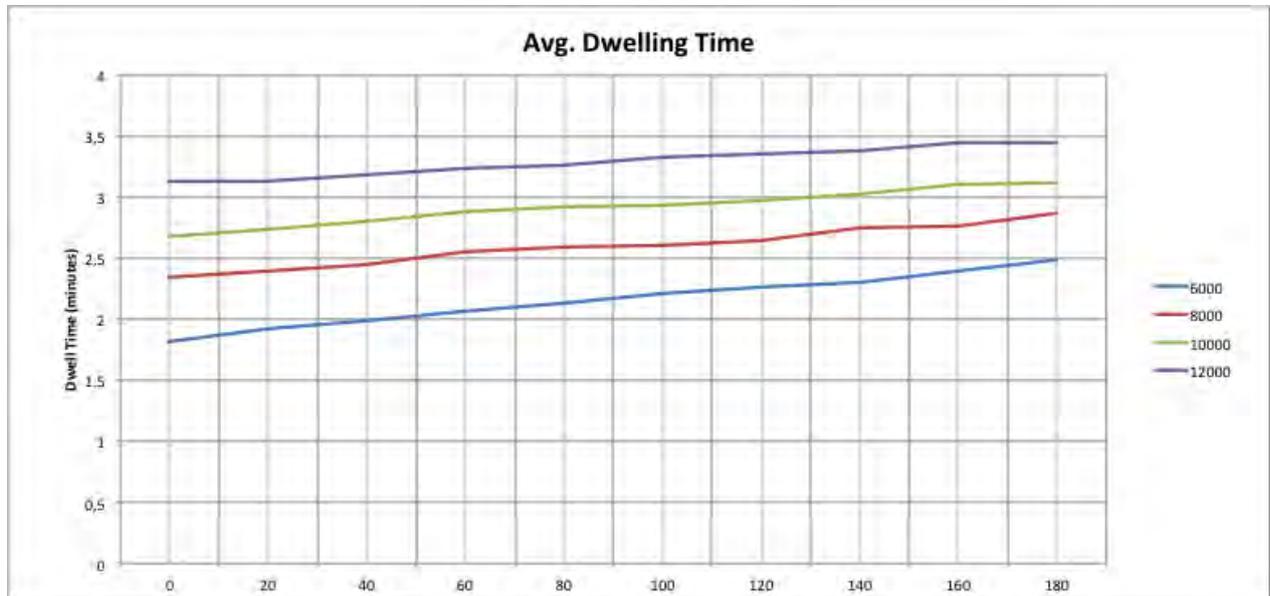


Observations

- The service levels of 5 min and 10 min are in principle not affected by any added duration of registration times up to 180 seconds. This can be seen in the graph by looking at the curves, which are more or less flat and superimposed. Independently of the added duration of registration and the percentage of travellers for which an individual file needs to be registered, these two service levels are not impacted. Still about 95% of travellers are serviced within 10 min (a typical service level goal for arrivals) and 80% of travellers are serviced within 5 minutes;
- At an expected percentage of first-time entries at 10% of the total volumes for TCNs, the service level of 2 min is not impacted. Independently of the added duration of checks, still about 38% of travellers are serviced within 2 minutes;
- At an expected percentage of first-time entries at 50% of the total volumes for TCNs, the service level of 2 min shows a decrease starting at around 30 seconds of added duration to the registration process and at 60 seconds of added duration the decrease curve becomes slightly steeper. So when about 50% of TCN travellers need to be enrolled (this is the case when EES starts because all VE need to be enrolled the first time), this service level starts becoming affected when the added duration for EES registration exceeds 60 seconds on average. For an added duration of 60 seconds, 35% rather than 38% of travellers use 2 minutes or less at the Border Crossing Point;
- The difference between arrival filter A and B were not significant despite their very different travel volumes and the difference in set-ups;

- The conclusion of this graph is that an added duration of less than 60 seconds on average for the EES registration, and using 30 seconds for verifications, does not show any significant impact on any of the service levels defined for the case studied. Even more time could be accommodated, when looking at compliance of service levels 5 and 10.

Dwelling time (Arrival filter B)



Observations

- The impact of added duration, in relation to dwelling time, shows a linear but rather limited increase. This increase tends to be even less important as the daily volumes increase but start from a higher average dwelling time as the superposition of the different lines of volumes of travellers/day indicate.;
- As an example, 60 seconds of added duration of the EES registration adds approximately 16 seconds of average dwelling time. The increased average dwelling time then goes from around 1 min 50 seconds up to 2 min 6 seconds for an arrival of 6,000 travellers per day. When the volume of travellers/day amounts to 10,000 then the average dwelling time increases only 13 seconds but moves from 2 min 40 seconds to 2 min 53 seconds.;
- The increase of dwelling time increases only slightly as the EES registration time becomes longer. From the graph for 10,000 travellers per day it appears that adding 80 and 100 seconds for EES registration adds respectively 14 and 15 seconds average dwelling time. The increased average dwelling time then goes from 2 min 40 seconds (zero added time) to 2 min 53 and 2 min 54 seconds.

Arrival filter A, with lower volumes but otherwise the same figures as above, shows an increase of around 18 seconds for the dwelling time.

Workload (Arrival filter B)



Observations

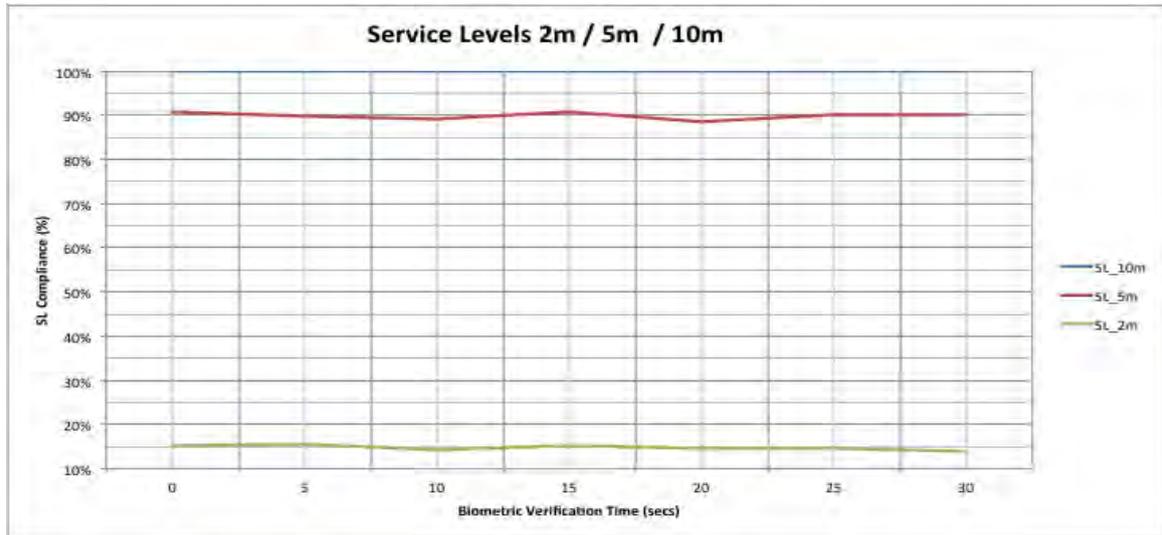
- The impact of added duration, in relation to workload, shows a linear increase which is an expected result. The simulation provides however a measurement on how steep this increase is;
- 60 seconds of added duration, for Arrival filter B, result in an increased workload of around 7 % (representing 185 minutes of added workload for 1 day). For 100 seconds of added duration, the workload increase amounts to 10,9% (representing 228 minutes of added workload for 1 day). The circumstances chosen as mentioned in the assumption being an average day within the busiest period;
- Filter A, with lower volumes, has a lower increase but comparable to Arrival filter B. 60 seconds of added duration would increase the workload by around 5,6% (representing 76 minutes of added workload).

At exit

The following graphs shows results at exit. The results are however representative for the situation at subsequent entries, where only verification and no registration of the individual file needs to be made.

The observations are made for filter D as it has the highest volumes. To avoid an overload of diagrams, the results for filter C are not shown but explained in the text.

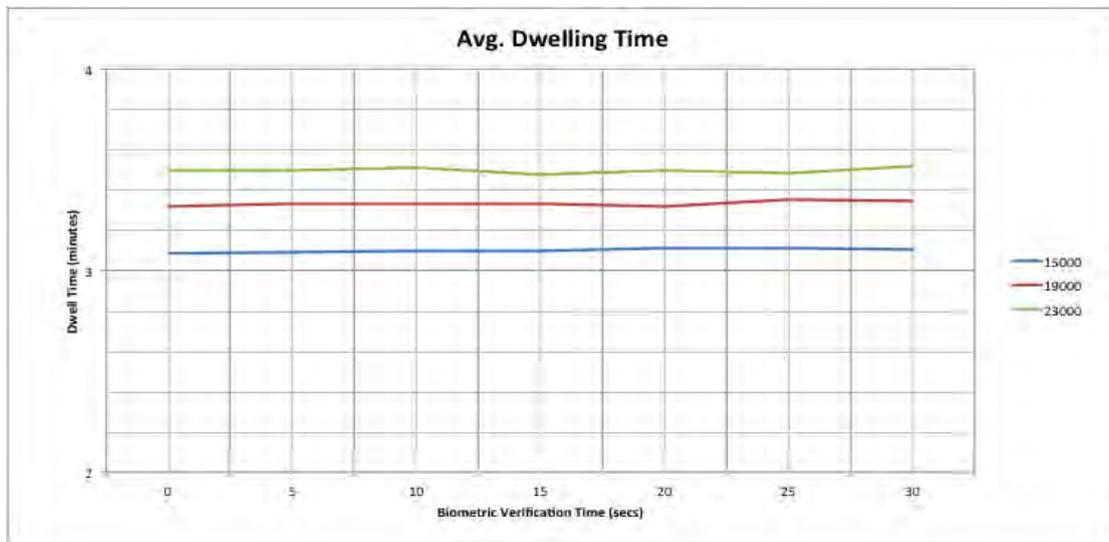
Service level fulfilment (Departure filter D)



Observations

- The Service levels are in principle not affected by the expected added duration for biometric verification time at exit;
- The difference between filter C and D is insignificant.

Dwelling time (Departure filter D)



Observations

- The added duration for biometric verification, within the interval, does not impact the dwelling time in principle.
- Departure filter C shows the same result.

Workload (Departure filter D)



Observations

- The impact of added duration or biometric verification, in relation to workload, shows a very limited and linear increase;
- 30 seconds of added duration (this is the maximum added time at exit), for filter D, results in an increased workload of around 1 %. Filter C shows a similar result.

Main observations – air border

The simulation is fully representative of the border crossing concerned, from where the real data and configuration of the border check were used.

It also provides results that can be used as indicators in the overall impact assessment of the EES and RTP. The indications below are chosen to be within the range of added duration for border checks that corresponds to the TOMs A, B and C (for EES) that are described in chapter 8.

1. An added duration of more than 60 seconds, at first entry, has the following impact:
 - A measurable impact on "service level 2", which has the objective of serving a traveller within 2 minutes. Once the additional tasks implied by EES equal 60 seconds, the decrease in service level becomes steeper;
 - Service levels of 5 and 10 minutes are in principle not affected by the additional duration;
 - Very limited impact on the dwelling time;
 - An impact of around 7% (at 60 seconds) on the workload necessary for the entry checks and around 11% (at 100 seconds).
2. At first entry, an added duration of less than 60 seconds on average for the EES registration, using 30 seconds for verifications, shows a limited impact on the service levels defined for the case studied. The dwelling time increases by less than 16 seconds and workload increases by less than 9.4% (at 40 seconds the increase is around 4.5%);
3. At subsequent entries and exits, an added duration of 30 seconds or less has in principle no impact on service levels, dwelling time or workload.

Simulation of land borders

Conditions for the simulation of land borders

The set-up and conditions of the land border simulation are different from the air border simulation; because a land border has different characteristics (a land border crossing point located on a road is used in this simulation).

The real data used in the simulation are the following:

Data used		Comment
Number of vehicles in month of observation	10 382	
Private vehicles	98%	The other vehicles (buses) have only a marginal occurrence, as at most land borders.
The chosen month's traffic in relation to the given year	9.1 % of yearly volume	The simulations were run for a month that is busier on average than the rest of the year, as the volume accounts for more than 1/12 th (8.3%) of the year.
Number of vehicles using the live queue	62%	
Number of vehicles using pre-reservation	38%	

Summary of the results – land borders

The summary takes into account the results at **exit** as seen for the land border included in the simulation. This is a normal case because for the entry, the queue cannot be measured as it is occurring on the other side of the border in the neighbouring country. The graphs shown are related to service level fulfilment, dwelling time and workload. The curves in the three types of graphs represent the results for the vehicles included in the simulation, passing through the specific border check.

The results presented in the graphs relate to the following areas:

Service levels

The service levels are the following:

- SL 10 = 10 minutes. This a very challenging service level for a land border of this type;
- SL 30 = 30 minutes. This can be seen as the most representative service level for this type of land border.

For comparison, service levels of 60, 120 and 180 minutes were also simulated (which might be more representative of a busier BCP).

Average dwelling time

Technical Study on Smart Borders – Final Report

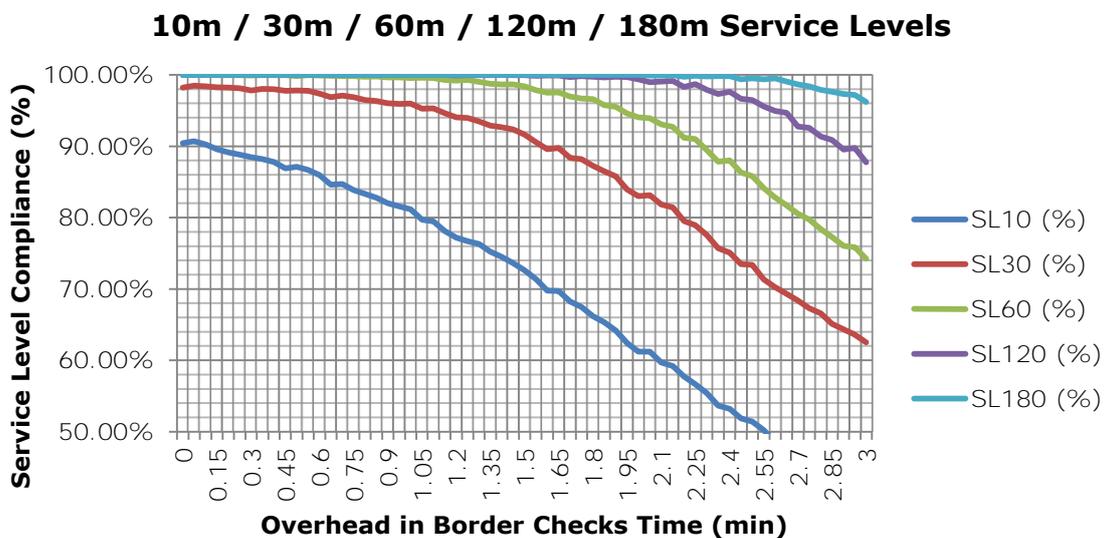
This graph shows the total average time the traveller has to wait for the purpose of a border check. It is counted from the moment the traveller arrives at the border check area, till the completion of the border check. The dwelling time represents the amount of time the traveller has to use for the purpose of the border check including the queuing time. The results are presented in relation to the same values as the service levels.

Usage factor (land borders)

The measurement at land borders is not defined as workload but as something called a “usage factor” that shows the percentage of activity (i.e. when checks are being done) for the border guards. At land borders, the flow and peak patterns differ from air borders and there is a need for continuous manning of booths. The usage factors also indicate the need for resources to replace the person in the booth at certain intervals.

The simulated border crossing is border checks at exit. Therefore, it is reasonable to use a potential added time of 30 seconds for the duration of the check against EES (biometric verification mainly) as a representative value. The time for added duration in the simulation is however per vehicle, which makes the comparison to the time it takes to verify 1 person more complicated. While preparing the simulation, it was seen that there was a certain degree of parallel activity and that the vehicles had an average occupancy of 1.5 to 2 persons. A value of 1 minute of added duration per vehicle could therefore be a representative value in this simulation. It should however be considered that if the occupants were to have to leave the car for such a verification, then the added time for the duration would presumably be longer.

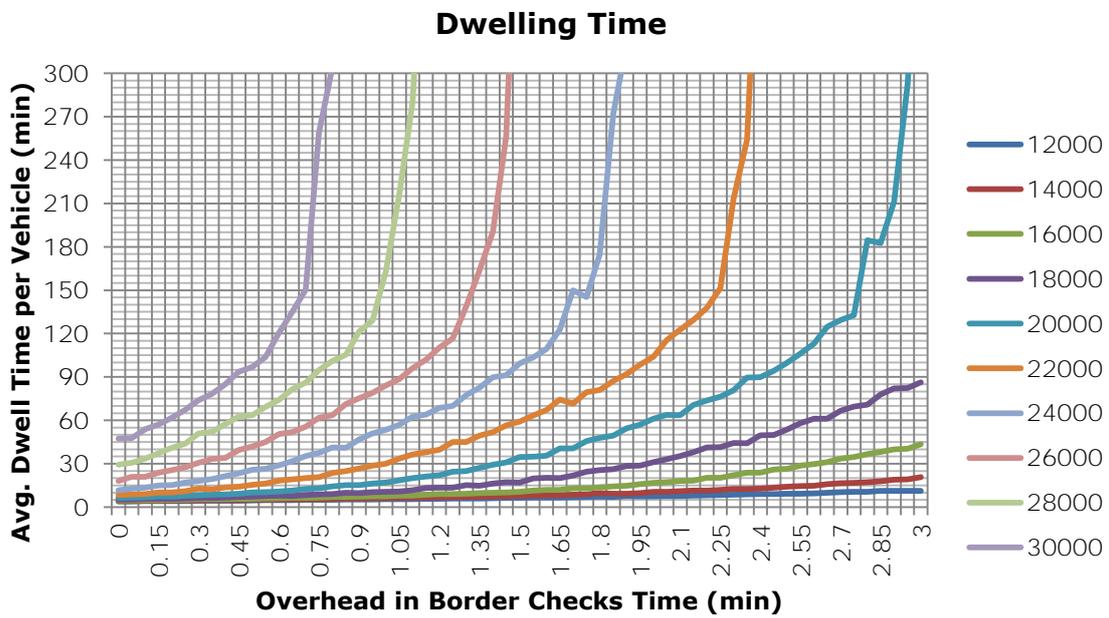
Service level compliance



Observations

- At 16 000 vehicles/month and 30 seconds of added duration, the service level of 30 minutes is in principle not impacted. For the same volume and added duration, there is a 3.3% degradation of the 10-minute service level. An added duration of 60 seconds would degrade the 30-minute service level by a bit more than 2 %;
- Unlike the air border, the service level at the land border is impacted directly with added duration to the border check. This is due to a more continuous flow of arrivals of vehicles and fewer opportunities for recovery time. In an airport the arrival and even departure of travellers is "bursty" meaning that there are successive peaks with time for recovery in between. At a land border crossing point, traffic comes in continuously, in this case even on a 24/7 basis.

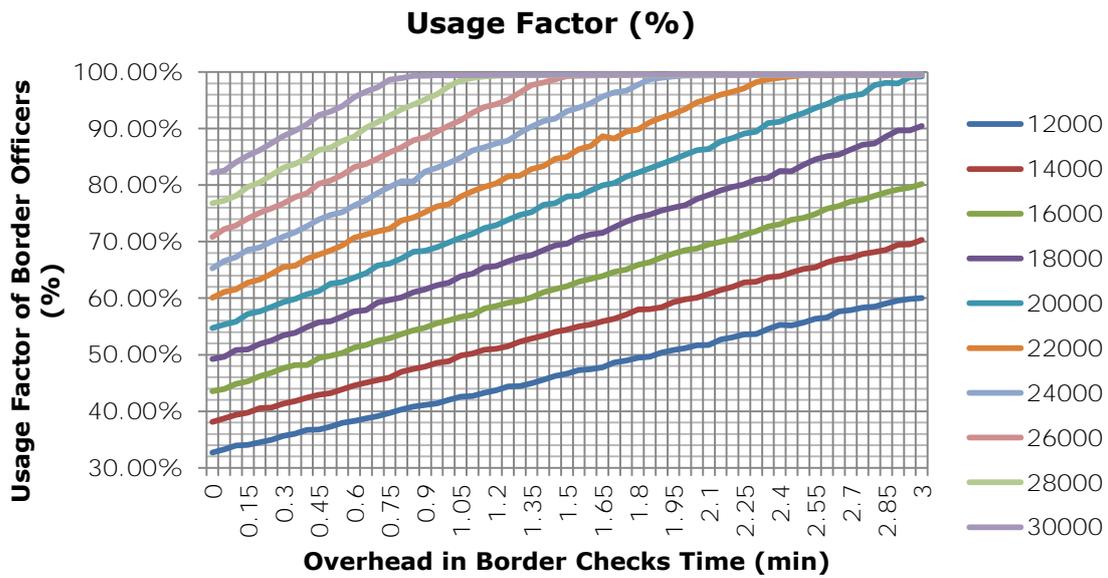
Dwelling time



Observations

- At 16 000 vehicles/month and 30 seconds of added duration, the dwelling time is not impacted. At 60 seconds of added duration, the dwelling time is increased by 3 minutes.

Usage factor



Observations

- At a volume of 16 000 vehicles/month, the guards are performing checks for 44% of the time, if no time is added. At 1 minute of added duration their usage factor is 56%, an increase of around 12% points. This still leaves some margin to handle peaks

Main observations – land border

The simulation is fully representative of the border crossing concerned, from where the real data and actual configuration of the border check were used.

It also provides results that can be used as indicators in the overall impact assessment of the EES and RTP. The indications below are chosen to be within the range of added duration for border checks that corresponds to the TOMs A, B and C (for EES) that are described in chapter 8.

- An added duration of 60 seconds per vehicle, at exit, has the following impact:
 - The service level of 30 minutes decreases by around 2%, which represents around 35 seconds of added time for the total time of queuing and being checked (i.e. the so-called "dwelling time");
 - The dwelling time increases by around 3 %;
 - The usage factor increases by 12 % points but this still leaves some margin to handle peak situations.
- A complicating factor, related to EES, would be if travellers needed to leave their cars for the biometric checks for instance.

Summary of the results – RTP

The simulation of the RTP could only be made at the air border. In this context RTP members are assumed to be able to use ABC-gates.

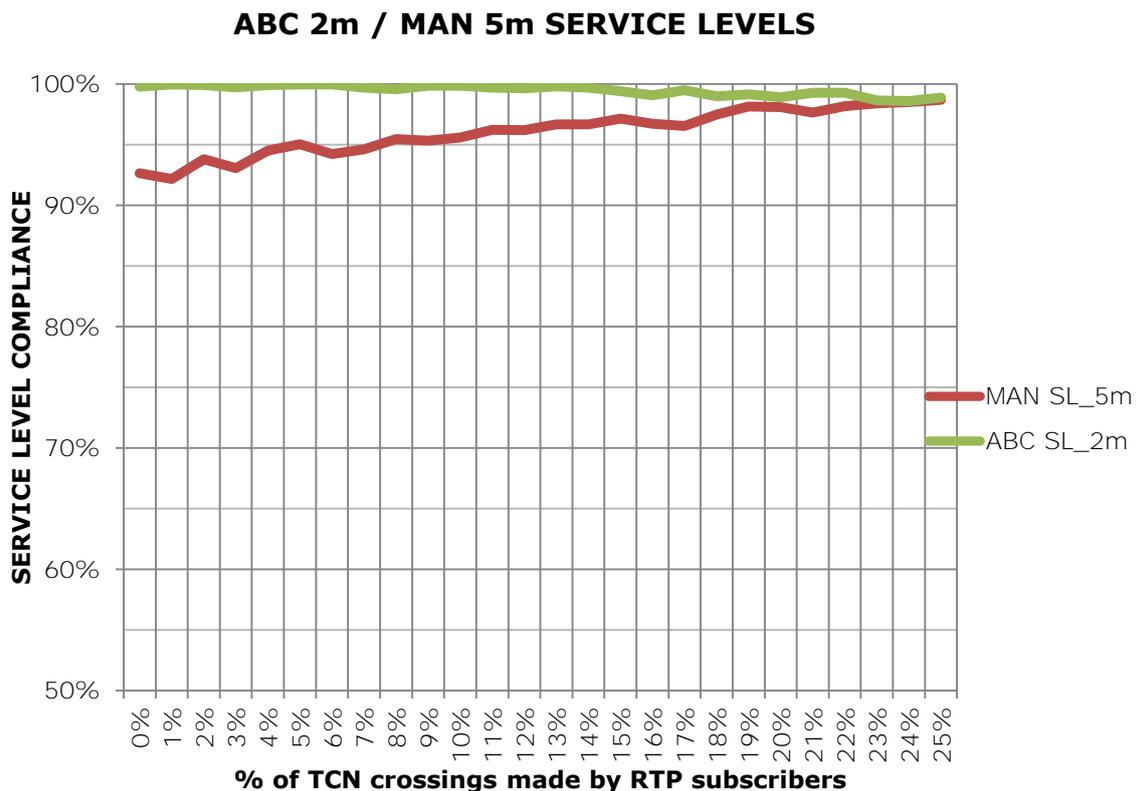
The summary takes into account the simulation conducted using arrival filter B and departure filter D, with high volumes and equipped with ABC gates. The ABC-gate has a service level of 2 minutes and the manual service level is at 5 minutes, for comparison with the service level of the ABC-gate.

The simulated variable is the percentage of border crossings made by TCN travellers with RTP status. In the diagram, this varies from 0 to 25%. To make the observations representative, the Study looked at the impact of 5% and 8%, respectively, of border crossings made by TCNs with RTP status.

The results of the simulations are shown in graphs representing arrival filter B. Departure filter D shows no significant difference, due to the fact that ABC gates are not dimensioned to sustain the increase of volumes (as explained in section J.2.3.2).

At entry

Service levels

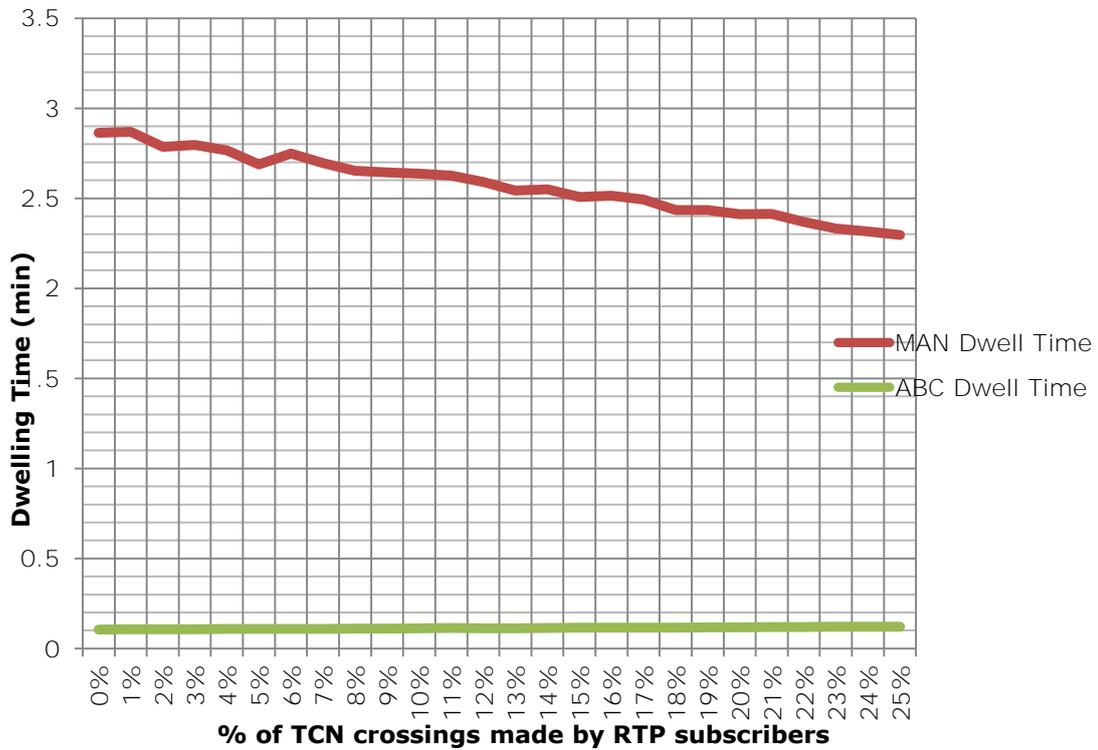


Observations

- In the case of 5 % of TCN crossings made by RTP subscribers, the service level of the ABC gate is not impacted while the manual service level is improved by 2% points (the MAN SL_5m moves from 93% to 95%). At a level of 8% of RTP crossings, the impact on the service level is the same as for 5%.

Dwelling time

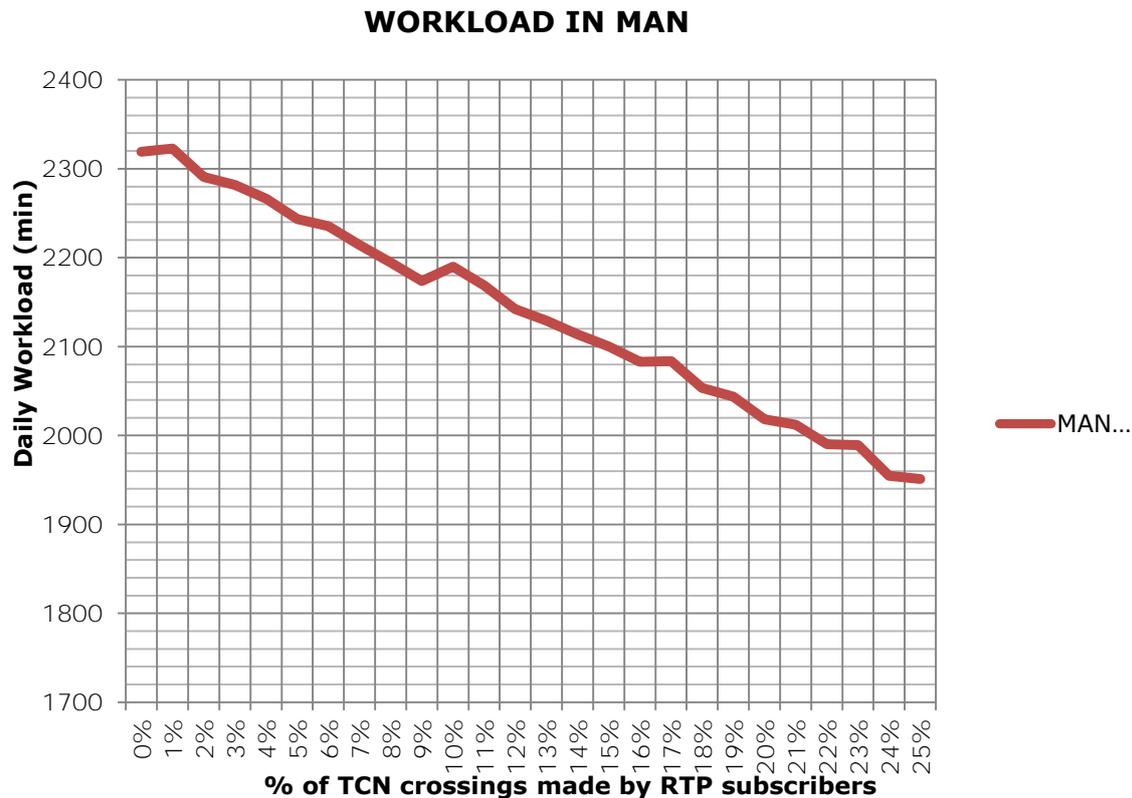
AVERAGE DWELLING TIME IN MAN AND ABC



Observations

- In the case of 5 % of TCN crossings made by RTP subscriber, the dwelling time related to the ABC gate is not impacted while the manual dwelling time decreases by around 10 seconds. At a level of 8% of RTP crossings, the dwelling time for ABC gates is still not impacted and the dwelling time for manual gates decreases by around 12 seconds.

Workload



Observations

- In the case of 5% of RTP crossings, workload at manual gates decreases by around 3% which represents around 76 minutes less per day in terms of workload.
- Taking the question reversely, in order to decrease the daily workload by border guards by 10%, there should be about 12% of TCN crossings made by RTP subscribers.

Main observations – RTP

The simulation is fully representative of the air border crossing concerned, from where the real data and actual configuration of the border check were used.

It also provides results that can be used as indicators in the overall impact assessment of the RTP. The indications below are chosen to be within the range of estimated usage for the RTP, as far as this can be estimated in the absence of comparable programs at EU level.

1. The use of ABC gates for RTP travellers makes it possible to keep a higher service level than at manual gates. The service level (2 min) used in the simulation includes dwelling time;
2. The general trend is that the more crossings are made by RTP travellers, the more the service level compliance at manual gates improves, the shorter the dwelling time becomes and the lower the workload;
3. The workload decrease when 5% to 12% of TCN border crossings is made by RTP subscribers can off-set part or the totality of the workload increase induced by the implementation of EES (additional first time enrolment and subsequent verification time). Having this percentage of border crossings done by RTP travellers remains consistent with the estimated number of RTP subscribers.

Technical Study on Smart Borders – Final Report

4. The results of the simulation with the departure filter D (no graph is presented here) revealed that if the ABC gates are not dimensioned for the increased number of crossings, the service levels and dwelling time are impacted negatively. The impact would be in direct relation to the increase of the percentage of crossings by travellers with RTP status. The positive impact on the manual gates would still remain.

Topics for further studies

The Study, during the course of its investigations, identified the following topics for which further analysis and work should be carried out:

- Simulations: carry out simulations targeted to areas that require further metrics and clarifications.
- Process optimisation: review the optimisation of processes at the border taking into account the options of the EES/RTP from the study.
- FastPass project: assessment whether the FastPass project could include activities that would be of value for the overall implementation of the EES and RTP (e.g. practical case studies on process optimisation in relation to ABC gates, or ABC gates combined with manual checks).
- TCN survey: launch a survey related to the interest in obtaining RTP status among eligible TCNs.
- Alternative proposal for RTP: detail description and risk assessment of the alternative RTP application (TOM N).
- Integration of EES and RTP: continued analysis for the merge of the systems at central level.
- Integration of EES/RTP with VIS: further detail on how one integrated system at central level would be conceived and implemented.
- Procurement and governance: assessment of the main challenges for the procurement and the governance of the EES and RTP.
- Data management model: continued analysis of the possible data management models for the EES and RTP.
- Active-active: assessment of the development of an active-active architecture for the central system.
- Integration costs with NUI for MS: further analysis of the exact scope of the integration required for the various MS.
-

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:
from the European Union's representations (http://ec.europa.eu/represent_en.htm);
from the delegations in non-EU countries
(http://eeas.europa.eu/delegations/index_en.htm);
by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm)
or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*). The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).



doi: