Council of the
European Union

Brussels, 3 March 2022
(OR. en)

6767/22

LIMITE

FRONT 87
COSI 61
IXIM 46
ENFOPOL 110
ENFOCUSTOM 33
COMIX 106

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Final Report Future Group on Travel Intelligence and Border Management

Delegations will find attached a report of Europol and Frontex on Future Group on Travel Intelligence and Border Management.

Final Report

Future Group on Travel Intelligence and Border Management

The Hague/Warsaw, 16 September 2021
EDOC 1182065 / Frontex No 9870

Table of Contents

1. The Future Group

Frontex and Europol have jointly established the 'Future Group on Travel Intelligence and Border Management'. This group brings together experts in the field of criminal investigation, border management, security, customs and migration with a view to identifying and elaborating new operational opportunities by bringing their respective professional domains closer together.

The new, emerging information management architecture at EU level creates an environment where a diversity of competent authorities at national and international level will work. Moreover, it creates new work flows and business processes that bring existing professional disciplines (e.g. border and migration management; customs; criminal investigations) closer together and adds new entities with important roles in the overall functioning of security and border protection, such as ETIAS NU[1] and ETIAS CU.

While several initiatives are on-going to implement the new instruments and revise the existing ones, Europol and Frontex saw a need to pro-actively bring the different professional disciplines at national and international level together to see how to maximize the operational benefits. This could allow for the identification of new ways of working together, for instance between investigative teams, border guards, migration management authorities and customs, and making optimal use of the information available to the different entities.

This covers the use of border and migration management information in support of criminal investigations as well as the use of data from criminal investigations in support of border and migration management and customs enforcement to address the cooperation gap between these communities. In particular, the opportunities stemming from the new border management and interoperability investments should be considered, combined with other information sources that are typical for the movements of persons and goods, such as PNR, API and Advance Cargo Information.

In addition to considering information management aspects to make optimal use of available information, the Future Group also looked at operational cooperation in practice between the various competent authorities involved at national or international level. In particular, the possibilities for multi-disciplinary cooperation across investigations, criminal analysis, targeting of movements and border or migration management were examined, identified and assessed. The group also investigated the operational cooperation and coordination structures and arrangements in place and analysed the impact of the new or enhanced EU information systems, including the new underlying legislation relating to the EU information systems and their interoperability.

This final report provides an account of the new cooperation opportunities and operational benefits that the evolving legal landscape and new architecture of EU information systems for borders, migration and security provides. It presents the different authorities operating as part of an EU Border and Travel Continuum rather than in silos. This report also includes an outline of an Integrated Border Control Model, which is not to be considered as a new standard that MS should implement, but rather as an operational vision and possible evolution building upon all the measures being already implemented that includes some short- and medium-term proposals.

[1] A list of abbreviations is provided in Annex III.

Frontex and Europol followed a bottom-up approach for the work of the Future Group, which always met at expert level. This final report is addressed to a large community, including the various national and EU stakeholders of Frontex and Europol.

Our most sincere appreciation goes to the many national experts from the various disciplines as well as colleagues from the Commission, eu-LISA and EASO, who accompanied and supported Frontex and Europol since September 2019 during the 11 workshops held by the Future Group. Their support was invaluable in achieving this collective outcome.

2. Interoperability, access to data and cooperation

2.1. Introduction

An important driver for the work of the Future Group is the recent legislative redirection of the collection and use of data in EU databases and other repositories for border management, migration, security and justice purposes. This changed the orientation from a strong division in function of the processing purpose towards a focus on interoperability in which the connection between data sets is sought across databases to improve the identification of individuals. It also facilitated access for the different competent authorities that require such access for their respective purposes.

However, this facilitated access to data does not imply that any national or international service can access and use all data for any law enforcement or border management purpose. This chapter aims to present the opportunities for data processing in a practical context to facilitate the understanding of what will be possible and what limitations need to be taken into account. It will also present some general ideas on how information can best be used within the broader framework of interoperability and smart borders.

2.2. Prime focus on travellers with emphasis on Third-Country Nationals (TCNs)

A tremendous legislative effort was made at EU level by the EU institutions over the last couple of years. Several new or revised legal instruments were adopted (e.g. SIS Regulations, Interoperability Regulations; EES; ETIAS; ECRIS-TCN; EU PNR Directive) while several others have reached an advanced stage towards adoption (e.g. VIS) or negotiation (Eurodac). For some legal instruments, adjustments are expected in the near future (e.g. API Directive).

The aim of these efforts has been to convert the individual EU systems into a coherent set that supports intelligent, integrated management of borders, migration security and justice. To achieve this, focus was placed on interoperability between the instruments and the more efficient use of data for multiple complementary purposes, while consistency between the legal frameworks was enhanced.

The adjustment of the focus towards interoperability and the use of data for multiple purposes are to a large degree (but not exclusively) aimed at improving identity management of travellers, and in particular TCNs. It should support processes related to granting TCNs permission to travel to/enter into the EU/Schengen Area; conducting risk assessments prior to arrival and the identification of individuals at the BCPs. The planned concept also covers checks on whether asylum applicants have already been registered under a different identity in any of the EU systems.

To make optimal use of the new possibilities, it is worth knowing what can be done with data collected and processed under the relevant legal instruments. An overview of the purposes for which the data can be used is presented in Annex I. The steps and overall mapping of the processes along the 'EU Border and Travel Continuum', as well as the analysis and conclusions on this continuum, are presented in chapters 3 and 4.

2.3. Movements of goods

The effective enforcement of borders, security and justice also calls for a focus on suspicious movements of goods. First and foremost, this relates to the domain of customs, including cargo shipments, courier and postal services. The Union Customs Code (UCC) dates back to 2013 and has not yet been integrated within the interoperability dimension. The legal instrument emphasises the confidential nature of information on shipments with few explicit exceptions. The Import Control System (ICS) is used by national customs authorities for the processing of advance cargo information that must be sent to the port of first entry of any shipment destined to the EU.

2.4. Processing purposes and access to data

The current realisation of a more interoperable and efficient use of information at EU level is expected to increase the effectiveness of the different competent authorities substantially.

Border guards, for instance, will have more information available to decide on admission or refusal of TCNs. For investigations, especially those with a cross-border dimension, it will become easier for national competent authorities to find out if there is any data available on the suspects they are looking for. That applies in particular where those suspects are TCNs, because of the increasing recording of their data in EU databases, such as ETIAS and EES. However, this does not imply that all data will be available to all authorities. Clear conditions and restrictions will continue to apply in terms of purpose and access.

To get a good understanding of the possibilities that national competent authorities and EU agencies have in using data related to travellers and shipped goods, it is worth distinguishing between the different kinds of access they may have. Essentially, four categories can be identified in this respect:

- Full access;
- Tailored/conditioned access;
- Hit/no hit access;
- Ability to request or receive data.

Full access means that the national competent authority or the EU Agency is in full control of the data. An example of this is the receipt of PNR data by national PIUs. Duly authorised staff can conduct different kinds of operations with the PNR data that the PIU has at its disposal. Such full access does not imply that there would not be any restrictions under which the data is to be handled.

Tailored/conditioned access means that a user can access data in the system, for instance by using search criteria, in a conditioned application in which certain predefined processing options and results are available. This may include all data or a subset of the data repository. Depending on the system, access may be limited to view access only, but can also include the possibility of editing and deletion. The insertion of new data into such a processing environment could also qualify as such, because after the insertion the limitations to the processing would also apply. The future use of ETIAS for border guards could serve as an example of tailored access. The current law enforcement access to VIS also falls under this category.

Hit/no hit access enables a user to check whether a data repository contains certain information, but without granting immediate access to the content. In most cases, the user can then request to receive the information upon submission of a duly justified request. Law enforcement access to data in Eurodac and the future access to ETIAS, EES and VIS within the scope of the Interoperability Regulations fall under this category.

Ability to request or receive data, finally, is where no form of access to the source is available to the requester/recipient, but the possibility exists to receive the data lawfully upon request or on the basis of a spontaneous provision by the entity that holds the data. This is often the basis for bilateral exchange of information between law enforcement authorities of different countries. This also applies to retrieving PNR data from national PIUs.

The instruments of relevance to Interoperability, Travel Intelligence and Integrated Border Management (IBM) contain a combination of some or all of the above types of access, which in most cases depend on the purpose for which the data is accessed.

In most of these legal instruments, the access is allocated in accordance with the functions that are fulfilled. The specific consequences for the access by competent authorities at national level depend on the allocation of those functions in each country. If a border guard service is also responsible for the processing of PNR data, then that border force has access to PNR data as it assumes the role of the PIU.

Furthermore, the composition of certain functions may also vary from one country to another. An ETIAS National Unit may be composed of representatives of multiple competent authorities. An authority responsible for national security may also be part of the PIU, the ETIAS National Unit and other entities, depending the national definitions and legislation.

Even though the relevant legal instruments enable data to be used for multiple purposes, the access remains limited to the relevant types of authorities specified in those legal instruments depending on the relevant processing purposes.

Looking more concretely at the types of databases, a clear differentiation can be made between systems that are associated to criminal offences, notably SIS and ECRIS-TCN, and administrative systems predominantly containing data on non-suspected individuals.

While the systems associated with criminal offences can often be consulted directly by law enforcement authorities, the access to administrative databases, such as PNR, Eurodac, EES, ETIAS and VIS, is much more restricted. Conditioned access to such administrative data for border forces and, where applicable, migration authorities is permitted, yet strictly limited to their respective functional needs. For the prevention and criminal investigation of serious crime and terrorism, access to those administrative systems is mostly limited to hit/no hit access and/or the ability to submit a duly justified request or to passively receive data.

The latter category, i.e. absence of access, makes the competent authorities dependent on other partners that do have access to the data and on their assessment of the relevance of sharing such information with those services that do not have access themselves, but are able to receive such data. The example of access to PNR data can be used to illustrate that. Only the PIUs have access to PNR data. The border guards and investigation services are dependent on the PIU's assistance, which the PIU can provide either on its own initiative or upon request of the dependant authority.

2.5. Information dynamics

In the practical functioning of the relevant legal instruments, data is collected, stored and used in the corresponding processing systems, such as VIS and SIS. The data processing in those applications is intended to function as a comprehensive system that supports border management, migration and security. To understand how that works from a holistic perspective, it is worth looking at three particular factors that influence the dynamics of data processing: the **triggering event**; the **interaction between processes** and the **evaluation**.

Triggering event

The 'triggering event' is the event that initiates the data processing. This can be, for instance, a query by an investigator in a system or the insertion of new crime-related information. In the context of border management and interoperability, the triggering event will often relate to the travelling of individuals or their intention to do so. This initiates the collection of PNR and API data and possibly the submission of an ETIAS or visa application. For travellers by car, it triggers automated checks of licence plates at external land borders and at seaports where vehicles come off ferries. In the domain of goods, the shipments of cargo, parcels and mail to the EU are the triggers for data processing by customs services.

Interaction between processes

This factor relates to the extent that processes 'communicate' with each other. This may take the form of a request-answer sequence, for example by cross-checking data in other databases. But it could also be that one process ends and triggers another one.

Especially in the fields of interoperability and IBM, the interaction between processes is essential. There are many examples that can be given on the basis of the existing practice and from the instruments that are currently being implemented.

For instance, based on the risk profiles received from the competent authorities, a national PIU identifies a risk concerning a certain traveller and informs the border forces. The PIU process ends upon passing on the information, which initiates the process for the border guard. But this process could also require a feedback from the border forces back to the PIU and Interpol/Sirene bureaux after interception of a suspect or further to the competent authorities that shared the risk profile in the first place.

As another example, a new entry to the ETIAS watchlist will trigger a query against previously granted travel authorisations. In case of a hit, it triggers the process by which the ETIAS travel authorisation is reassessed and possibly revoked.

Evaluation

The term 'evaluation' refers to the interpretation of the content of the information within the operational reality and in particular taking into account all other relevant contextual information.

As an example, customs services apply risk assessment techniques to select and prioritise which incoming shipments to check. This risk assessment is based on contextual information related to fraud schemes, trafficking practices and security threats. Depending on the data available, a container from Canada carrying car parts may be evaluated differently to a shipment of shoes from Singapore.

Also the decisions to grant or refuse visas and future ETIAS travel authorisations are taken on the basis of an evaluation of the individual application, taking into account all available contextual information. That contextual information may be a concrete hit in SIS or be more general information on overstayers or an elevated security threat of individuals that match a specific risk profile.

2.6. Strengths and Weaknesses

The dynamics of the information management processes can give a good indication of their potential, but it can also help to understand in which ways the effectiveness can be further enhanced. To analyse in that sense the combined set of instruments related to interoperability, travel intelligence and border management, the factors mentioned above will be concisely discussed in terms of strengths and weaknesses.

Strengths

The combination of VIS, ETIAS, PNR, API, SIS, Eurodac and EES will ensure – if all fully implemented and applied to travellers to and from Schengen – a very large number of **triggering events**. Each TCN travelling to the Schengen area will initiate checks at several stages of the travel/border continuum. Moreover, API data is processed for each extra-EU flight (also for EU citizens) and PNR data will also be collected for intra-EU flights by most MS[2], as they connect airlines progressively. In that respect, the increasing collection of data on travellers is highly valuable for border control, migration management and security.

The positive effect of the large quantity of triggering events on the use of available information for border management and security is made even stronger by the **interaction** between the different processes involved. Many of those interactions have been foreseen in the relevant legal instruments. There are even specific components envisaged in the Interoperability Regulations to accomplish that, such as the MID, ESP SBMS and CIR, enabling integrated searches against multiple databases.

In many instances, the interaction with other processes will be fully embedded or even automated in the practical functioning of the instruments. This gives the assurance that the related processes are factually initiated as a result of that interaction. A good example of this are the envisaged border checks for TCNs, comprising, depending on the applicable regulation, the collection of fingerprints and the facial image of the TCN, the registration in the EES, the check of biometric and biographic data against the available records in the EU central systems, a check of valid ETIAS travel authorisation or the presentation of the visa data, as applicable, to the border guard.

Using that example, also for the **evaluation**, the presentation of relevant data from multiple sources enables the border guard to assess the specifics of the traveller and to decide on admission on the basis of the complete picture. Some systems provide additional options to further extend the possibility for refined evaluation. ETIAS, for example, allows the marking of certain issued travel authorisations in order to bring these aspects to the border guard's attention. SIS includes articles outlining further checks or other procedures related to individuals crossing the Schengen border. Obviously, having as much contextual information as possible augments the quality and accuracy of decisions to be taken by the first or second line officer on the ground.

Weaknesses

While the revised systems and processes ensure a comprehensive approach, including higher data quality and faster response, there are also some limitations to consider. This applies to all three factors – the triggering event, the interaction between processes and the evaluation – and to the combinations of the three elements.

[2] Subject to the way the EU PNR Directive is implemented at national level.

The fact that information processing is actively triggered in high volumes by the movements of persons and goods is positive, but bears the risk of competent authorities trusting too much in the system and becoming predominantly reactive at the expense of their vigilance. In addition, it may have a negative impact on the real-time processing, especially when it triggers multiple hits. It might take some time until all data is retrieved, or alternatively, until the corresponding data has been consulted in the respective systems in which a hit was found.

Furthermore, the interaction between processes does connect across the relevant policy/enforcement domains, nor between the respective competent authorities dealing with them (customs, migration authorities, law enforcement and border guards). In other words, there is relatively little interaction between the respective processes of customs services, migration, police and border forces. And if they do interact, mostly the one process stops where the other process starts.

To illustrate this, let us assume that, over a period of a few weeks, three Foreign Terrorist Fighters (FTFs) from Bosnia-Herzegovina apply for an ETIAS travel authorisation, indicating their intention to stay in Denmark. Two applications hit German alerts in SIS for refusal of entry, while the third one triggers a hit against a Slovenian entry in the ETIAS Watchlist. The German and the Slovenian ETIAS National Units refuse the respective ETIAS travel authorisations. While that meets the objective of ETIAS, surely the Danish security service would be interested to know about this. Will it be informed? Possibly, but it is not foreseen in the process. It depends on the German and Slovenian ETIAS National Units, and since they are deciding only on the individual cases, they may not see the relevance of sharing it.

The interaction between processes is especially weak where it concerns the link between persons and goods. Customs are, according to the current EU legislation, quite disconnected from the processes related to travellers from third countries. As to the cooperation between different competent authorities, the movements of goods are to some extent linked to law enforcement, but not at all to migration.

As an example of the latter, an Afghan national whose visa expired 18 months ago is receiving in Portugal air freight from Paraguay. While that may sound fine, as long as tariffs are paid and the goods are imported lawfully, no link is made to the legitimacy of the recipient on European soil. Could the fact of overstaying by the recipient influence the evaluation of the shipment by customs authorities? Possibly. It might, at least, improve the quality of decisions in the interest of security and justice. In addition, the destination of the shipment could be of use to trace the whereabouts of the overstayer and possibly lead to his or her repatriation.

Concerning the evaluation, it is worth highlighting that the contextual information generated by the various systems in the interoperability, travel intelligence and border management domain is predominantly linked to concrete individuals or shipments. A border guard may receive a hit from one or multiple systems on an individual that intends to enter into the Schengen area. That is mainly operational data on known suspects. Strategic information, for instance on risk areas, criminal modi operandi and prevalence of overstaying, is not generated by those systems. For such strategic information, the competent authorities often depend on the voluntary sharing of information by other partners.

Also in this respect, the boundaries of the processing purposes appear to limit the sharing of strategic information between the respective competent authorities. A national visa authority is not necessarily updated on crime trends. So, for instance, in the evaluation of a visa application, the officer may not be aware of specific crime areas that significantly correlate with the profile of the applicant, neither as potential suspect, nor as possible victim. Yet for strategic information, it must be stressed that there is no legal impediment for sharing. It simply does not happen in practice due to the disconnect between the different domains.

2.7. Opportunities to make optimal use of legal instruments

The weaknesses presented in the previous paragraph are not intended as criticism. With perhaps the exception of interlinking the instruments more closely with customs, the comprehensive set of legislative measures was compared to probably the maximum of what could be achieved bearing in mind the reality of previous years. Instead, it is the way the tools and processes are implemented and operated in practice that might make the main difference in resolving at least partially the issues described. Those points mentioned in the previous paragraph are the ones that can be addressed in the actual functioning to make the respective instruments work optimally and in full compliance with the intentions of the legislator.

To get the most value out of the legal instruments and systems, it is essential to place them within an appropriate interactive and interoperable composition of competent authorities at national and international level. The business processes and workflows should be such that officers can work efficiently with the data, where needed across the boundaries of the country and the professional disciplines.

Where the work of customs connects to that of criminal investigations, it must be possible to set up an immediate, almost seamless cooperation with counterparts in an applicable investigation department, either at national level or with international partners.

The same applies to links that call for cooperation between migration, visas and border management authorities. For the three functions, the decisions affect all Schengen partners. Normally a TCN that has been granted a visa by one country will in principle travel (at least for the first trip) to the issuing country, but holders of short-stay and long-stay visas may travel to all Schengen countries. Where issues arise, immediate cooperation and communication is needed between the services involved.

The effective use of the data on travellers in the various systems would also benefit from the proactive sharing of strategic information, trends, patterns and modi operandi between the cooperation partners. Law enforcement can learn from what migration authorities observe; border forces can have an advantage in knowing what customs services discover. Thus, a mutual sharing practice would be valuable for all actors involved. Moreover, the explicit articulation of needs between these disciplines could actively stimulate the gathering and sharing of relevant details and insights.

In addition, it is worth considering concrete operational issues from the different professional disciplines. To give an example, let us assume that there is a specific group of overstayers who come from a region in South America. They enter the Schengen area through Spain and some are reported in police reports as victims of varying types of crimes in Belgium, during the period that their visa was still valid. What happened to them? Are they victims of trafficking in human beings? Did they fall victim to sexual or labour exploitation? What are their means of subsistence during their enduring stay? Are they in contact with their families? Do they send any money to relatives? Or do they receive any funds? Do they send or receive any goods to or from abroad? Migration, customs, border forces and law enforcement can all contribute to looking into concrete cases like these. And more importantly, they can all benefit from the answers collected. After all, it helps officers to put their work in a more informed and complete context, enabling them to take better decisions and actions.

Issues like the one mentioned in this example, where the professional competences of the different services are all concerned, are manifold. Ideally, there would be an active skimming for such issues and a collective response to the most pertinent cases.

As such, the creation of notably an interactive, multi-disciplinary partnership between border forces, migration authorities, customs and law enforcement can take the effectiveness of the interoperability and smart borders package to a higher level.

While these points address the possibilities for optimal use in principle, more concrete examples and suggestions will be presented in the following chapters. This will be done largely on the basis of a description and analysis of the individual steps of the border and travel continuum in chapters 3 and 4. Concrete suggestions on how to organise the multi-disciplinary partnership at national and international level will follow in chapter 5, which deals with the Integrated Border Control Model.

3. The EU Border and Travel Continuum

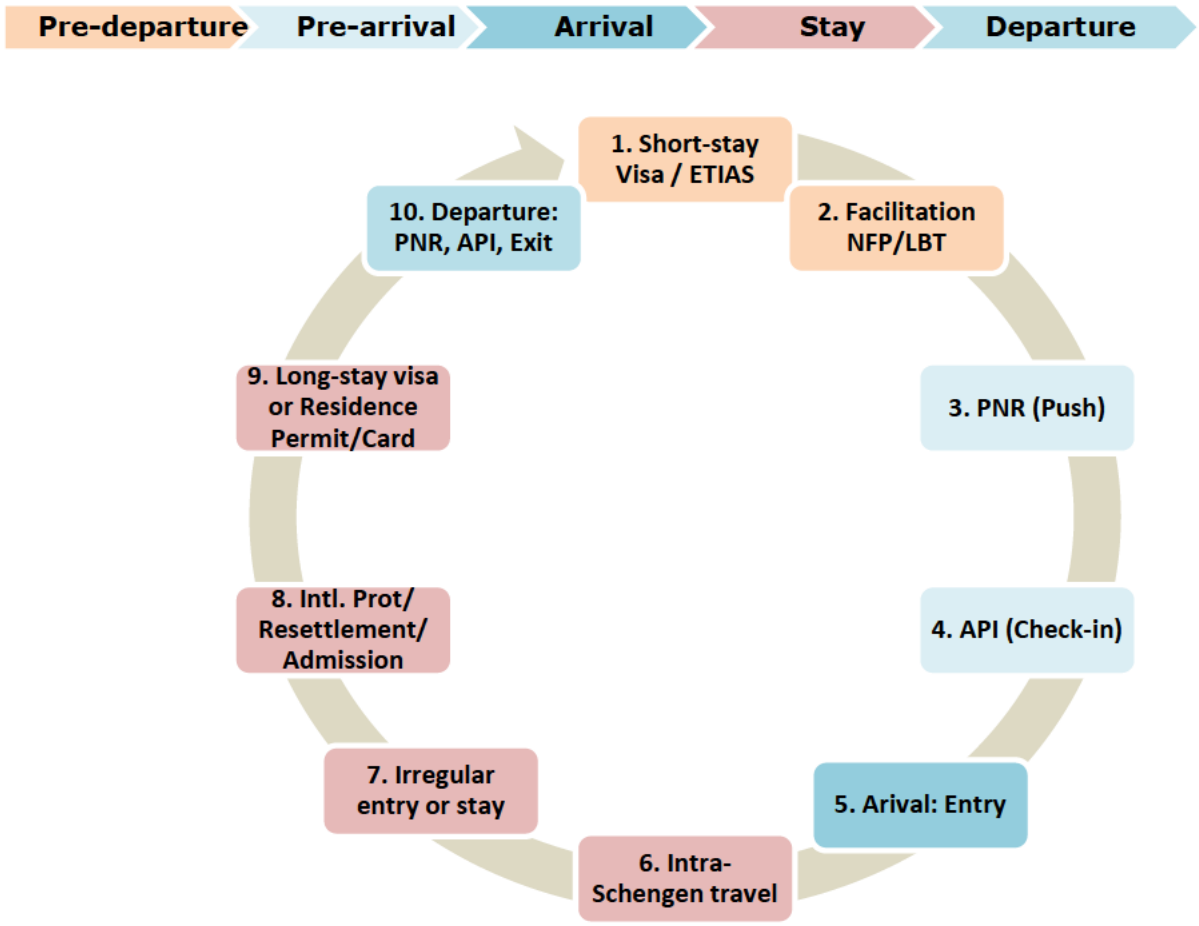
3.1. The 'EU border and travel continuum' concept

One of the main foundations of the work of the Future Group is the so-called border and travel continuum. The term 'continuum' emphasises the strong connection between the different steps of the journey or stay of any traveller to and within the Schengen Area. The term 'Border' (continuum) stresses the particular focus on entry and stay of TCNs while the term 'Travel' (continuum) reminds us of the fact that some of these steps apply to all travellers, meaning also EU citizens or beneficiaries of free movement.

The 10 steps of the continuum, presented below, are regulated by different legal instruments under the responsibility of different authorities with different decision-making process and consultation arrangements and supported by various information systems and tools. However, they are all interconnected and are part of a whole set of measures that support the integrity of the Schengen free movement area and also the EU internal security and migration management policies.

These 10 steps are mapped in the present chapter. This mapping is also inspired by the ICAO TRIP Guide on Border Control Management, which has been adapted to the EU context.

They are ordered according to a natural sequence of events (see cycle below) which does not necessarily apply to all travellers or TCNs. Furthermore, the sequence of particular events or steps in the continuum may not necessarily follow the order in this graphic and following table: for instance, a request for long-stay visas (step 9) is normally made and processed before the entry of the TCN into the Schengen Area.



These 10 steps of the border continuum will be developed in chapter 3.2 in accordance with the following table, which provides an outline.

Outline of the EU Border and Travel Continuum

Steps	1. Pre-depart.: Short-stay Visa/ETIAS	2. Pre-depart.: Facilitation NFP/LBT	3. Pre-arrival: PNR (Push)	4. Pre-arrival: API (Check-in)	5. Arrival: Entry	6 Intra-Schengen Travel	7. Irregular entry or stay	8. Intl. Protect. /Resettlement Transfer	9. L/S visas or residence permit/card	10. Departure: PNR, API, Exit
Sectorial EU Law	Visa Code + VIS Reg. / ETIAS Reg Interop Reg.	SBC EES Reg / LBT Reg. + Bilateral Agreement with TC	EU PNR Directive	API Directive SBC, CISA ETIAS Reg. EES Reg. Maritime Single Window Reg. ILO Reg.	SBC EES Reg. Carriers Liability Directive Interop Reg. ETIAS Reg.	Free Movement Directive. SBC EU PNR Directive (intra-EU)	Return Directive. SBC Facilitation of illegal immigration Directive. Eurodac and SIS Recast Interop Reg.	Asylum Procedure & Qualifications Directives, AMMR, Screening Regulation and Eurodac Recast Regulations Interop Reg	VIS Reg. Uniform Format Reg. SBC, CISA, SIS Recast Interop Reg	EU PNR and API Directives SBC EES Reg Interop Reg.
Who	TCNs: visa required / visa exempted	Registered travellers Intl. airports / TCNs residents in border area	All travellers (EU citizens and TCNs) in an EU inbound (and outbound) flight	All travellers (EU citizens and TCNs) in a Schengen inbound flight	All travellers (EU citizens and TCNs) TCNs: EES registration/ verification	All travellers (EU citizens and TCNs)	TCNs who do not fulfil (anymore) conditions for entry or stay	TCNs applying for Intl. Protection including those being relocated between MS or being resettled from a TC	TCNs applying for residence permits or long-stay visas	All travellers (EU citizens and TCNs) TCNs: EES registration / verification
Main systems/ Tools	National System + VIS / ETIAS	Intl. Airport RTP register / MS LBT permit central register	National PNR systems	National API Systems	National Border Control System + EES connected to VIS & ETIAS FADO	National PNR System (if the MS applies PNR Directive to intra-EU flights)	National Migration or Return Case Management System (RECAMAS) + Eurodac and SIS II EES, VIS and ETIAS	National Asylum case management System + Eurodac.	National Migration or Visa System + VIS	National Border Control System + EES connected to VIS & ETIAS FADO

Steps	1. Pre-depart.: Short-stay Visa/ETIAS	2. Pre-depart.: Facilitation NFP/LBT	3. Pre-arrival: PNR (Push)	4. Pre-arrival: API (Check-in)	5. Arrival: Entry	6 Intra-Schengen Travel	7. Irregular entry or stay	8. Intl. Protect. /Resettlement Transfer	9. L/S visas or residence permit/card	10. Departure: PNR, API, Exit
		ID/TD data, residence data (LBT)	PNR Data: ID/TD data itinerary booking, co-travellers; seat no; luggage; ticket no, travel agent, payment means	**Main data processed**	ID/TD data, Biometrics (only for VIS), residence, occupation, education	(API)/PNR Data: ID/TD data itinerary booking, co-travellers; seat no; luggage; ticket no, travel agent, payment means	ID/TD data Biometrics. Place/date of apprehension or removal (Eurodac)	ID/TD Data Biometrics responsible MS, Place and date of registration, date of decision, status	ID/TD data biometrics, place and date of the decision, expiry date, status, type of document (residence permit or long-stay visa)	All travellers: ID/TD data API/PNR data TCNs in EES: ID/TD data Biometrics Place (BCP) and date of exit, duration of stay
Databases Checks	SIS, VIS, EES, ETIAS, ECRIS-TCN, Eurodac Watchlist Europol data SLTD/TDAWN List of valid travel documents	SIS and National DBs? EES (for overstayers and refusals of entry)	SIS, National DBs, Interpol SLTD + National DB/ Watchlist Europol	SIS and National DBs Interpol SLTD	All travellers: SIS, Interpol SLTD National DBs TCNs: EES, VIS, ETIAS and CIR for identification of the TCN	For (API)/PNR data: SIS and National DBs Interpol SLTD	Identification of TCN against the CIR Security checks against SIS, EES, ETIAS, VIS, Europol, and Interpol SLTD /TDAWN.	Eurodac (for Intl Protection and Dublin Reg. purposes) VIS (for Dublin Reg. purposes)	SIS, VIS, EES, ETIAS, ECRIS-TCN, Watchlist Europol and SLTD/TDAWN	All travellers: SIS, SLTD National DBs TCNs: EES, VIS, ETIAS.

Steps	1. Pre-depart.: Short-stay Visa/ETIAS	2. Pre-depart.: Facilitation NFP/LBT	3. Pre-arrival: PNR (Push)	4. Pre-arrival: API (Check-in)	5. Arrival: Entry	6 Intra-Schengen Travel	7. Irregular entry or stay	8. Intl. Protect. /Resettlement Transfer	9. L/S visas or residence permit/card	10. Departure: PNR, API, Exit
Risk Assessment	Risk indicators on irregular migration, security and public health		Movement history analysis, targeting rules	Targeting rules	Local (BCP level) risk indicators.	Movement history analysis, targeting rules		Potential Security Risk assessment for Eurodac and Exclusion criteria for Asylum process		Targeting rules
Support criminal investigation	Queries against Europol data, watchlist and SIS alerts Law enforcement access to VIS & ETIAS data	N/A	PNR data are processed primarily for criminal investigation	Defined in national legislation	Sensitive SIS alerts Law enforcement access to EES data	(API)/PNR data are processed primarily for criminal investigation	Law enforcement access to Eurodac data	Law enforcement access to Eurodac data	Queries against Europol data, watchlist and SIS alerts Law enforcement access to VIS data	Sensitive SIS alerts Law enforcement access to EES data

Steps	1. Pre-depart.: Short-stay Visa/ETIAS	2. Pre-depart.: Facilitation NFP/LBT	3. Pre-arrival: PNR (Push)	4. Pre-arrival: API (Check-in)	5. Arrival: Entry	6 Intra-Schengen Travel	7. Irregular entry or stay	8. Intl. Protect. /Resettlement Transfer	9. L/S visas or residence permit/card	10. Departure: PNR, API, Exit
Decisions	Issue, refuse, revoke or annul Schengen Visas or Travel Authorization Resolution of MultID cases	Issue Registered Traveller Card or Pass / Issue, refuse, revoke LBT Permit	No decision required. Issue an alert on a traveller	Eu-LISA Carrier gateway 'Ok' or 'not Ok' response for TCNs. Alert on a traveller for the border control process	Entry, refusal, revoke or annul Schengen visa or ETIAS Issue visa at border, invalidate document, detain person resolution of MultID cases	No decision required. Exceptional decision to restrict free movement. Issue an alert on a traveller (PNR).	Put TCNs in detention, Issue return decision or refusal of entry or stay (SIS), Referral of vulnerable TCN. Resolution of MultID cases	Decide on the responsible MS (take charge / take back) Decide on International Protection granted, rejected, withdrawn. Resolution of MultID cases	Issue, refuse, extend or withdraw Residence Permit or Long-stay visas, Resolution of MultID cases	Decide on exit, detention, revoke or annul Schengen visa or ETIAS, issue entry ban, Resolution of MultID cases
Responsible authorities	Visa authorities or VIS DA / ETIAS CU and ETIAS NUs	Airport or Border Management Authorities / Consular or Administrative Authorities (application)	PIUs	PIUs Border Management Authorities (API Centres)	Border Management Authorities Customs	Public order Police authorities (free movement). PIUs (PNR)	Border/Migration Management Authorities	Asylum Authorities Dublin Unit.	Migration and Visa Authorities or VIS DAs	Border Management Authorities (API Centre) PIUs Customs
Other authorities involved	Other MS visa authorities or VIS DAs / Other MS ETIAS NUs	Border Management Authorities and TC authorities (LBT)	National (crime-related) Competent Authorities, Other MS PIUs, Europol,	ILO/ALOs	Customs SIRENE Bureaux. Europol Frontex	Other MS public order or police authorities including SIRENE (Free	Migration or Asylum Authorities from the same or other MS (Eurodac) Other	Other MS Asylum Authorities or Dublin Units. Visa or Migration Services (VIS). EASO	Other MS visa or immigration authorities or VIS DAs and Europol. Other MS Migration	Customs SIRENE Bureaux Europol Frontex

Steps	1. Pre-depart.: Short-stay Visa/ETIAS	2. Pre-depart.: Facilitation NFP/LBT	3. Pre-arrival: PNR (Push)	4. Pre-arrival: API (Check-in)	5. Arrival: Entry	6 Intra-Schengen Travel	7. Irregular entry or stay	8. Intl. Protect. /Resettlement Transfer	9. L/S visas or residence permit/card	10. Departure: PNR, API, Exit
	Europol Frontex (ETIAS CU) SIRENE Bureau.		customs			Movement). Other MS PIUs, Europol, customs or other National (crime-related) Competent Authorities	Migration or Schengen visa authorities, SIRENE Bureau, Frontex	UNHCR, IOM	authorities via SIRENE Bureau.	
Commercial or private actors	External Service Providers (VIS), Third party submitting ETIAS / Schengen Visa application on behalf of the traveller	Airport Authorities (RTP)	Carriers, travel booking companies	Carriers	Transport authorities or Operators Carriers	Carriers or travel booking companies (API/PNR)	Private individuals or companies (Smuggling networks)			Transport authorities or Operators. Carriers, travel booking companies

3.2. The 10 steps of the border and travel continuum

The description of these steps takes into account and makes reference to existing as well as proposed EU legal instruments, but in no way prejudges the outcome of the on-going legislative procedures. The proposed legal framework includes the VIS revision, recent Eurodac recast and TCN Screening Regulation, which are both part of the recent Commission Immigration and Asylum Pact, ETIAS consequential amendments proposals and Commission mandate for the negotiation of an EU-Interpol Agreement.

Step 1: Short-stay visas and Travel Authorisations (Pre-departure)

Short-stay visas

The processing and issuance of short-stay visas is primarily regulated in the EU Visa Code[3], including the applicable procedures and conditions. The VIS Regulation[4] establishes a system for storing and exchanging information between MS on Schengen visas. The revision of the VIS Regulation[5] is being finalised.

The list of countries whose nationals require a Schengen visa is set out in the Visa Regulation[6]. Amendments of the 'visa lists' of countries are based on different criteria relating among others to illegal immigration, public policy and security.

The issuance of a Schengen visa is supported by the VIS, which is connected to the national visa systems through which the national consular or visa authorities input the relevant applicant data and decisions taken on Schengen visa applications.

The processing of Schengen visa applications implies i.a. the processing of the TCN's ID/TD data, biometrics, residence and profession of the applicant.

Currently, visa applications are only screened against a subset of SIS data and national DBs, and a biometric check is made in the VIS itself. The VIS revision will allow users to make full use of the interoperability components so that Schengen visa applicants are checked more thoroughly against the SIS and also against EES, ETIAS including its watchlist, Eurodac, ECRIS-TCN, Europol data and Interpol SLTD/TDAWN.

The VIS revision also foresees an automatic check of the visa applicant's TD against a list of valid travel documents recognised for crossing the external borders to be integrated into the VIS.

---

3 Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code).

4 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).

5 Proposal COM (2018) 302 final for a Regulation amending Reg. (EC) No 767/2008, Reg. (EC) No 810/2009, Reg. (EU) 2017/2226, Reg. (EU) 2016/399, Reg. XX/2018 [Interoperability Reg.], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA.

6 Regulation (EU) 2018/1806 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement.

Risk management in the context of the visa process is mainly done by the MS individually in consulates and/or at central level. The VIS revision establishes an EU risk management framework similar to the one in ETIAS to be implemented by the ETIAS CU with the support of a VIS screening board where the MS and Europol will participate. Specific risk indicators on illegal immigration, security or risk to public health are to be introduced in the VIS for Schengen visa processing.

The queries against sensitive categories of records in SIS, Europol or the future ETIAS watchlist proposed in the VIS revision enables more effective use of law enforcement data in a preventive manner, in particular by avoiding the issuance of visas to suspects and convicts of serious crime and terrorism. Where visa applications and issued visas relate to on-going criminal investigations, the revised legal instrument may provide opportunities for gathering criminal intelligence on suspects by the competent national authorities and Europol to support those criminal investigations. The current VIS Law Enforcement Decision[7] already allows access to VIS data for law enforcement purposes under strict conditions.

Consular or other competent national authorities or VIS DAs, depending on the sensitivity of the case, take decisions on issuing (length of validity and number of allowed entries) or refusing visas. Decisions on the annulment, revocation or extension of visas are generally taken by the various national authorities in the MS, including border management authorities. These decisions are stored in the VIS.

In addition, due to the new Interoperability Regulations[8], consular or other competent visa authorities will be required to take decisions related to MultID cases which have been identified as a consequence of the biographic and biometric data enrolment of Schengen visa applicants.

Prior consultation of other MS during the visa application is already foreseen in the current EU Visa Code. Such prior consultation may concern nationals of specific TCs or specific categories of such nationals. However, consultation between the VIS DAs or other competent national authorities for the purpose of issuing visas will be reinforced by the proposed VIS revision. The consultation may also include Europol when a match against Europol data is obtained or ETIAS NU when there is a hit against the ETIAS watchlist.

Notification to a SIRENE Bureau in case of a hit against SIS alerts is also required and authorities having issued the alert are also informed.

The VIS review also foresees Frontex (EBCG Team Members, future Standing Corps members) access to VIS for border control purposes to support MS in the context of its deployments at the EU external borders.

External private actors, such as the service providers, collect visa applications for the MS, including the enrolment of biographic and biometric data, but these service providers do not have access to the VIS.

---

[7] 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.

[8] Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa; Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.

Electronic Travel Authorisations

The issuance of electronic travel authorisations through the new ETIAS is an important measure to reinforce external border controls. It will allow an advance assessment of whether the presence of a visa-exempted TCN in the Schengen area poses a security, irregular migration and public health risk and whether a travel authorisation should be denied. The obligations and conditions for obtaining the electronic travel authorisations and the IT system itself are regulated in the ETIAS Regulation[9].

ETIAS will be the system used for processing electronic travel authorisation applications. It will be an end-to-end system, with no additional national ETIAS system required for processing travel authorisation applications. The ETIAS Central System will provide the end-user application for ETIAS NUs and ETIAS CU staff.

ETIAS travel authorisations will imply online submission of ID and TD data as well as other background information (e.g. residence, education, profession) by the visa-exempted TCN.

Subject to the adoption of ETIAS consequential amendments[10], ETIAS will make full use of the interoperability components as soon as it is operational, namely the ESP for checking ETIAS applications against SIS, EES, VIS, Eurodac, ECRIS-TCN, Europol data and Interpol SLTD/TDAWN. The checks in the Interpol DBs are subject to a prior successful conclusion of an EU-Interpol International Agreement. In addition, within the ETIAS Central System itself the travel applications are cross-checked against the ETIAS watchlist.

ETIAS applications will also be checked against screening rules on irregular migration, security and public health. These rules will be prepared by Frontex (ETIAS CU) in consultation with the MS and Europol in a screening board and subject to consultation with a Fundamental Rights Guidance Board.

As for the envisaged visa process, queries against sensitive categories of records in SIS, Europol or the future ETIAS watchlist enable more effective use of law enforcement data in a preventive manner. Vice versa, ETIAS application data provide opportunities for competent national authorities and Europol to gather information on suspects in order to support criminal investigations. The ETIAS Regulation also allows access to ETIAS data for law enforcement purposes under strict conditions.

Decisions regarding travel authorisation applications will be to a very large extent positive and automatically issued to the TCN. Where human intervention is required, leading to a decision to refuse, annul or revoke a travel authorisation application, the ETIAS CU will perform in most cases the initial manual processing (verification whether the identity of the applicant corresponds with the data that triggered the hit, except for watchlist entries), but the decision to refuse or revoke the travel authorisation can only be taken by the competent ETIAS NU. The decisions to issue, refuse, annul or revoke the travel authorisation application are to be stored in ETIAS which will provide, therefore, the status of the visa-exempted TCN.

The decision-making process includes consultation between the competent ETIAS NU with other ETIAS NUs or Europol depending on the result of the cross-checking of other databases. In case of SIS hits, the SIRENE Bureau shall be notified and, for certain sensitive categories of SIS alerts, the SIRENE Bureau must ensure the follow-up.

---

9 Regulation (EU) 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS) and Regulation (EU) 2018/1241 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS).

10 Proposal COM (2019) 4 final for a Regulation establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Reg. (EU) 2018/1240, Reg. (EC) No 767/2008, Reg. (EU) 2017/2226 and Reg. (EU) 2018/1861.

In addition, the ETIAS CU or NUs might be required to take decisions related to MID cases as a consequence of new ETIAS applications with different identities but identical travel document in accordance with the Interoperability Regulations.

It is important to note the responsibility of the traveller, who must be aware of the new obligation of having an ETIAS travel authorisation in advance and also because the traveller will have to submit his/her data online via the dedicated online application form. This makes ETIAS an exceptional case among the EU information systems.

Step 2: Facilitation - RTP and LBT regimes (Pre-departure)

This step includes the programmes or regimes which facilitate the crossing of the EU external borders by a TCNs. The facilitated (rail) transit documents are not primarily intended for this purpose and is therefore excluded from the analysis.

Registered Traveller Programme or National Facilitation Programme

An EU RTP legislative proposal as part of the Smart Borders Package was initially proposed but later withdrawn by the Commission. The current national/airport based RTPs are not regulated in EU law but must comply with the rules of the SBC[11].

The requirements regarding RTPs (NFPs) are established in the amended SBC[12] which will only apply as from the date on which the EES becomes operational[13].

An RTP may lead to an agreement with a particular Third Country to provide for eligibility of the programme to their nationals who may also use e-gates. The beneficiaries of existing RTPs are exclusively TCNs who are frequent travellers using specific international airports. EU citizens or other nationals benefiting from free movement do not have to register to use an e-gate.

The enrolment into the Programme is supported by a specific RTP Register. The relevant TD data will be processed and stored in the register and queried to use the e-gate. The EES shall also include an attribute in the TCN traveller file about the NFP from which the TCN benefits. The TCN member of an RTP/NFP, once enrolled in the EES and after verification in the self-service-kiosk, should be able to use the e-gate.

SIS and relevant national databases are checked as part of the screening process of the candidate to become a member of the programme. The EES must also be searched to check whether the TCN applying for a national facilitation programme has exceeded the authorised stay or was refused entry.

The EES Regulation establishes that the first access to the national facilitation programme shall be granted for a maximum of one year. The decision to issue the pass or card by the Border Management Authorities or Airport Authorities in cooperation with the competent law enforcement authorities may also be revoked in case the member no longer fulfils the criteria. The member of the RTP programme must be in any case subject to border checks in accordance with the SBC when crossing the external borders.

RTPs might be established in close cooperation and association with the relevant airport authorities, which provide the enrolment facilities, and which may also provide for expedited security checks, apart from facilitating the border crossing.

---

11 Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

12 Regulation (EU) 2017/2225 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

13 Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES).

Local Border Traffic Regime

The LBT Regime is regulated by LBT Regulation[14]. This legal framework is completed by the relevant Bilateral International Agreements concluded between the EU MS and neighbouring Third Country.

The beneficiaries of the LBT Regime are those residing in a clearly demarcated border area for facilitating their crossing of the external border through designated BCPs.

The LBT Regulation sets out the obligation for the MS to establish a central register for LBT permits which must include permit applications as well as issued, extended, cancelled or revoked permits. In this register the MS will store relevant ID/TD data including residence data. The MS must check the applicant against SIS and national DBs prior to issuing the permit.

The Commission included the LBT permits in the initial scope of the feasibility study of the new VIS, but it was later discarded. Holders of LBT permits are excluded from the scope of the EES Regulation and, therefore, not subject to registration in the EES.

Consular authorities or other designated administrative authorities are responsible for examining the LBT application and issuing the permit. No consultation of other authorities is foreseen according to the LBT Regulation. There is potential for cooperation with TCs for the screening of their nationals when applying for an LBT permit.

Border Management Authorities also play a role in the management of the designated BCPs that holders of an LBT permit can use.

Step 3: PNR data push (Pre-arrival)

The EU **PNR** Directive[15] and national legislation transposing the Directive regulate the transfer by carriers of PNR data to the MS and the conditions for its processing by the national competent authorities and Europol. The WCO, IATA and ICAO have also established guidelines or recommended practices for the collection and transmission of PNR data.

All travellers (EU citizens/residents and TCNs) travelling on an EU inbound or outbound flight as well as intra-EU flights (when foreseen in national legislation) are affected by the EU PNR Directive. ID/TD data, itinerary, booking, co-travellers, seat number, luggage information, ticket number, travel agent and payment means (if available in the reservation) are the main PNR data processed in the national PNR system. Certain data fields of API data can be added as a subset of PNR data.

The PNR Directive foresees in Article 6(3)(a) the possibility for PNR data to be checked against databases for the purpose of preventing, detecting, investigating and prosecuting terrorism and serious crime. These databases are not stipulated in the Directive but Passenger Information Units (PIUs) may query (screen) PNR data against SIS, Interpol and national DBs and may also perform queries against Europol data.

Risk profiles (rule-based targeting) may be applied during the automated processing of PNR data in the form of (inter)national and specific targeting rules or watchlists.

---

14 Regulation (EC) No 1931/2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention.

15 Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

PNR data are processed primarily for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and are stored and exchanged in accordance with the conditions of the aforementioned Directive and national transposing legislation.

This step of the travel border continuum, reservation, does not require any sort of formal decision by an official authority.

PIUs are the responsible authorities for processing PNR data and may issue an alert on an individual for border management or airport security authorities and also for relevant competent authorities responsible for the prevention, investigation and prosecution of serious crime and terrorism. These alerts may lead to a more thorough border check, preventive action, (covert) data collection or arrest at the airport.

The responsible PIU may exchange PNR data with other PIUs, Europol or other national competent authorities responsible for the fight against crime and terrorism. Relevant national competent authorities, including customs, as well as intelligence services may also be represented in the PIU.

The operational running of the PNR regime relies heavily on the role of commercial actors such as carriers or travel agencies, which provide the PNR from the traveller to the national PIU. This process is facilitated via specific bilateral agreements or arrangements concluded between the commercial actor and the PIU.

Step 4: Check-in or boarding (Pre-arrival)

The legal provisions regarding the transmission of **API** data at check-in or boarding by the air carrier to the competent national authorities are established in the API Directive[16] and national transposing legislation. The SBC also establishes the possibility of systematic checks against EU databases to be carried out in advance with API data.

The implementation of the Directive has been evaluated by the Commission and new legislation on API is to be proposed in 2021. The WCO, IATA and ICAO have also jointly established international standards for the transmission of API data.

For general aviation, namely private flights, the SBC includes an obligation for the captain to prepare a declaration with information concerning the passengers' identity.

In the maritime domain there is International Law, e.g. FAL Convention, as well as Union legislation establishing reporting obligations for maritime operators, e.g. the SBC (Annex VI), under which passenger and crew lists must be communicated by the master of the ship (or any person duly authorised) to the border guards before arriving in the port. This information is transmitted electronically to a national Single Maritime Window[17]. A European Single Maritime Window is to be implemented by the MS by 2025. For pleasure boats the SBC also establishes in specific circumstances an obligation to deliver a declaration regarding persons on board.

The ILO Regulation[18], which aims at reinforcing cooperation, coordination and exchange of information among ILOs deployed to non-EU countries, is also of relevance in this context.

All travellers, including EU citizens and TCNs arriving by air to the Schengen Area, fall within the scope of the API Directive. A few MS also collect API data for Schengen-outbound flights. The collection of API data is not required for intra-Schengen flights, but it is being considered as a potentially valuable addition to the current collection of advance passenger information.

National border management authorities are recipients of the API data and responsible for their processing, which may lead to an alert issued on a particular traveller for the border control process.

API data are processed in national API systems. Several MS use a single window which processes both API and PNR data within the respective purpose limitations, and their PIUs use elements of the API data as a subset of PNR data.

Carriers process and submit travellers' ID and TD data, travel date and time, place of departure and arrival (BCP) and carrier-related information, including flights number, to the national border management authorities, which can store them for a very limited time (24 hours) to support the border control process.

API data may be cross-checked against SIS and (inter)national DBs prior to the arrival of the traveller at the BCP. Some MS also apply national or local (BCP level) targeting rules for automated API data processing to identify travellers who may pose a risk.

---

16 Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API data).

17 Regulation 2019/1239 establishing a Single Maritime Window and replacing the Reporting Formalities Directive. (This Regulation is not reflected in Annex 1 because it does not establish any new or specific access rights to personal data. Instead, it relies on the already existing mechanism in which access is granted under the national schemes and rules of the individual Member States.)

18 Regulation (EU) 2019/1240 on the creation of a European network of immigration liaison officers.

The API Directive does not regulate access for law enforcement purposes, but leaves this option open for the MS to implement this through national legislation. The short retention period of in principle 24 hours limits the potential of API data for the purpose of border control. The data retention for law enforcement purposes is subject to national law and, to the extent it is incorporated within the PNR data, to the provisions of the EU PNR Directive and the related national transposition.

The API Directive has not established an interactive API system, requiring national border management authorities to provide a 'board' or 'no board' message or decision to the carriers. However, the EES, ETIAS and the proposed VIS Regulation provide de facto for such mechanism in which the carrier (air, sea, coach, but not trains) has to perform a query through a dedicated gateway for TCNs in order to receive an 'ok' or 'not ok' message.

ILOs or ALOs can also play an important role because they can be present in-situ at departure hubs for the Schengen Area and among their tasks they must provide support to carriers during the check-in phase on questions related to documentation or more generally regarding admissibility of the TCN into the Schengen Area.

Carriers are critical actors for this stage of the continuum since they need to perform during check-in or boarding a verification based on a valid travel document that ID data of the traveller match those of the reservation, and transmit the API data to the national border management authorities at the destination.

In accordance with the abovementioned EES, ETIAS and proposed VIS revision Regulations and by using a specific gateway, carriers must perform a first electronic admissibility check for the TCN to enter into the Schengen Area, which does not preclude the final decision by the border management authority. This check will allow the carrier to know whether the TCN has a valid Schengen visa, travel authorisation or national residence document, e.g. residence permit or long-stay visa, which is of relevance for permitting passengers to board.

Step 5. Arrival: Entry

The SBC (Schengen Border Code) establishes the rules that apply on persons for **crossing the external borders**, including conditions to enter into the Schengen Area. The legal framework is also composed of the EES Regulation and of amendments to the SBC as regards the use of the EES at the external borders, which together establish the rules for registering entries, exits and refusals of entries of TCNs at the EU external borders. The ETIAS and VIS Regulations are also amending the SBC which will apply as from the entry into operation of the respective systems.

All travellers (EU citizens and TCNs) are subject to border checks. TCNs are subject to registration and verification in the EES unless one of the exemptions foreseen in the EES Regulation is applicable.

MS have their own national border control systems and applications, which must be connected to several other EU, national and international information systems and databases. Particularly important will be the interface of the national systems with the EES, which will connect also to ETIAS and VIS for checking the entry conditions of the TCN into the Schengen Area, including possible flags and related notifications on expected arrivals.

All travellers (EU Citizens and TCNs) should be checked against relevant EU and international databases on entry and exit as required in the SBC as amended by the 'Systematic Checks Regulation'[19], which implies also electronic processing of their ID and TD data. TCNs are

[19] Regulation (EU) 2017/458 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders.

furthermore subject to the collection and registration of their ID and TD data, including facial image and fingerprints in the EES. This also includes the recording of the place and time of entry and allowed duration of stay for the TCN in the Schengen Area. Registration or verification of TCNs in the EES should also lead to queries in the VIS or ETIAS, depending on whether it is a visa holder or visa-exempted traveller.

The implementation of the Interoperability Regulation and particularly the use of the ESP, CIR and SBMS allows for the simultaneous search of the TCN in multiple systems (SIS, VIS, Eurodac, ECRIS-TCN, EES and ETIAS) allowing the detection of multiple identities and possible abuse cases. However, the legal framework for accessing or making use of these systems for the purpose of border checks is not affected by the Interoperability Regulations, but remains specified in the individual legal instruments regulating these systems.

The FADO system, of which the functionalities will be reinforced by the new FADO Regulation[20], is also part of the border management information ecosystem.

Risk management in view of border checks is performed by the border guards, where possible with the support of advance information and by observation or raising specific questions to the travellers during the border check, including as part of the EES registration via a self-service system. The risk profiles and indicators are developed and implemented at national or local level. Frontex and Europol together with the Commission have developed joint risks indicators for FTFs in the form a booklet.

Border Management authorities will decide on entry, refusal (only for TCNs) or referral to second line, of the traveller. In case of a TCN, entry or refusal decisions will be stored in the EES providing also the status of the TCN and the remaining period of her/his valid stay. Border Guards or Border Police officers can also decide to issue a Schengen visa or revoke the visa as a consequence of a refusal of entry. A refusal of entry of a TCN in possession of a valid travel authorisation should also lead to the re-examination of the travel authorisation by the competent ETIAS NU.

Border officers may also face cases of MultID generated due to biometric enrolment of a TCN in the EES in accordance with the MID process established under Interoperability Regulations and may also proceed to invalidate a travel document.

In the event of a SIS hit, there must be a notification to the SIRENE Bureau from the BCP or Border Management Authority which must collect the required information, as foreseen in the relevant SIRENE form. This may lead to a consultation with the authorities of another MS responsible for issuing the alert in accordance with the SIRENE Manual.

The Commission proposal[21] allowing Europol to issue 'information alerts' on suspects and criminals as a new alert category in SIS is also of relevance here. This may trigger a communication from the frontline officer (e.g. border guard) via the national SIRENE Bureau to Europol to determine whether further measures are to be taken apart from informing that the person was located and checked.

Frontex may support national border management authorities during border checks, in particular through deployments at specific BCPs of EBCG Team Members (future Standing Corps).

---

20 Regulation (EU) 2020/493 of the European Parliament and of the Council of 30 March 2020 on the False and Authentic Documents Online (FADO) system and repealing Council Joint Action 98/700/JHA.

21 Proposal COM (2020) 791 amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol.

Airport or other transport authorities and even carriers, e.g. cruise ship companies, play an important role when they have to provide the infrastructure for the border control booths and the new biometric enrolment devices and equipment required for the EES, such as self-services systems, kiosks or automated border control systems.

Carriers have the obligation to return to their original destination those TCNs who have been refused entry at the external borders in accordance with the Carriers' Liability Directive[22], which supplement Article 26 of the CISA.

Step 6: Intra-Schengen Travel

Intra-Schengen travel, including the right of free movement, is laid down in the EU Treaties, Charter of Fundamental Rights and regulated in the EU Free Movement Directive[23]. The SBC, which as a rule abolishes systematic internal border controls, also comes into play here. This applies not only to EU citizens and family members enjoying the right of free movement under the EU Treaties (Residence Card holders) but also to TCNs who are holders of a long-stay (national) visa or residence permit. Other TCNs who come to visit the Schengen Area and fulfil the conditions for crossing the external borders can also travel freely in the Schengen Area during the allowed period of stay.

There are neither EU nor national information systems which underpin intra-Schengen Travel. However, 22 EU MS apply the EU PNR Directive for intra-EU flights, meaning that their national PIUs collect and process data from individuals travelling within the EU (which does not entirely correspond to the Schengen Area).

The processing of PNR data for intra-EU flights allows the PIUs as responsible authorities to issue an alert on an individual for police or airport security authorities and national crime authorities. Such alerts may lead to law enforcement intervention including a preventive action or arrest at an international airport.

The possibilities and conditions for the processing of (API)/PNR data were presented under process step 3: PNR (Push).

Intra-Schengen travel is not subject to any check or formal decision by any authority. However, free movement and travel within the Schengen Area might be limited by an MS decision to reintroduce internal border controls in accordance with the SBC. In case of internal border controls reintroduced in accordance with the SBC, MS may also request API data to carry out advance checks.

Besides, the Interoperability Regulation in particular by means of the CIR (Central ID Repository) allows for identity checks of TCNs travelling within the Schengen Area under certain conditions and subject to national law.

---

22 Council Directive 2001/51/EC supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985.

23 Directive 2004/58/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States.

In exceptional cases, national competent authorities may restrict the right of entry (or residence) of a person enjoying the right of free movement on grounds of public policy, public security or public health. The assessment of the two first grounds may require, if considered essential, to examine if the person has any police record in other MS. The formal decision to restrict the right of free movement will prevent the issuance of the registration certificate or residence card, and lead to the expulsion of that person from the territory of the MS. The SIS legal framework also includes specific rules and procedures when issuing an alert for refusal of entry or stay to a TCN benefitting from the right to free movement.

Step 7. Irregular Entry or Stay

Although irregular entry should theoretically be part of the 'arrival' phase in the continuum, all the activities and decisions linked to the processing of an irregular migrant must be done under the jurisdiction of a MS which is triggered by the fact that the TCN is de facto already on the territory of that MS and can be subsumed under the 'stay' phase.

There are several pieces of EU legislation that either regulate or are related to irregular entry or stay of a TCN in the EU. The Return Directive[24] establishes rules including procedures and safeguards for the return of TCNs.[25] The SBC includes rules on border surveillance to prevent irregular entry into the Schengen Area and also ensures at the same time that TCNs apprehended while crossing irregularly the external border have the possibility to request international protection. The Eurodac Regulation[26] and in particular the proposed Eurodac Recast[27] and screening of TCNs at the external borders Regulations[28] will become essential pieces of EU legislation for processing data from TCNs who have entered or are staying irregularly in the EU, while the SIS Recast Regulations[29] dealing with borders and return completes the legal framework for the introduction of SIS alerts on refusals of entry or stay and on return decisions.

This step concerns only TCNs who do not fulfil the conditions for entry, stay or residence within the territory of a MS, including those apprehended crossing illegally the external border and may be subject to a return decision.

---

24 Directive 2008/115/EC on common standards and procedures in Member States for returning illegally staying third-country nationals.

25 Proposal COM (2018) 634 for a recast Return Directive.

26 Regulation (EU) No 603/2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 (Dublin Regulation).

27 Proposal COM(2020) 614 on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or 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 Regulations (EU) 2018/1240 and (EU) 2019/818.

28 Proposal COM (2020) 612 introducing a screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817.

29 Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals and Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks.

MS must have their own national systems (e.g. national biometric DB) to store data from the TCNs who have crossed illegally the EU external border or are staying irregularly in a MS or have been disembarked following a SAR operation in order to feed into the Eurodac system. The Eurodac Recast Regulation enlarges the scope of the Eurodac system since it will allow for the introduction of biographic data (e.g. ID and TD data) apart from biometric data. It must also store data from TCNs found staying illegally in a MS apart from those who have crossed irregularly the external border.

MS will also use their national systems for recording entry bans that will generate refusal of entry or stay in the SIS and national return case management systems (RECAMAS) that will lead to the issuing of a return decision and corresponding alert in the SIS.

Both systems, SIS and the proposed new Eurodac, will store TCNs ID and TD data, as well as facial image and biometrics. The SIS will also contain details about the national decisions on refusals of entry or return applied to TCNs, while Eurodac contains information regarding the MS of origin and place and date of apprehension. In case the TCN has left or has been removed, the TCN record in Eurodac has to be updated in line with the proposed Eurodac Recast Regulation.

According to the Eurodac Recast Regulation, any new Eurodac record for these two categories of TCNs will be searched against the rest of Eurodac records.

There are, however, Council conclusions from 2017 with recommendations on security database checks for irregular migrants which include SIS, VIS, Europol data, Interpol (Nominal, SLTD, FTFs, AFIS, TDAWN) as well as national investigative DBs and AFIS (biometric) systems. The recent proposal of screening TCNs at the external borders will introduce two mandatory processes which are of relevance in this context. The identification of the TCNs against the CIR based on EES, ETIAS, VIS, Eurodac and ECRIS-TCN ID data and standard security checks that include SIS, EES, ETIAS, VIS, Europol, Interpol SLTD/TDAWN and ECRIS-TCN.

The Eurodac Regulation, including Eurodac Recast Regulation, foresees access to Eurodac data for law enforcement purposes under strict conditions.

The SIS Recast establishes that a new alert on refusal of entry or return of the TCN requires a check whether the person has a valid long-stay visa or residence permit. This may trigger a consultation via SIRENE with the competent migration service which issued these documents.

The VIS, EES and ETIAS Regulations also foresee access to these three EU information systems for migration or border management authorities in order to identify and determine whether the TCN fulfils the conditions for entering or staying on the territory of the MS, which may lead to a return decision.

The competent national border or migration management authority responsible for the apprehension of the TCN can take different decisions which can include keeping the person in detention, issuing a return decision in some cases accompanied by an entry ban, defining a voluntary departure period and even proceeding with the removal.

In case the TCN has requested or requires protection, these authorities may also refer the person to the competent asylum authority or other public services or organisations responsible for vulnerable persons, in particular minors.

National authorities responsible for the introduction of a new record in the proposed Eurodac (which will contain also biographic data subject to the adoption of the recast proposal) or in the SIS may also have to deal with MultID cases in accordance with the Interoperability Regulations.

Consultation or more generally the interaction between asylum and migration services of the same MS or with other MS will be more frequent and complex as a result of the proposed Eurodac Recast Regulation. The introduction in Eurodac of a new record of a TCN having crossed irregularly the border or staying illegally may trigger a hit against the same categories of data stored by the same MS or other MS, which should assist in the identification and possible return procedure. However, the hit may also provide information on whether TCN has applied for or been granted international protection or was issued residence documents (marking of data).

Frontex supports the MS in the detection and identification of TCNs having crossed irregularly the external borders. The Eurodac Recast proposes Frontex (EBCG Team Members, future Standing Corps Members) access to Eurodac to transmit records of TCNs to support MS in the context of its deployments at the EU external borders.

The illegal entry, transit or residence of TCNs might be facilitated by smuggling networks consisting of private individuals or companies. These private actors might be subject to criminal sanctions according to the relevant EU legislative acts[30] and national transposing legislation.

Step 8. International Protection including resettlement or admission procedure

The presentation of the Commission's Pact on Asylum and Migration at the end of 2020 entails fundamental changes for the Common European Asylum System (CEAS). In particular, the proposal for a new Regulation on Asylum and Migration Management replacing the current Dublin Regulation, as well as modifications to EURODAC and the Asylum Procedures Regulation relaunches the reform of the CEAS through the establishment of a common framework that contributes to the comprehensive approach to migration management.

This step would apply to TCNs applying for or benefiting from an international protection status, including those in the process of relocation between MS and subject to admission or resettlement procedures into an EU MS from a third country.

MS have their national asylum case management information systems to process applications. These systems need to be connected to Eurodac in order to ensure exchange of information among MS. Currently, Dublinet supports the bilateral exchange of information between national Dublin Units / Asylum services to deal with individual cases regarding the responsibility and requests of MS for taking charge of or taking back applicants for international protection.

[30] Council Directive 2002/90/EC defining the facilitation of unauthorised entry, transit and residence; Council Framework Decision 2002/946/JHA on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence; Council Decision 2006/616/EC on the conclusion, on behalf of the European Community, of the Protocol Against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention Against Transnational Organised Crime.

According to the proposed Eurodac Recast Regulation, MS are to introduce ID and, where available, TD data as well as the biometrics (fingerprints and facial image) of the applicant for International Protection. The MS responsible, in accordance with Dublin Regulation or the shift of responsibility in accordance with the proposed new Regulation on Asylum and Migration Management, the date of arrival and date of the decision on international protection and whether the person is granted international or national humanitarian protection are also data to be added in the Eurodac file.

New records on International Protection Applicants are cross-checked against other existing Eurodac records for the purpose of determining which MS is responsible and prevent 'asylum shopping'.

A search in the VIS by the competent national Dublin Unit or asylum service is foreseen in the VIS legislation for the purpose of determining the responsibility of the MS. This allows the officer in the asylum service to see if the TCN has applied for or been granted a short-stay visa and in the future it will also allow the officer to see if applicants possess a long-stay visa or residence permit (VIS revision). The results of the security checks to be performed according to the proposed TCN screening regulation also need to be flagged in the new Eurodac.

Access to Eurodac data for law enforcement purposes is included in the current Eurodac Regulation and will be slightly reinforced in the Eurodac Recast proposal.

The competent national asylum authorities, in particular the Dublin Unit, shall decide on MS' responsibilities, including the issuing of 'take charge' or 'take back' requests to another MS and transfers. Asylum Authorities decide on the International Protection application which might be granted, rejected or withdrawn and on the concrete status awarded to the TCN.

National authorities responsible for the introduction of a new record in the proposed new Eurodac, which will contain biographic data, may also have to deal with MultID cases in accordance with the Interoperability Regulations.

Other authorities to be involved include the Dublin Unit and Asylum Services from other MS as follow-up to hits in Eurodac or Migration or Visa Services, in case the International Protection applicant is found in the VIS.

EASO supports the MS in asylum procedures and decision-making, including the registration of applications and preparation of decisions. The Eurodac Recast proposes that EASO asylum expert teams and EBCG team members should have access to Eurodac to gather and transmit all TCN data in the context of their operational deployments on behalf of the host MS.

Step 9. Long-stay visas, residence permits and residence cards

The procedures and conditions for issuing national long-stay visas or residence permits and residence cards are covered by national legislation and several EU Directives. The CISA and SBC refer to them as valid documents for crossing the external borders and/or moving within the Schengen Area. A uniform format for residence permits, including technical specifications, has been laid down by an EU Regulation[31] while another EU Regulation[32] laying down a uniform format for Schengen visas is also applicable to long-stay (national) visas. The VIS revision proposes to extend the scope of the VIS in order to include long-stay visas and residence permits, but not residence cards.

The procedure and conditions for issuing residence cards to family members of Union citizens is laid down in the EU Free Movement Directive while the Regulation strengthening the security of identity cards of Union citizens and of residence documents [33] establishes the minimum security features and integration of biometric data in residence cards.

MS rely on their national or regional migration or visa systems for processing applications and issuing these documents. The national systems must be connected to the future VIS to ensure that these national documents are stored and exchanged with other Schengen States.

In accordance with the proposed VIS revision, MS must process the applicant's ID/TD data, biometrics (facial image and fingerprints). The decision on the application, the place and date of the decision, expiry date, status and type of document (residence permit or long-stay visa) issued will be added in VIS.

The creation of a file following a new application before the competent national authorities will entail queries against VIS, SIS, EES, ETIAS (including the ETIAS watchlist), Europol data, ECRIS-TCN and SLTD and TDAWN.

The queries against sensitive categories of records in SIS, Europol or the future ETIAS watchlist of long-stay visas and residence permits enables law enforcement data to be used preventively by enabling the refusal of requests from applicants who pose a threat. Vice versa, the possibilities for law enforcement to access the available records under strict conditions provide opportunities for the gathering of intelligence on suspects by competent national authorities and Europol to support criminal investigations. The VIS Regulation also foresees access to VIS data for law enforcement purposes.

The migration or consular authorities are competent for the issuing of these national documents. These authorities may issue or refuse the application; they can also extend the validity of the permit or visa or withdraw it. The VIS DAs also play a role when the processing of applicant data generates hits against other information systems.

Other authorities involved in the decision making process according to the proposed VIS revision can be the VIS DAs of other MS or Europol, based on the result of the hits generated by the new application.

---

31 Regulation (EU) 2017/1954 amending Council regulation (EC) Nº1030/2002 laying down a uniform format for residence permits for third-country nationals.

32 Regulation (EU) 2017/1370 amending Council Regulation (EC) No 1683/95 laying down a uniform format for visas.

33 Regulation (EU) 2019/1157 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

The SIRENE Bureau should also be involved in order to ensure consultation with the MS competent authorities which issued an alert on return or refusal of entry of the TCNs prior to granting or extending the residence permit or long-stay visa according to the SIS Recast.

Step 10. Departure: PNR, API and Exit

The description provided in the pre-arrival stage, namely steps 3 and 4 (PNR and API) and arrival in step 5 are also largely valid for the departure step. It may be interesting here to merely draw attention to some legal particularities:

- The API Directive establishes only the obligation for the air carriers to submit data on Schengen inbound travellers, but the MS can also request the air carriers to submit API data for Schengen outbound trips.
- There is no such differentiation, i.e. arriving or departing flights, for the processing of PNR data in the PNR Directive.
- Border checks for TCNs at exit are less stringent than at entry since entry conditions established at SBC are not to be verified.

4. Analysis and conclusions from the EU border and travel continuum

4.1. Strategic dimension

Understanding the continuum

As explained earlier, the 10 steps composing this continuum fall under the responsibility of different national authorities and are regulated by different sectorial legislation. The risk, therefore, that the various competent authorities operate in silos is very high.

It is essential that all these authorities, either competent or involved in the decision-making process for each step, gradually develop a common understanding of being actors in this border and travel continuum and are, therefore, interconnected. These authorities remain responsible for their particular step in the continuum, but their decisions or actions are also part of an overarching set of measures related to the management of international mobility. The new or enhanced EU information systems, including their interoperability, are an important enabler to understanding this continuum, but those are by no means sufficient as such to make it work in a coherent and integrated manner.

It is essential that the different authorities deciding on individuals arriving, visiting, travelling or staying in the Schengen Area are able to learn of and from each other's decisions and assessments made, and not only from data collected at different steps of the continuum. These authorities are very often dealing with the same person, or group of persons, just at different moments in time. It is also vital that those in the frontline (e.g. border guards, visa, migration or asylum officers) can factor properly into the decision-making process the results from those officers who are working on analysis, including criminal investigations and vice-versa.

For instance, a border guard who is examining in the second line more carefully whether a TCN fulfils the conditions for entering into the Schengen Area would not only benefit from knowing, and indeed should know, that this same TCN also triggered doubts and was subject to a more thorough assessment during the visa processing. A migration or asylum officer examining an application of a TCN should also know that the applicant matches a specific security or irregular migration risk profile developed either by the law enforcement community to be applied to PNR data, or by the border guard community to be applied during border checks or API data processing.

Understanding the continuum also means the need to understand that the identification, security screening and risk management are iterative processes applied at different steps when new information about the individual is made available. The picture of the individual becomes more and more complete at each step of the continuum.

The amount of time that frontline (border, migration, asylum or visa) officers will have to devote to the assessment of an individual will increase not only due to more information being potentially available, but also because interoperability is making possible a more rigorous re-vetting and revocation mechanism. Indeed, the SIS and the future ETIAS watchlist are to be continuously updated and a new alert or record issued to a holder of a valid ETIAS travel authorisation will trigger the need to re-examine the case and whether the TCN still meets the conditions. The new VIS does not included such types of automated notifications to the competent authorities for re-vetting the holders of short-stay visa, long-stay visas or residence permits when new information is available in SIS or the ETIAS watchlist, although this would make sense.

There are other cases where an update of the databases being checked in the initial issuing process will not trigger an automated notification for the re-examination of the visa or ETIAS. A good example in this case is when a TCN having been issued and still in possession of a valid ETIAS travel authorisation or short-stay visa is entered later in the EES as an overstayer; it will be up to the national authorities to ensure follow-up and take the appropriate decision.

In addition, law enforcement searches of new crime-related information against VIS and ETIAS will reveal operational links with TCNs who were granted a visa or ETIAS travel authorisation or residence permit. Such a connection to a criminal event may give reason to reconsider that decision and possibly revoke the visa, residence permit or ETIAS travel authorisation.

In any case, these new opportunities for the revision of valid ETIAS travel authorisations, visas or residence permits with new information generated by the TCN along the travel or border continuum enable users to check whether the decisions taken in the past remain sound because the TCN still meets the conditions linked to specific entitlements to visit or stay in the Schengen Area. The same would apply to a TCN who has been granted asylum or protection status.

Reviewing the decision-making process

Neither the continuum concept nor the interoperability of EU information systems should alter the division of competences at national or EU level. However, it should affect the decision-making process. The fact that new or more information about the individual is or could be made available to the competent officer is critical for a sound decision making process. As explained before, new information about the individual is not only to be factored into the examination of the initial ETIAS, short-stay visa, residence permit or asylum application process, but also into the review or possible revocation of the initial decision.

The ETIAS and also the proposed VIS revision represent an interesting test case on how the decision-making process is to be shaped or reviewed (for Schengen visa processing) in the light of interoperability. In fact, there are many common elements to the work carried out by the ETIAS CU and NUs when processing travel authorisation applications and the visa or immigration authorities or VIS DAs for processing Schengen visas, residence permits or long-stay visas.

First of all, both communities have to look at the results of applications being queried via the ESP (European Search Portal) against several databases included in the interoperability framework, namely: SIS, VIS, EES, ETIAS, ECRIS-TCN, Watchlist, Europol and SLTD/TDAWN. False hits should be discarded as part of the initial processing of the application. This is a task which corresponds to the ETIAS CU and the competent visa or immigration authority or VIS DAs respectively.

The competent ETIAS NU will have to consult other ETIAS NUs from MS which have introduced data into the EU information system triggering the hits. A similar consultation process has to be followed according to the proposed VIS revision where the competent visa or immigration authority or VIS DA has to liaise with the visa or immigration authority or VIS DA from the other MS whose data have triggered the hit. Similar to ETIAS, these authorities must also conduct a consultation with Europol in case the hit corresponds to Europol data. Due to the wide range of databases to be checked according to adopted or proposed legal frameworks, it is required that other additional authorities may support the decision-making process.

A very good example here is the role of the SIRENE Bureaux which are actually the entities which will receive the notification from the ETIAS Central System when the automated processing leads to a hit against certain sensitive categories of SIS alerts. For instance, where the TCN applying for an ETIAS travel authorisation is subject to discreet or specific checks, this will require careful assessment on whether it is more important to let the person travel and collect the information requested in the alert when the suspect is crossing the external border or to refuse the travel authorisation. In the latter case, a contact with the competent ETIAS NU is required because it is the only entity that can take such decision. The impact of interoperability on decision making, e.g. which data are accessed or required and which other authorities are to be consulted or intervene, is much less clear or developed for other steps, such as 5, 7, 8 & 10 in the EU Travel and Border Continuum where interoperability is or could be available and formal decisions are required.

As regards step 7 (irregular entry or stay) and 8 (international protection), the proposed new screening regulation represents an important step forward for making full use of the interoperability components in the identification and security checks of TCNs who arrived irregularly in an EU MS. The results of the screening process, including the collection of ID and Biometric data, should be later stored in Eurodac along with a mark specifying whether the person could pose a threat to internal security. The information stored in Eurodac should be of high relevance for the subsequent asylum or return procedures, but the proposed legislation does not foresee consultation mechanisms for asylum and migration authorities where the identification process or security checks revealed data from the TCN registered by other MS or simply by other national authorities.

Strategic, operational and tactical analysis and joint work on thematic issues

It is important that, in addition to the daily, more routine work based on case handling including decision making on individuals, the various authorities or communities can also find the time and devote resources to develop strategic insights and operational or tactical analysis with overall trends, patterns and modus operandi.

The products resulting from this analytical work, when available, are normally shared only within the same authority or within the community, i.e. the same or equivalent national authorities from several MS with the support of the relevant EU Agencies.

However, there is a need to move one step further and develop analytical products that are designed for use by several communities responsible for visa, migration, border management, law enforcement or criminal investigations. This requires the creation of multidisciplinary teams or task forces that work on thematic or horizontal issues capable of extracting, from an ever-increasing amount of data, only the most essential information and jointly analysing it for the benefit of several communities.

Communication with individuals and public-private partnership with the transport industry

Travel and international human mobility in general are the results of choices made by individuals and are very often facilitated by commercial actors. It is essential therefore to understand the roles of both individuals and commercial actors as part of the analysis of the continuum.

The will or need of the individual to move or travel is always the starting point and it is important for the person to understand which authorities decide or otherwise intervene in the process, including also which information or data are required and for which purpose they are used. The authorities must therefore communicate clearly on the new requirements, such as having a valid electronic travel authorisation, the need to collect or process biometric data upon arrival at the BCP or provide new data in application forms in asylum, visa or migration processes. This commitment will build trust and ensure cooperation from individuals to comply with the new requirements regarding the processing of their personal data.

The importance of commercial actors in the travel continuum cannot be stressed enough. Carriers not only facilitate international human mobility by providing commercial services, but also collect and process the personal data for step 3 (PNR) and step 4 (API).

Carriers have emphasised the limited added value of sending API at the present time, since the national implementation of the current API Directive does not prevent the travelling of clearly inadmissible TCNs. However, the situation will change with the start of operations of the EES, ETIAS and proposed VIS revision and use of the carriers' gateway, which constitutes de facto an electronic admissibility check of the TCN to travel into the Schengen Area.

This will have a significant impact considering the experiences of partner TCs which have implemented equivalent iAPI systems and bearing in mind that this new obligation on carriers will apply to almost all travel modes (air, sea and land). A structured dialogue with carriers is needed on data quality, data collection and data transmission, in particular in view of the admissibility check. It should be noted that carriers are also required to perform a document check that includes the handling of exceptions, for instance when TCNs must produce a specific national residence document to prove that they are exempted from the ETIAS regime.

This public-private partnership is a must if the changes we are envisaging for our border management systems are to succeed. Following experiences from USA, Canada or Australia, this will also require centralised EU support with ICT tools and operational assistance for carriers by eu-LISA and Frontex, as well as the appointment of national entities to act as the carriers' counterparts, and EU or national ILOs/ALOs to provide assistance on the ground.

Transport authorities, including airport and seaport operators, also play a critical role when it comes to making investments and deploying new infrastructure and equipment at BCPs which support border checks at arrival or departure (Steps 5 & 10). Transport actors such as airport operators are also vital in the implementation of facilitation programmes (RTPs/NFPs).

Cooperation and exchange of information with Third Countries

The aspect of cooperation and exchange of information with third countries, which also has a strategic dimension, has not been discussed so far. It is still important to note that MS and EU Agencies have many international cooperation channels at their disposal to receive additional information supporting them in the decision-making process or in operations concerning certain individuals. The use of Interpol DBs, namely SLTD and TDAWN as laid down in the new EU legislation for border checks, processing of travel authorisations, visas or residence permits is essential.

In the law enforcement domain, data sharing can be enhanced further, in compliance with the international agreements in force, via the Police and Customs Cooperation Centres. In particular, the receipt of data from non-EU partners on suspected and convicted TCNs enables Europol to contribute to the envisaged assessment processes of ETIAS and possibly visa applications in the future.

4.2. Technical/ICT aspects

Challenges related to the current hybrid ICT architecture

The majority of the information systems supporting national authorities during the border and travel continuum follow a hybrid architecture, meaning that national authorities use their own national system connected to the EU information system. This applies for border checks at arrival and departure, short-stay visas, long-stay visas and residence permits (proposed VIS recast), international protection applications and cases of irregular border crossing or illegal stay (proposed Eurodac Recast) and return case management.

API and PNR systems as well as RTPs/NFPs and LBT registers are strictly national or even local. ETIAS is the exception since it is strictly an EU information system for which no national systems or applications are required for the processing of ETIAS applications. It should be noted that law enforcement systems which are not specific to any step of the continuum but are more horizontal and contain crime-related information about individuals and support security screening, namely SIS, Interpol and Europol systems or even ECRIS-TCN, have not been included in this analysis.

ETIAS will be an important test case to see how much a central IT system, conceived end-to-end for the ETIAS CU and NUs with case management functionalities, supports more effectively the implementation of common EU policies. Another particularity about ETIAS is that it will be partially fed directly by travellers and not via a national system.

Other systems, such as the proposed new VIS or Eurodac, also include additional sets of data about the TCN, which bring them closer to the category of case management systems. However, they cannot function independently and still need a national system to which the end-user is actually connected.

The hybrid ICT architecture described above is complex and will become even more complex due to the interoperability of central systems. Changes and improvements in the central EU information systems require adaptations and changes in national systems.

A good example will be the development of interfaces for the numerous national systems and end-users who may have to deal with MultID cases and must categorise links and process data in the CIR itself. The interface should allow the competent national officer to easily visualise the ID data to show if these are similar or do not match to help him/her to make a decision on the case.

In conclusion, the introduction of interoperability components such as the ESP, CIR, MID as well as the sBMS, offer the possibility for the competent officer to receive information from various information systems. However, the national systems including interfaces, applications or case management systems need to be adapted in such a way that they comply with the obligations under the Interoperability Regulations, and hence make full use of the potential of interoperability. This should be the case when performing border checks or processing residence or long-stay visas, international protection, migration management or return-related cases and applications which rely primarily on the national systems.

Interoperability between systems: main gaps.

Not all information systems supporting national authorities in their decision making or assessment during the different steps of the continuum are linked to interoperability.

As mentioned before, the API or PNR systems, as well as LBT or RTP registers, are purely national or even local and fall outside the scope of the new EU interoperability framework. However, alignment between EU PNR and API regimes, including the relevant data processing purposes, would facilitate the interoperability of national PNR and API systems, the establishment of national single windows and joint processing of advance information on travellers.

The API and PNR Directives have laid down minimum standards for the MS to implement their national API and PNR systems. There are several important aspects that the EU legislation has not regulated which would support interoperability between both systems:

- There are no common standardised processes for the capture, transmission, receipt, validation (data quality) of the API or PNR data collected by the carriers and submitted to the national authorities.
- There is no common platform for the transmission of API or PNR data. While API data is channelled through the Departure Control System, the PNR data is collected and transmitted through the carrier's reservation system. Carriers have different providers and platforms for sending API and PNR data and must enter into bilateral agreements with the competent authorities of the MS where they are flying to or from for the provision of data.
- There are no common standards on risk management and on the creation or sharing of risk profiles or indicators among the national API or PNR communities.
- There are no common standards as regards databases to be checked during API and PNR processing.
- Processing of API data against PNR data. PNR data can only be accurately verified with API data, but we do not have API data for intra-EU flights.

The processing of advance information would also largely benefit from the use of interoperability components, at least from the ESP and CIR since this would substantially enhance and make more effective the work of the border management authorities in preparing the border checks.

National or local registers for holders of LBT permits or RTPs cards or passes (National Facilitation Programmes) are currently rather small systems compared to the other systems underpinning the other steps. However, their importance may grow due to a larger demand for facilitation schemes by eligible TCNs as a result of the introduction of the EES. The future development of RTPs (or NFPs) may benefit from the fact that they become interoperable, meaning that membership of one RTP would also expedite crossing of the Schengen external border, allowing the use of e-gates at other International Airports where another RTP exists. This could be possible thanks to the EES, which will include in the traveller file information indicating that the TCN is enrolled in a specific NFP. This process is further facilitated by the implementation of the minimum standards and requirements for the NFPs established in the revised SBC following the entry into operation of the EES. The applicant for a NFP could then decide whether to share his/her data with other MS for enrolling in their NFPs and maybe even with Third Countries where a bilateral agreement on RTP exists.

Customs authorities may also process API and PNR data, but their information systems have not been included in the mapping of the EU travel and border continuum because their primary focus is on the control of goods. However, the interoperability between customs and borders, migration and security information systems is being explored.

Standardisation

The new EU information systems and their interoperability also implies a standardisation process. This includes data quality and data transmission standards. As regards data quality, the standardisation process is to be implemented via Commission Implementing and Delegated Acts and eu-LISA's governance mechanisms.

Regarding the exchange of information, as part of the interoperability and border management processes, UMF will serve as the basis for the standardisation of the data formats. UMF was initially designed for the law enforcement community on the initiative of the MS with the support of Europol and is currently being extended to support the development of EU information systems.

Frontex also supports the standardisation of border control equipment with the development of the technical standards which will be formalised through a Frontex Management Board Decision.

The agreement on common standards, also across sectors, is indispensable for efficient cooperation between border and migration management authorities, customs services and law enforcement. The Roadmap for Standardisation for Data Quality Purposes[34], proposed within the scope of the IXIM Working Party[35] is one of the initiatives to support the wider adoption of standards across sectors with the aim of improving data quality and facilitating access to data.

[34] Council document 11824/2/20 REV 2.
[35] Working Party on JHA Information Exchange.

4.3. The identification process, completing the picture of the individual

Collection and consolidation of ID and other traveller/TCN data

Identification is a critical standard process during the 10 steps of the continuum. In fact, if the identification process is erroneous, all the subsequent decisions and actions will be flawed.

In most cases, the collection of ID and TD data as part of the identification is done by the competent authority in the presence of the person in question. The main exceptions are when processing API, PNR data or ETIAS travel applications. The collection of ID and TD data for API processing should be done in the presence of the individual but under the responsibility of the carrier, and not by a national authority.

Despite some differences in general, the content and type of ID and TD data collected and processed from the traveller during the continuum are fairly similar, which enables consolidation of ID data and improves the accuracy and reliability of the identification. This is particularly interesting in the context of processing PNR data which are non-confirmed data and where important ID related data, such as the date of birth, are missing. The travel continuum approach offers the possibility to correlate ID data obtained from the prior PNR submission with confirmed ID and TD data in API retrieved from the travel document and obtained later. It should be noted that API data, if permitted under national law, can enrich PNR data for the purpose of preventing and investigating terrorism and serious crimes, but such PNR data cannot be used for border management without a concrete link to a suspicious case.

In the case of a TCN, the ID and TD data of the individual will be completed by adding the biometric data as part of the enrolment process in the EES.

Correlation and/or consolidation of data about the individual during the different steps of the continuum provides many other opportunities, also for migration or asylum officers. For instance, when dealing with an international protection applicant or an irregular or undocumented migrant, the case officer, in order to prepare the paper work for an asylum or return decision, should have access to the various EU information systems via the ESP in order to have an accurate picture of the ID and status of the TCN. Eurodac, SIS, EES, VIS or even ETIAS all may provide valuable though fragmented information about the TCN which in its totality is indispensable for sound decision making.

For return case management, it is suggested that RECAMAS[36] should be technically interconnected with the N.SIS so as to improve efficiency and data accuracy in the process of issuing SIS alerts on return and refusals of entry or stay alerts based on an entry ban. Ideally, the future RECAMAS should also integrate the use of the ESP so that complete, accurate and updated data on the TCN can be retrieved for decision making in the return process.

[36] See Frontex model RECAMAS v 1.0 of 19 February 2019.

The MultID cases and resolution

The MID and more precisely the obligation for the national authorities to deal with MultID cases are foreseen under Step 1 (Visa/ETIAS), Steps 5 & 10 (Arrival and Departure) and Steps 7, 8 and 9 (irregular migration, international protection, residence permit or long-stay visas). MultID cases may also occur when entering new SIS alerts.

There are therefore several national authorities and countless end-users which might be confronted with a situation where they must determine whether there is a legitimate or illegitimate case for the MultID and categorise the link accordingly. A check by a fingerprint expert may also be needed to confirm the biometric match.

This type of manual processing will not only require having the ICT tools to visualise all the identity related information of the TCN, but also the possibility to reach out to the national authority which entered the ID and TD data on the TCN in the first place. This consultation might provide information that allows officers to corroborate or confront the information obtained during the interview with the TCN. National contact points or national MID offices or teams could help the competent officer in the resolution of the MultID case.

The work to be done by the ETIAS CU during the transitional period to review all the yellow links generated by cross-matching all existing historic biometric files from EES, VIS, Eurodac and SIS prior to the start of operations of the MID could be a good opportunity to establish a robust network of national contact points. The ETIAS CU would have to involve the relevant MS (owner of the data) in the decision-making process to categorise the links.

A swift communication or consultation via these national contact points is even more important when the MultID case was triggered as part of the EES enrolment or registration since border control processes are much more time-critical than asylum, visa or migration processes. It is difficult to hold a TCN for a long time during a second line interview at the BCP to resolve a MultID case and yellow link. The resolution of the case will be also linked to the inspection of the TD of the TCN which might be invalidated.

TD check and inspection

SIS and Interpol systems support TD checks since they contain details of TD which have been stolen, lost, misappropriated or invalidated. The ability of the officer to inspect the TD at the external borders should primarily be based on an electronic authentication of the TD (where possible) and shall be reinforced with the future FADO and FIELDS system to be developed by Frontex in cooperation with Interpol, which will include forgery detection elements and provide images of valid documents. The integration of these new capabilities into the national systems for first- or second-line checks is an important aspect that has not been analysed in this report.

The VIS revised proposal includes a new functionality to support visa officers in determining whether the TD is recognised or not for crossing the external borders. This check would be integrated into the visa application processing. Such an electronic check on the list of recognised TDs could also be integrated into the national systems for the border check process.

The future of the identification process, the digital ID and DTC

One Future Group workshop focused on the concept and developments regarding digital identity and its uses for international travel. Its main conclusions and recommendations and described below.

There has been significant progress on the development of digital technologies to support the adoption of verified travel and health credentials for use during the border and travel continuum. However, the regulatory process needs to catch-up with these technological developments as the only way to reach harmonised and globally interoperable solutions.

To date, there is no consolidated standard or framework that could be regarded as being universally adopted by nations across the globe. This very much mirrors the development track experienced with seamless travel and digital identity solutions.

Furthermore, despite the intense digitalisation process, we must still be able to implement paper-based or offline solutions as back-up and also in order to address the need to leave no one behind.

The DTC developed by ICAO is to play an instrumental role in implementing digital identity models for international travel and where the root of trust for the validation or authentication of the data remains with the countries' official document-issuing authorities.

Carriers or other actors intervening along the travel continuum must, therefore, comply with ICAO specifications when creating DTCs based on eMRTD chip data.

The DTC can provide much added value in terms of efficiency of data transmission and accuracy or data quality in the pre-departure (booking, electronic travel authorisation) and departure (API) steps of the border and travel continuum. Especially for PNR, the accuracy can be increased significantly by using DTC. Moreover, their use can be extended to all travel modes and not limited only to air carriers.

Carriers would need in any case a unified response as part of the 'ready to fly/travel' from the submission of travellers' DTC to the competent authorities.

For the different DTC use cases, there needs to be a binding between the traveller and the claimed identity carried out through biometric matching which is the basis for solutions like the one proposed by IATA One ID for seamless travel.

Border control systems, including document inspection equipment, need to remain up-to-date in order to be compliant with the latest ICAO standards supporting proper authentication or validation of DTCs. Furthermore, there is also the important aspect of end-user (i.e. border guards) understanding, acceptance and trust so that these technological changes provide the expected operational added value for the implementation of their tasks.

4.4. Screening of travellers and TCNs

Database checks and access

The ESP provides the possibility to search several EU information systems simultaneously in order to contribute to the correct identification of persons present in those systems and for those systems that contain law enforcement data to check if the persons are wanted or pose a security risk. However, the Interoperability Regulations have not altered access rights to the information systems; this is regulated in EU sectorial legislation or the Interpol legal framework for SLTD and TDAWN.

The sectorial legal framework, which establishes access rights to the various EU information systems underpinning the different steps of the continuum, as well as to the horizontal law enforcement systems, is often complex.

There are contradictions when it comes to access rights to some systems. The border guard may only know that the TCN is registered in ECRIS-TCN, if and only if the TCN would cross the external border using a different identity than the one included in the criminal justice record due to the operation of the MID. However, the border guard might need to know that the TCN being checked at the border has been convicted of a terrorist offence or other serious criminal offence independently if he or she are using a false identity. This will be the case for the ETIAS or visa officers if the relevant Commission VIS proposal regulating access to ECRIS-TCN is adopted.

Access to ECRIS-TCN data is a very specific case, given the judicial nature of the data requiring a clear and common understanding by the competent authorities on how past criminal convictions should be taken into account in the decision-making process.

However, the interoperability framework, and in particular the ESP, also technically enables access to other law enforcement and criminal investigation systems such as Europol or Interpol. The conditions of access for new authorities and use of the data and follow-up to hits or matches need to be addressed in the specific sectorial legal framework and aligned with the current community practices. In the case of Europol, the deployment of its data for the purpose of processing ETIAS, visa and residence permit applications has been regulated or at least proposed, but not for purpose of conducting border checks. Such deployment in the context of border checks is beyond the scope for which the data was collected by and shared with Europol and would therefore require careful consideration and possibly an amendment of the Europol Regulation, depending on the way the process would be designed. If the cross-check of traveller data against Europol data is to inform the border management process, it comes at the risk of revealing on-going investigations. This may well undermine the trust with which the competent authorities share such law enforcement data with Europol. Also, Europol's legal framework would have to be adapted. However, if the cross-check is exclusively performed to reveal the movements of suspects to the investigating authorities without signalling the hit directly to the border management authorities, then the current legislation of Europol may possibly suffice, while the legal basis on the border management side would then probably have to be adjusted.

There are other cases where there is no reciprocal access. For instance, while national services or Europol conducting or supporting criminal investigations can have access, although in a limited manner, to Eurodac data, asylum or migration officers do not have an equivalent limited access to information held by law enforcement on the TCN. Access to this information might substantiate a negative decision or exclusion of the TCN from international protection or residence status.

Despite the prior example, there is a general and logical trend in the adopted or proposed EU legislation to provide access to law enforcement systems and related data to new authorities.

When it comes to the SIS, which remains the main horizontal law enforcement system, we can observe that the proposed VIS recast provides full access to visa or migration authorities which so far were only able to access SIS alerts for refusal of entry. Among the new SIS end-users, we will also have the ETIAS CU and NUs staff or EBCG Standing Corps members (Frontex staff). This has implications also for the SIRENE Bureaux which shall receive information on the expectedly increasing number of hits and ensure a follow-up.

It is not the objective of this chapter to provide justifications for reviewing or extending the access rights of certain authorities or communities to the various information systems. This issue can also be addressed from a perspective of working processes and inter-agency cooperation arrangements so that the competent authority is supported by multidisciplinary teams or task forces that jointly contribute not only with data, but also with expertise and context to the information collected.

Screening public health risks

The impact of public health threats such as COVID-19 for human mobility, including international travel, has been so critical that it is difficult to predict when or whether international mobility will ever come back to the pre-COVID-19 levels.

From a border management perspective, during step 5 there is a clear need to identify individuals who represent a public health threat. This requires a risk-based approach since it seems neither feasible nor proportionate to perform a health screening of all passengers upon arrival. The use of advance information like API or PNR providing route or itinerary or even seat information could help, but there are current legal barriers to process this data for such purpose, in particular PNR.

The ETIAS legal framework and the proposed VIS regulation include legal provisions allowing the development of public health (high epidemic) risk profiles. Such types of risk profiles have not been implemented before in automated processing and will have to be carefully assessed. In any case, the match of a risk profile should never lead to an automated refusal of the application, but only to a more thorough examination.

Furthermore, COVID-19 may also provide impetus for developing future border control solutions that diminish the risk of queues and promote contactless technology for travellers, including TD inspection equipment to minimise physical contact and a risk of infection. The verification of COVID vaccination certificates or test results proving that the person is not infected or has recovered are becoming a must as part of the conditions for entering into the territory.

4.5. Risk management

Lessons learned from customs authorities

Two specific Future Group workshops were focused on learning from customs authorities' practices in risk management. These were the main lessons learned:

Customs authorities' practices in risk management summarised in the general principle 'assessing in advance and control when and where required' fits well in the discussions held in the Future Group on the Integrated Border Control Model and cooperation with law enforcement actors. It is suggested, therefore, that border management, customs and criminal investigations services extend their cooperation in this domain at national and EU level.

Customs authorities' robust risk management systems require the processing and analysis of data collected during the various stages of the customs (international trade) supply chain, which includes risk assessment and potential controls of the goods. The application of this iterative process in risk management has similarities with the concept of the 'border and travel continuum' for travellers' movements into and within the EU or Schengen Area, and can provide valuable lessons.

Customs authorities' targeting or profiling systems with automated selection tools to provide a risk score require the processing of large amounts of data generated throughout the supply chain. For performing proper risk management and profiling, the customs authorities' systems not only process data from the import declaration (cargo manifest, ENS) but also include in the automated processing information available from the parties or operators involved (e.g. authorised economic operator) from other systems. The manual assessment of the target by the analyst or investigator and further instructions to mobile units or customs officers on the ground to perform a control or check, as well as the feedback from the intervention, are critical.

From the perspective of the Future Group we can propose the following recommendations:

- Border management should also rely on automated targeting or screening systems for performing risk management on the travellers with advance information. It would be beneficial, from an operational perspective and for the purpose of assessing the risk of the individual traveller, if the targeting system were to include not only API, PNR, and Visa or ETIAS application data, and if the risk management were to include combinations of these data. The experiences of border authorities outside the EU have demonstrated the operational added value of this. This would require legislative changes and most likely the use of AI to combine those sources effectively. The use of strategic information and risk profiles across the steps of the travel continuum does not require any fundamental changes of legislation and should be actively encouraged.
- The future of checks on travellers must also rely on a solid working relationship or dynamic between frontline officers (e.g. border guards) and analytical teams working in a back office. Customs authorities have valuable experience in the establishment of analytical capabilities following multidisciplinary approaches which could be shared to further develop the integrated border control model developed in the context of the Future Group.

A more practical workshop involving the various communities processing advance information from travellers and cargo could be organised to follow-up on these two aspects focusing on practical scenarios and use cases.

Risk management also includes the use of watch lists with information on individuals or entities which require attention from customs officers. The cooperation with law enforcement and criminal investigation services should lead to a systematic check of SIS and possibly Europol databases pending the feasibility study for ICS2. Since these are all EU systems, a direct connection between ICS2 and these law enforcement systems seems the most effective option.

Europol actively promotes synergies between the work of customs authorities and criminal investigations. It has a strong representation of customs officers in its liaison network and actively recruits staff with a customs background to fulfil duties within its operational domain, such as analysis projects dealing with customs-related crimes, including the trafficking of stolen and counterfeit goods, as well as various forms of tax fraud.

Frontex, as the European Coast Guard Agency, has developed in cooperation with EMSA new tools to perform risk management in the maritime domain and to establish lists of vessels of interest (IMO numbers) which could be introduced in customs' automated targeting systems (ICS2). Further tools will be developed in cooperation with the MS and other partners for enhancing maritime intelligence and risk profiling of vessels. The EBCG 2.0 Regulation provides Frontex with increased capabilities for land and sea border surveillance and detection of smuggling activities which will strengthen opportunities for cooperation with the European Commission and MS customs authorities.

Risk management for border checks, visa and migration

Border checks and migration or visa processes should become more risk-based, meaning that attention and time are devoted to those travellers or TCN applicants that present a risk. Although training and experience of the officer always play a critical role, risk management requires risk profiles that are developed with sound data, using proper methodologies and subject to rigorous testing and validation processes.

When it comes to risk management along the border continuum, namely at step 1, there should be many similarities and potential synergies in the processing of travel authorisations and Schengen visa applications according to the ETIAS Regulation and proposed VIS regulation. Both communities, Schengen visa and ETIAS officers, will be using equivalent risk indicators related to irregular migration, security and public health. These risk indicators shall be established according to a very similar combination of data which will be applied to the automated processing in the form of screening rules.

This should imply that the methodologies, including data analysis processes, data sources and the final presentation of risk indicators, should be very similar. The ETIAS screening board, where ETIAS NUs, Frontex and Europol will issue opinions, guidelines and recommendations to the ETIAS CU for the preparation, implementation, evaluation and revision/deletion of ETIAS specific risk indicators could be a reference for the similar work to be carried out in the field of short-stay visas in the context of the proposed VIS screening board. This should also aim at applying an equivalent level of risk management for ETIAS and short-stay visas.

Risk management and targeting rules are also implemented in the context of API and PNR data processing, although these rules and underlying indicators are strictly national. This is particularly noteworthy in the context of API data processing since this is an instrument supporting the border control process, where security screening standards including risk management should be harmonised.

The complementary analytical capabilities of Europol and Frontex in the security and irregular migration domain could support the MS in the use of a method/standards for the development of risk profiles and in the preparation of risk indicators to be used in step 4, which deals with API processing. The model of establishing a specific board, similar to the ETIAS screening board composed of national experts through which the MS can contribute information to develop common risk indicators, supported by both Agencies, is worth exploring as a pilot. For PNR, this is already done by the PIUs' operational analysts and Europol.

The EES does not include any central risk management tool. However, Border Guards may ask the traveller or TCN very simple questions (e.g. point of departure and destination, the purpose of their journey and whether they have means of subsistence for their intended trip) which help them to assess the risk. These questions could be raised and answered by the TCN when performing the enrolment or verification of biographic and biometric data in a kiosk or self-service machine required for the EES. This may alert the border guard of any specific risks of the traveller just before performing the manual check.

There is no common risk management framework either when dealing with irregular migration or returns. The proposed Return Directive Recast includes some objective criteria for determining the risk of absconding. Risks to public policy and to public security are also considered as part of the asylum procedure and possible exclusion of international protection, as well as for the justification of detention in the case of a return procedure.

4.6. Criminal investigation

The legislative developments on technical interoperability between systems which, on one hand underpin the management of different steps of the continuum, e.g. VIS, ETIAS, including its watchlist, EES or Eurodac and, on the other hand support law enforcement and criminal investigations, e.g. SIS, Interpol and Europol, can be addressed from two different - but complementary - angles. This depends on whether criminal investigation authorities play a supporting role in the decision-making process or are being supported by having access to the data collected during different steps of the continuum.

Criminal investigation authorities supporting the decision-making process (administrative process)

The processing of travel authorisation applications, as well as short-stay (Schengen) or long-stay visas and residence permit applications, includes queries against sensitive categories of SIS alerts (e.g. alerts on persons for discrete or specific checks or missing persons), Europol data and a future ETIAS watchlist.

However, more important from this angle is the fact that the competent national authority, prior to taking a decision (visa, residence permit or travel authorisation), will have to consult the data owner. This should be regarded primarily as an administrative process.

This consultation process is in some cases, like for hits against Europol data, explicitly laid down; the ETIAS Regulation and revised VIS Regulation foresee a consultation process with Europol.

In the case of the ETIAS watchlist, the competent authority that enters the data in the watchlist is to be part of the ETIAS NU. This authority would provide advice regarding the issuance or refusal of travel authorisation. A similar process is being designed for the visa processing where the ETIAS NU which entered the record in the watchlist is to be consulted by the visa or immigration authority or VIS DA. As such, a trusted environment is created where data on suspects can be used in a preventive manner with a minimal risk of exposing the data unnecessarily.

The situation when dealing with hits against sensitive categories of SIS alerts in the context of ETIAS has already been discussed. The VIS revision also provides for matches against these types of SIS alerts for the processing of visa or residence permits. The legislative framework is in both cases silent as regards the concrete follow-up action for a hit or possible consultation in order to decide whether to issue the travel authorisation, visa or residence permit.

Criminal investigation authorities being supported (criminal investigation process)

The hits against certain categories of SIS alerts, Europol data or watchlist may enrich ongoing criminal investigations supporting the work of the competent national authorities and of Europol.

For the most complete and up-to-date information for taking a decision on the granting or refusal of ETIAS applications and possibly visa applications in the future, a hit against any of these systems or data would immediately generate a notification or communication via the relevant channel to the national authority which owns the data or record, and which has introduced the suspect or person of interest in the system. This data may not be used for law enforcement purposes and has to be deleted once it is no longer needed for the process of issuing the visa or ETIAS travel authorisation, or for the related appeal procedure. If the national authority wishes to use the information in support of a criminal investigation or any other law enforcement purpose, it has to issue a duly justified request for accessing data from ETIAS or VIS for law enforcement purposes in accordance with the procedures foreseen in the relevant legal instrument. It can then retain the data in accordance with the applicable law enforcement data protection regime, and as long as necessary for the specific purpose for which it was requested.

In order to maximise the opportunities to enrich ongoing criminal investigations, there needs to be a possibility for the national authorities or Europol leading or coordinating the investigation to communicate in a swift manner with their national counterparts in the MS which is responsible for the administrative process in order to receive the required ETIAS and visa application data through the envisaged retrieval process.

Within the boundaries of national criminal law, the interview with a suspect, for instance during a second line check at the border, may provide opportunities to raise some specific additional questions to support an ongoing investigation or even form the basis for a new investigation. In the case of SIS alerts for discrete, specific or inquiry checks, the information sought is already included in the alert, but a swift notification to the competent authorities can be used to complement or adapt the request for additional information, depending on the case.

The proposed screening regulation for TCNs at the EU external borders lays down that the security checks shall make use of the interoperability components and access the abovementioned categories of systems. The normal debriefing of an irregular migrant apprehended either at the external borders or in the territory could then be complemented with specific questions provided by the national authorities which have entered the alerts or data. The same would apply to interviews with applicants for international protection where the new Eurodac record has generated a hit against these types of sensitive alerts or data.

4.7. Border Checks

The Future Group has paid special attention to this matter and an Integrated Border Control Model is outlined in chapter 5.

Access to systems and decision making in a time-critical environment

Border checks will be enhanced by making use of the new EU information systems and their interoperability. TCNs will be enrolled or verified in the EES, allowing the performance of the required check of ETIAS and VIS and also the detection of MultID cases.

The ESP could be used for border checks not only when registering or verifying TCNs ID and biometric data in the EES. The ESP provides potential for technical access to SIS supporting biometric searches and Interpol (SLTD), which are mandatory according to the SBC, and the ESP could also ensure technical access to Europol data. However, such use of the ESP for border checks which also apply to EU citizens or beneficiaries of free movement is not planned in the current legislative framework.

Border Management authorities shall take into account the results of these queries for the decision on entry, refusal or referral to the second line or to other competent authorities. Contrary to the situation of other officers dealing with visa, migration, asylum or travel authorisation applications, border guards must decide in a time-critical environment.

The SIS Recast and future SIRENE Manual have included cases where the hits are to be reported immediately, which may lead to the national authority having introduced the alert to change the category of alert or action to be taken in respect of the individual. However, there is hardly any time for consultation or feedback from the authorities responsible for the investigation when dealing with a suspect at the BCP.

Advance information (API/PNR) potential and challenges

Advance information, in particular API, enables the frontloading of database queries from the moment the traveller has checked in, either remotely or at the departure hub, which can be complemented with the application of specific security risk profiles on PNR data by the respective PIU.

The use of advance information should provide the border management authorities with some extra time to perform better queries and be better prepared for the border check and, where needed, still request feedback or supplementary information via SIRENE or other appropriate channels from the relevant national authorities or Europol. This approach will also make it possible to maximise the rare opportunity of having a law enforcement officer in direct or indirect contact with the suspect or person of interest.

The extension of the carriers' obligation to collect and transmit advance traveller information to other travel modes (e.g. ferry, cruise ship[37], railway or coach services) would have clear operational benefits from a border management and law enforcement perspective. In addition, there is also a significant gap in terms of collection of passenger data from business or general aviation. The SBC points to the obligation of the captain to prepare a general declaration with a flight plan and information concerning passengers' identity, but it does not specify how and when this declaration is to be submitted. From an operational perspective it would be ideal if this were understood as an obligation to transmit the required information by electronic means in a predetermined format. The Commission inception impact assessment for new API legislation refers to 'business aviation' as one sector which could be examined.

API data can also allow border management authorities to better anticipate the workload e.g. proportion of TCNs vs EU citizens, how many TCNs require first biometric enrolment in the EES and, therefore, manage their resources more effectively.

Furthermore, it makes little operational sense to keep API and PNR data streams and processing activities separate for the purpose of supporting border checks from the perspective of preventing and investigating serious crimes and terrorism. An example of added value of joint processing of API and PNR data has already been mentioned in point 5.3.1 concerning the accurate identification of the traveller.

However, there are several obstacles inhibiting more effective use of advance traveller information for supporting border checks, such as:

- First and foremost, the different legal purposes for the processing of the traveller data, i.e. border control vs. fight against serious crime and terrorism. Although both purposes may converge, the national implementation, including the legal interpretation, may vary substantially.
- The geographical scope of both instruments changes significantly. The API legislation is building upon Schengen Acquis and applies, as 'Category 1' instrument to all MS[38] and SACs. Not being an instrument building upon the Schengen Acquis, the PNR Directive applies only to EU MS and not to SACs. In practice, this means that there are various scenarios or routes where joint PNR and API are simply not possible because one of them is missing.
- The different data retention period. API must be deleted after 24 hours from arrival of the passenger, while the retention period for PNR is 5 years. Where API can be sent by air carriers as part of the PNR data, the data retention rules of the latter take precedence.
- There are often no single windows in the MS for the receipt of both types of data and there are few national targeting centres which have the mandate and possibility to process both type of data for the purposes established in both the API and PNR legislations. Direct sharing of API/PNR Hit results from PIUs with Border Guards is not a standard process either.
- There is an increased workload for the MS when processing advance traveller data upon receipt of the different pushes of either PNR or API data requiring increased analytical capacity for assessing the hits against databases or risk profiles.
- Quality and incompleteness of PNR data.

---

37 Maritime operators must already provide passenger lists to border authorities ahead of arrival, cf. SBC Annex VI, 3.1.2.

38 Ireland takes part in the API Directive. Denmark has decided to implement the API Directive in its national law.

Controls at land borders

The challenges for effective border management accumulate for land borders, where several steps of the border continuum might be missing or present themselves at the same time.

Travellers using their own means of transportation are not announced by any form of advance passenger information. Hence, checks cannot be made prior to the arrival at the border. Moreover, it might be that passengers were not even aware of the requirement of having a valid travel authorisation. A permission to board on the basis of an interactive API check may prevent travellers from initiating their travel to the Schengen area, but for persons travelling by private car this warning mechanism does not exist.

The biometric enrolment of TCNs on their first entry (since the launch of the EES) will also put a burden on the process. The absence of any indication of the numbers of travellers to expect makes it even more difficult to organise the border checks in practice.

For unannounced travellers, the checks could be improved through close cooperation with neighbouring countries, in particular by means of agreements on the exchange of information and mutual assistance. The border crossing could also be made more efficient by enabling a separate intake for TCNs that already had their biometric data recorded on a previous visit.

What also could be considered is the possibility for TCNs to send their ID, TD data, car plate number and expected date and time of arrival at the BCP in advance in exchange for priority treatment. The security checks and the verification of the valid visa or ETIAS can then be conducted prior to arrival, allowing faster processing for the benefit of the traveller and the frontline officer.

4.8. Fundamental Rights including free movement and intra-Schengen travel.

Lawful and effective access and use of personal data processed in various systems

The conditions for access and use of data processed in the EU Information Systems for Borders, Migration and Security are the result of a thorough legislative process in which fundamental rights, data protection, migration aspects and security have been duly factored in and carefully/thoroughly considered.

Lawful processing is mainly assessed on the basis of the relevant legal provisions in the sectorial legislation determining i.a. the purpose for the processing, the data categories and other conditions for processing the data and the authorities with the right to access these data.

It should not be difficult to make the case for the competent authority on the need to access certain data as far as they are required for a thorough assessment of the cases and proper decision-making process. There should be no dichotomy between rights like data protection, on the one hand, and rights to security, good administration or effective remedy, on the other hand. They are all at stake when law enforcement or migration authorities are taking decisions or actions according to their legal mandates.

The concept of the Travel and Border Continuum can help individuals and policy makers to understand that, while data should preferably only be collected once by an authority or commercial actor, they will be used at different moments or steps/stages in the continuum for different purposes and by different authorities. This has many advantages for the authorities but also for the individuals. It should prevent the unnecessary creation or multiplication of new databases that would make it more difficult for the data subject to find out in which system or which authority is holding the data, it should facilitate audits and in general improve data quality standards and also avoid asking the data subject to provide again and again the same data.

Risk management vs discriminatory profiling

We are progressively moving to smarter and more risk-based border and migration management control models. This is essential given that not all travellers at the EU external borders or TCNs involved in migration procedures require the same degree of time and attention.

It is important, as pointed out in FRA's guide to preventing unlawful profiling, that the risk profiles should be based on objective and reasonable grounds of suspicion. It also points out that specific and up-to-date intelligence will more likely support these requirements.

The establishment of multidisciplinary teams or taskforces, as mentioned before, that can pool expertise and intelligence for the different security or irregular migration risks areas would greatly contribute to preparing sound and lawful risk profiles.

The trustworthiness of risk indicators and risk profiles applied by national officers also rely heavily on the quality of the data. In many cases, there is no better and more accessible and reliable data source than those generated through the mandatory and systematic use by national authorities of the EU Information Systems. This is why EASO, Frontex or Europol have stressed repeatedly the importance of the future CRRS as a critical source of high-quality data for risk management.

Finally, the third element to be taken into consideration for implementing risk profiles in the processing of ETIAS, API, PNR or future VIS data is a regular review process and quality control mechanism which ensure that these risk profiles are accurate and up-to-date. This review cannot take place without feedback from those officers on the front line who must perform a more thorough screening or interview with the person, as result of a match received against a risk profile. Indeed, the matching of a risk profile will never lead to an automated decision; there is always a need for a human intervention. Best practices suggest that all types of matches should be verified following the four-eye principle.

As mentioned earlier, the ETIAS Regulation also provides some governance mechanisms, including a screening board composed of ETIAS NUs, Frontex and Europol experts and a fundamental rights guidance board, which can both be of relevance to other authorities or communities applying risk profiles along the border and travel continuum. This will be the case for short-stay visa processing, where the preparation of risk indicators by the ETIAS CU and the work of the VIS screening board will be supervised by the abovementioned fundamental rights guidance board.

Border checks and beneficiaries of free movement

The specific challenges related to checks on EU citizens and family members at BCPs were raised during the Future Group discussions. The new interoperability tools, in particular the MID detector supporting enhanced identification of travellers, only apply to TCNs. EU citizens or TCNs benefiting from the right of free movement, holding a residence card, are excluded from biometric checks against the MID detector. SBC foresees for this category of travellers the possibility of biometric verification against one of the biometric identifiers included in the TD when there are doubts about the authenticity of the TD or of the ID of its holders.

Where there are serious doubts, for instance where the traveller might be committing identity fraud, the person could be checked against the different EU databases which should include the CIR and MID to check whether the individual is registered in the system as a TCN with a different identity or nationality. However, the current legal framework does not support this use of the interoperability components for border checks of EU citizens or beneficiaries of free movement.

The new Regulation[39] strengthening the security of national identity cards or residence documents issued to those benefiting from the right of free movement and which can be used for crossing the external borders should also enhance the identification process by introducing aligned minimum security and quality standards for such documents.

Intra-Schengen travel

As mentioned in chapter 3, intra-Schengen travel is exempted from border checks unless a specific situation foreseen in the SBC has been declared, in which the MS have reintroduced internal border controls.

EU citizens, as well as their family members and other categories of TCNs as described in chapter 3 (Step 6), enjoy unimpeded movement within the Schengen Area.

The only information from travellers collected and processed in intra-Schengen movements might be PNR data. It should be noted that 22 MS are applying the Directive to intra-EU flights and intra-EU flights do not correspond necessarily to intra-Schengen flights.

The PNR data processing in this context would allow the possibility to issue an alert on a specific traveller enabling a police check or other type of law enforcement action such as observation or surveillance, interview or detention, always in the context of the fight against serious organised crime or terrorism.

While the case currently before the ECJ questioning the proportionality of the collection of PNR data for intra-EU flights is still pending, one could argue that the processing of PNR data could also be envisaged as a compensatory internal security measure for the maintenance of the Schengen free movement area by supporting specific law enforcement actions and cooperation measures.

[39] Regulation (EU) 2019/1157 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

However, currently PNR processing cannot completely fulfil this role because the PNR Directive does not build upon the Schengen acquis and its geographical scope does not match that of Schengen-related measures. Furthermore, the quality of data provided by the carriers is far from optimal for the accurate identification and subsequent law enforcement action on an individual traveller in the context of intra-Schengen movement. Quality could be substantially improved if PNR could make use of an automated reading of the MRZ of the travel document or implement DTCs. This could already be done as part of the booking process by capturing the MRZ from the TD or ID, using the camera of the mobile device of the traveller. This would improve the quality of the names of travellers in the record and would also enable the collection of the date of birth. In combination with the names derived from the MRZ, this would give much better results for cross-checking.

The obligation for carriers to require the MRZ as part of the reservation process can be justified by the *know-your-customer* principle. While financial institutions, for instance, are required to apply due diligence to verify the true identity of their customers to prevent money laundering and the financing of terrorism, one can easily argue that the risks of crime and terrorism associated to the (collective) transportation of passengers are proportionate to the efforts required to collect reliable identity data from passengers. Notably, this risk is sufficient to submit all air passengers to a physical security check at the airport for each and every flight.

The Commission impact assessment for the new API legislation may include the option of extending the scope of collection of API data to intra-Schengen travel. API data processing possibly enriched with PNR (e.g. for risk profiles) would provide a more reliable tool for law enforcement authorities for taking measures in the context of intra-Schengen travel. It is clear that API collection in the context of intra-Schengen travel should never amount to any sort of border control contrary to the principles established in EU legislation, including the free movement directive and SBC. The collection and processing of API data for intra-Schengen travel can, therefore, only be for law enforcement purposes.

The collection of API data in the context of intra-Schengen movements that could be extended from air to sea and land travel modes should be retrieved directly from the TD as per current international API standards and practices. The TD in this context would also include national IDs for which the ongoing harmonisation process, e.g. security features including chip, should facilitate the electronic and secure retrieval of data.

New API legislation could also address a gap with regard to the identification of travellers in intra-Schengen movements. In fact, EU transport security legislation does not require carriers to perform ID checks prior to boarding and the ECJ[40] has clarified that the SBC prevents MS from establishing an obligation for the carrier to perform an ID or TD check on the passenger for intra-Schengen travel.

When comparing the added value of collecting the MRZ as part of the booking for the quality of the PNR data and the added value of collecting API data, which can also increase the quality of the PNR data if they are combined, the former offers the additional benefit that the PNR data including the MRZ can be transmitted to the PIU already 48 hours before the flight. This gives extra time to work with the data, compared to receiving the API part of the data only at the time of departure.

[40] Cases C-412/17 and C-474/17.

5. An integrated border control model

5.1. Introduction

The development and operation of border control systems is a national prerogative and responsibility. The proposed integrated border control model represents high-level guidance material or a vision that the MS may want to use for the modernisation and digitalisation process that border control is already undergoing. The model is, therefore, merely a suggestion which is neither prescriptive nor exhaustive. MS remain fully in charge and responsible for the organisational set-up as well as for the national infrastructure, including ICT systems. In addition, if the model were to be implemented, the national competent authorities would remain fully in control of their data, including access and conditions applicable to their processing, as well as the extent to which they make use of elements of the model.

Furthermore, the national circumstances differ from one country to another and depend on the type of borders i.e. sea, air, or land borders. This model may look more suitable for international air travel, but there is potential for implementing it in other travel modes e.g. maritime, railway, or coach connections as far as advance traveller information is collected and made available to border management authorities.

Aside from the border control perspective, some of the components of the model can also be seen in relation to intra-Schengen or intra-EU movements which are part of the EU border and travel continuum, although no systematic checks are in place. These types of movements as well as the movements of goods also generate significant interaction between competent authorities from different countries and between their information processes to fulfil their respective roles.

5.2. Why are we proposing this model?

The main objective of this model is to enable competent authorities to keep the external borders of the EU open but - simultaneously - safe. COVID-19 has temporarily decreased the pressure on border management authorities due to the decreased influx of travellers. It is estimated that international travel will resume and the challenges in terms of security and safety will again increase, including the additional complexity of verification of health or vaccination certificates, because of the pandemic. These are four concrete objectives of the proposed model:

1. The need to ensure **optimal implementation** and maximise the operational added value of the recently adopted or proposed EU legislation establishing new or enhanced EU information systems for borders, migration and security. This model should address the risk of a widening gap between the fast-evolving policy and legal framework with the reality on the ground and the end-user's or practitioner's perspective.
2. Use the opportunities that **digital transformation** of government, including security sectors, provide to overcome bureaucratic legacies, verticality and silos and foster horizontality, integration, coordination and synergies between different competent authorities. This is reflected in our model, inspired by the need to close the gap between border guards and those working in criminal investigations, counter-terrorism, customs, migration, or even public health.
3. The need to implement **consistent and high security standards at the EU external borders** in terms of database checks for security or identification

purposes and the need to promote common approaches to risk management. The Schengen Area cannot afford having different control and risk management standards at its external borders.

4. A **seamless border crossing** experience for legitimate travellers thanks to the collection and effective usage of advance traveller information together with the new information systems for the border control process. Thereby performing most of the routine checks and risk assessment before arrival of the travellers at the BCPs, allowing officers at the external borders to focus on the individuals who pose an elevated risk for security, migration or public health.

5.3. What is included in this model?

Rather than a revolution, the proposed model represents a possible evolution considering the new EU policies and legislation and taking also into account the modernisation of border control processes in other parts of the world.

The proposed model is function-oriented in the way that important tasks like traveller data analysis, manual review of hits, management of risk profiles or cooperation between various national or international partners are boosted. We recommend the designation or, where needed, the creation of a 'back office' to support border officers. This back office could be linked to the PIU and other entities that support the pre-arrival screening of travellers. Any such back office could also be supported by a joint analytical capability managed by Europol and Frontex as part of a new risk management component and boosted by the usage of new and dedicated analysis tools.

It is suggested to follow a person-centric data management approach to ensure that database checks and risk assessment are done in the best possible way with all relevant data about the individual being accessible and visible for prompt decision making. This leads to the suggestion to assess the feasibility of the European System for Traveller Screening (ESTS), including a uniform interface and case management system at the disposal of the competent national authorities in the back office or PIU. The proposed model also provides an overview of the workflow including the main processes, actors and systems to offer a complete and integrated perspective.

5.4. How is this model going to work?

The model is composed of three main components which would mutually reinforce each other as part of a whole and overarching workflow.

5.4.1. **Organisational component: back office.**

The **back office** will be the main organisational component which could either be incorporated in an existing national operational centre or represent a new one. Depending on the national context this back-office could very well be connected to or integrated within the respective PIUs. It should be noted that national PIUs work in a decentralised manner supporting other national authorities by processing PNR data.

We can cluster the back-office functions in three main groups

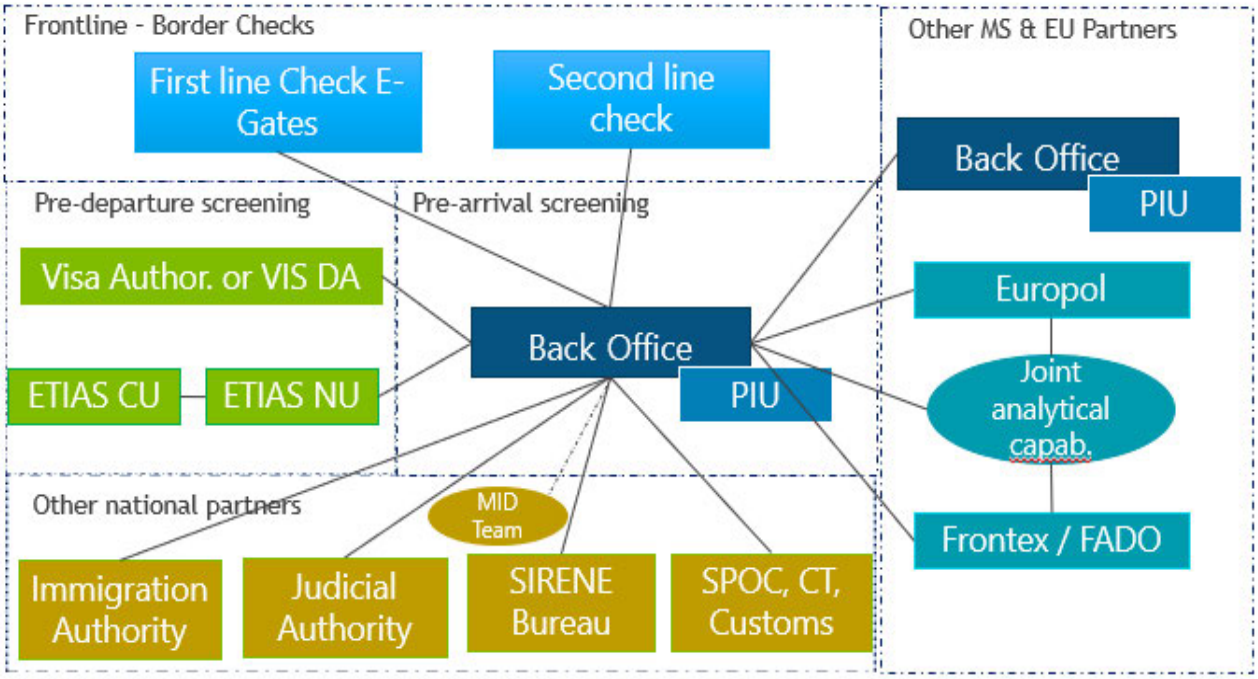
- **Operational** tasks to be implemented with the support of the ESTS.
  - Review and where required de-conflict and merge ID and TD data of incoming travellers including future DTCs obtained by correlating API and, to the extent obtained from PIUs, PNR data, and links with ID and TD data stored in EU information systems via the CIR.
  - Verification of the hits obtained with consolidated and verified traveller data against European and national databases and information systems as well as risk profiles. This also includes travellers with flagged (conditional) ETIAS travel authorisation.
  - Prepare lists of 'travellers of interest' for the first- or second-line inspection, including questions to raise and/or actions to take for first or second-line officers.
  - Prepare, if applicable, a list of travellers for whom the hits have been reviewed and later discarded and should be disregarded (white list).

Further operational support that the back-office could offer:

  - Support for the border officer during interviews with the traveller e.g. when requesting additional information for decision making.
  - Support for the border officer by facilitating the identification of the traveller e.g. other identities detected in the EES or other EU information systems (MID process) or during the documentation inspection and use of FADO.

- **Analytical** tasks:
  - Develop, test, and evaluate risk indicators and screening rules, based on European or national risk profiles (see point 5.4.2).
  - Apply validated risk profiles and screening rules to the traveller's consolidated data and collect feedback from border officers following interviews with the traveller.
  - Collect and analyse information from specific incidents at the external borders, including those reported via Eurosur with contextual information to provide input for new entries into the ETIAS (VIS) watchlist or risk profiles.
  - Liaise with the Europol and Frontex joint analytical capability (see point 5.4.2).
- **Liaison** tasks (consultation, coordination and exchange of information):
  - SIRENE Bureau, Interpol NCB, Europol, ETIAS NUs in case of matches with SIS, Interpol SLTD/TDAWN or nominal, Europol data or ETIAS watchlist respectively.
  - ETIAS-NUs, VIS-CAs or Migration Authorities when there is a need to review and revoke, annul or cancel a travel authorisation, Schengen visa or national residence permit or visa following interview of TCN.

- Other MS' back-offices as a follow-up to matches with their national risk profiles or databases (see point 5.4.2).
- National Judicial Authorities and Asylum or Migration Management Authorities, if searches via CIR reveal matches with ECRIS-TCN or Eurodac.
- National MID teams (if established) or national identification/biometric offices in case of multiple identities and when biometric expertise is required.
- Frontex Centre of Excellence on Documents in questions related to FADO or documents.
- The national PIU (if a separate entity) when needed to request specific PNR data.
- Connection to national law enforcement authorities, possibly through the National SPOC for law enforcement or International Cooperation Unit as well as counter-terrorism services.
- Customs risk analysis and operational units.



5.4.2. **Risk management component**

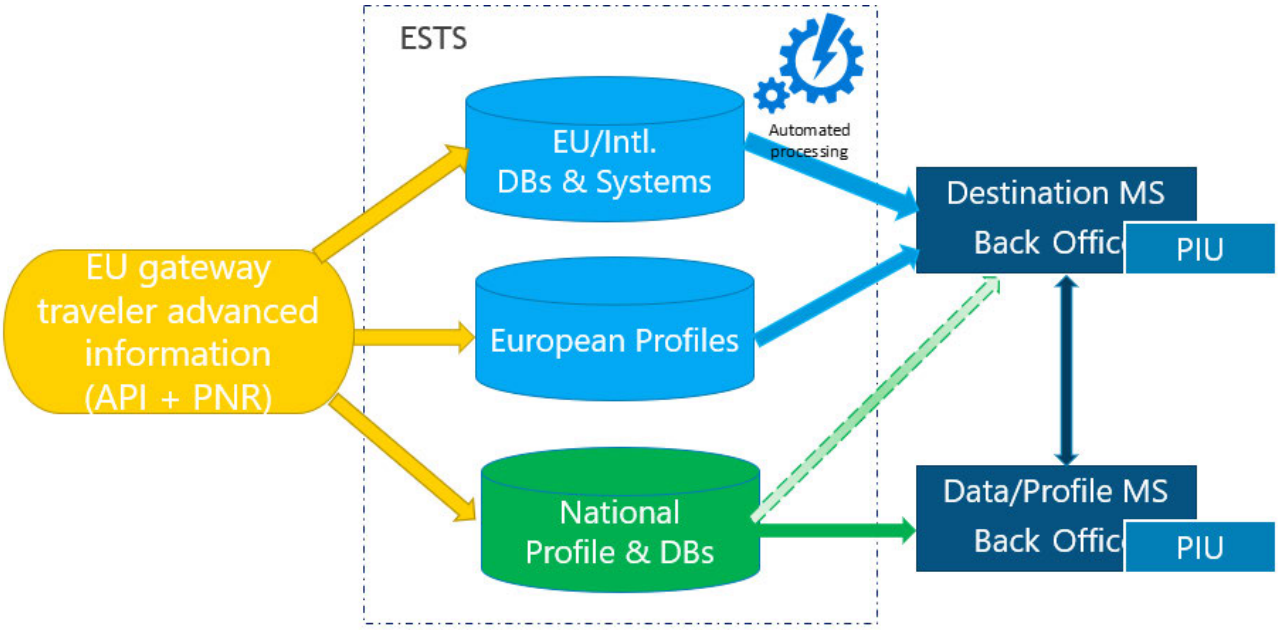
Complementary National and European layers

While the trend should be to increasingly use common screening approaches and methodologies, including risk assessment of travellers entering the Schengen Area, MS will also be able to implement strictly national risk profiles and checks against national DBs[41], possibly taking advantage of common ICT components - namely the proposed ESTS.

[41] An entry into the common ETIAS watchlist should be a good alternative to the use of national DBs.

The EU Gateway and the ESTS would allow MS to run checks with API- and PNR-data of all Schengen-inbound travellers against national risk profiles, watchlists and DBs without having to share them with the other MS. This is not possible today and would significantly boost the risk management component and overall security of the external borders and Schengen Area.

The back office/PIU of the destination MS would continue to be the sole entity authorised to process advance information on 'their' inbound travellers, including data quality review and hit analysis. They would only receive advance information on travellers heading to any other Member State on a case-by-case basis because of a hit against one of its national profiles or databases stored in the ESTS. In view of the sensitivity of certain risk profiles and watchlist entries, the authority which owns the data or risk profile might be the only one initially notified about the hit. This authority may then decide to inform the back office/PIU of the destination Member State if a specific action is to be taken upon arrival of the traveller.

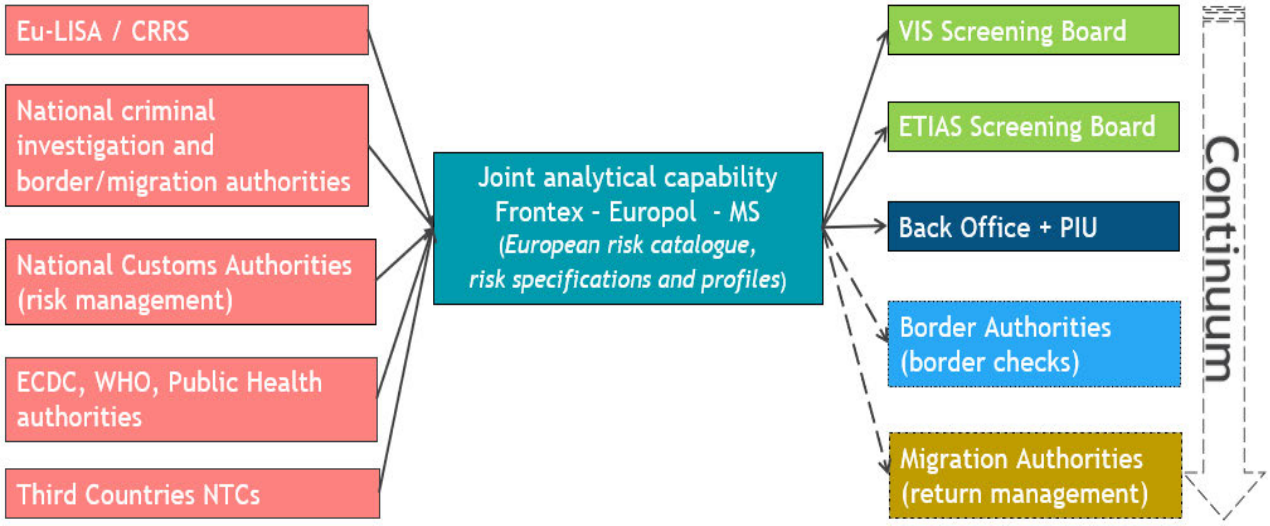


Joint Analytical Capability

This risk management component would additionally be supported by a joint Member State-Frontex-Europol analytical capability in which both Agencies and their respective national counterparts would put analytical resources and strategic or depersonalised data to mutual use when it comes to establishing a European risk catalogue, risk descriptions, and even risk profiles. This joint capability could also be called upon flexibly to analyse specific issues that relate to border management in combination with serious crime or terrorist threats, and possibly including links to illegal migration and/or the smuggling of goods. The results of such analysis can then be used for enhanced screening of passengers and cargo. The composition would depend on the issue at hand, determining the expertise required from the agencies and the involvement of the relevant competent authorities of the MS concerned. Such initiative could also be put in the context of the recent discussions at COSI, promoting joint analysis by JHA Agencies.

Joining efforts and working with multidisciplinary teams would prevent creating new silos when defining specific security or irregular migration risk indicators. In cooperation with eu-LISA and other partner agencies, the joint analysis capability could leverage the full potential of the CRRS as a data source for analytical purposes and develop appropriate analytical tools for risk assessment with the support of AI. The perspectives and information from other authorities such as customs, as well as public health authorities, for instance for the high epidemic risk indicators for ETIAS and VIS, could be taken into account and cooperation with analytical teams in Third Countries' National Targeting Centres would also be facilitated.

This integrated approach should reinforce the risk assessment function not only for the pre-arrival screening under the responsibility of the national back-offices and PIUs, but also for other national authorities responsible for other steps in the border or travel continuum. This would apply in particular for the ETIAS and new VIS, where common risk indicators and screening rules are required, whereas the risk catalogues and descriptions could also support border checks (e.g. questions raised during the TCN enrolment in the EES) or migration management procedures. In order for this joint analytical capability to properly assess and evaluate the performance of these common risk profiles, it would be beneficial if the national competent authorities were to provide regular feedback from frontline officers responsible for interviewing those individuals that have been singled out as a result of the risk management process.



5.4.3. **ICT component: 'European System for Traveller Screening' (ESTS)**

The border control process should become more effective and efficient by way of increased upstream implementation of database checks for security and identification purposes and risk profiles. This will provide significant operational benefits for border guards being at the frontline, who have very little time to assess and decide while at the same time enhancing the use of e-gates or other facilitation measures for bona fide travellers. The ESTS would perform the core automated data processing activities and additionally offer a person-centric case management functionality and interface between back-office and end-users and, depending on the degree of integration, for PIU officers in charge of pre-arrival traveller screening.

The ESTS support to pre-arrival screening would be delivered in two phases:

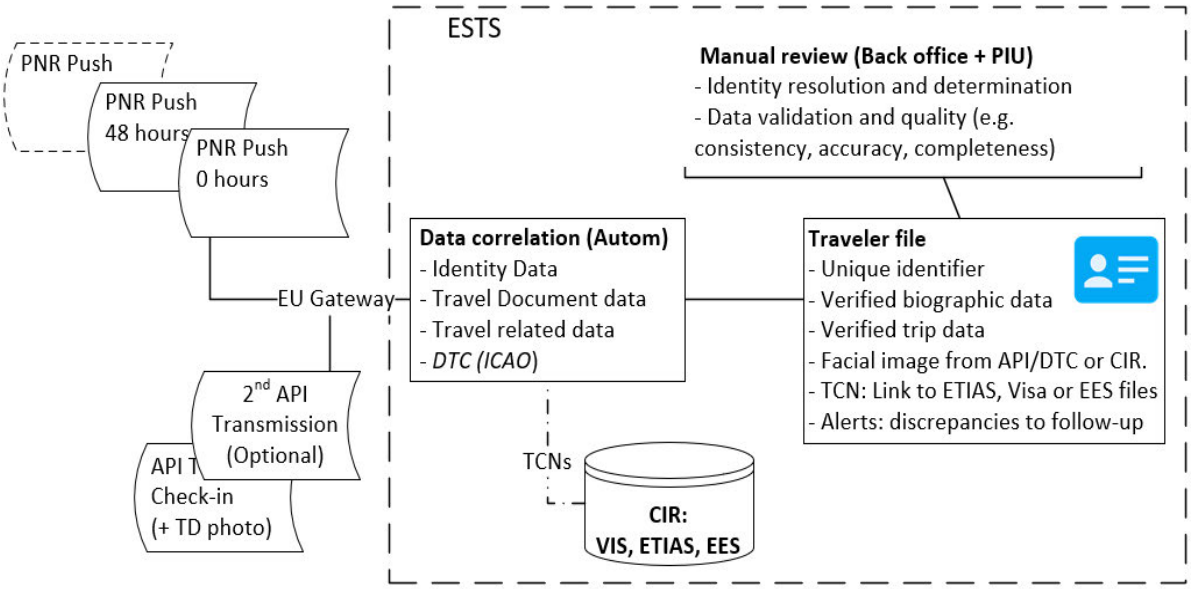
Phase I: Traveller identification and creation of the file.

The submission of PNR data (unconfirmed) and later API data (confirmed), will provide the identity of the individual. Dates and further travel details of the trip towards the EU or Schengen Area should trigger the creation of an individual traveller file. The correlation of PNR and API data provides many operational benefits, as the recent evaluation of the API Directive by the Commission has confirmed. It improves the process of identification for inbound or outbound travellers. However, legislation will be needed regarding the possibility of systematically processing PNR data to enrich the traveller file and prepare border control authorities. Until such legislation is in place, the combination of PNR and API data can be facilitated in the ESTS within the existing legislation that implements the two instruments at national level. In practice, this will imply that the API data can be used to complement the PNR data, whereas the PNR data can be used for border management purposes if the PIU function has identified that specific PNR data would qualify as relevant and has shared it for that purpose.

The integration of these two sources of information from the same individual must start with the identity determination or identity resolution to ensure that API and PNR data sets are, indeed, from the same person. This is the foundation for a person-centric data management process. The automated processing of identity data could be based on the definitions and standards (e.g. data sets) being laid down in the Interoperability Delegated Acts. The name, surname, date of birth, gender, nationality or TD data are data sets that are (or should be) available in API and PNR and would be used to establish a (potentially) common identity. The identification process in the case of a TCN traveller could be enhanced by using the CIR, which contains identity data collected by systems such as the EES, VIS or ETIAS. Furthermore, the traveller file generated for TCNs could be used to pre-populate the EES, which could speed up the registration or verification process at the BCP. The quality of API data could be further improved during the check-in stage. This includes the use of mobile applications or self-service kiosks that can digitally retrieve data from the passport chip, which could include also a facial image of the traveller. The implementation of ICAO recommendations regarding DTCs could further enhance the quality or accuracy of traveller advance information.

Travel data, such as route, flight number and BCP to be used, reveal critical information related to the person's trip to the Schengen Area which supports the border control process, in particular for the purpose of risk assessment. Here also PNR and API offer sufficient common data sets for correlation, e.g. departure points, BCPs of entry, departure date and time, carrier and flight number, which complete the creation of a single traveller file. The inclusion of the PNR number in the API submission would also support the correlation of both data sets.

The creation of unique traveller files based on a person-centric data management concept would apply to all travellers (EU citizens and TCNs) entering or exiting the Schengen Area. The creation of the traveller file during this phase should be fully automated thanks to the ESTS, manual processing including the use of the case management function by the competent back office/PIU should only be exceptional when doubts regarding the identity of the traveller arise.



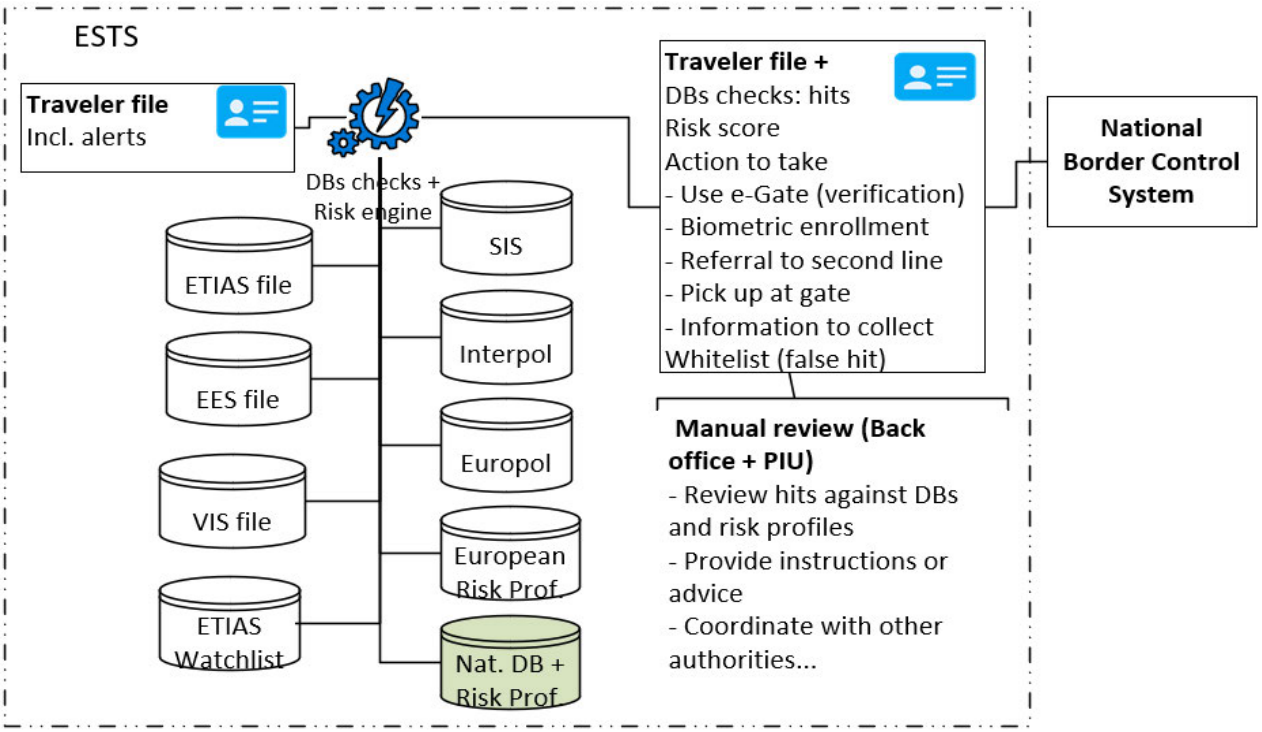
Phase II: Traveller screening

The second phase would start once the individual traveller file has been created. This second stage would also be implemented largely through automated matching of consolidated and verified traveller data (traveller file) against relevant security and migration-related databases using the ESP as well as European and national risk profiles. The results of this automated processing will require manual verification in the case of a hit, making it possible to add to the traveller file the results of the hit analysis and the action to take or information to be collected for the border officer.

There might be flags or other information intended to assist the border guard to decide on admission or referral to the second line. For instance, the traveller could match a risk profile, but there was no further supporting evidence to corroborate the risk of the traveller. The manual processing may also lead to the conclusion that this was a false hit and the traveller file would be added to a whitelist to facilitate the legitimate traveller's border crossing. The traveller file should contain the key data fields for the identification of the traveller, alerts regarding changes of API and PNR data, possible hits and results of the manual review or assessment presented in one single screen, see annex II. The case management system should also allow the officer to easily retrieve additional information on the traveller that is not presented in the main overview and to which the officer has legal access. This applies especially to the sources that caused the hits. By clicking on the values concerned, the back office or PIU officer would navigate to the underlying full sets of information to assess the issue. Embedded workflows in the case management functionality should lead to subsequent actions, decisions and the recording of any reasoning.

The ESTS case management functionality could include AI technology to implement self-learning processes from previous case handling, including actions or decisions taken without the need to store additional personal data. These tools can assist the officers and help them spend less time on repetitive tasks, but can never be a substitute for their individual assessment.

The ESTS must be connected to the national border control systems so that they can be pre-populated to speed-up first line and second-line border checks. The border officer may have to access the traveller file and may even add additional information or feedback for the back office/PIU following the interview with the traveller. The ESTS traveller files should be deleted once the border control process ends, unless they need to be kept longer for law enforcement purposes.



5.5. Workflow

The simplified workflow, as shown below, combines the aforementioned organisational, risk management and ICT components. Four other aspects should be underlined:

- Carriers' critical role in submitting API and PNR data for all travel modes[42]. The EES, ETIAS and proposed VIS Regulations already require that air, sea and land carriers should send API data and consult the eu-LISA carriers' interface to perform the mandatory verification of the status of TCNs, i.e. validity of short-stay visa, travel authorisation and residence permits prior to boarding. An operational support centre for carriers would allow them to effectively deal with technical and business-related issues which may arise when using the carriers' interface and the 'ok' or 'not ok' responses.

42 This will not apply when people arrive via private flights (general aviation) or pleasure boats which may also represent security or irregular migrations risks.

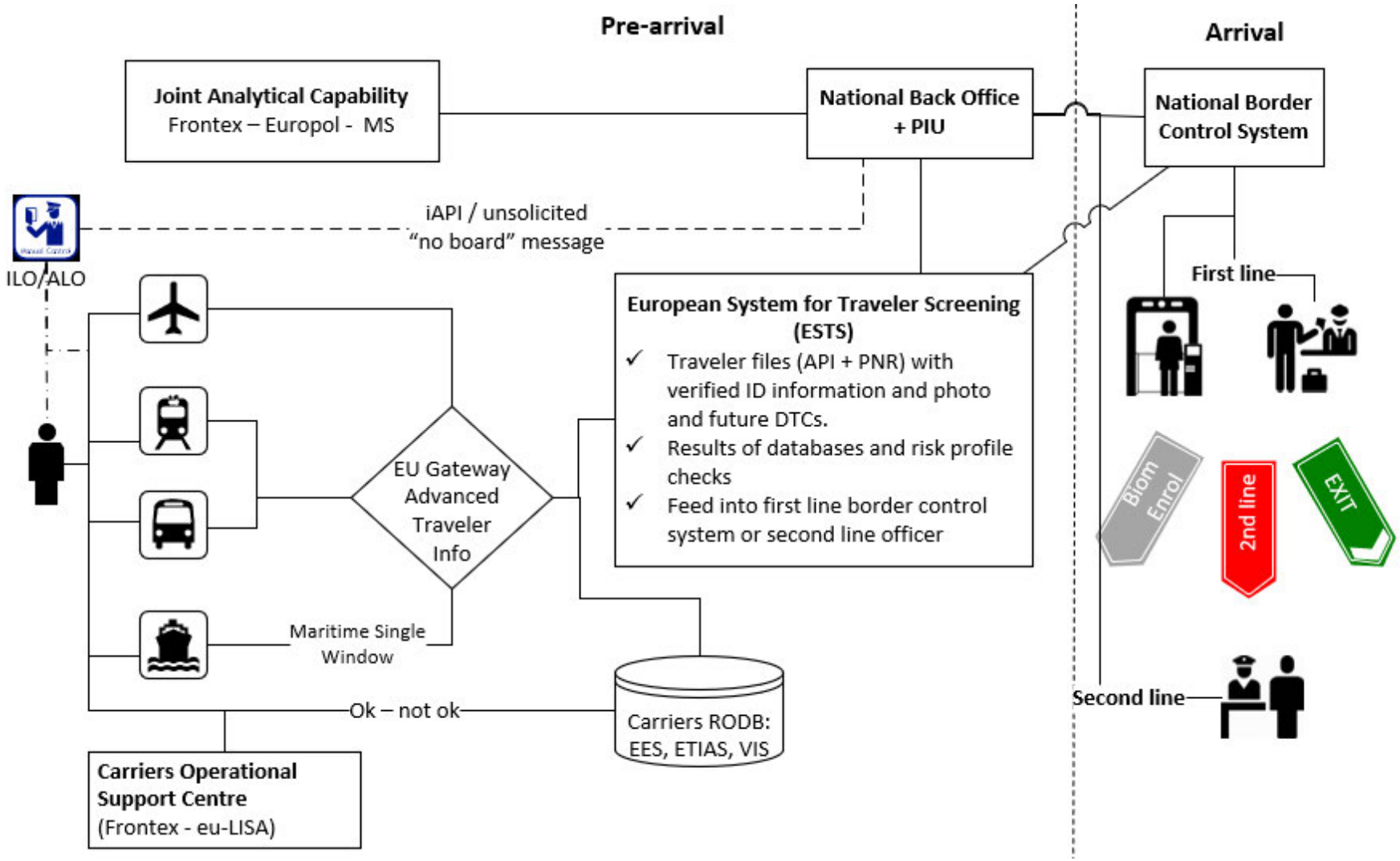
- An EU Gateway or single interface[43] could be introduced to harmonise the routing from carriers to the national authorities and to facilitate carriers' compliance with API and PNR legislation as well as with EES, ETIAS and VIS Regulations. In return, national authorities currently collecting API and PNR data would be able to make a common front and exercise via the EU increased pressure vis-a-vis the transport industry to improve the completeness and accuracy of the data. An EU Gateway would also enable the collection of reliable statistical data on travel to or from the Schengen Area or the EU, which has an invaluable analytical potential.

- iAPI and role of national officers on the ground. The pre-departure screening including refusal or later revocation of short-stay visas or ETIAS travel authorisations should prevent the boarding of clearly inadmissible TCNs. However, the pre-arrival screening performed by the back office/PIU may reveal new inadmissibility grounds for TCNs or other concerns regarding a particular traveller. The back office/PIU could instruct the carrier to refuse boarding either via an iAPI message or through a verbal notification to the carrier. This could be done directly or via an ALO/ILO on the ground whose importance in supporting carriers is expected to increase significantly.

- Facilitation: a robust pre-arrival screening would allow a more systematic use of e-gates and anticipate the travellers who require more attention at the border and need to be interviewed either because they are suspects or even criminals or because they are potential victims of crime and need help. The pre-arrival screening could also help to accurately anticipate which travellers still require a first biometric enrolment (e.g. EES) while facilitating the border crossing of the large majority or remaining travellers. Land borders will remain a particularly challenging environment from a facilitation perspective, even in a possible future scenario where coach or railway line companies could transmit advance traveller information because of the many travellers arriving by their own transport means. Close cooperation with the neighbouring Third Country border management authorities at BCP level will remain essential to maintain the flow of passengers and goods.

43 Suggestions for a single interface were already made in policy discussions concerning smart borders and interoperability.

Border control model workflow



6. Summary and next steps

The concepts presented in this report are the result of informed discussions with experts in the various fields associated with border management, security, law enforcement, migration and customs. They build upon adopted or proposed EU legislation concerning interoperability and smart borders.

The proposed integrated border control model – in the wider sense – could serve as a linking pin between the national centres tasked with border management and related law enforcement functions. And as such it would strengthen the eco-system within the EU/Schengen domain, establishing a decentralised, yet EU-wide, screening function for travellers.

The translation of the policy developments into the practical dimension, to find ways for implementation of the changes in a rational and efficient manner that achieves real operational benefits, is challenging. But it is important to get it right, and in some respects, it is worth looking beyond the technical and legal boundaries to see what might be possible in due course. One of the main legal challenges the EU may face for establishing such a model is that the legal cooperation frameworks and underlying ICT systems were mainly conceived to support cooperation in a specific sector, e.g. border management, visa, asylum, law enforcement or fight against organised crime or terrorism, but were not designed to support cooperation across the sectors. A typical example in this regard is to what extent PNR data can be used to support border controls considering the limited purpose for the processing of such data, but recognising at the same time that border management authorities are also tasked with fighting serious organised crime and terrorism. However, it is worth emphasising once more that legal changes are not a prerequisite for working towards the suggested model. It can and, if so, should be implemented in compliance with the scope and processing purposes of the underlying legal instruments. Nevertheless, certain adaptations in the legislation might make the functioning of such a model more effective. Moreover, as practitioners we are also aware that legislative efforts on their own will not suffice, and must be accompanied by a stronger inter-agency cooperation culture to become effective.

Frontex, Europol and eu-LISA could jointly sponsor an ESTS feasibility study under the framework of the EU Innovation Hub for this purpose. National, international and EU experts also from Commission, FRA and EDPS should be involved in conducting this study.

This feasibility study should cover the case management system and interface to be used by the back office/PIU officers as well as the connection with the national border control system. It should also look at the relationship between national and central ICT facilitation. In other words, what is processed within national systems and what is supported from a central infrastructure which may lead to the phasing out of national legacy systems. Also, the resource requirements for enabling the various degrees of implementation should be assessed by the study as well as data security and data availability aspects including quality of service.

In conclusion, there are critical operational, cultural, technological, legal (e.g. purpose of processing, access rights and geographical scope of API and PNR regimes), data protection and other fundamental rights (e.g. non-discrimination) aspects which must be carefully assessed for the development of the ESTS. The possible use of AI and machine learning algorithms must also be carefully scrutinised as regards the potential risks, with due consideration for the new standards being proposed and discussed by the EU legislator.

In preparation for or as a complement to this study, Frontex and Europol would also be willing to learn more from PIUs and API centres' best practices on pre-arrival traveller screening, as well as customs' risk assessment units, and would also like to propose joint workshops with MS experts on travellers risk management and opportunities and challenges for the elaboration of common risk profiles.

The potential for the use of AI in this envisaged integrated border management context is a topic to be studied in its own right and with the right expertise. This could be a specific part of the ESTS feasibility study or could be conducted as a separate assessment. In both cases, the work could be brought under the umbrella of the EU Innovation Hub.

The integrated border control model is a possible and hopefully attractive objective to work towards. It can be perceived as a conclusion in general of this report to be the most promising way forwards on the basis of the facts and considerations presented in the previous chapters. However, it deserves to be offered along with a number of practical suggestions to take advantage of the findings already in the short-term and without substantial effort.

The benefits to be gained by all competent authorities related to travel intelligence and border management relate primarily to receiving more information from each other, enabling a better functioning of the services concerned and more informed decisions on the movements of persons and goods.

Concretely, the potential for closer partnership and enhanced information exchange lies essentially in the sharing of:

- data on specific suspects and criminals by means of watchlists;
- strategic information providing insights into particular modi operandi, patterns, risks and threats;
- targeting/screening rules and risk profiles that facilitate the identification of unknown travellers or shipments that pose an elevated risk;
- feedback on concrete operational interventions initiated on the basis of information received from partners;
- know-how, expertise and lessons learnt in the area of risk management, screening and converting strategic information into risk profiles and screening/targeting rules;
- ICT tools and software for data processing in the context of travel intelligence, border management, migration and customs enforcement.

To take advantage of this potential, it is recommended that the relevant competent authorities concerned at national and EU level consider the following steps:

1. Raise awareness among operational entities within the organisation of the potential that increased cooperation and information exchange can offer;
2. Incentivise staff to identify which information available to other partners could be of relevance to their own service, and which information available internally could be of relevance to external partners;
3. Identify the most obvious and relevant partners at national and international level to intensify the cooperation with and to reach out to those to initiate a joint assessment of the operational possibilities;
4. Identify, in consultation with relevant operational partners, the possibilities, conditions and limitations of what can be done to step up the sharing of information;

5. Set up practical pilots with the relevant partners to experiment with the opportunities identified for enhanced cooperation;
6. Evaluate the results; improve and extend the scope where possible; and share the results within the broader community, so that also others may learn from the experience.

Europol and Frontex are willing not only to actively facilitate the establishment of these multi-disciplinary partnerships, but also to contribute as partners to intensifying the operational cooperation, as well as the sharing and processing of information in support of the collective interests, as and where relevant.

It was suggested to keep the Future Group 'alive' as an expert network that could be consulted as and when needed on the practical implications of policy matters and for the sharing of best practices and experiences. The latter could go hand-in-hand with the initiation of operational partnerships between different types of competent authorities to strengthen the cooperation and to increase the sharing and exchange of information.

Finally, there were recurrent discussions around remaining gaps in the border security architecture. These relate, among others, to conditions in which no advance information is collected, such as at land borders, or received ahead of arrival, which applies to general aviation and cross-border maritime traffic, especially where it concerns recreational trips. Data quality concerns were also expressed where PNR data cannot be complemented by API data for enhanced accuracy, for instance on intra-Schengen and outbound flights. Hopefully, these and other operational challenges mentioned in this report can be considered and possibly addressed at policy level.

ANNEX I: Processing purposes in relevant EU legislation

Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
API Directive 2004/82/EC	Art. 1; Art. 6(1), last sentence	Improve border control.	Combat illegal immigration.	Law enforcement purposes, if provided for under national law, in particularly in line with the explicit purpose the data was collected for.	Law enforcement purposes, if provided for under national law, in particularly in line with the explicit purpose the data was collected for.	
EU PNR Directive 2016/681	Art. 1(2).			Preventing, detecting, investigating and prosecuting serious crime.	Preventing, detecting, investigating and prosecuting terrorist offences.	
Schengen Information System - Regulation 2018/1862 Police and Judicial Cooperation	Art. 1; Art. 2.		Maintenance of public security and public policy and the safeguarding of security; - Police and judicial cooperation in criminal matters.	Maintenance of public security and public policy and the safeguarding of security; - Police and judicial cooperation in criminal matters; - ensure the application of the provisions of Chapter 4 and Chapter 5 of Title V of Part Three TFEU relating to the movement of persons on the territories of the Member States.	Maintenance of public security and public policy and the safeguarding of security; - Police and judicial cooperation in criminal matters; - ensure the application of the provisions of Chapter 4 and Chapter 5 of Title V of Part Three TFEU relating to the movement of persons on the territories of the Member States.	Maintenance of public security and public policy and the safeguarding of security (missing persons);

Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
Schengen Information System - Regulation 2018/1861 Border checks	Art. 1; Art. 2.	Maintenance of public security and public policy and the safeguarding of security; - Refusing TCNs entry into and stay on the territory of the Member States; - Ensure the application of the provisions of Chapter 2 of Title V of Part Three TFEU relating to the movement of persons on the territories of the Member States.	Maintenance of public security and public policy and the safeguarding of security; - Refusing TCNs entry into and stay on the territory of the Member States.			
Schengen Information System - Regulation 2018/1860 Return illegally staying TCNs	Art. 3(1).		Verifying for TCNs subject to a return decision, that the obligation to return has been complied with, and supporting the enforcement of the return decisions.			

Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
Visa Information System (Based on COM Proposal 16 May 2018)	Art. 2(1);	Facilitate checks at external border crossing points and within the territory of the Member States; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific check.	Facilitate the fight against fraud; - Facilitate checks at external border crossing points and within the territory of the Member States; - Assist in the identification and return 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; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry.	Facilitate the fight against fraud; - Contribute to the prevention, detection and investigation of serious criminal offences; - Contribute to the prevention of threats to the internal security of any of the Member States; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks.	Contribute to the prevention, detection and investigation of terrorist offences; - Contribute to the prevention of threats to the internal security of any of the Member States; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to persons wanted for arrest or for surrender or extradition purposes, and on persons for discreet checks or specific checks.	Facilitate the visa application procedure; - Prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; - Assist in the identification of persons who have gone missing; - Facilitate determining the Member State responsible for examining an application for international protection and enabling common procedures for granting and withdrawing international protection.

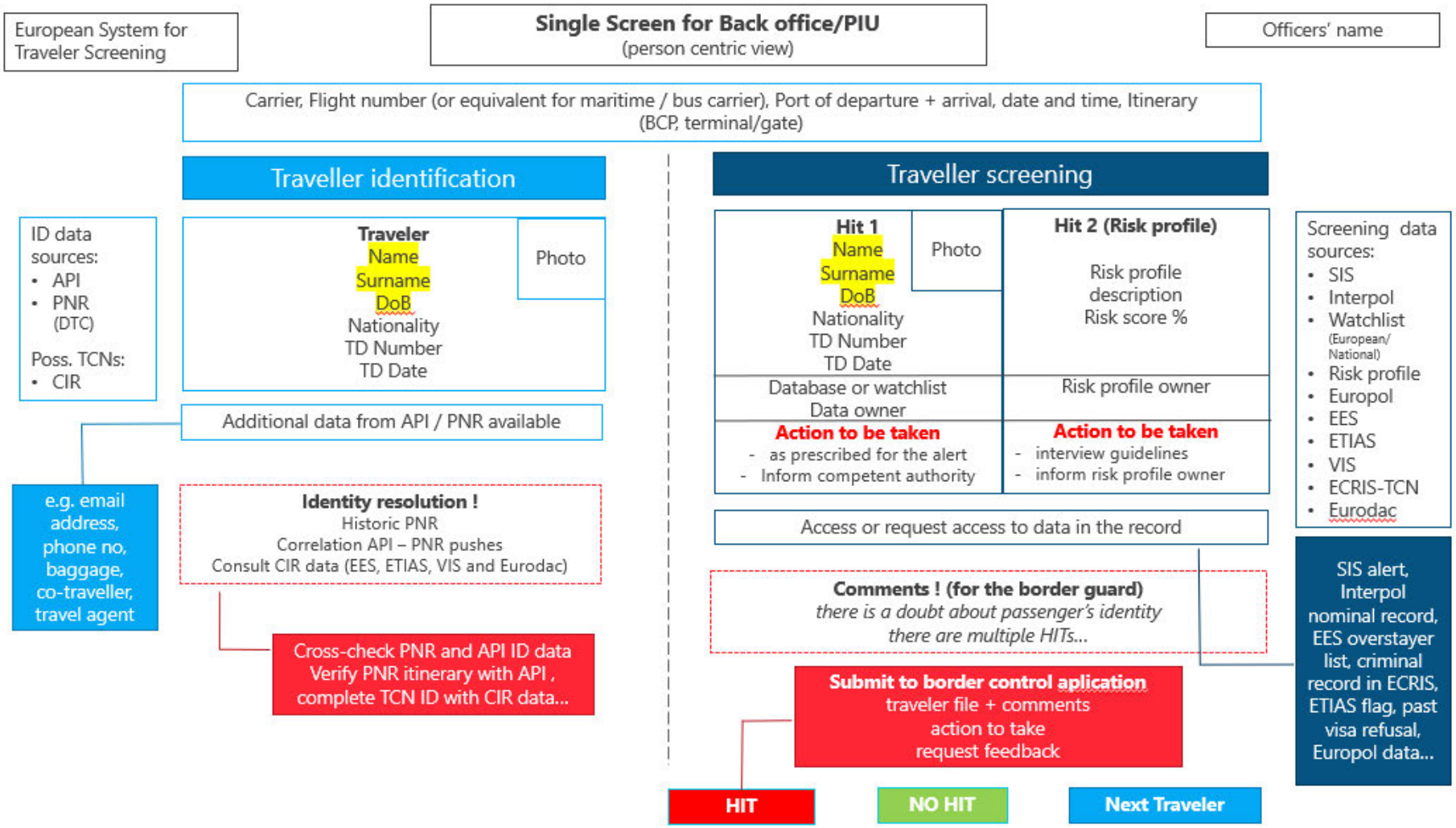
Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
VIS (continued) - Long-stay visas and residence permits (See instrument above)	Art. 2(2)	As regards long stay visas and residence permits: - enhance the effectiveness of border checks; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry, persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific check.	As regards long stay visas and residence permits: - enhance the effectiveness of checks within the territory; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry, and on missing persons.	As regards long stay visas and residence permits: - support a high level of security by contributing to the assessment of whether the applicant is considered to pose a threat to public policy, internal security or public health prior to their arrival at the external borders crossing points; - enhance the effectiveness of checks within the territory; - Contribute to the prevention, detection and investigation of serious criminal offences; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry, persons wanted for arrest or for ...	As regards long stay visas and residence permits: - support a high level of security by contributing to the assessment of whether the applicant is considered to pose a threat to public policy, internal security or public health prior to their arrival at the external borders crossing points; - enhance the effectiveness of border checks and of checks within the territory; - Contribute to the prevention, detection and investigation of terrorist offences; - Ensure the correct identification of persons; - Support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry, persons wanted for arrest or for ...	Facilitate determining the Member State responsible for examining an application for international protection and enabling common procedures for granting and withdrawing international protection.

Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
ETIAS Regulation 2018/1240	Art. 1(1) Art. 1(2)	Enabling consideration of whether the presence of third-country nationals in the territory of the Member States would pose a security, illegal immigration or high epidemic risk and if so, to prevent access.	Enabling consideration of whether the presence of those third-country nationals in the territory of the Member States would pose an illegal immigration risk and if so, to prevent access.	Enabling consideration of whether the presence of those third-country nationals in the territory of the Member States would pose a security risk and if so, to prevent access. Prevention, detection and investigation of serious criminal offences.	Enabling consideration of whether the presence of those third-country nationals in the territory of the Member States would pose a security risk and if so, to prevent access. Prevention, detection and investigation of terrorist offences.	
Entry-Exit System Regulation 2017/2226	Art. 6(1)	Enhance the efficiency of border checks [...]; - Assist in the identification of third-country nationals who do not or no longer fulfil the conditions [...]; - Allow refusals of entry in the EES to be checked electronically; - Enable automation of border checks on third-country nationals; - Combat identity fraud and the misuse of travel documents.	Enhance the efficiency of border checks [...]; - Assist in the identification of third-country nationals who do not or no longer fulfil the conditions [...]; - Allow the identification and detection of overstayers and enable the competent national authorities of the Member States to take appropriate measures; - Allow refusals of entry in the EES to be checked electronically; - Combat identity fraud and the misuse of travel documents.	Combat identity fraud and the misuse of travel documents.	Combat identity fraud and the misuse of travel documents.	Enable visa authorities to have access to information on the lawful use of previous visas; - Inform third-country nationals of the duration of their authorised stay; - Gather statistics on the entries and exits, refusals of entry and overstays of third-country nationals in order to improve the assessment of the risk of overstays and support evidence-based Union migration policy making.

Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
EES (continued)	Art. 1(2); Art. 6(2).			Contribute to the prevention, detection and investigation of serious criminal offences; - Enable the generation of information for investigations related to serious criminal offences, including the identification of perpetrators, suspects and victims of those offences who have crossed the external borders.	Contribute to the prevention, detection and investigation of terrorist offences; - Enable the generation of information for investigations related to terrorist offences, including the identification of perpetrators, suspects and victims of those offences who have crossed the external borders.	
Eurodac (Based on COM recast proposal 4 May 2016)	Art. 1(1)	Assist with the control of illegal immigration to the Union.	Assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation.	Prevention, detection or investigation of serious criminal offences.	Prevention, detection or investigation of terrorist offences.	Assist in determining which Member State is to be responsible for examining an application for international protection.

Instrument	Article(s)	Border control	Illegal immigration	(Serious) crime	Terrorism	Other
ECRIS-TCN Regulation 2019/816	Art. 2	Identifying the Member States where convictions of third-country nationals and of citizens of the Union who also hold the nationality of a third country, were handed down. (To be clarified if ECRIS can also be used in combination with ETIAS/VIS and border checks)		Identifying the Member States where convictions of third-country nationals and of citizens of the Union who also hold the nationality of a third country, were handed down.	Identifying the Member States where convictions of third-country nationals and of citizens of the Union who also hold the nationality of a third country, were handed down.	
Interoperability Regulation 2019/818 Police and Judicial Cooperation and Interoperability Regulation 2019/817 Borders and Visa	Art. 2(1); Art. 20(1)	Improve the effectiveness and efficiency of border checks at external borders.	Improve the effectiveness and efficiency of border checks at external borders; - Contribute to the prevention and the combating of illegal immigration.	Contribute to the prevention and the combating of illegal immigration; - Contribute to a high level of security within the area of freedom, security and justice of the Union [...]; - Contribute to the prevention, detection and investigation of serious criminal offences.	Contribute to a high level of security within the area of freedom, security and justice of the Union [...]; - Contribute to the prevention, detection and investigation of terrorist offences.	Improve the implementation of the common visa policy; - Assist in the examination of applications for international protection; - facilitate the identification of unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack. Enable the identification of persons in the conditions set out in Art. 20(1)(a) to (e). - (a) where a police authority is unable to identify a person due ...

ANNEX II: Single Screen



ANNEX III: List of abbreviations

ABC	Automated Border Control
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
ALO	Airport Liaison Officer
API	Advanced Passenger Information
BCP	Border Crossing Point
CA	Central Authority (for VIS)
CIR	Common Identity Repository
CISA	Convention Implementing the Schengen Agreement
CRRS	Common Repository for Reporting and Statistics
CU	Central Unit (for ETIAS)
DBs	Databases
DTC	Digital Travel Credentials
EBCG	European Border and Coast Guard
ECJ	European Court of Justice
ECRIS-TCN-	European Criminal Records Information System for TCNs
EES	Entry Exit System
ESP	European Search Portal
ESTS	European System for Traveller Screening
ETD	European Travel Document
ETIAS	European Travel Information and Authorisation System
ETIAS CU	ETIAS Central Unit
ETIAS NU	ETIAS National Unit
Eurodac	European Dactyloscopy
FADO	False and Authentic Documents Online
FIELDS	Frontex Interpol Electronic Library Documents System
FTF	Foreign Terrorist Fighter
iAPI	interactive Advanced Passenger Information
IATA	International Air Transport Association
IBM	Integrated Border Management
ICAO	International Civil Aviation Organization
ICS	Import Control System
ID	Identity
ILO	Immigration Liaison Officer
LBT	Local Border Traffic
MID	Multiple Identity Detector
MS	European Union Member States and – where relevant – also Schengen Associated Countries
MRZ	Machine Readable Zone
MultID	Multiple Identities
NFP	National Facilitation Programme (also RTP)
NUI	National Uniform Interface
PIU	Passenger Information Unit
PNR	Passenger Name Record
RECAMAS	Return Case Management Systems
RTP	Registered Traveller Programme
SAC	Schengen Associated Countries
SAR	Search and Rescue (operation)
SBC	Schengen Border Code

SBMS	Shared Biometric Matching Service
SIRENE	Supplementary Information Request at the National Entries
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TCN	Third Country National
TD	Travel Document
TDAWN	Travel Documents Associated with Notices
TRIP	Traveller Identification Programme (of ICAO)
UCC	Union Customs Code
UMF	Universal Message Format
VIS	Visa Information System
VIS DA	VIS Designated Authority
WCO	World Customs Organization