Study on the Feasibility of Improving Information Exchange under the Prüm Decisions

Written by Deloitte Consulting & Advisory CVBA
May – 2020

Deloitte.

EUROPEAN COMMISSION

Directorate-General for Migration and Home Affairs
Directorate D — Law Enforcement and Security
Unit D.1 — Police Cooperation and Information Exchange

E-mail: HOME-NOTIFICATIONS-D1@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Advanced Technical Report

Final Version

Directorate-General for Migration and Home Affairs

May - 2020

Luxembourg: Publications Office of the European Union, 2020

DR-02-20-311-EN-N
Doi 10.2837/1710
ISBN 978-92-76-18456-0

EXECUTIVE SUMMARY

The Prüm Decisions are considered to be a major tool in the context of law enforcement collaboration when investigating criminal offences. However, multiple issues and concerns have been raised by stakeholders since the introduction of the system.

The Advanced Technical Report describes a broad list of fifteen improvement opportunities for the Prüm Decisions that have been assessed to address some of the issues in the five following areas:

1. **Improving the automated data exchange:** Incremental solutions are presented to facilitate the exchange between Member States, the portability of the data with other systems and the adjudication process.
   a) *Expand the scope of the Prüm framework:* It is suggested to establish a level playing field by expanding the scope of the Prüm framework and allow searching for missing persons and identifying deceased persons in future.
   b) *Revise Prüm technical standards:* The study recommends a standardised approach for the automated data exchange to be aligned with best practices and interoperability solutions across the EU, namely ANSI/NIST-ITL 1-2011.
   c) *Fingerprint efficiency:* The study analyses 7 possible improvement opportunities: (i) standardised image quality metrics; (ii) reporting on usage and accuracy; (iii) improving candidate lists (match scores); (iv) priority-based scheduling; (v) pooled quota; (vi) vendor feature set support and (vii) the XML data exchange file format (XML).
   d) *Improve DNA matching:* The study analyses 3 possible improvement opportunities: (i) a configurable minimum loci threshold and ESS support; (ii) usage reporting; and (iii) a standardised data exchange format.
   e) *Vehicle Registration Data:* The study suggests the exchange of additional data categories and search mechanisms.

2. **Improving the follow-up procedure:** The study provides suggestions to accelerate the information of core follow-up information in the Prüm context.
   a) *Enforce a quick answer in the follow-up procedure:* It is suggested that a common set of core follow-up information would be exchanged under an agreed timeframe.
   b) *Single communication channel:* Member States would agree to use by default the same communication channel, Siena.
   c) *Implement UMF:* The currently UMF3+ model would be used for the communication of follow-up information.

3. **Introducing new data categories:** Clear recommendations are provided on the introduction of data types that can be exchanged in an automated manner.
   a) *Facial images:* The study recommends the use of facial recognition technology for the automated data exchange of facial images.
   b) *Driving licenses:* European driving licenses should be made available to law enforcement cross-border searches.
   c) *Ballistics & firearms:* The study explores the possibility to exchange ballistic & firearms data, but do not yet recommend the implementation of an automated data exchange system.
   d) *Biographic data:* The possibility of improving the exchange of police records leveraging the EPRIS-ADEP technology in the Prüm context is recommended.

4. **Introducing a new IT Architecture:** The introduction of a central component will facilitate the setup and maintenance of connections.

- *Central router:* The introduction of a hub-and-spoke system is recommended to replace the current mesh topology.
- *Common ABIS matching system:* The possibility to re-use a central component of the interoperability solution as matching solution has been looked into, but has been discarded.
- *Web-service communication:* The use of web services is recommended, given the nature of the data format being exchanged.

5. **Adding interoperability solutions:** An assessment is provided on the integration of the Prüm landscape with certain interoperability features.
   a) *Integration with interoperability:* The implementation of an interface between the central router and the ESP would benefit the Prüm participants.
   b) *Integrating new stakeholders:* It is recommended to integrate Europol in the Prüm framework.

The implementation of the aforementioned improvement opportunities will lead to:

- An updated material scope of Prüm to allow searches for missing persons and unidentified human bodies for a level playing field.
- The Prüm network will be scalable, and all participating countries will be connected one to another.
- Member States' law enforcement authorities will have further streamlined work flows to query biometric data available to them.
- The data format used will be consistent, and interoperable with other national and EU systems.
- Member States will have to the possibility to query broader data sets (i.e. facial images, driving licences and biographic data)than today for the purpose of prevention and investigation of criminal offences.
- Europol, as a hub of European law enforcement cooperation, is integrated in the Prüm framework.
- Lead times in providing answers to follow-up requests will be shortened.

TABLE OF CONTENT

This page has been left blank intentionally.

FIGURES & TABLES

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF ILLUSTRATIVE TABLES

DEFINITIONS, ACRONYMS AND ABBREVIATIONS

ABIS – Automated Biometric Identification System

ACRO – Criminal Records Office

Adventitious match – DNA profiles from two individuals, who are not identical twins, which match by chance

AFIS – Automated Fingerprint Identification System

AIMs – Ancestry Informative Markers

Allele – Alternative forms of a DNA sequence at a particular locus

BSG – Biometric Services Gateway

CBE – Cross Border Enforcement Directive

CEPOL – The European Union Agency for Law Enforcement Training

CEU – Presidency of the Council of the European Union

CJEU – Court of Justice of the European Union

CODIS – Combined DNA Index System

COREPER – Committee of Permanent Representatives in the European Union

CPIA – Criminal Procedure and Investigation Act 1996 (as amended)

DAPIX – Working Party on Information Exchange and Data Protection (former Ad Hoc Group on Information Exchange)

EC – European Commission

ECRIS – European Criminal Records Information System

EFSA – European Forensic Science Area by 2020

ENFSI – European Network of Forensic Science Institutes

EP – External Person

ES – External Stain

ESS – European Standard Set (of loci)

EU – European Union

EUCARIS – European CAR and driving licence Information System

EURODAC – European Dactyloscopy, the European fingerprint database for identifying asylum seekers and irregular border crossers

EUROPOL – European Police Office

FDP – Forensic DNA Phenotyping

FP – Fingerprints

FSP – Forensic Science Provider

I 24/7 – Interpol's global police communication system

INTERPOL – International Criminal Police Organization

LOCI – Plural of Locus

LOCUS – Specific location of a DNA sequence on a chromosome; for forensic analysis it refers to areas that vary between individuals

MAP – Mutual Assistance Procedures

MCT – Mobile Competence Team

MLA – Mutual Legal Assistance

MS – Member State(s)

NCP – National Contact Point

NDNAD – National DNA Database

NFO – National Fingerprint Office

OP – Own Person

OS – Own Stain

OS-EP/OP-ES – Own Stain-External Person/Own Person-External Stain

PCR – Polymerase Chain Reaction

PIES – Prüm Implementation, Evaluation, and Strengthening of Forensic DNA Data Exchange

PoFA – Protection of Freedom's Act 2012

sBMS – Shared Biometric Matching Service

STR – Short Tandem Repeat

SV – Severe and Violent Crimes

TFEU - Treaty on the functioning of the European Union

UMF – XML format standard for data exchanges for interconnecting law enforcement systems

VIN – Vehicle Identification Number

VRD – Vehicle Registration Data

This page has been left blank intentionally.

VERSION HISTORY

Version number	Purpose/change	Author	Date
0.1	Draft version	Deloitte	05/07/2019
0.2	Comments to clarify and adapt the draft version	DG Home	17/07/2019
0.3	Updated based on DG HOME's comments	Deloitte	14/08/2019
1.6	Updated from non-biometric topic review by DG HOME and internal review	Deloitte	14/10/2019
1.7	Updated from non-biometric topic review by DG HOME and internal review	Deloitte	16/10/2019
1.10	Updated based on DG HOME's comments	Deloitte	08/11/2019
1.20	Updated based on DG HOME's comments	Deloitte	06/12/2019
2.4	Updated based on DG HOME's comments	Deloitte	13/02/2020
2.5	Updated based on DG HOME's comments	Deloitte	14/04/2020
2.6	Final version	Deloitte	07/05/2020

This page has been left blank intentionally.

1. INTRODUCTION

The present Advanced Technical Report presents the preliminary conclusions on 15 themes to improve the information exchange under the Prüm Decisions. The report defines and develops these improvement themes for the Prüm framework and arranges them into five groups.

The topics have been whittled down from an initial list of 40 after consultation with representatives from the Member States and technical experts looking at their potential benefits and technical feasibility.

Improvement area	Improvement topics
1. Improve the current exchange of Prüm data	1.1. Enlarge the material scope of Prüm 1.2. Revise technical standards 1.3. Improve DNA matching 1.4. Fingerprint workload reduction 1.5. Vehicle Registration Data changes
2. Improve the procedure to follow up on a match	2.1. Initial step in the follow-up procedure 2.2. Single communication channel 2.3. Implement UMF
3. Introduce new data categories under the Prüm Decisions	3.1. Facial images 3.2. Driving licenses 3.3. Firearms & ballistics 3.4. Biographic data
4. Introduce a new architecture	4. Update the current IT architecture
5. Link to central EU systems and interoperability solutions	5.1. Update the architecture for interoperability 5.2. Integrate new stakeholders in Prüm landscape

Table 1 – Improvement topics assessed in the Advanced Technical Report

The report assesses the 15 improvement options based on (i) operational implications for end-users; (ii) technical and security considerations; (iii) legal and data protection aspects; and (iv) financial implications.

Based on this assessment, the report recommends whether to include the improvement opportunity into a 'single composite option' for a next-generation Prüm framework, documented in the final report with a cost assessment. The cost assessment has been carried out in a separate report, and includes the assumptions and parameters for the financial analysis.

This Advanced Technical Report has been structured into six chapters. The first five chapters present one improvement theme or topic with one or several options, 15 in total. The last chapter briefly describes the upcoming tasks that are still pending.

The reader will find, for each option, a current analysis, potential solution, feasibility assessment, and conclusion. It finishes with the next steps toward the final report.

FIVE AREAS TO IMPROVE THE DATA EXCHANGE UNDER PRÜM

1. **Improve the current exchange of data:** Although most forensic experts agree that the automated data exchange is currently working well, a few points for improvements have been raised. The legal scope is considered to be not equivalent for all Member States, the exchange standards under Prüm are considered as outdated and additional information could be made available to law enforcement officers within EUCARIS.

2. **Improve and streamline the procedure to follow up on a match**: the exchange of personal data and other follow-up information after a hit are governed by national law; the response to a request for follow-up can take too long to investigate efficiently or effectively prevent crime.

3. **Introduce new data categories under the Prüm Decisions**: it is possible to include new data categories in addition to the exchange of DNA, fingerprints and vehicle registration data; special attention is given to facial imaging, a technology that is being used increasingly by public administrations and law enforcement.

4. **Introduce a new technical architecture of Prüm data exchange**: in the current mesh type architecture, Member States have set up bilateral connections for automated data exchange; there is a possibility to improve on the current architecture and/or introduce a new architecture.

5. **Link to EU information systems and solutions for interoperability**: as central EU systems are undergoing significant changes (SIS, VIS, EURODAC) and new ones are being established (ETIAS, EES & ECRIS-TCN), these systems will be made interoperable gradually; there will be great business value for law enforcement from integrating the Prüm framework into these future interoperable solutions.

2. IMPROVING THE AUTOMATED DATA EXCHANGE

This first chapter introduces several improvements to the challenges Member State administrations face when exchanging information on DNA, fingerprints and vehicle registration data (VRD) as covered by the Prüm framework.

As laid out in Council Decision 2008/615/JHA[1], the automated exchange covers the search and comparison of data, the notification of a hit or no-hit and the supply of reference data. The VRD exchange has been fully automated, through the EUCARIS application.

The chapter addresses several improvement topics, including (i) expanding the scope of the Prüm Decisions, (ii) adopting a common data format for the data categories, and (iii) enhancing process efficiency and added features for the data categories exchanged under Prüm today.

First, we will look at expanding the scope of the Prüm framework to include searches to find missing persons or identify deceased ones to the benefit of those Member States that are not allowed to do so under current national legislation.

Next, we analyse current data exchange standards for biometric data sharing and propose a best-practice common standard to the future data exchange under Prüm to promote future interoperability and portability of data across the EU.

Finally, the chapter goes into details for each major data type by looking at the current approach for sharing fingerprint images, DNA profiles and vehicle registration data within Prüm, it proposes solutions and recommendations for improving the data exchange and assesses what are the impacts of such changes.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615

2.1. *Expand the scope of the Prüm framework*

The Prüm framework has been established to help prevent and investigate criminal offences, but Member States apply this scope in function of national legislation. On the one hand, law enforcement authorities launch queries via Prüm to search for missing persons and identify deceased civilians, if those situations are considered part of a criminal investigation under national legislation. On the other hand, in some Member States, e.g. Italy, law enforcement officers are not entitled to use Prüm in these cases. This, however, decreases the possibility of finding missing persons and identifying human remains in these Member States.

2.1.1. Proposal

The differences in national legal frameworks prevent law enforcement authorities from leveraging Prüm for one and the same purpose. Therefore, it is suggested to establish a level playing field, expand the scope of the Prüm framework and allow searching for missing persons and identifying deceased persons in future.

2.1.2. Assessment

Operations and end-users

Expanding the scope of the Prüm framework is likely to increase the number of searches, particularly from those countries where searches for missing and unidentified human remains are not allowed currently under Prüm.

The likely higher number of searches will impact workloads and may hit daily quota for searches. Member States will need to implement changes to relevant work procedures and processes to accommodate for this new query option.

Technical and security

This scope expansion should not imply technical nor security implications, given that queries over the Prüm network will be identical to those exchanged today.

Legal and data protection[2]

This solution would require the material scope of the Prüm framework to be adjusted.

From a data protection perspective, enlarging the scope of the Prüm framework under the proposed solution would entail:

Increasing the number of data exchanges and, hence, the number of data that will be shared and exchanged between the Member States, given that new individuals will be added in scope (missing persons and unidentified human bodies – to the extent that those can be linked to identifiable natural persons, see point 2 below -). Yet, the increase

[2] The application of the current Prüm framework requires that the provisions in the Law Enforcement Directive (EU) 2016/680 (hereinafter, "LED") be taken into account, particularly with processing activities related to preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties, including the safeguarding against and the prevention of threats to public security (Article 1 of the LED). Any data processed should be secured in accordance with, inter alia, Article 29 of the LED.[2] Based on the current technical specification, the security and encryption of personal data comply with LED requirements.

of the volume of data is not a blocking factor per se for not enlarging the scope of the Prüm framework on condition that Member States can ensure that the IT security measures and procedures that are currently in place to ensure the confidentiality, integrity, availability and privacy of the current data can work properly and be resilient to any type of security risks in case that new volumes of personal data are added for processing. In this regard, it would be recommended to the Member States, ideally with the Commission's support and guidance, to perform an IT risk assessment of their local IT systems supporting the automated data exchanges and transmissions under Prüm in order to assess whether those are robust enough to support the processing of larger volumes of data. It might be that reviews or updates of the current organisational or IT security measures may be needed to enable the smooth and secure exchanges of information pertaining to missing persons or unidentified bodies.

The increase of searches is most likely to be marginal and for a few Member States, which leads to believe that the IT systems should be robust enough to cope with it.

Enlarging the categories of data subjects, being the individual, natural persons of whose data will be processed. The category of "missing persons" and likely of other persons (presumably deceased, corresponding to "unidentified human bodies") should be added next to the categories of persons covered in the existing Prüm framework, being often individuals having a criminal history or record, suspects of criminal behaviour, persons subject to investigation, prosecution or any other law-enforcement or security measure, incl. criminals.

The following considerations will need to be taken into account:

1) First, missing persons are typically considered under Member State law as natural persons, with active rights and obligations, until a certain period of time elapses and such persons may be considered deceased for legal purposes. Searches performed on missing persons will therefore be subject to the Prüm framework, including data protection rules, as searches for identified persons.

2) Second, vulnerable categories of population may fall in the category of "missing" individuals besides the criminals, such as elderly persons, persons suffering from psychological/psychiatric problems or history, children and others. Practically, the handling of the data of those vulnerable categories of population in the same systems would require the adoption or update of additional security measures (procedures and IT measures) or, to the minimum, confirmation and double-checking of the current measures to ensure that the latter protect adequately the privacy and related fundamental rights of the new categories of data subjects. In particular, data retention rules, procedures related to the access rights of end-users in the national systems (e.g., national contact points) or even the need to add new categories of end-users in the Prüm ecosystem are a few of the domains that will have to be reviewed. Moreover, segregating the data flows referring to searches, hits or no hits of "missing" and deceased persons (incl. storage of their data on national systems) vs. the data flows and storage related to "criminals" (currently covered in scope) should be looked into.

3) Third, at present, the automated transfer and supply of the data elements provided for in the Decision (DNA profiles, fingerprints, etc.) are inherently linked to the prevention and investigation of criminal offences, thus law enforcement purposes. Therefore, the legal basis will need to be adapted to include the two new categories. We would recommend that the new legal instrument explicitly mentions: i) the new dimension of processing, ii) the fact that other categories of data subjects may be affected besides the criminals and iii) the necessity to ensure that the IT system(s) and data handling practices that Member States follow in the framework of the current data transmissions and supplies

appropriately take into account that data of other persons than criminals may be subject to the processing that would probably requires the strict respect of current safeguards (e.g. only duly authorized officers have access to the data). The clarification of the material scope will also benefit the Member States as it will provide legal certainty to all of them as to the meaning and extent of the processing activities covered in the scope of the Prüm decision, and this by comparison to other similar EU legislative initiatives in the area of law enforcement and beyond.[3]

4) Regarding the searches performed on "unidentified human bodies", it should be considered that the purpose of the searches may result in identification of deceased persons. While the scope of protection of the EU data protection regulations do not apply to deceased persons, it is left to the discretion of the Member States to determine whether deceased persons should benefit from extended protection under their data protection or privacy rules. This is currently not the case in the majority of Member States. In addition to the data protection and privacy rights, it should be noted that other rights might apply to deceased people, such as: rights of protection of one's image, dignity, reputational or other moral rights (the definition and scope of protection of these laws may vary from country to country). Member States should also assess the protection they might want to bring to these rights. The restrictions and conditions that have been discussed above apply *mutatis mutandis* in the situations whereby data related to "unidentified human bodies" may be processed.

In conclusion, as long as appropriate safeguards are implemented and/or respected, the Prüm legal framework could be enlarged in terms of material scope.

2.1.3. Conclusion

There is an opportunity to create a level playing field across Member States by expanding the scope of the Prüm framework to include searches for missing people and deceased ones. It would benefit a limited number of the Member States, which cannot use Prüm currently to these purposes due to different national legal frameworks.

In terms of its implementation, no technical changes would be required, while the operational and legal changes are considered to be minimal.

However, from a legal and data protection point of view, the suggested enlargement of the material scope would require *specificity* and *clarification* with regard to the data processing purposes and the (new) personal data subject categories affected. Such specific and/or additional language should, ideally, be enshrined in a revised Prüm decision or secondary (implementing) regulation complementing the Prüm framework. Moreover, Member States will possibly have to consider additional IT security and

[3] Large scale information systems that have been subject to further analysis, in order to improve their interoperability and the potential of information sharing between those are for example: the Schengen Information System (SIS), the Eurodac system and the Visa information System (VIS), while others are on the way (e.g., ETIAS, ECRIS…). Although enhancing the interoperability between those and other systems being functional today is considered as important, the European Data Protection Supervisor (EPDS) also expressed its concerns about how those systems, that do not aim to serve exactly the same purpose (law enforcement vs. migration management) may at the end contribute to creating assimilation between terrorists, criminals and foreigners. The same concern can well be found in the situation where there is a risk to assimilate missing or deceased persons to criminals as discussed above (EDPS Opinion 4/2018 on the Proposals for the two Regulations establishing a framework for interoperability between EU large-scale information systems, April 16, 2018, p. 9.

operational elements for their national automated transmission systems and, consequently, to review and update those in view of the enlarged scope.

Because of its benefit to a certain number of Member States, this opportunity should be part of a future revamp of the next-generation Prüm framework.

2.2. *Revise Prüm technical standards*

This paragraph analyses the current standards of the Prüm framework for sharing biometric data[4] and recommends a standardised approach to how data exchanged could be aligned to best practices and interoperability solutions across the EU.

The proposal presented here remains at high level with the particular implementation details of each data type (fingerprint, DNA and facial images) documented in the subsequent paragraphs of the report.

Throughout the analysis of the topics for facial images, fingerprint workload and DNA improvements, this study identified the following key observations.

- Each biometric data type shared within Prüm is based on a different standard and data structure. This is a complex and costly approach as each data category has to be implemented and supported using different technologies.
- The addition of other data categories such as facial images may introduce even more data exchange standards, increasing the implementation complexity and support cost for Member States.
- Current standards do not support interoperability with other information systems or agencies outside of Prüm, restricting easy data sharing should this be required.
- Current standards for fingerprints do not easily support integration with modern technology platforms such as web-based services.
- ANSI/NIST-ITL 1-2011 is known to be widely adopted or planned with many international agencies and is specifically designed for the sharing of biometric data within law enforcement and is supported by Interpol and eu-LISA.

Finally, given the level of adoption of ANSI/NIST-ITL 1-2011 within law enforcement and its suitability to the needs of Prüm, the following proposal focuses on the suitability of the standard as a common framework for biometric data exchange between the Member States. Other standards such as ISO/IEC 19794 that define biometric interchange formats can be considered, however, they already form the basis of ANSI/NIST-ITL 1-2011 which is specifically designed for law enforcement and criminal investigations.

2.2.1. Proposal

The proposed solution is to adopt a single standardised Prüm exchange format for all data items which is also aligned with the standards used by other law enforcement authorities and agencies.

- ANSI/NIST-ITL 1-2011 is to be adopted as the standard framework for the transmission of biometric data between Member States;
- Prüm shall define the requirement as ANSI/NIST-ITL 1-2011, version 2015 or later. This will allow the Member States to implement latest versions of the standard as they become available;
- Data will be exchanged using XML NIST containers to allow easier integration between Member State authorities and interoperability between other agencies;
- Member States should implement the new standard in a phased approach to gradually adopt a more interoperable solution.

[4] For biometric definitions and acronyms used throughout this section refer to annex.

As with any implementation of ANSI/NIST-ITL 1-2011, the application to Prüm would be specific and certain aspects of the standard will be extended for the application of sharing between Member States.

The record types defined for compliant NIST containers relevant to Prüm are:

- Type 1 – Transaction Information (Mandatory)
- Type 2 – User Defined Fields
- Type 4 – Fingerprint Image (grayscale)
- Type 9 – Minutia Data (Fingerprint)
- Type 10 – Face and SMT (Scars, Marks and Tattoos) Images
- Type 13 – Latent Ridge Images
- Type 14 – Variable Resolution Ten-Print Images
- Type 15 – Variable Resolution Palm Images
- Type 18 – DNA Data

ANSI/NIST-ITL 1-2011

ANSI/NIST-ITL 1-2011 is a standard defined to provide interoperability between agencies such as those in law enforcement that share biometric data between disparate systems. It describes the file format and quality expectation of data shared. The standard was last revised in 2015.

The standard is based on transactions (the process of sharing data). An ANSI/NIST-ITL 1-2011 compliant file (NIST container) can contain a set of one or more records and may contain data relating to one or more identities.

Each record contained within a file is defined as a specific record type. Each record type includes definitions for several mandatory and optional fields and their structure for different types of transferrable items.

A NIST container will usually contain multiple records and is implemented in a traditional file format (in which case it is referred to as a file) or as an XML structure referred to as an exchange package. Modern system implementations tend to use XML code due to the ease of integration.

ANSI/NIST-ITL 1-2011 incorporates and builds upon many other standards from a range of agencies for record formats, image quality and other areas such as compression (WSQ used for fingerprint image compression etc.).

The standard is intended to be backwards compatible as it is recognised that implementing authorities will likely differ in implementation. The standard is only ever added to so non-breaking changes are made, providing implemented systems are built to ignore new fields.

NIST containers will contain the following minimum records:

- 1 x Type-1 record entry containing transaction and header information
- 1 x Type-2 records containing custom data items

In addition, they will have zero or more of the other record types supporting the transfer of facial, fingerprint, DNA and latent/palm prints between supporting agencies.

NIST containers support the transmission of multiple subjects, the specification defines a field called information designation character (IDC) which allows a reference to be defined for each subject contained within. This IDC is defined in a registration field within the header (Type-1) record and is then referenced in each of the subsequent record entries.

The remaining records of a NIST container will be made up of the other biometric record types, e.g. for fingerprint, DNA or facial image data.

ANSI/NIST-ITL 1-2011 is widely adopted within law enforcement for sharing of data between authorities. Several agencies have implemented specific applications of the standard. For example, FBI (EBTS) and Interpol all extend the standard in various ways but remain fundamentally compatible which provides interoperability of systems that share biometric data and also adopt ANSI/NIST-ITL 1-2011.

The Type-1 header record, required in every NIST container, provides information to the requested authority about the transaction and data contained within. Key fields include:

- Version Number – the version of ANSI/NIST-ITL 1 that is used for the file creation;
- Transaction Content – defines the records that are stored within the file aligned to subjects (defines IDC entries);
- Priority – optional and can be used to indicate the urgency at which a request should be processed;
- TCN\TCR – transaction control number and response (ID's) that should be used for requests and follow-ups (TCR is the requested TCN ID);
- Originating\Destination 'Agencies' – unique identifier for both the sending and receiving agency (note the standard refers to authorities as agencies);
- Other – definitions for standard resolutions used for images, agency information, universal time stamp and application-specific support (such as for EBTS).

Although not mandatory, it is normal for files to contain at least one Type-2 record and specific information also to the implementation such as demographics, reason for request, contextual information regarding a case, name of authorising officer etc. For each record, the following is implemented:

- ICD – the reference to the subject this relates to as defined in the Type-1 record
- User Defined – a set of fields specific to the application. For example for law enforcement, this usually would include crime reference numbers and contextual information

Each NIST container sent between Member States would include:

- One Type-1 record transaction information;
- One Type-2 record containing Prüm specific information;
- One or more additional records containing fingerprint images or feature data, facial images or DNA along with relevant meta-data

Type-1 records for Prüm would include, at a minimum:

- Version Number – Prüm would adopt the 2015 revision, therefore the value '0500' would be included in all requests;
- IDC Registrations – a registry of the biometric records contained in the Exchange Package. Each unique subject has an IDC which is referenced by the other records in the message;
- TCN – unique identifier for the transaction that should be used for follow-up to requests (in the TCR field);
- Originating\Destination 'Agencies' – unique identifier for both the sending and receiving law enforcement authority. This would be the currently used ISO country code for the requesting and requested Member States;
- Priority – numeric value between 1 and 9, with 1 being most urgent.

Each NIST container would include one Type-2 record containing data items agreed for sharing between Member States to ensure compatibility and tracking of results. The fields within this record will contain at a minimum:

- IDC – reference to the subject this relates to as defined in the Type-1 record
- Case Number – a unique identifier for the case in the requesting Member State
- Criminal Reference Number – a reference number specific to the individual contained within the request, where they are known
- Respondents List (for responses) – an indication of if a search resulted in a hit or no-hit, the number of candidates the search produced and an index identifying

the current message's position in the candidate list. Where multiple candidates are found, multiple messages will be sent

The proposed standard is aligned to other EU platforms and this allows exploring interoperability solutions. The recommended changes will ensure that Prüm data sharing is compatible with other similar frameworks throughout Europe and could be considered a European standard. The other record types for fingerprint DNA and facial images are detailed in this document.

2.2.2. Assessment

The Prüm framework itself need not amending for any user, security or legal reasons. Adopting a common standard should drive data quality and compliance.

Operations and end-users

Once technical changes are made by Member States and they complete the adoption of the standard, one should not expect any operational or end-user impacts.

The underlying exchange format and its technical implementation are transparent and do not impact application processes or user experience. Few end users in the Member States have any knowledge of the underlying protocols used for the data exchange.

The only perceived risk to users and operations is during the switch over of existing data exchange communications (either through existing SMTP or a new web-services based approach) where downtime, delays or technical issues could cause an impact. An implementation plan would need to be agreed on a per Member State basis.

Member State representatives have been asked how long they estimated it would take to migrate an existing exchange to a new format, assuming it has already been developed and tested. The results are below.

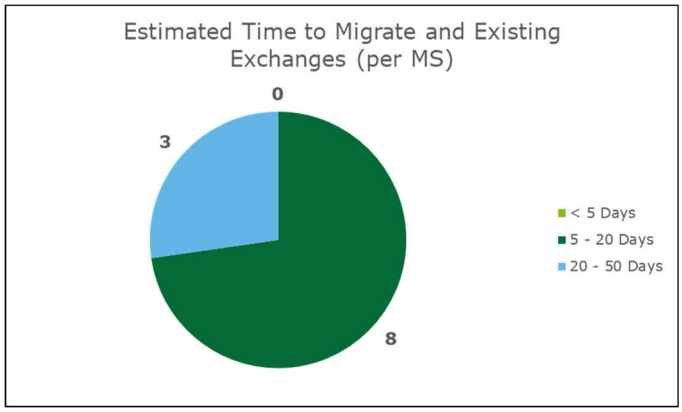


Figure 1 - Estimated Time to Migrate and Existing Exchanges

The majority of Member States indicate up to 20 days would be required per format change (DNA and fingerprint). 27% estimate an effort that is more than double this number at 40 to 50 days. Member States also highlighted that more analysis is required to truly understand the impact on an individual Member State and biometric data type basis.

Technical and security

Member States will need to update existing systems for DNA and fingerprint data. For fingerprints, the change is not expected to be significant as the new ANSI/NIST-ITL 1-2011 (2015) standard is well aligned to the records and fields used in the current specification.

However, it does require changing to an XML based code of files which requires some development effort from the Member States. For DNA data the change would require moving to a new structure, but, the encoding used would still be XML based and should allow easy migration to the new schema.

The technical effort required for fingerprints is to change the code implementation. For DNA the main effort is in defining the Prüm specific fields that would be needed in the interface control document (ICD) and then adopting the revised XML schema.

Security is not impacted directly by this change as existing measures such as encryption would remain as-is. However, it is worth noting that adopting an XML based encoding along with web-services provides opportunities to establish security mechanisms that allow for the use of centralised technology components such as a central router. These options are explored in chapter 5.

During workshop discussions with Member States concerns were raised that ANSI/NIST-ITL 1-2011:2015 may not suitable for DNA profile transfer. Or more so, other standards (such as ISO/IEC 19794) may be more relevant or that the existing XML based communication framework is sufficient and specialised for use within Prum. The study believes that ANSI/NIST-ITL 1-2011 offers an opportunity to introduce a standardised framework for all biometric data exchanges and that it does provision the ability to share non-coding DNA information between Member States (with specialisation for Prüm). Furthermore, the standard is specifically designed to enable transfer of data within the context of law enforcement and is in fact itself based on elements of the ISO/IEC 19794 standard. The statement below is an extract from the ANSI/NIST-ITL 1-2011:2015 standard for Type-18 records (used for DNA profiles).

"The Type-18 record shall contain and be used to exchange DNA and related data. It was developed to provide a basic level of interoperability with the draft format of the ISO/IEC 19794-14 DNA data interchange format. 21 With full consideration to privacy, this standard only uses the non-coding regions of DNA. The regions of the DNA that encode phenotypic information are deliberately avoided."

The study takes on-board the feedback and proposes the change on the basis of consistency of standards. However, it is acknowledged that expert individuals within the DNA community may prefer to retain the current and specialised format currently in place. If this is the case, the recommended standards change are still recommended for use when sharing fingerprint and facial image data.

Legal and Data Protection

The changes introduced by this solution are not expected to entail negative issues from a data protection perspective, as there is no significant impact to the data categories being processed, the purposes behind the processing activity, or the measures taken to secure personal data.

Concretely, the key fields encompassed in the Type-1 header record do entail filling-in of data that can directly identify a transaction but not a person (record transaction information). The field "IDC Registrations" may be more sensitive in this regard, as it defines the biometric records stored within the Exchange Package that, if linked with the Type-2 record, may reveal contextual data specific to an application. Therefore, some additional protection may be considered for the "IDC Registrations" field compared

to the rest of fields. Those measures can be providing for a very restricted access to this field (e.g. through permissions to a very limited number of end-users). The latter can be operationalised through additional (stricter) user authentication and/or strict definition of the authorisations that will be defined in the role-based access management procedure to be implemented by the Member States.

Regarding the Type-2 record, the "Case Number", the "Criminal Reference Number" and the "Respondents List" fields include data (unique identifier, the number of candidates produced by the search and others) that, indirectly, can identify an individual (suspect candidate "criminal" person) when either one-by-one or put together, are linked with other identifying data. Similarly to the first "IDC Registrations" field above, the fields in question of the Type-2 record must also be subject to stricter procedural and IT measures to ensure the high confidentiality restrictions that should normally be applied to those types of data. In particular, these fields should be subject to strict access and view/readability requirements. For instance, only a very limited number of individuals from the agency identified in Type-1 record should be able to view and read this information and this on a strict "need to know" basis along with strict logging controls to ensure that whatever a user does with this information (copy, extract, etc.) prior, during or after its transmission is constantly monitored and can be traced back.

One solution that Member States should practically consider is to apply the stricter security measures explained above (restricted access, strict logging controls, etc.) on all data fields of the Type-2 awhile maintaining a less strict level for the Type-1 record as the latter contains only transactions' related data.

Other requirements that should be considered with regard to the protection of the Type-2 record related also to data retention/deletion, meaning that those highly sensitive information should be subject to very short data retention periods, while pseudonymisation or anonymization may also considered if certain data fields would need to be kept for longer purposes and, ideally, "emptied" from data that could potentially identify individuals.

It has to be noted that this information is already exchanged by Member States. No particular concerns regarding the exchange of this information has been raised by stakeholders.

Apart from the above considerations, the content of the Type-1 header record and Type-2 records based on the typology of the ANSI/NIST-ITL 1-2011 standard appears to align with the current data protection requirements of data minimisation and proportionality.

The data protection and confidentiality threats are in effect more related to the management of the containers of the confidential information by the agencies rather than the containers' content as such (being the minimum necessary and proportionate to the purposes of the research. Training should be put in place by the Member States, if needed under the guidance of the Commission, so that agencies' officials are aware of the sensitive nature of this information, particularly of the Type-2 record data and are trained as to how they should handle this information confidentially. Agents' background checks before the hiring process, signature of special confidentiality clauses in their labour contract are a few of the measures that can ensure the hiring of competent and reliable staff to handle this information. Moreover, regular audits of the IT measures and procedures put in place to protect the sensitive nature of data, as well as of the agents' hiring and performance process could ensure that the special protection attached to the containers' data is effective.

To note that the above procedures and awareness may not be anything new compared to what the Member States and their respective agencies have already implemented under the current transmission system. Yet, the introduction of new data exchange standards create the right momentum to check the effectiveness of those procedures, the need for reviewing them while stressing their importance of those rules and

procedures to staff through updated training and ad-hoc awareness. To the extent that the proposed measure gives rise to specific categories or labels of personal data, any defined maximum retention periods should apply to such categories as well.

Cost Implications

The cost of implementing the suggested standard will vary between Member States depending on the structure of their existing internal systems.

The switch for DNA data, which already have a similar XML based approach will incur minimal costs. However, the fingerprint format will incur higher costs as the current exchange is based on a different technical approach.

To support this, Member States were asked to estimate the development costs to change their technical platforms to support an ANSI/NIST-ITL 1-2011 (2015) compliant exchange format for DNA and fingerprint data items.

63% of Member States indicate that development to support the new exchange for DNA requests would be less than EUR 50,000.

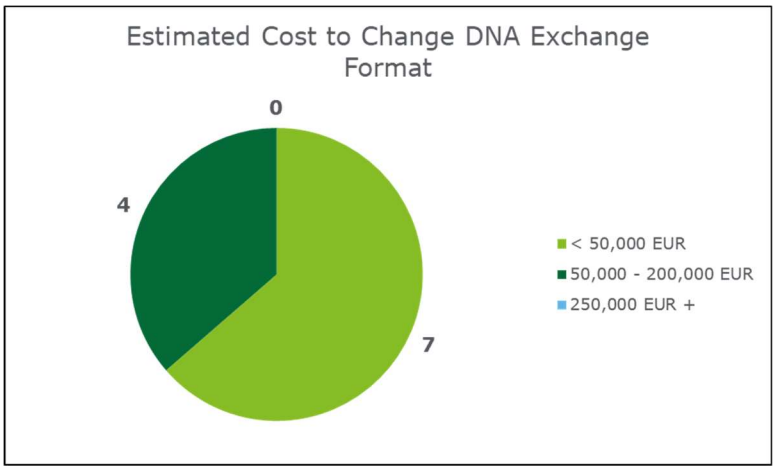


Figure 2 - Estimated Cost to Change DNA Exchange Format

However, 80% of Member States expect adopting the new standard for fingerprint data to be between EUR 50,000 and 200,000 with the other 20% indicating it could even be higher.

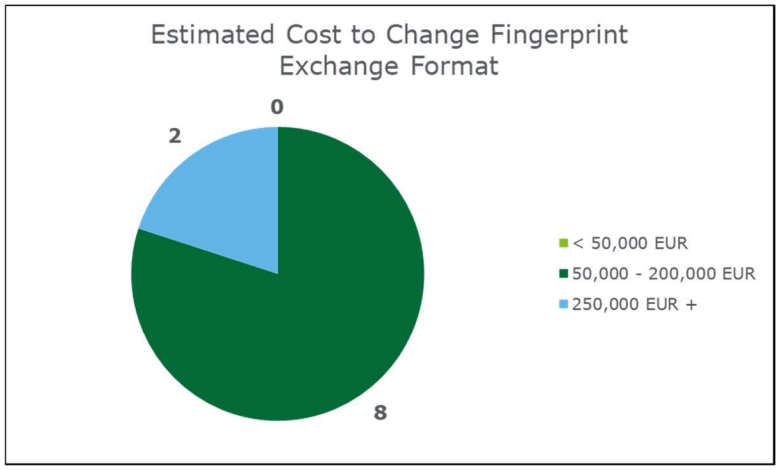


Figure 3 - Estimated Cost to Change Fingerprint Exchange Format

These responses indicate that for most, the total cost of adopting the standard for DNA and fingerprint data would, at a minimum, demand a EUR 250,000 investment.

2.2.3. Conclusion

As a conclusion, the Member States should adopt a common ANSI/NIST-ITL 1:2011 standard for exchanging biometric data. Although the change would not bring any immediate benefits to the users – in fact, the change should be transparent to them – a standard, interoperable exchange format will bring easier integration and lower overheads for supporting Prüm requests.

Moreover, from a privacy and confidentiality point of view, the adoption of the new standard does not seem to bring forward any different and particular risks related to data minimisation, purpose limitation and proportionality, although the content of some records is qualified as highly sensitive. In this regard, it would be worthwhile checking to what extent all the IT measures, procedures and training that are now in place for the current data exchanges are still effective and pertinent to the new data formatting and typology that will be introduced.

A phased approach to implementation can be considered to minimise the impact of the changes, for example:

- **Facial Images** – the new standard could be adopted for all new Member State connections upon initial implementation; this will also provide a core support by Member States of the ANSI/NIST-ITL 1-2011 standard.
- **Fingerprint** – any new Member State exchanges that are set up should adhere to the new standard; existing exchanges should be migrated within a defined period identified and agreed as part of the working group.
- **DNA** – any new Member State exchanges that are set up should adhere to the new standard; existing exchanges should be migrated within a defined time period identified and agreed as part of the working group.

The work in supporting the standard could be completed as part of the facial image implementation. The work required to support facial images would build the fundamental integration of the ANSI/NIST-ITL 1-2011 Prüm standard which can then be adopted more easily for the other record types i.e. DNA and fingerprint.

2.3. *Fingerprint efficiency improvements*

Automated Fingerprint Identification Systems (AFIS) have been in use for over 30 years and have provided forensic law enforcement with an indispensable tool for identifying criminal suspects using both ten-print and latent fingerprint images.

Fingerprint images for data exchange and adoption of AFIS platforms have been included in Prüm for over 10 years and it is widely accepted that the sharing of data between Member States, for forensic fingerprint recognition, has been highly successful.

Please refer to Annex 1 – The current Prüm framework for fingerprints for more information on the current standards being used.

The current important differences in accuracy reported between Member States are anecdotal as the Prüm framework lacks a mechanism for reporting on accuracy or any levels that ensure a minimum level of image quality.

Although Member States representatives and experts agree that one cannot expect any revolutionary changes from the next-generation Prüm in the area of fingerprint data, it may be possible to evolve current agreements and procedures to address current challenges. These include the following aspects:

- **Quota** – many Member States have identified quota limitations causing operational problems; these quota are designed to limit the overall demand on a Member States infrastructure;
- **Performance** – Member States agree that the current framework does not allow measuring or reporting use and accuracy and that information on confirmed hits and position in lists may be useful, however, most indicate this would only be useful for usage data (sent, received, error etc.).
- **Vendors** – we found that ~70% of the known Member State AFIS platforms are supplied by just three vendors; this means many of the exchanges in place are transferring image data between systems that may be made compatible by sharing template data; this could reduce demand on target Member States as they would not need to process raw image data; requesting Member States would only be required to extract, match and respond if they were supplied with a compatible template; however, it should be noted that even Member States with the same vendor may differ in algorithms used;
- **Standards** – the current ANSI/NIST-ITL 1 standard (Interpol version) is dated and transition to a later version would allow consistency with other EU agencies and databases; additional features of the standard could be used to capture other opportunities such as vendor feature data, priority and XML transmission encoding.
- **Quality** – the standards adopted across Member States for fingerprint image quality vary and Prüm does not define a minimum quality threshold of images; each system will assess quality and suitability for use differently.

The main areas of improvement are in technological advancements Member States can make, many of which use dated AFIS platforms, and in establishing common standards for data exchange and quality. These will help improve the effectiveness of the fingerprint data exchange and help future proof the performance of Prüm fingerprint requests.

Having a common way of communicating quality between Member States would allow understanding the confidence of results received. It is acceptable that lower image quality should be supported. However, understanding the quality being handled could significantly assist the end user.

2.3.1. Proposal

The current standards for the exchange of fingerprint images and method for recognition between Member States are considered to be successful and no major issues have been identified. The overall implementation of fingerprint sharing works well and the approach should not change fundamentally. However, several possible areas of improvement have been identified.

This paragraph presents seven ways to improve the fingerprint data exchange, their scope, potential impact and high-level implementation: (i) standardised image quality metrics; (ii) reporting on usage and accuracy; (iii) improving candidate lists (match scores); (iv) priority-based scheduling; (v) pooled quota; (vi) vendor feature set support and (vii) the XML data exchange file format (XML).

Standard Image Capture Quality

The Prüm Decisions are currently vague in its description of the quality requirements of fingerprint images deeming they should simply be suitable for automatic matching with an AFIS. Although difficult to quantify due to a lack of data, it is known that Member States vary significantly in the quality control methods regarding the storage of ten-print data into AFIS systems.

It is proposed that a standard Prüm quality metric be adopted based on NFIQ or NFIQ2. Member State data exchanges would include a quality metric for each fingerprint image. Member States will use the standard to ensure minimum quality of ten-print images and allow rejection of search requests in a standardised manner. This solution proposes the following changes to core Prüm principles:

- Ten-print data shared between Member States should use a common standard for communicating and ensuring a minimal level of quality.
- The standard quality framework would be NFIQ or NFIQ2.
- Ten-print image data would have minimum quality values defined. For example, for NFIQ a suitable minimum level for ten-print data could be Level 4 (5 being the highest). With NFIQ2 a minimum score of 75 (scale running 0-100) would be required. NFIQ2 would be the preferred option. These would need agreeing between Member States.
- Member States would include the NFIQ or NFIQ2 score for all images exchanged. This quality value would be included in each exchange.
- Latent and ten-print searches should be logically separated. This implies that Member States will be required to isolate each data type by having different gallery databases or using meta-data/grouping to separate from searches. This will not incur a large impact given transaction types are already defined and most Member States will already separate data types. However, this will ensure consistency for any Member States who do not do this already.

Member States were requested to provide details of their existing support for any international standard for image quality reporting.

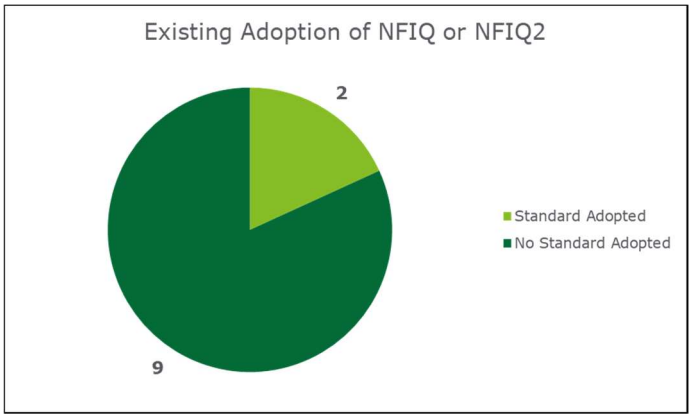


Figure 4 - Existing Adoption of NFIQ or NFIQ2

82% of Member States adopt a proprietary quality assessment method that is supplied by their AFIS vendor. Only 18% currently support NFIQ. Therefore for this solution to be adopted, it is expected most Member States will need to upgrade system capabilities and system integration with Prüm.

Most AFIS platforms provided by leading vendors (and adopted by Member States) do not include NFIQ or NFIQ2 as standard in their software packages. In fact most only include a proprietary based quality assessment and scoring mechanism which is built to complement their own algorithm. Therefore, adoption of one of these quality metrics (NFIQ2 preferred pending its readiness for use) will require one of the following options:

- Option #1 – Member States request the inclusion of NFIQ2 in their AFIS platform from the providing vendor;
- Option #2 - Member States develop an external quality assessment prior to enrolment of images into the AFIS and then store the metric in the platform along with other meta-data currently saved.

Option #1 would likely be an expensive approach as it would require vendors to customise their AFIS software. Option #2 would be lower in cost but would require development at a nation level and increase the complexity of the overall solution. Note there is no cost in acquiring or using NFIQ2 quality assessment tools which are provided by NIST.

Usage Reporting

Prüm can be updated to define a set of minimum usage and accuracy statistics that should be stored for all requests and responses received. This could allow Member States to understand and report statistics on their search usage, requests received, errors, downtime and various other system metrics. The usage data would be stored locally at each Member State and would support annual reporting to the European Commission.

The above approach is based on the existing de-centralized solution however if a central router is adopted then this usage data can be captured centrally by the hosting EU agency. This would reduce the cost as databases, software and support will only be needed once rather than for each Member State.

It is proposed that the Prüm ICD be updated to define the minimum data items that should be stored automatically by all Member States (or the central router should it be adopted). The full data dictionary would need to be agreed within the working group, however would likely include the following (at minimum) for each request AND response handled:

- Date\time
- Type of transaction (ten-print to ten-print, latent etc.)
- Number of candidates (responses only)
- Status code (response only) indicating success, error (with reason)

Accuracy Reporting

In addition to usage data a proposed solution is defined to allow receiving Member States to record back the confirmation of a hit once it has been manually verified. This would be enabled through a user interaction (confirming a hit) that would result in an automated message being sent to the requested Member State indicating the outcome of the request. This would enable a Member State to receive and store match accuracy/hits for their own AFIS.

Note that this is not part of or related to the subsequent Prüm Step 2 follow-up. This is an updated message workflow to aid the capture of data, therefore the revised message flow would be:

- Requesting Member State send search image;
- Requested Member State returns candidate list results;
- Requesting Member State users reviews results and confirm a hit/no-hit;
- Requesting Member State system communicates results to requesting MS;
- Requested Member State stores this data locally (central router if adopted);
- Requesting Member States follows up with Prüm Step 2 (as current).

Member State searches are open-set, meaning it is not known if a subject being searched for (for example with a latent image) is actually present in the target gallery. Therefore it is not possible to implement a reporting structure for misses. However, it is still possible to provide statistical reporting on (i) a confirmation of a hit or no-hit following requesting Member State review; and (ii) feedback on the rank position of a correct match within a candidate list.

For latent to ten-print searches where up to 10 results could be supplied by the requested Member State, reporting of hit/no-hit along with, for hits, the rank position of the correct candidate would be supplied back to the requested Member State.

It is proposed that this solution would be implemented to report the following data items in response to each data request.

- Hit or No-Hit – indication if the returned results actually contained a true hit
- Rank Position of Hit – allow the Member State to understand the distribution of rank position for true matches
- Length of Candidate List Received – confirmation of the length of the list

To not introduce additional demand on human capacity, it is recommended to automate this process within the Prüm interface agreement. To support this, the current standards for data exchange could be updated to include an additional message exchange using the existing NIST container file format.

It is proposed that an automated response be sent from the requesting Member States once they have completed a manual review of the match results. The NIST container could include the following:

- Type-1 record with a standard header and reference to the TCR of the resulting package. This would allow tracing to the original request if needed.
- Type-2 record containing fields for hit/no-hit (flag), position of correct match, reported position and optionally the reference to the correct match. It would also include the original case number and crime reference.

This type of information would allow Member States to review their performance and make data-driven decisions on how to best serve the requirements of Prüm. For example, it may be found by some Member States that accurate matches most commonly appear in the top five positions and allow the reducing candidate lists.

Improve Candidate Lists (Match Scores)

The current Prüm framework defines the maximum candidate list for latent searches to be 10 and it has been highlighted that this can cause privacy concerns for the non-match data and impact infrastructure bandwidth.

However, most Member States agree that reducing candidate list sizes would increase the chances of misses and is not welcomed. In fact, some Member States indicate the candidate lists could be higher.

Without access to usage and performance data on the usual rank position of matches, it is not possible to make recommendations on the reducing candidate list sizes.

With the capability of AFIS platforms across Member States likely to vary significantly, it is not possible to state an optimal candidate list size. The limit needs to be large enough to cater for all Member States – for some it is possible that a limit of 10 is indeed already too small and results in misses, whereas for others five may usually be sufficient. There is no one size fits all.

Looking for other ways to improve usability of multiple large results lists, this solution proposes the inclusion of match scores in search results sent to requesting Member States. This will allow receiving Member States to compare the relative match scores of each result and focus on those with highest confidence.

Match scores are a proprietary metric generated by AFIS platforms which indicate the confidence of two images or templates being the same individual. A higher score usually indicates a higher confidence in the match.

For example if presented with the following match scores with nil (0) being lowest confidence and 1000 the highest, it is clear the top three results have significantly higher confidence then the remaining seven.

925, 762, 750, 126, 98, 88, 69, 59, 45, 14

If Member State receive these match scores they can quickly highlight those of interest. For Member States who operate the same AFIS technology, these scores would also allow the combining of results received from multiple Member States for the same request. For example, if a requesting Member State received five candidate lists each containing 10 records (50 total) it may be possible to combine the match scores and produce a single candidate list. This could offer a significant time saving when verifying match results from multiple Member States.

However, it is important to note that this capability would only be viable where AFIS tech stacks and algorithms were the same across Member States. If Member States were receiving match scores from a range of AFIS systems for which they did not understand the scores, then having these may well cause additional confusion. For this reason this solution should only be optional allowing Member States to agree sharing only where deemed useful, if indeed it is adopted.

Priority-based Scheduling

A common concern for many Member States is daily quota and their impact on the ability to perform a sufficient amount of searches. Some Member States struggle to deal with the demand of the combined national-level and Prüm requests for fingerprint searches.

Both from a technical or infrastructure aspect and administration point of view. The key impact of the enforced quota levels is that it impedes the law enforcement capability of requesting Member States.

We have considered ways that quota could be increased or changed to allow more requests to be served without impact on the technical or human bandwidth of a requested Member State.

The proposed solution would be to change the existing principle of the Prüm framework which defines a single service level agreement (SLA) of 24 hours, to adopt a priority-based approach.

Priority levels need agreeing, the following are presented as examples:

- Priority Level 1 – request must be processed within 12 hours
- Priority Level 2 – requests must be processed within 24 hours
- Priority Level 3 – requests must be processed within 48 hours

Where possible, requesting Member States should send requests with a priority 3, which would have the largest daily quota. Priority 1 would have the smallest daily quota and likely be reserved for serious crimes. Daily quota would need agreeing between Member States.

Quota would still be defined, however, these would be per priority with the intention of not being on reducing workload for requested Member States, but providing the ability to control the demand in a more manageable way. Wherever possible, requesting Member States should send requests with a low priority level and it is expected that high priority requests would be limited to a very small number for use in investigations that are most time-critical.

The existing data exchange standards defined in the Prüm framework already support this process by way of the 'priority' field that is defined as an optional parameter on NIST files. The standard would not need to be updated. However, it is suggested the Prüm core principals be updated to define revised SLAs to support this.

This 'priority' field is defined as a numeric value of 1-9 with 1 indicating the highest priority. This field is currently defined as optional. It is not expected that this would be changed to mandatory and Member States could still have the option.

Pooled Quota

In addition to priority scheduling, it is also proposed to change the Prüm principles to support sharing of pooled quota limits. This would allow capacity saved due to low activity from some Member States to be utilised to serve Member States who have high demand.

The simplest way of achieving this is to adopt single daily quota for Member States. Member States will define how many requests per priority level (or in total if priority-based scheduling is not adopted) they can receive per day and requests served on a first-come, first-served basis. Once the total daily limit exceeds the limit the Member State stops processing new requests.

Adopt ANSI/NIST-ITL 1:2011 (2015 or later)

It is recommended that NIST/ANSI-ITL 1:2011 (2015 update) be adopted as the standard for the exchange of all data items within Prüm. For fingerprint, the standard:

- Provides a high level of interoperability with other ANSI/NIST-ITL based systems and standards such as EBTS and Interpol. Although systems use varying versions

of the standard, integration if easily adopted providing systems are implemented correctly
- Would be aligned to the transfer of facial images within Prüm which would need implemented Member State systems to fundamentally require the support of the standard anyway.

The general structure and header information for NIST containers are detailed in this document.

The current Prüm ICD definitions for all fingerprint record types would remain the same as currently defined as all current fields would be supported.

The current NIST format (Interpol) defined for Prüm is based on the traditional file encoding based approach using ASCII files which are encrypted and then attached to emails sent over SMTP. Many modern systems adopt an XML based encoding for NIST containers as it offers a range of benefits such as:

- Allows easier integration with other systems and modern technologies
- May remove the need for external technologies for reading NIST files
- Supports the adoption (if applicable) for Web-service communication
- Easier to transform files between different standards such as EBTS

Along with the updated NIST version, the Prüm definition would be amended to support both traditional encoding and XML based encoding. Member States would be required to then adopt the XML schema for their exchange implementations. It is expected that this would be a gradual process which slowly moves towards a more interoperable Prüm solution.

Type-9 Vendor Feature Set Support

Survey shows that the majority of Member States use AFIS platforms from the same two or three vendors. The ANSI/NIST-ITL 1-2000:2011 standard defines, for Type-9 minutia based records, several reserved fields to transmit proprietary feature data between disparate systems based on the same underlying framework. This is in addition to the ANSI INCITS 378 standard for minutia data.

This solution proposes that Member States who share a common AFIS technology vendor could agree to use these reserved fields for the transmission of pre-encoded feature data and avoid or compliment the transmission of image data.

This would offer the following advantages:

- Assured interoperability of biometric data between the Member States;
- Faster processing as quality check, image processing and encoding are avoided;
- Sharing match scores and greater integration between AFIS platforms.

This solution would require an update to the current (or inclusion in the new standard) Prüm framework data exchange format in order to define the use of these field. In addition, it would require agreement between Member States to use these optional fields and developing the integration into existing data exchanges. This is an optional mechanism for Member States and not a replacement of image sharing.

The following diagram shows the various stages of processing incurred by requested Member States for both the image based on a feature-based approach.

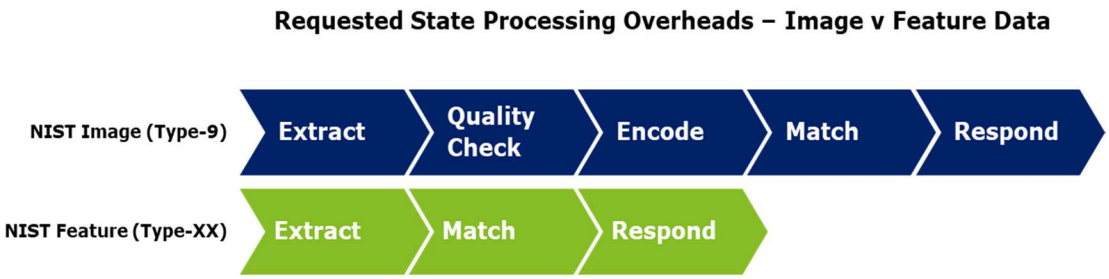


Figure 5 - Requested State Processing Overheads

This approach could improve processing overheads and possibly allow the increase in quota due to not needing to process the images.

2.3.2. Assessment

Each of the proposed solutions impacts individual Member States in different ways.

Operations and end-users

The only solution that incurs an operational impact is the potential change in SLAs based on different request priorities. It is anticipated that some training and alignment of Member State processes would be required to align with the new SLAs and determine how to prioritise their requests.

As many Member States use different AFIS vendors the inclusion of match scores in response as mandatory would not be recommended. In addition, many Member States already adopt a micro matcher approach to handling results which negates the need to understand rank position and match confidence in the response. Therefore, the study concludes that the communication of match scores should not be mandatory for Member States. However, the standard does permit the communication of match scores should Member States choose to.

Technical and Security

Adopting a standardised image quality metric such as NFIQ2 across Prüm will impact the majority of Member States. The majority indicated they did not currently have a standard quality metric in place and those who did were based on NFIQ and would therefore need to be updated.

To implement automated reporting of hit data, Member States would need to update existing applications and systems to allow the sending of additional NIST container message.

- Automate sending the following up data based following confirmation of a hit or no-hit by a forensic user
- Handle the receipt of incoming data and storage within a database for future reporting and store within a national level database

To support priority-based requests Member States will need to implement systems that can schedule requests on their infrastructure based on the priority level assigned by the

requesting state. They would also need to change their quota enforcement polices to restrict based on priority.

Lastly, to support the transmission of vendor feature data, Member States would be required to change their requests to include vendor specific templates in addition to raw images. Requested Member States would need to change current processing middleware to extract the template and send directly for matching. Image quality assessment and processing is the most expensive part of the overall match pipeline and the reduced demand could have a significant positive impact on Member State bandwidth.

Legal and Data Protection

Overall, the proposed solutions would have a reduced impact from a data protection perspective, owing to the fact that no additional categories of data are envisaged, and the purposes underlying such processing remain the same.

Yet, it is worthwhile mentioning or confirming following considerations with regard to data protection:

1) Usage Reporting: Reporting on aggregate data does not entail the processing of any personally identifiable information. However, Member States should be reminded of the practices to be followed when statistics are produced at local level. In particular, statistics information should only be based on aggregate data and their content should never identify or spot out individuals; it is recommended to keep the statistics report segregated from the pure analysis data on which they are based. Appropriate training of the agents generating those statistics on how best they could ensure the generality of reporting and its "non-traceability" to personal data would help to ensure the no-named and neutral nature of such reporting. Yet, the above recommendations are general with regard to any type of reporting based on aggregate data and they do not concern only the revision of the existing Prüm framework.

2) The potential generation of reporting at centralised level, thus by the European Commission or another body/entity to which this activity may be delegated do not entail any particular data protection considerations either, based on the proposed architecture herein below (Section 5.3.1).

   Firstly, the requests contain non-coding parts of fingerprints as reference data – therefore can only indirectly be used to identify an individual (i.e. through matching processes in the AFIS platforms, processes that remain under the full control of Member States). This data is outside the scope of the reporting.

   Secondly, assuming that the reporting will take place at centralised level, the proposed design states that the central router will never have access to the underlying payload of biometric (or response) data. Indeed, in Section 5.3.1, a multi-layer encryption process is proposed with regard to the data exchanged through the central router - this would mean that the central router only ever has access to the header information, being type of request, originating country, target country, date/time and, for responses, an error or success code. Access to this information is necessary for routing and reporting purposes. Yet, this set of information does not directly identify a person and it is very difficult to practically almost impossible (depending on the strength of encryption) to link these data to a person. In other words, no directly identifiable data is transmitted by the Member States and, if ever, a central router will be used for transmission, the central router will not have access to such identifying data either. Thus, in case that reporting at central router will be generated, this will consist only of data that cannot identify directly a person.

3) Accuracy Reporting: With regard to the underlying data processing activities referring to informing the requested Member State of the success or not of a "hit", no personal data are reported. Actually, the only Type 2 data that the requesting Member State will report back to the requested one are restricted to: "hit/no-hit" (true/false), position of "hit" in results and length of the results. The aim being that the requested MS can then understand the quality of the match process performed. The only reference number here would be TCN/TRN (reference to the original request). These data cannot directly identify an individual; if a requesting MS wants the directly identifiable data they have to request it through their national representative. Moreover, the data that will be sent from the requesting Member State when reporting accuracy is not enriched with more personal data. This suggested approach does not replace the existing follow-up procedure which is used for requesting personal data. The data contained in the additional message flow will always remain meta-data only relating to the match verification process, in order to confirm to the requested Member State that the results provided has resulted in a "hit".

4) Improve Candidate Lists (Match Scores): From a privacy point of view, there is no "yes" or "no" answer as to whether the candidate lists must be shorter or longer than the 10 records provided, being the current rule.

   On the one hand, shortening the current list presents advantages in terms of data minimisation and proportionality given that less data transfers will practically occur between the Member States. However, this may not be the most suitable option for attaining the objectives of the fingerprint image sharing, as, according to the majority of the Member States, it will increase the number of potential matches. While this solution poses less privacy issues, it may impede attaining the legitimate objective of the fingerprint exchange, being the identification of the right candidate in the wide framework of preventing and combating crime.

5) Type-9 Vendor Feature Set Support: In general, the introduction of a standardised way for encoding fingerprint image data can bring some benefits also from a data protection perspective. In principle, having to fill in a restricted number of pre-determined fields should enhance the data quality in the provisioning process amongst the Member States. There are no specific legal or data protection consideration given that only the format for exchange would be adapted.

Cost Implications

The cost implications of each the solutions vary significantly, the following points describe the key implications for each:

- **Image Quality** – the cost of changing and adopting NFIQ is not expected to be high with a small amount of development work required by Member States to implement restrictions on their AFIS systems. Survey responses from 11 Member States indicate only 18% current adopt a standard framework such as NFIQ or NFIQ2.

- **Usage Reporting** – Member States would need to provide a statistical database to support the storage of usage data. Where not already implemented, logging would be required to ensure adhering to Prüm. Cost of this solution would be low and at least 3 Member States have already indicated existing availability of the technical components. However, if a central router is adopted then these costs could be further minimised as the implementation and support would only be done once at central level by the hosting EU agency.

- **Accuracy Reporting** – this solution would require some significant changes to Member States' existing systems and requires the development of a whole new message process to report back with. Member States would also need a national statistical database for the collection of accuracy data which will increase the overall technical and delivery costs.

- **Priority-based SLAs** – the cost of implementing scheduling systems will differ a lot between Member States. Some will have existing message queue systems which can automatically schedule the incoming requests with minor changes to the scheduling. Others will need to develop this capability from scratch. Member States who operate federated national systems (for example where databases are split with different law enforcement authorities each having a separate database) the implementation of such an approach would be highly complex as each separate sub-system would require update.

- **Data Exchange Standards** – brings significant cost in changing to the XML based messaging format from that currently used. The benefit of this cost is hard to demonstrate in the short-term as it brings no performance and usability improvements. Costs are detailed in this document.

- **Vendor Feature Data Support** - the technical costs with Member States adopting feature-based matching is not expected to be high. However significant costs may be incurred through the testing and deployment of such exchanges with other Member States.

All cost drivers and estimates are supplied in the CBA provided with this study.

2.3.3. Conclusion

The following points highlight the key conclusions and recommendations for the fingerprint data exchange.

- **Standardise Image Quality Metric** – the Prüm core principles should be updated to state a standard quality framework such as NFIQ or NFIQ2. The study does not recommend enforcement of the quality however it should be promoted and offered as guidance for all Member States to follow;
- **Usage Reporting** – this study does recommend that recording a mandatory set of usage data items be defined by Prüm to ensure the systematic gathering of data that correlates across Member States for consistent reporting accuracy;
- **Accuracy Reporting** – changes would allow Member States to collect data on their matching performance. However, image quality should be the key focus and the complexity of implementing should a reporting mechanism would be very high. This study does not recommend this solution and advises the adoption of usage data capture only;
- **Improve Candidate Lists** (Match Scores) – operational efficiency improvements could be experienced by users if Member States' AFIS technology is aligned. However, it is not expected that this would be useful for all Member States and if enforced (and used) as mandatory could cause confusion. It is agreed that this could still be useful in some scenarios and that there is a low cost of implementation to achieve it. Based on this, the study recommends updating Prüm to define an optional field for the reporting of match scores in search results. This can be used between Member States who wish to utilise it, i.e. they share a common scoring mechanism/technology;
- **Priority-based Scheduling** – this study does not recommend the implementation of multiple SLAs within Prüm or the deployment of scheduling systems. Through discussions with Member States representatives and survey of usefulness and complexity to implement, the study found the value would not outweigh the cost;

- **Pooled Quota** - the feedback from Member States has indicated that there is no desire to change the existing per Member State approach to managing bandwidth; although some Member States reported some issues hitting quota, only two Member States indicated it was a major point of pain; pooled quota are not recommended;
- **Data Exchange Standards** – it is recommended to update current standards to support the latest ANSI/NIST-ITL 1:2011 standard using XML encoding; full details of this are covered in previous paragraphs;
- **Vendor Feature Set Support** – the adoption of support for vendor or Member State specific feature sets could improve the processing overheads of handling requests and this study recommends that they be adopted as an optional set of fields. Member States should be able to choose, as they establish or update a connection, to share data using feature data. It should be noted that only Member States with compatible template types will be able to share data in this way. Compatible templates will be of the same algorithm version and vendor. It is not expected that the uptake of this feature will be significant, but given the interest expressed, it has value in being defined as an option in the ICD.

From a data protection point of view, the improvements or changes highlighted above would not entail as such any particular implications or threats with regard to personal data protection.

Finally, the study has given consideration to the architecture options 1 and 3 (central router and web-services)

- **Architecture (Central Router)** – should a central router (SMTP or Web-service based) be implemented, fingerprint requests would be packaged up as XML NIST containers and directed to the central router. No particular changes are expected to accommodate this solution. The adoption of ANSI/NIST-ITL 1:2011 (2015 or later) will allow this central router to handle only 1 data type for all biometric data and therefore if this architecture option is adopted, the change to a standard transfer type will increase the ease of the implementation.
- **Architecture (Web-services)** – should a Web-service-based integration model be implemented, requests would be packaged up as XML NIST containers attached to outgoing Web-service calls. No specific changes would be needed for the data exchange format. It would be attached as an XML payload on the outgoing/incoming Web-service calls. Again the adoption of a common biometric sharing standard will make this much easier to implement and make data sharing consistent across all biometric data types. Note that to support this, the fingerprint data exchange standard would need to be adopted and this would incur significant change, as detailed in section 1.2.
- **Interoperability** – by supporting ANSI/NIST-ITL 1:2011 (2015 or later) maximum support for interoperability can be achieved. Compatibility with any system that complies with the standard will be supported with minimal integration effort. This study believes the adoption of a common standard across European systems should be a key goal of all Member States for future-proofing of all systems and ensuring ease of deployment of new integration requirements.

The adoption of common standards and consistency with external agencies should be a key goal. All other recommendations made do not impact the architectural approach in any way.

2.4. *Improve DNA matching*

The sharing of DNA data under Prüm was defined in 2008 with the expectation that Member States would have implemented data exchanges by 2011. Whilst this, there were significant delays due to a range of legal issues and technical limitations. As of 2019, twenty-three Member States have operational DNA exchanges and with this wider adoption, it is a suitable time to seek to identify areas to improve it.

- **Loci Match Threshold** – there is a strong argument for both retaining the existing minimum number of matching loci and increasing them; in order to accommodate for all Member States capabilities and needs, the number of loci should be low, as the rule needs to accommodate for all Member States.
- **DNA Profiling Standards** – feedback from Member States indicated the level of analysis and quality of DNA profiles across and indeed, within Member States is wide ranging; Member States differ significantly in the number and type of loci they support; the lack of defined standards in the processing and storage of DNA profiles is seen as a limitation within Prüm.
- **Usage and Accuracy Data** – DNA exchanges in Prüm lack reporting capabilities, which would allow usage and performance statistics to be understood and used to drive decision making; this does not allow a global level of reporting and understanding of the number of DNA matches performed, hits identified, hits confirmed and stored along with the number of matching loci.
- **Inconsistent Exchange Format** – the XML based message scheme for sending and receiving DNA data are not aligned to any international standards or in fact, the other biometric types within Prüm; however, the current XML implementation appears to work well and provides a modern approach that could allow future easy integration into a web-service based architecture.

2.4.1. Proposal

The current standards for the exchange of DNA profiles between Member States are widely considered to be successful and there are no major issues identified other than the point raised of standardised exchange formats.

However, there is much debate on the success of DNA matching, based primarily on the lack of standards that govern the analysis and storage of DNA profiles across Member States, and on how match results should be determined and interpreted.

Based on these key findings, improvement opportunities have been identified in the areas of (i) a configurable minimum loci threshold and ESS support; (ii) usage reporting; and (iii) a standardised data exchange format.

Configurable Minimum Loci Matching Threshold

The minimum number of loci should remain the same at six, primarily because there is no one-size-fits-all and because the threshold needs to be low enough to meet the needs of all Member States. As with other groups, the Member States are inconclusive on a common agreed increase.

However, a new field in the DNA data exchange could allow Member States to define an alternative threshold level to be used. This field would allow the minimum number of loci threshold to be set in the header of each request.

This field would allow Member States to establish differing matching requirements as part of bilateral agreements with other Member States. For example, a Member State may decide to adopt seven as a minimum number of loci with one Member State, but 10 with another. This will allow, wherever possible, Member States to increase the

number of loci they would like to receive matches for from other states. To be clear – it is not suggested this would be set dynamically. Only to pre-agreed minimum levels.

To support this, Member States will need to ensure DNA processing capabilities are aligned and that samples are analysed using the same standard set of loci – for example, the European Standard Set (as already referenced in Prüm). It is expected that the current loci defined in Prüm (from the ESS) will likely need extending to accommodate all Member State needs. The exact loci to be defined and included needs to be agreed as part of Member State working groups.

Prüm should define that Member States agree matching loci on a bilateral basis however, to ensure symmetrical matching performance, the number of loci from the ESS should be the same for requests in both directions. A different minimum number of loci could also be defined for specimens and stains. For example, 12 matching loci for specimens and seven loci for stains. The key goal is to provide Member States flexibility in how they adopt DNA exchange rules.

Usage Reporting

Prüm can be updated to define a set of minimum usage statistics that should be stored for all requests and responses received.

This could allow Member States to understand and report statistics on their search usage, requests received, errors, downtime and various other system metrics. The usage data would be stored locally at each Member State and would support annual reporting to the European Commission.

The above approach is based on the existing de-centralized solution. However, if a central router is adopted (see chapter four) then this usage data can be captured centrally by the hosting EU agency. This would reduce the cost as databases, software and support will only be needed once rather than for each Member State.

It is proposed that the Prüm ICD be updated to define the minimum data items that should be stored automatically by all Member States (or the central router should it be adopted). The full data dictionary would need to be agreed within the working group, however would likely include the following (at minimum) for each request AND response handled:

- Date\time
- Type of transaction (stain, person etc.)
- Number of candidates (responses only)
- Status code (response only) indicating success, error (with reason)

Member States were surveyed on how useful recording of usage data would be with 70% indicated this would be desirable.

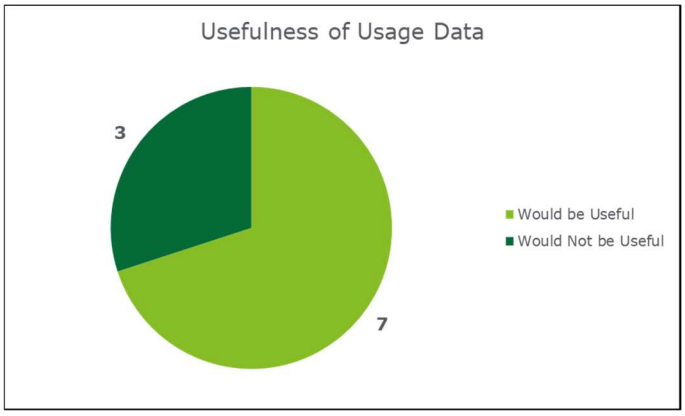


Figure 6 - Usefulness of Usage Data

Standardised Data Exchange Format

As defined in section 2.2 of this report, it is recommended that NIST/ANSI-ITL 1:2011 (2015 update) be adopted as the standard for the exchange of all data items within Prüm. DNA exchange could be transitioned to the same XML based file structure as also recommended for fingerprint and facial image data types. This would provide a common framework and long-term benefits from having a single exchange format to support.

Nevertheless, the current data exchange works to a perfectly acceptable level and is a well-defined XML based structure. There are no other reasons to adapt the exchange format other than consistency to the standard. It is the long-terms benefit in reduced complexity which make the transition to a standard format desirable.

If ANSI/NIST-ITL 1-2011 is to be adopted for DNA data exchanges it would require the adoption of Type-18 DNA record types. The Type-18 fully supports the existing fields defined in the Prüm DNA ICD.

It should be noted that the standard ANSI/NIST-ITL 1-2011 schema would need extending to define the fields required for Prüm and many fields defined in the standard would not be required or defined within the Prüm ICD. This is common to the application of ANSI/NIST-ITL 1-2011 for a specific use.

2.4.2. Assessment

Operations and end-users

Only the implementation of a new standard loci set would impact end-users and operations, as it may be necessary for some Member States to evolve their processes and technology to support the standard.

The implementation of bilateral agreements between Member States for matching loci levels would allow optional increases in the threshold to be used. This would decrease the number of matches returned and therefore the amount of manual verification required to process results would be less. For Member States who retain the current threshold, operational impact would remain as-is.

For example, users may be required to adopt new software and data collection kit in order to process DNA samples to the appropriate level of loci needed for Prüm (from the ESS). This would require training and process updates.

Technical and Security

Implementation of standard exchange formats and reporting methods in place would require significant IT investment. For example:

- Updates to existing DNA databases (CODIS and nationally developed non-CODIS) and analysis software to support the defined ESS loci set for Prüm;
- Changes to existing field definitions in the ICD to support new fields;
- Implementation of software to ensure loci information is correctly packages in the new message exchanges.

The process of adopting ANSI/NIST-ITL 1:2011 (2015 or later) will require Member States to change the XSD schema they adhere to for the packing of messages to be sent and received to other Member States.

Security would not be impacted as all existing communication mechanisms and encryption would be used.

Legal and Data Protection

Embedding an additional field that would indicate the number of loci threshold to be set for each specific request does not entail any data protection issues as such, given that data minimisation principle is even further met.

1) Usage Reporting: Reporting on aggregate data does not entail the processing of any personally identifiable information. However, Member States should be reminded of the practices to be followed when statistics are produced at local level. In particular, statistics information should only be based on aggregate data and their content should never identify or spot out individuals; it is recommended to keep the statistics report segregated from the pure analysis data on which they are based. Appropriate training of the agents generating those statistics on how best they could ensure the generality of reporting and its non-traceability to personal data. Yet, the above recommendations are general with regard to any type of reporting based on aggregate data and they do not concern only the revision of the existing Prüm framework.

2) Potential generation of reporting at centralised level, thus by the European Commission or another body/entity to which this activity may be delegated do not entail any particular data protection concerns either. In this regard, the explanations provided above with regard to the centralised reporting based on fingerprint data apply to DNA images too. In summary, the usage data that will be subject to reporting, through a central router will contain only reference data, being: the type of request, originating country, target country, date/time and, for responses, an error or success code. If a central router is used, access to this information from the central router will be necessary only for routing and reporting purposes. However, the above data do not directly identify a person.
   With regard to the reporting of usage data, the only data that would be subject to such reporting are reference numbers/meta-data to allow the requested MS to understand the match results. Directly identifiable personal information will only be communicated in subsequent follow-up requests and, hence, it will be outside of the "request" flow. This modality aligns with the data minimization and proportionality requirements of the data protection legal framework applicable.

Cost Implications

Adopting the new data exchange format will require Member States to adapt their existing systems. The cost of this has been surveyed and is discussed above.

The costs related to the adoption of a wider set of the ESS would be wide-ranging for each Member State. For example, the change could result in new kit and training of

forensic experts to be required in addition to significant analyses and database upgrades.

However, as the recommendation involves the optional ability to change the number of matching loci, Member States would be free to extend the scope of their systems and kit as and when they are ready. Upgrades will only be required when they need to start processing matches with a higher minimum level of loci.

Only four Member States indicated they currently capture over 12 loci from the ESS. The other ones did not provide this level of information. Indications were that the costs would not be too high in comparison to the value of allowing them to have a higher loci matching threshold.

2.4.3. Conclusion

The following points highlight the key conclusions for the DNA matching:

- **Configurable Minimum Loci Threshold** – it is clear that most Member States wish to increase the number of loci used in determining matches. However, the solution needs to be flexible for all Member States. The adoption of a new field supporting matching thresholds is recommended in addition to the current Prüm scope for defining bilateral matching thresholds. This provides all Member States with the ability to change matching loci threshold as required in the future and aligned to the capabilities of their technology and operational processes. The loci set defined for Prüm (from the ESS) needs agreeing as part of the discussions during definition of the new ICD.
- **Usage Reporting** – it is recommended to implement reporting requirements into Prüm, since if a future version of Prüm is to be effective and allow data-driven analysis and decisions to be made, data must be recorded and made available; the data items will allow Member States and the Commission to understand the adoption and use of DNA exchanges and match results can be analysed for a number of loci to determine optimum minimum threshold levels.
- **Standardised Data Exchange Format** – a common standard that is interoperable with other EU systems is highly desirable and such the long-term benefits of moving DNA to the new schema will be worth it. Therefore this study does recommend the adoption of ANSI/NIST-ITL 1-2011 for DNA data exchange however this should be done in a timescale suitable to the Member State. A target completion date should be set for the transition of all data items to the new standard.

From a data protection point of view, the improvements suggested by the proposed solution are in line with data protection requirements. Regarding the configurable minimum loci threshold that will be left at the discretion of the Member States, no data privacy issue are raised, given that the minimum matching threshold will remain similar (six common matching loci or more). In addition, the suggested improvements related to the centralised reporting of usage data and the types of data that will be used for reporting purposes do not entail any particular data protection considerations given that only reference data will be used and the central router will only have access to the data strictly needed for routing and transmission purposes.

The following points describe consideration for architecture options 1 and 3 (central router and Web-services).

- **Architecture (Central Router)** – should a central router (SMTP or Web-service based) be implemented, DNA requests would be packaged up as XML NIST containers and directed to the central router. No particular changes are expected to accommodate this solution. The adoption of ANSI/NIST-ITL 1:2011 (2015 or

later) will allow this central router to handle only 1 data type for all biometric data and therefore is this architecture option is adopted, the change to a standard transfer type will increase the ease of the implementation.

- **Architecture (Web-services) –** should a web-service based integration model be implemented, requests would be package up as XML NIST containers attached to outgoing Web-service calls. No specific changes would be needed for the data exchange format. It would be attached as an XML payload on the outgoing/incoming Web-service calls. Again the adoption of a common biometric sharing standard will make this much easier to implement and make data sharing consistent across all biometric data types.
- **Interoperability** – by supporting ANSI/NIST-ITL 1:2011 (2015 or later) maximum support for interoperability can be achieved. Compatibility with any system that complies with the standard will be supported with minimal integration effort. This study believes the adoption of a common standard across European systems should be a key goal of all Member States for future-proofing of all systems and ensuring ease of deployment of new integration requirements.

The adoption of common standards and consistency with external agencies should be a key goal. The recommendations made do not impact the architectural approach in any way.

2.5. *Vehicle Registration Data changes*

Member States exchange vehicle registration (VRD) data through the EUCARIS platform as foreseen in the Annex to the Council Decision 2008/616/JHA. This platform supports different applications made accessible to different end-users. The current exchange of VRD only covers part of the possible collected data in a vehicle's life cycle. The EUCARIS' Prüm application currently includes:

- Vehicle Registration Data (VRD): registration data and a subset of the technical vehicle data, originally delivered by the vehicle manufacturer in the certificate of conformity (CoC), stored at first registration of the vehicle in the national register and sometimes changed during the life cycle of the vehicle, after a modification of the vehicle;
- Vehicle status data: informing on theft of the vehicle itself, its plates or its documents, events concerning the vehicle, such as severe damage or destruction, and registration changes, e.g. after export.

2.5.1. Proposal

Four improvement solutions have been identified for VRD exchanges:

- Make the country field optional when performing a vehicle search;
- Implement a search log for all international searches;
- Allow searches of all vehicles registered under a single person or entity;
- Include vehicle colour and mileage as new items in the EUCARIS data set.

Make the country field optional when performing a vehicle search

Today, users of EUCARIS application, when searching for the VRD, have to mandatorily specify the license plate's country of origin. The study proposes to turn this requirement optional for cases of vehicles with unidentifiable country of origin. This would allow Member States to perform a single search that will look for matches in all Member States' databases.

This solution brings benefits in terms of timing efficiency, since Member States will avoid performing multiple licence plate searches, and will receive responses all in one place.

Make the search log for all international searches available

When looking up a vehicle, law enforcement officers are not made aware if any other EU law enforcement authority has performed Prüm searches on the same vehicle in the past, unless an alert has been issued on SIS.

The study proposes to introduce a new data field with the history of the licence plate's searches for each vehicle. This search log would include (i) the date of the search; (ii) the Member State that searched for the vehicle, including the requesting organisation within that Member State and the user involved; and (iii) the reason for the search.

All these data items are already present in the header of each message and available from the logging of EUCARIS concerning previous inquiries. These logs are currently being stored in EUCARIS but are not accessible to end users, and are stored only for auditing purposes.

Allowing traceability of international searches conducted to national databases would enable Member States to improve case coordination and facilitate identifying connections between different investigations.

In case of sensitive investigations, law enforcement officers should be able to not make their search log available to other Member States.

Search all vehicles registered under a single person or an entity

Currently, Member States are not able to perform searches on vehicle owners, only chassis number and licence plate. Allowing EUCARIS Prüm users to perform searches of all vehicles registered under a single natural person or legal entity would enhance the capacity to conduct investigations and connect cases.

DG TAXUD is already leading the development of the search feature for multiple vehicle ownership for tax authorities, the EUCARIS VAT application. Its official implementation due date for Member States is the 1st of January 2020.

EUCARIS could introduce a similar Prüm-specific feature, but it would be advisable to wait for the results of the VAT application implementation and use before implementing the feature in Prüm.

Include vehicle colour and mileage as new items in the EUCARIS data set

EUCARIS could add vehicle colour and mileage as data items in the data set of the EUCARIS Prüm application, bringing additional information that could increase the likelihood of a match and help law enforcement officers.

2.5.2. Assessment

Country Field

Operations and end-users

During 2017, EUCARIS Prüm network supported more than 10 million inquiries among all Member States. Excessive usage of the possibility of performing searches to all national databases without specifying the country field will lead to an increase of requests on the system and ultimately imply a greater use of IT resources.

As such, law enforcement authorities should always specify the license plate's country origin if possible. If this is not possible, the following process would take place:

- A law enforcement officer uses a new EUCARIS service to search for the origin (country of registration) of a vehicle by entering only a vehicle licence plate number as input data;
- The request is sent to all countries connected to EUCARIS Prüm; the response contains a minimum set (VIN number, country of origin, and vehicle make, commercial name and category code) of vehicle data allowing the officer, in case of multiple possible candidates, to select the right vehicle and its country of origin;
- Based on this response the officer is able to perform the search with the exact country and seek for the owner/holder of the vehicle.

The advantage of this approach is that it avoids the exchange of personal data related to vehicle owner/holders that are not relevant for the case (false positives).

Technical and Security

EUCARIS would develop the new service and deploy it to the EUCARIS Prüm application as a feature. There is no technical limitation in allowing users to perform license plate searches without specification of a country code. Then, the Member States should add the feature in their national applications.

Even though this could benefit some specific investigations, e.g. where the country of registration is not clear, this new search feature could lead to a capacity overload of the Member States' systems since instead of performing a search in a specific country, searches would query all Member States' system servers to search for the license plate number. Nevertheless, since most times end-users are able to identify the country of origin, this should not affect current capacity.

Legal and data protection

Vehicle data are considered as personal data under Article 3(1) of the Law Enforcement Directive (hereinafter, LED) to the extent that they lead to the identification of a natural person. The processing of this personal data can take place by competent authorities in the context of the performance of tasks of criminal investigations as set out in Article 1(1) of the LED5. In addition, data processed should be compliant with data protection principles foreseen in Article 4(1) of the LED. Specific emphasis should be given on data minimisation and purpose limitation principles, meaning that data processed should be adequate, relevant and limited to what is necessary for which they are processed.

If multiple vehicles are returned for a search, a minimum set of data should be provided to the law enforcement officer in order to identify the appropriate vehicle. The study suggests to return the license plate, the origin, the brand, the model and the colour of the vehicle. Limiting the response to these types of data appears from a first sight to align with data minimisation and proportionality rules, provided that all those data elements are necessary in order to limit the research to a very narrow number of cars, and ideally a single one only, and thus, a single driver.

Making the country field optional would therefore be fully aligned with the EU and Member State data protection laws, given that the process will be limited to a minimum set of data as long as this restriction does not impact on the quality of results and correct "hits".

The proposed measure would not entail the processing of additional categories of personal data, or processing for purposes other than those that informed the initial collection of data. From this perspective, it is unlikely that the proposed measure would entail additional risks to the rights and freedoms of data subjects when compared to present data processing activities.

The mandatory characterisation for the data item "Country of registration" in Point 1.2.2.2, Chapter 3 of the Annex to the Council Decision 2008/616/JHA would have to mention an exception for when Member States fail to identify the country.

Changes would appear as shown in the **Error! Reference source not found.**.

Item	M/O (1)	Remarks	Prüm Y/N (2)
Data relating to vehicles			
Country of registration	O (3)		Y

(1) M = mandatory when available in national registry, O = optional
(2) All the attributes specifically allocated by the Member States are indicated with Y
(3) Optional when Member States are unable to identify the country of registration of the searched vehicle
(4) Only available and mandatory when "country" field is left empty

[5] See Article 1(1) of the Law Enforcement Directive: *"This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".*

Illustrative Table 1 - Changes in data items for data relating to vehicles

Search Log

Operations and end-users

If one of the inquiries is relevant for the case investigation, Member States will now be aware of other investigations that took place. In order to contact these case investigators, the procedure should follow the steps of the Prüm follow-up procedure that are detailed in chapter 2. If the proposed follow-up procedure cannot be implemented, classic police cooperation as described in the Swedish Framework should take place.

Technical and Security

In order to implement such a solution:

- EUCARIS would develop an index containing the searches per vehicle, ensuring that Member States will not get any direct access to each other's logging, only to this index;
- The EUCARIS platform would keep this registration available for an agreed period of time due to data minimisation reasons. Currently, the maximum time that EUCARIS can keep this data is two years;
- EUCARIS would include this field automatically in the current messages, implying a technical development;
- The possibility to not render the search log available should be made available to law enforcement authorities;
- Member States would have to assure that this new information is available in their user application's database, and not just the auditing one.

Legal and data protection

Point 3.2.1, Chapter 3 of the Annex to the Council Decision 2008/616/JHA, referring to general features, would have to include these features.

New data items would also have to be included in Point 1.2.2.2, Chapter 3 of the Annex to the Council Decision 2008/616/JHA:

Item	M/O (1)	Remarks	Prüm Y/N (2)
Data relating to vehicle search history		The items below will not be included in hidden requests	
Date/time of the search	M		
Requesting country	M		
Requesting user-id	O		Y
Reason for the search	O		

(1) M = mandatory when available in national registry, O = optional
(2) All the attributes specifically allocated by the Member States are indicated with Y

Illustrative Table 2 - New data items for search history

As a first step, a legal provision to make Member States' search history accessible in future responses is necessary. Member States can include this decision via a configuration within EUCARIS.

From a data protection perspective, the IT implementation envisaged herein appears to align with the "data protection by design" requirement. We would recommend following improvement points for full alignment with data protection laws:

- The introduction of the index containing the searches per vehicle should only contain the elements that would be strictly needed to identify a very limited number of vehicles (e.g., reporting country but not the reason resulting in reporting on the national database – which might lead to information identifying a person);
- The herein suggested retention period of 2 years should be justified and reviewed if needed in consideration of the amplified now scope, i.e., why it is necessary to keep the index data so long and if yes, if this is needed for all data of the index.
- Additional IT measures and procedures may have to be put in place to ensure the accuracy and correctness of the information in the user application's database. Training of the law enforcement agents may be needed to remind rules regarding data accuracy but also in order to provide them with directions on how handling the information if they access searches of other police officers (see below).
- Appropriate logging controls at the level of index search but also for the national user applications must be put in place or reviewed.

Law enforcement officers should be able to decide if their EUCARIS searches are accessible by other police officers. Manual processing will be applied and it will permit police officers ticking a box to decide the accessibility of their searches to other police officers. This scenario would also require the setting-up or reviewing of a data access procedure defining, amongst other elements:

- The criteria based on which the access to requesting officers will be granted;
- The content that should be accessed (e.g., limitations to certain fields or access of those through additional procedural steps such as specific justification or per seniority level);
- The scope of authorisation (e.g., "view" only access, "access and copy", etc.);
- The type of access (on an ad-hoc basis or more general at certain levels);
- Logging capability (e.g., for which actions on the data);
- Review and withdrawal process for the granted access; and
- Log-in credentials (e.g., two-factor authentication, other, etc.).

As the data collected will be specified, explicit and used for legitimate purposes (i.e. for sake of criminal investigation procedures and criminal offences including processing of sensitive personal data), it is deemed that these searches will comply with the LED (see Article 4(1)(b)).

Moreover, search findings should be made available only to criminal investigators in charge or responsible for a given case and not to all patrol police officers in order to respect the proportionality principle. Keeping logs of the types of searches initiated by each criminal investigator on EUCARIS and their actions on the retrieved data (e.g. extract or copying data out of the system, types of searches initiated) would be a means to verify the lawfulness and proportionality of processing activities, in line with Article 25 LED.

In particular, Member States' competent authorities should implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing of EUCARIS search logs is performed in accordance with LED and its scope is respected. Those measures shall be reviewed and updated where necessary. These measures shall include the implementation of appropriate data protection policies by the authorities, as data controllers. The dedicated data protection policies have to include and provide for proportionate processing of driving licenses data and as a result a

balance will be achieved between the means used for processing of data (EUCARIS service) and the intended aim (processing of data related to search logs).

Under the aforementioned proposed solution, countries connected to EUCARIS service, should provide for a periodic review of the need for the storage of history of the search logs related to specific vehicles as well as procedural measures, e.g. privacy statement referring to the retention period of data concerned and who is responsible for review. The latter can also be defined through a governance plan, ensuring the time limits (Article 5 of the LED).

Vehicle Search

Operations and end-users

This feature would consist of a two-step approach, working for both natural and legal persons:

- The requesting Member State searches one of the suspected vehicles in its EUCARIS Prüm application;
- If the data received from the request includes the owner's name, the requesting Member State searches EUCARIS using the owner's name as a search parameter. Further biographic data can be added as search criteria to further filter the results, should it be available;
- Result: the requesting Member States receives all existing vehicles owned by that specific owner.

The biographic data should include the owner's date of birth and ID number. These items are to be discussed between Member States, to account for different natural legislations. The two-step approach is necessary because of:

- Possible typing and misspelling errors;
- Multiple persons with the same name;
- Companies with different names in different countries.

Given the risk to provide information of another entity or physical person, and the high likelihood of false positives, the study recommends the two-step approach.

Technical and Security

This solution implies implementing a specific search feature present in the EUCARIS VAT, and make it completely independent from it.

EUCARIS needs to copy this feature and user group under another service name, from the VAT application to the Prüm application, since there can be no connection between them.

The feature would allow the searching of vehicles using license plate as an input parameter and returning a VRD and Owners Name in the output. The second step would take Owner Name as input and return all VRD associated to it.

Member States would have to install this feature in their national applications.

EUCARIS should technically block the availability of the second step of the proposed approach (search by name) until the first step is performed (search by licence plate), thus guaranteeing the scope restriction mentioned before.

Legal and data protection

The design and process as explained above aligns at first sight with data protection requirements. It seems that the Owner Name will only be used as a second step of the search, namely when the input received after the first request (i.e., by inputting vehicle's chassis number or registration number) includes the owner's name (that, at present, does not figure in the mandatory list of data types the requested Member State should report). Keeping the owner's name only as trigger for the second step of the research and as optional element are, in our view, two factors to ensure that data proportionality is being considered.

To align with the same principle (proportionality) but also data minimisation, the insertion of other biographic data in the second step would in principle also be considered as essential depending on the needs of the specific case at hand. It should be examined whether other biographic data are really critical in the case at hand for achieving the most accurate results when the owner's name alone would not be sufficient for achieving this. On this point, the combination of both the unique identification number of a person (e.g. eID or passport number) and of the date of birth should be necessary in order to receive accurate results (identify the correct person and avoid "false positives").

The above two-step approach and its modalities could be further elaborated in the revised Prüm framework. In addition, it would be worthwhile conducting a more elaborated analysis on how ensuring the best "privacy enhancing" implementation of this approach at operational level.

Elements that could for example be considered as essential from a data protection point of view could be:

- Give appropriate training to the officers who will conduct the searches on the EUCARIS data exchange system on how practically triggering and enriching their searches, step-by-step, in compliance with data minimisation and proportionality rules.
- Implement adequate logging capabilities at the legacy systems of the Member States connected to EUCARIS; moreover, check periodically the efficiency of those logging capabilities in order to trace the respect of the above principles by the national officers conducting the searches.

Colour and mileage

Operations and end-users

In order to include vehicle colour and mileage in Prüm, Member States will need to collect the data and store it in their national databases that are connected to the EUCARIS Prüm application, so that they will be made available for requests. The regular collection of mileage data should be enforced for this opportunity to be implemented.

The EUCARIS mileage application's features could be included in the EUCARIS Prüm application. Mileage data should be an optional field, as some countries do not have this type of information or do not register mileage until three years after the vehicle's initial registration.

When receiving vehicle colour information, Member States need to take into account that re-painting vehicles is easily done in some European Union countries.

All legal changes concerning the Prüm Decisions would have to be included in the next-generation Prüm legislation. All VRD changes need to undergo the following process:

- EUCARIS delivers a quotation for all extensions and changes;
- All Member States discuss and agree to the changes in the EU decision making framework and subsequently in the yearly EUCARIS General Assembly meeting;

- At this point the changes can be included in Prüm legislation;
- EUCARIS develops the solution;
- The solution undergoes an acceptance test by a technical working group composed by EUCARIS Member States;
- EUCARIS supports Member States' technical implementation and tests it;
- Member States are able to use the additional services.

Technical and Security

Adding new data items would require changes to Member State applications and the EUCARIS Prüm application's data set. Whilst colour would be a simple text entry field and incur low implementation overhead, mileage would require integration with the EUCARIS mileage application and therefore would incur higher technical complexity, since the data needs to be updated on a regular basis.

Legal and data protection

The Annex to the Council Decision 2008/616/JHA would have to include the new data items, specifically Point 1.2.2.2 of Chapter 3 (VRD complete data set). The inclusion would appear as shown in the table.

Item	M/O (1)	Remarks	Prüm Y/N (2)
Data relating to vehicles			
Mileage	O		Y
Colour	O	(R (3)) e.g. Red, Blue, etc.	Y

(1) M = mandatory when available in national registry, O = optional
(2) All the attributes specifically allocated by the Member States are indicated with Y
(3) Harmonised document abbreviation, see Council Directive 1999/37/EC of 29 April 1999

Illustrative Table 3 – New data items for data relating to vehicles

For colour, the naming system will be the one on the Council Directive 1999/37/EC. In the Council Directive 1999/37/EC, there is no abbreviation for mileage. Nevertheless, in order to avoid misunderstandings, end-users should enter the vehicle mileage with the corresponding metric (Kilometres/miles).

The mileage data shared may go from simply exchanging the last registered mileage to exchanging a more exhaustive list of items from the mileage history, such as registration date, country and authority, odometer details, etc. The proportionality and data minimisation rules should be applied in order to determine which exact types of mileage data should be exchanged. A step-by-step approach built in the search (as in the case of owner's name), meaning providing at first only the most recent and relevant data type and then amplifying the research in follow-up searches on a "need to know" basis, could be beneficial from a data protection point of view.

Overall cost implications

According to the EUCARIS Treaty, any costs related to any changes in EUCARIS technical applications are covered by Member States, equally shared among them. Member States also need to cover their national costs of implementation, at police and registration authority level. The costs are as follows and will ultimately be borne by the Member States:

Solutions	Cost assessment

A) Make the country field optional when performing a vehicle search	The study foresees significant costs with developing the feature for searching without specifying country of origin, along with the minimum set of vehicle data.
B) Implement a search log for all international searches	Implementation costs relate to the creation an index, a new data field, develop the queries and include the option to not share the log in the index.
C) Search all vehicles registered under a single person or an entity	This change would imply limited costs of new developments in the Member State applications, since the implemented feature is already developed for the DG TAXUD application.
D) Include vehicle colour and mileage as new items in the EUCARIS data set	EUCARIS can transfer the mileage data item from the EUCARIS Mileage application. Additional costs would depend on Member States' maturity regarding the collection and storage of the data items mentioned.

Table 2 - Cost assessment

2.5.3. Conclusion

Overall, the added solutions in the EUCARIS Prüm application would bring benefits to Member States by improving process efficiency and efficacy. The proposed features and data items would increase the amount of data available for vehicle-related investigations, promote international cooperation and decrease end-user workload. All solutions are fairly easy to implement and do not require substantial investments.

When implementing these solutions, Member States will face several constraints, such as the collection of mileage or ensuring that data is consistently captured and shared.

In conclusion, it is proposed to include the four solutions, (i) making the country field optional for searches, (ii) making the search log available, (iii) searching all vehicles registered under a single person or entity and (iv) including the vehicle colour and mileage, in the next-generation Prüm. From a data protection point of view, these solutions do not raise any specific data protection considerations as long as the "privacy enhancing" approach is respected when operationalising those solutions. In light of the afore-mentioned analysis, it appears that the way the searches based on the above elements will be built are in line the purpose limitation and data minimisation. Ideally, this could be confirmed through a more elaborated analysis at the time the solutions receive a "go" towards implementation.

All improvement solutions are expected to have a minor development time. Copying and adapting existing applications to the EUCARIS Prüm application will take longer than creating new data items, but should be manageable in about two years.

3. IMPROVING THE FOLLOW-UP PROCEDURE

When a hit has been confirmed in a data exchange under Prüm, the follow-up procedure can take place. This follow-up communication, unlike the first step, is not covered by the Prüm Decisions. Instead it is "governed by the national law, including the legal assistance rules, of the requested Member State".[6] The efficiency and efficacy of the follow-up procedure affect the overall performance of Prüm information exchanges.

The difference in national legislations and processes has led to operational inefficiencies in the exchange of follow-up information between Member States, namely in:

- **National and international procedures:** The current follow-up procedure can be lengthy, hampering the Prüm exchange. In extreme cases, Member States have had to wait for several months before receiving follow-up information, mainly due to national processes;
- **Communication channels:** The use of different communications channels creates unnecessary coordination efforts, while also affecting the statistical analysis of the data exchanged;
- **Data exchanged:** Undefined data sets make the information exchange non-harmonised, prone to misunderstandings and can lead to the supply of information in several sets.

In order to tackle these issues, four different solutions are proposed:

- **Enforce a quick answer in the follow-up procedure**: An initial step in the follow-up procedure for the fast exchange of the most relevant investigation data will improve overall communication speed and reduce current workload;
- **Provide a limited core-data set by default with high-accuracy searches:** For a limited sub-set of fingerprint searches, such as ten-print to ten-print identifications, the accuracy of the match is generally high-enough to validate a correct hit by default. In the majority of cases, only one candidate will be returned by the National system. For this category of searches, a limited core-data of names, (gender), date-of-birth, Nationality and crimes, could be returned by default without a human follow-up;
- **Single communication channel**: Deciding on the default channel for international communications will promote both the process efficiency and the collection and analysis of data exchanged;
- **Implement UMF**: A standardised data exchange format that allows disparate systems to communicate data sets in a consistent manner which reduces complexity, data errors and improves processing overheads.

3.1. *Enforce a quick answer in the follow-up procedure*

After a confirmed hit, Member States decide on initiating the follow-up procedure to ask for additional information. As mentioned, the follow-up procedure is covered by national rules, and not by the Prüm Decisions. Member States have reported in extreme cases having had to wait for several months before receiving case-related information, hampering the criminal investigations and prosecutions.

3.1.1. Proposal

Introducing a step where the core information of the identity details would be shared in a reasonable timeframe would greatly benefit the information exchange for the purpose of preventing and investigating criminal offences.

[6] Articles 5 and 10 of the Council Decision 2008/615/JHA

This step would consist in sharing between Member States, after a confirmed hit, a common minimum data set with information relative to the respective biometric profile. This process should be governed by Prüm legislation, with clearly defined timeframes to answer the request. The proposal for the minimum data set is the following:

- First name and surname (mandatory);
- Date of birth (mandatory) and place of birth (mandatory where available);
- Gender (where available);
- Nationality or Nationalities (mandatory);
- Most recent offence in which the fingerprints/DNA-profile (and possibly facial images) were collected (mandatory);
- Contact details of the law enforcement authority responsible for the case (mandatory);
- Additional DNA, fingerprints and mugshots (optional).

It should be clearly stated in the answer if a data item is not available in the requested country's database or if it could not be shared. The rest of available information in the minimum data set should be shared, except optional information.

After the minimum data set is received, and only in cases in which it is needed, Member States could request more detailed information on the suspect as a "Step 3", which would then follow the traditional law enforcement cooperation framework.

Furthermore, well-defined SLAs will need to be established to support this new step in the process.

The new process could be implemented through the proposed web-service communication system, (see 5.3.3) or through the use of a single communication channel (see 3.2).

Member States should promote the implementation of automated solutions to retrieve the minimum data set and sharing it with the requesting Member State that will allow even faster exchange of follow-up information. Alternatively, a process of manual authorisation or the release of core identity data could be foreseen.

In the latter case, the process would go as follows:

1) After a hit has been validated, a follow-up request is automatically sent out by the forensic expert.
2) A Member State receives a follow-up request after a confirmed match with the reference number of the biometric profile, with a mention of the already available information they possess;
3) The system will automatically retrieve a minimum data set of personal identity information based on the reference number of the biometric profile from the national database and send it to the requested NCP;
4) Then, the requested NCP would use the release function: consists in a quick validation screen with the minimum data set presented and an action button for authorizing the sending of the data;
5) If it is approved, it will automatically create a message and share it with the requesting Member State through the communication channel.

The exchange of information for both the exchange of minimum data set and for the follow-up process of complementary information (so-called step 3) should be UMF-compliant. This matter will be developed in the section 3.3 - Implement UMF.

If Member States implement the proposed solution, the study foresees that requesting Member States would get faster access to relevant data and would be able to avoid a lengthy follow-up process, when there is no need for additional information.

3.1.2. Assessment

Operations and end-users

Member States would have to define nationally how they would accommodate the new step in the follow-up procedure.

Differences in national procedures will imply different implementation efforts between Member States.

Technical and security

The proposed step requires the definition of new processes. The need for changes in national infrastructures (hardware, software, etc.) depends on Member States' existing national procedures, relevant entities and their chosen solution for incorporating the minimum data set sharing step in Prüm exchanges.

No technical solution has been described for this opportunity on the basis that agreement on the exchange of the minimum data set should be done over existing infrastructure, i.e. the communication channels.

Legal and data protection

In particular, Article 11(2) LED provides that Member States' exchange of information shall not be based solely on automated processing, including profiling, with regard to sensitive personal data e.g. genetic data, biometric data, referred to in Article 10 LED, unless suitable measures are in place in order to safeguard the data subject's rights and freedoms and legitimate interests are in place. Automating this new step is highly recommended where there is little possibility for error, such as a ten-print identification retrieving one single candidate.

It is however relevant to maintain the human intervention in the key point(s) of the process in line with Article 11 LED, where latent-searches, facial-image searches and DNA searches are concerned. Additionally, some Member States have expressed their wish to manually authorise the release of personal data in the form of the quick answer.

In this case, as biometric data are processed, if no automated system will be implemented, the enforcement of a quick answer will not trigger any concern related to data protection in the context of the LED. To be also noted that the nature of data exchanged over the quick answer will be similar to what is exchanged today under the current system, the only difference being the timeframe.

Overall, based on the above, no data protection issues arise in the context of the proposed solution.

Cost implications

The main costs drivers refer to:

Cost driver	Assessment
Possible hardware and software development	Each participating country has different national systems in place with different complexities. As such, the possible need for additional hardware/software will be dependent on the Member State. In this sense, costs may vary greatly.
Training	Since the solution implies changes in national procedures, Member States might propose training programs and awareness initiatives for end-users.

	The European Commission may also provide initiatives to present this change to Member States' representatives, namely workshops.

Table 3 - Main cost drivers

3.1.3. Conclusion

The resulting benefits from including an additional step in the follow-up procedure for sharing a minimum data set are the accelerated access to the most relevant information, the reduced workload with regard to eliminating possible unnecessary requests for additional information and effort from the requested Member State to gather that data and, consequently, the increase in end-users' capacity to carry out other relevant tasks.

On the other hand, there are constraints to the adoption of this solution, as it implies organizational efforts from the Member States, due to the creation of a new process in the follow-up procedure.

The implementation time of this solution would vary greatly between Member States since it is highly dependent on the complexity of each current national procedure.

As a conclusion, the study considers that this additional step ("new step 2") of the follow-up procedure will bring impactful structural changes to Prüm. Streamlining the follow-up procedure is one of the greatest needs for Prüm and should be included in a next-generation Prüm legislation.

3.2. *Single communication channel*

As indicated in Article 6 of the Prüm Decision, any existing channels for international law enforcement cooperation might be used for the exchange of information. Therefore, Member States can make use of different communication channels for the follow-up procedure.

It has become obvious that the current situation with regard to the choice of channel poses challenges. In interviews, stakeholders have argued that the current situation is chaotic. For example, there are cases where a response is not sent via the same channel as the request or where Prüm's requests are sent via different channels. At present, Member States use the channels for varying purposes and to a varying extent. The actual choice of channel through which an information exchange request is communicated depends on many factors, which are not consistent across and not even within Member States. Instructions on the choice of channel exist at EU level and in most Member States, but personal considerations, including preferences for a certain channel, also play a role. As a result, under the current framework, the unstructured choice of channel causes complexity in the context of the SPOC.

Although most Member States usually respond via the channel through which the requests were submitted, some highlighted the need to harmonise the communication channel for the sake of efficiency in the follow-up procedure. Some Member States pointed out the fact that not all police units had access to every communication channel. They have to rely on colleagues to receive and forward their communication. Each communication channel presents their own specificities and features, and each Member State is used to use their preferred channel, accommodated to their own needs.

Currently, the following communication channels are or could be used by the Member States for the follow-up procedure:

- **Interpol** — I-24/7 communication channel;
- **Europol** — SIENA information exchange tool;
- **SIRENE** — the national SIRENE bureaux in each Member State serve as contact points for the SIS II, the Schengen information system for alerts on persons and objects.[7] Its scope covers national security and criminal investigations, meaning it could be used in the Prüm context;
- **Liaison officers' network** —with the reported communication channel, being emails[8];
- **Police custom cooperation centres** — these contact points, mainly focused on border control cooperation, also cover the exchange of information regarding 'petty and moderately serious crimes'.[9]

The most used communication channels currently are Europol's (SIENA) and Interpol's (I-24/7) communication channel. Based on our survey results, out of 19 replies, 58% of the Member States indicated SIENA and 42% I-24/7 as their preferred communication channel.

[7] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[8] Manual on Law Enforcement Information Exchange

[9] Manual on Law Enforcement Information Exchange

3.2.1. Proposal

This solution suggests to use one communication channel by default: SIENA. This means that law enforcement authorities will use this main communication channel for Prüm follow-up exchanges.

Likewise, the level of priority of the requests is also an issue that should be harmonised. Having one common communication channel, the understanding on the different levels of priority and timing should be agreed and shared by all the national authorities.

Currently, SIENA allows law enforcement authorities to indicate the priority of their request. There are three levels of priority: Low, Normal and High. In addition, "Very urgent" and "Urgent" can be written in the "Subject" or "Crime-related content" fields. There is, however, no common rule about time limits for the answer.

Despite not having common time limits rules under SIENA, the Swedish Framework Decision[10] could be used as a reference as the Prüm information exchange falls under its scope. Particularly, Article 4 of the Swedish Framework states time limits for the provision of information and intelligence. Depending on the urgency, law enforcement shall provide the information requested within eight hours, one week, or 14 days.

This topic suggests to include clear time limits features (based on the Swedish Framework Decision rules or by introducing Prüm specific time limits) in the SIENA communication channel. This would allow for a clear overview on the urgency of each request, and help law enforcement authorities in prioritising requests. Europol could then also log statistics related to the communication time, to allow data-driven decision making.

3.2.2. Assessment

Operations and end-users

A single communication channel would ease the exchange of data between the Member States. Nevertheless, both SIENA and I-24/7 present pros and cons, as displayed in the table below.

[10] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006F0960&from=EN

	SIENA	I-24/7
Pros	• Managed by Europol, the central law enforcement agency of the EU • Secure and fast European network • Content-neutral • Accessible in a decentralised manner via a browser, no local software installation is required • Can be integrated into national systems, supporting efficiency gains • Prepared to accommodate the UMF model • Accredited for the exchange of classified information up to the EU confidentiality level • Compliant with Council Decision 2013/488/EU on the security rules for protecting EU classified information • High-quality translation service to be included	• Secure email technology • Accessible via one or several points of contact, depending on the country • Gives access to Interpol databases, including notices on wanted and missing persons, arrest warrants and extraditions • Monitoring 24/7 by Interpol • Available in four languages (English, French, Arabic, and Spanish)
Cons	• Not monitored 24/7 by a minority of SIENA-using countries • Despite being user-friendly, training are mandatory • Costly implementation to comply with EU restricted confidentiality levels, unless SIENA BPL becomes available	• Managed by an international agency • Despite being user-friendly, training is key to ensure its successful use • Not compliant with EU restricted confidentiality levels

Table 4 - Pros and cons of SIENA and I-24/7

Based on the replies received to our survey and supporting anecdotal feedback provided by Member States, SIENA is indicated as the preferred communication channel. The main reasons behind such choice are the easiness to use SIENA, its decentralised access, its standardised format, and its high-security and confidentiality compliance. In addition, the survey showed that 58% of Member States preferred SIENA for the default communication channel.

In order to adopt SIENA as the communication channel by default, Member States will need to reach an agreement as described in the legal assessment below.

In terms of operational implications, Member States would need to make some adjustments, in order to ensure their human resources are compliant with the Council 2013/488/EU, Article 7 referring to the personnel security measures (i.e. individuals have to be security cleared, and briefed on their responsibilities).

Operationally, Member States will need to train the end-users in the use of SIENA (if not already) and implement new work procedures to ensure its use as the default communication channel. Any end-users who do not already use SIENA will need to ensure compliance with the EU level security and confidentiality requirements.

To maximise the benefits of using one single channel, SIENA will need to be adjusted to the needs of the Prüm community, i.e. the priority and monitoring deadlines.

Technical and security

Establishing SIENA as the communication channel by default does not entail major technical implications. The Member States have already access to it, and will not need to bear implementation costs.

In terms of security, Member States will need to comply with the EU level security and confidentiality requirements.[11] This means that Member States will need to ensure personnel security, i.e. only authorised personnel compliant with the requirements laid down in Annex I of the Council Decision 2013/488/EU on the security rules for protecting EU classified information, has access to the data; physical security, i.e. physical protection of premises, buildings, offices, rooms, and equipment; and management of classified information. If SIENA is already used by a Member State then they are already compliant. Additionally, the recent technical changes and the development of SIENA Basic Protection level by Europol, will facilitate the use and embedding SIENA related workflows in national case management systems.

Legal and data protection

The establishment of a communication channel by default needs to be legislated.

To be pointed out that, based on the Swedish Framework Decision referring to the communication channel, sole flexibility of law enforcement authorities is provided in order to allow them to use any communication channels where it is deemed necessary. These channels are provided for purposes of exchanging information and intelligence in the context of international law enforcement cooperation. However, in the context of the next-generation Prüm, a main common communication channel "SIENA" is proposed to be used by default.

In addition, from a data protection perspective, no LED-related impact is foreseen to establish SIENA as the communication channel by default. Member States have access to the SIENA communication channel, which is already an accredited secure channel. Therefore, the choice for SIENA will not bear any legal implications and will be justified also for specific purposes in the context of criminal investigations.

The main common communication channel 'SIENA' could be established by default.

Cost implications

The adoption of SIENA as the communication channel by default will not imply significant costs as EU Member States are already connected to it. However, the implementation of SIENA is costly as it is compliant with EU level restricted security requirements. Aware of this constraint, Europol is currently developing the Basic Protection Level (BPL), expected to be available next year. SIENA BPL would ease the implementation of SIENA and reduce related costs.

In any case, training activities would be necessary to ensure end-users can properly use it.

[11] Council Decision 2013/488/EU on the security rules for protecting EU classified information,

3.2.3. Conclusion

The adoption of a default communication channel will bring benefits to the Member States using the Prüm framework. It will allow all law enforcement authorities to exchange the information via the same channel. Using the same communication channel by default will bring the opportunity to tailor the channel to the real needs of the users, the law enforcement officers across the Member States.

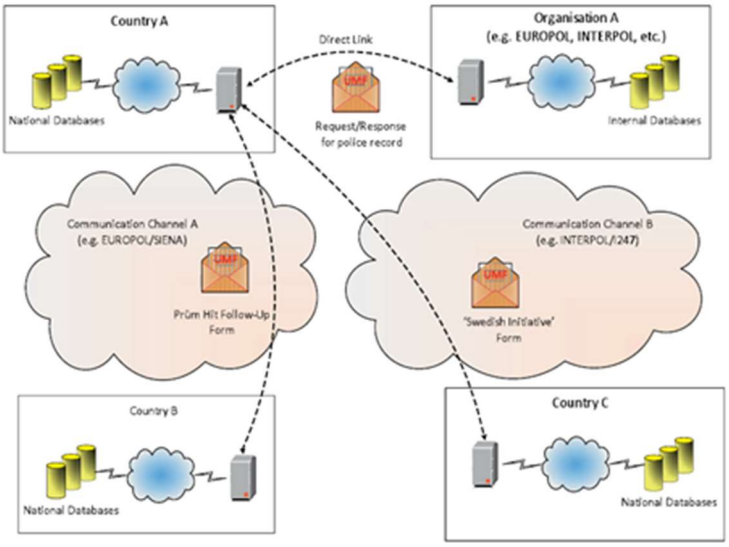
SIENA is the recommended default channel as it is handled by Europol, an EU Agency, complies with EU level security and confidentiality standards, and is already the preferred option by the majority of Member States.

Overall, it can be concluded that a default communication channel should be adopted in the next-generation Prüm. It is noteworthy to mention that if the automation of the follow-up procedure (as explained above) is not retained, a single communication channel by default is all the more necessary.

3.3. *Implement UMF*

3.3.1. Proposal

UMF is an XML-based data format that acts as a layer between systems/databases. It is an information exchange standard created by the Member States, Europol and other EU and international bodies, and could be used whenever structured messages across national borders are sent between law enforcement systems.



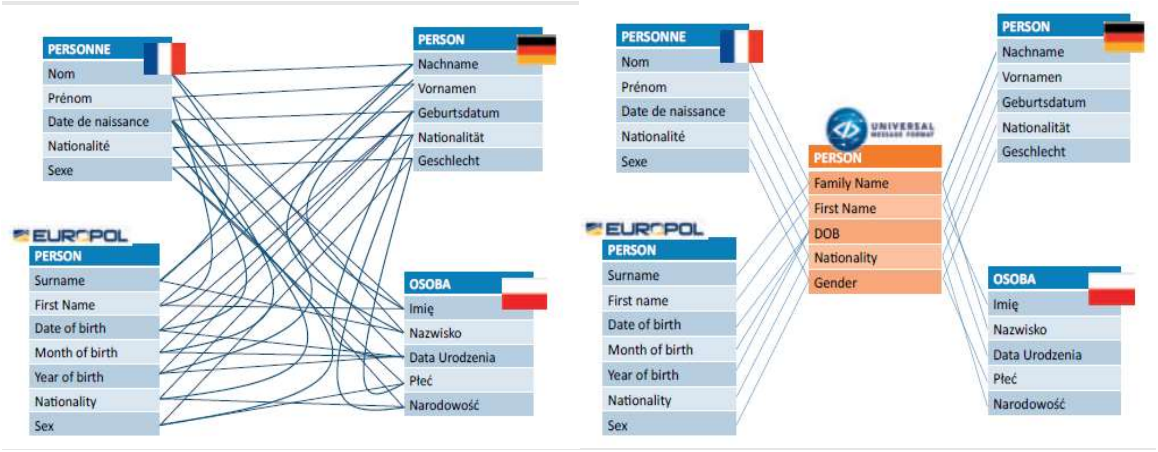
Source: Universal Message Format brochure from 2014, a European Union publication by Europol[12]

Figure 7 - Universal Message Format (UMF) operational model

UMF format is under continuous review and is amended as new business needs arise, ensuring adopting Member States that necessary updates will be possible. Adopting Member States can also propose additions to the format, as they will be considered by the developing entities.

Currently, a specific team in Germany is leading the development of the most recent UMF version, supported by the European Commission, Europol and several Member States. UMF maps different fields, e.g. name, surname or place of birth, in the national database/system. UMF would allow Member States to communicate without translation efforts that are often prone to human error.

[12] https://publications.europa.eu/en/publication-detail/-/publication/3b2cc49f-72bb-419f-8742-eb21cd15e35c/language-en



Source: Universal Message Format brochure from 2014, a European Union publication by Europol[13]

Figure 8 – Data translation before and after introducing UMF

This mapping allows Member States to ask for specific data items in their national data set, and requested Member States will receive the request in the their national data set structure (or be able to translate from UMF to their national data set structure).

Implementing UMF would streamline system-to-system communication, making it faster and uniform.

By ensuring its use by all Member States in Prüm, one can expect benefits at the following levels:

- Increased data quality and collection, due to the standardised message format that avoids multiple data entries and possible data losses;
- Elimination of language barriers, as UMF translates its various data fields;
- Improved quality of data statistics;
- The use of a common format for police cooperation and communication.

Some Member States are known to use UMF for some aspects of their national level law enforcement systems and are well prepared for adoption when sharing data between Member States.

In order to implement UMF, Member States would need to map their national data items to the UMF format. Only then, they would be able to export, import and read UMF data.

National contact points (NCPs) would use UMF in the Prüm follow-up process, both for the minimum data set step and the request for additional information, to harmonise communication standards. This will help to enhance the quality of the information exchanged and the speed of response.

To ensure its success, the use of UMF would have to be enforced to all countries, since it has exponential benefits (as the number of countries using UMF increases, the benefit of using UMF increases as well).

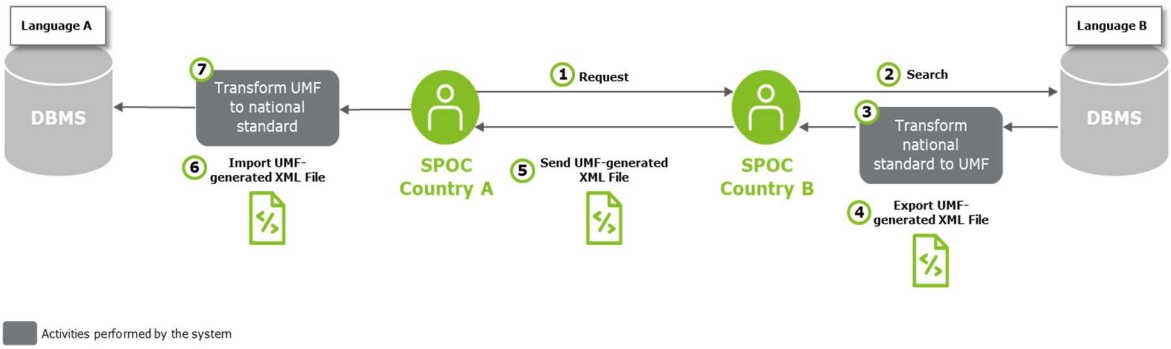
[13] https://publications.europa.eu/en/publication-detail/-/publication/3b2cc49f-72bb-419f-8742-eb21cd15e35c/language-en

3.3.2. Assessment

Operations and end-users

Since UMF is a back-office format (designed to support data exchange between systems, not users), end-users continue to see, write and send information in a common format. The process would go as follow:

1) The requested Member State receives the request for information;
2) Requesting Member State proceeds to search its national databases for the required information;
3) The data is transformed from the national language to the UMF format by the system;
4) The requested Member States exports in UMF format;
5) The UMF format is sent back to the requesting Member State;
6) After the requesting Member States receives the UMF format, information is imported;
7) Information is automatically translated to the national standard, allowing the requesting Member State to process the information without human translation efforts.



Source: Deloitte Touche Tohmatsu Services, Inc.

Figure 9 – Prüm follow-up procedure, with the use of UMF

Nevertheless, the entity performing the UMF translation may change between Member States, as it is dependent on their national procedures. The figure illustrates an example.

National technical experts may require training in order to implement UMF nationally, if they are not acquainted with it, and also for future maintenance needs.

In the ongoing project, a UMF project team in the Bundeskriminalamt (BKA) from Germany is supporting Member States in the implementation of UMF. A UMF contact point (CP) is present in each Member State participating in the UMF3+ project, which could share their experiences in the implementation phase. The governance of the UMF standard is expected to be transferred from the project team to the European Commission or EU agency in 2021.

Technical and security

All Member States can access the UMF format documentation in the Europol Platform for Experts (EPE).[14] Authorised national technical experts may download all the required documentation for implementing UMF in their national systems.

This documentation consists of the UMF schema to be implemented and its technical considerations, as well as the business model documentation. Technical experts will have to:

1) Develop or adapt a system that can accommodate the schema definition, with importing, exporting and reading capabilities;
2) Integrate the schema definition;
3) Map the national data sets to the UMF schema, which will allow for the translation of data.

The difficulty of the implementation process is linked directly with the complexity of the system implemented at national level.

Having implemented and mapped UMF, Member States can exchange information with other Member States or EU bodies that use the format. Data items will vary according to the data category. Member States should also guarantee that every data item is mapped with UMF, for each data category.

It is important to ensure backward compatibility when implementing the current UMF version (UMF v2.0) or the most recent version at the time of implementation. This property would allow Member States that decide to implement more recent versions of UMF to still be interoperable with Member States using older versions of the standard.

Legal and data protection

A provision would have to be added in order to enforce the use of UMF as well as in order to accommodate the use of the message format.

Under the new legal framework, all Member States would have to agree on the inclusion of UMF in order to maximise its potential. Therefore, it is highly recommended to define its use as mandatory.

UMF per se does not add data security concerns, as it is not creating or allowing the exchange of new types of data, and its use is provisioned for the channels already being used. If a Member State requires new IT components for implementing UMF, Member States will have to ensure these are secure (see Article 29(1) of the LED –Security of processing). Moreover, the introduction of a uniform information exchange standard across the Member States, like UMF, the quality over the information collection, sharing and reporting over the data. Hence, it will reduce the likelihood of erroneous or multiple data entries, improving Member States' data management practices and preventing data losses. Member States will control better the information subject to sharing and will attain effectively the minimisation objective.

Cost implications

Costs for implementing the UMF vary considerably and depend heavily on the national system of each Member State.

[14] https://epe.europol.europa.eu/

Table 5 - Cost implications

Criteria	Assessment
Complexity of system	More complex national systems would require more personalised and specific implementation efforts, which may result in added costs. Countries with simpler systems will have significantly less costs.
Equipment	Software (development) would have to be considered in order to implement the mapping for the UMF format.
Technical experts	Labour cost from the technical experts, as they are in charge of implementing UMF and mapping the national data items to UMF's format. The decision to employ own developers or to sub-contract will also affect the costs. This will, however, be a one-time cost, with no added costs foreseen for the actual use of UMF. If new software/hardware is required, extra costs with technical experts will occur, for possible development, implementation, support and maintenance.
Training	With a new capability included, national technical experts may require further training for mapping UMF. If new software/hardware components are acquired, training may also be necessary for implementation, and future maintenance.

3.3.3. Conclusion

Implementing UMF brings benefits to the Prüm follow-up process in terms of maximising data quality and collection, as well as minimising data loss, since the needed information will be stated clearly. It eliminates language barriers and increases the process efficiency by making it faster. In terms of long-term benefits, UMF will make the introduction of new data categories and interoperability options easier.

As regards to potential constraints, implementing UMF requires effort from the Member States technical experts to adapt national systems. The complexity of this will range between Member States depending on their existing data structures and systems. For example, where data is located across different national databases the complexity of combining the required data and returning a single UMF message will be high. Where data is located in a single database, the implementation complexity with be lower. Finally, Member State systems that implement UMF will need to be designed to be resilient to different versions of UMF and be backward and forward compatible to allow integration with Member States using different versions.

In conclusion, even though implementing UMF would not solve any structural Prüm inefficiencies, it would help to structure data exchanged between Member States in the Prüm follow-up procedure and make it more efficient. Implementing UMF would have a considerable impact in Prüm by increasing data quality and minimising data loss. It is highly recommended for UMF to be part of the next-generation Prüm legislation.

For each country, the study estimates an implementation time of six months to two years. This duration would depend on available national expertise, infrastructure, funding for development, implementation and maintenance of IT components and support for implementation efforts.

The fact that some Member States have already implemented the standard and the dedicated team for UMF development in the German Bundeskriminalamt are additional factors in favour of this implementation.

4. INTRODUCING NEW DATA CATEGORIES

The emergence of new technologies and investigation tools in the law enforcement area have fuelled discussions about the inclusion of data categories in a similar fashion as done under the Prüm Decisions today.

These technological advancements not only promote new types of exchangeable data categories, but may also allow the exchange of previously discounted ones when the Prüm Decisions were initially drafted.

Throughout various consultation moments, Member States indicated several new data categories that would better fit Prüm: facial images, driving licences, firearms and ballistics, and biographic data.

The maturity of the technology supporting the exchange of the data category is an important factor to take into account. Technology need not necessarily be mature enough today if it is to be deployed in a few years. The next-generation Prüm must look ahead and be future-proof as the pace of technological change is exponential.

4.1. *Facial images*

Automated facial recognition technology has been in development for over three decades and has seen accelerated growth in recent years with an ever-increasing level of adoption in law enforcement, public safety and intelligence.

In annex the reader can find an overview of (i) common use cases of facial recognition and a description of common technical components; (ii) a description of the international standards governing the exchange of facial images and quality restrictions; and (iii) a detailed review of current capabilities of facial recognition technology in terms of accuracy limitations.

4.1.1. Proposal

Based on the extensive review of the technology it is recommended to include facial images within Prüm and propose participating Member States adopt facial recognition technology. The analysis performed as part of this study and the key considerations highlighted in the review of facial recognition technology have allowed formulating the following proposals.

- Adopt facial image exchange into Prüm;
- Adopt facial image quality guidelines;
- Candidate list sizes;
- Priority-based Scheduling.

The following describes each of the solutions and related recommendation.

Adopt Facial Image Exchange into Prüm

The proposed solution consists of including face images into Prüm and agreeing standard data exchange and image quality guidelines between Member States sharing face images.

The solution proposed focuses on adopting facial image exchange only and is agnostic of the technical architecture, processes and standards that are used for sharing data under Prüm. The recommendations made do not depend on any changes to the current technical architecture and exchange standards and should be considered as valid regardless of any other decisions made.

At a high level, it will require the following for (preferably all) Member States.

- Implement or update national police facial recognition systems;
- Integrate FR systems with existing or future Prüm application architecture;
- Build user interface capability with their existing Prüm application;
- Train staff on the use of facial recognition for Prüm;
- Establishing connections to each of the other Member States (depends on the future technical architecture of the renewed Prüm).

The anticipated workflow and architecture is based on the existing data exchanges and process for fingerprint data. This is shown below.

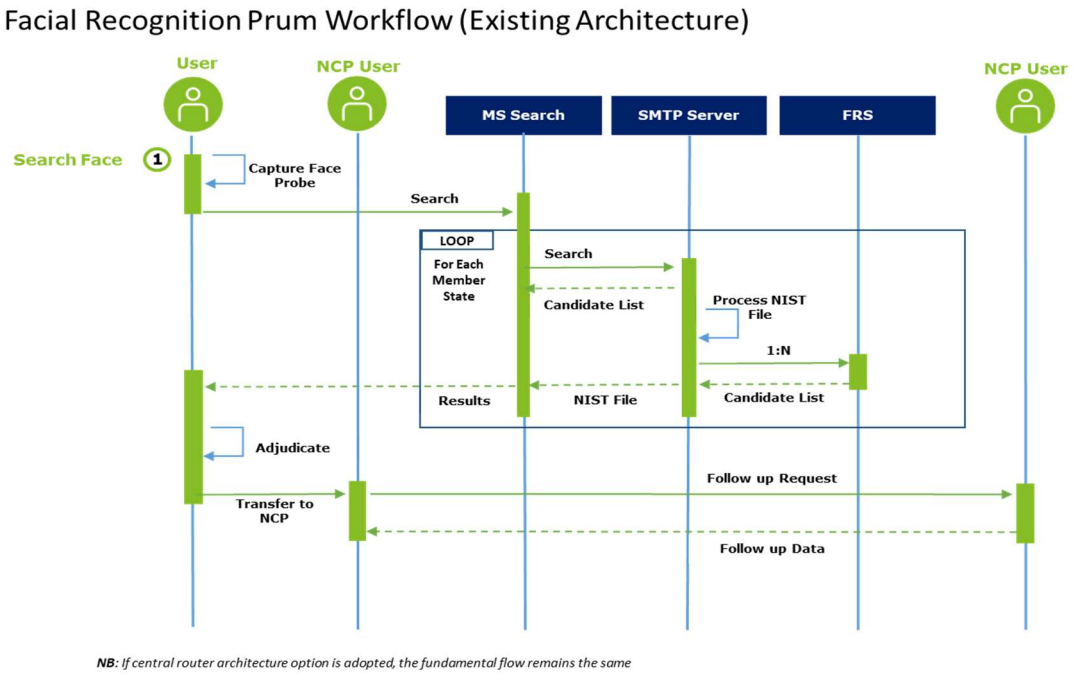


Figure 10 - Facial Recognition Prüm Workflow (Existing Architecture)

The high-level process is described as follows. The lower level implementation details, best practise and file formats will be discussed in the following sections.

- Requesting MS captures a facial image adhering to best practices;
- Requesting MS packages compliant request file;
- Request is sent to each target MS using existing Prüm architecture;
- Requested MS's perform a 1:N search against 'Mug Shot' style galleries;
- Requested MS's return results to requesting state;
- Requesting MS performs adjudication;
- Requesting MS confirms hit/no-hit and follows existing step 2 procedures.

To support the exchange of facial image data it is thought that the following high-level principles will need to be added to Prüm.

- Requests made using facial images will be responded to quickly in an automated manner;
- Member States will seek to ensure 24/7 availability of facial recognition capabilities;
- Member States shall ensure transmitted faces are of best available quality to be used with automated facial recognition matching systems;
- Exchanges of data between Member States will be based on daily quota which need to be defined on a bilateral basis and depend on the technical capabilities of each Member State when dealing with requests.

These are in line with the existing high level principals currently in place for DNA and dactyloscopic data and implies that many if not all Member States will, therefore, seek to implement a suitable facial recognition platform (if not already).

The proposed approach will allow Member States to issue requests to other Member States as follows:

- Contain one or more facial images;
- Contain image data for one subject only;

- Include a crime reference number (as per existing approach for fingerprint);
- Include a reason for request;
- Include an optional parameter for defining maximum results list.

It should be noted that requests should also be supported in (limited) batches as with other data types.

Responses provided back to requesting Member States will:

- Contain a maximum of 50 match candidates;
- Reference to the original request;
- Be sent even if 0 matches are found. This is unlikely as no threshold is applied;
- Will provide information on rank order and match scores;
- Will respond if an error occurs with a suitable error code.

The proposed solution will conform to the exchange and quality standards outlined in the following technical sections.

Facial Image Quality Standards

In order to ensure a minimum level of accuracy across Member States, it will be vital that a 'as high-quality as possible' facial gallery is maintained in all national-level systems.

As shown in the NIST FRVT 2018 results analysis (see Annex 3 – Facial recognition, standards and technology), the best accuracy is achieved when the gallery images adhere to 19794-5, Type-10 or ICAO 9303 records.

The quality guidelines defined in these standards are not all relevant to automated matching and indeed it is not expected that all images will be of the required quality to, for example, pass an ICAO quality check. However, it is important that Member States adopt procedures to aim for the best possible quality of the gallery aligned to the factors from these standards that are important for automated matching. These are defined below.

Probe data quality is also linked to accuracy. However, having bad image data in the gallery affects all requests whereas a bad probe impacts that request only. As shown, having a bad gallery and bad probe results in a big impact on accuracy.

It is recommended that all galleries used for serving Prüm requests by Member States should comply with 19794-5, Type-10 or ICAO 9303 Part 9 compliant images where ever possible.

It is noted that not all elements of the standard impact the performance of automated facial recognition and only the following are considered as key ones:

- Minimum resolution (eyes) of 90px (recommend 150px);
- Full-frontal pose (maximum +/- 5 degrees pitch, roll, yaw);
- Removal of headwear, e.g. sunglasses, hats, etc.;
- 1:1 aspect ratio (the image is not stretched);
- Consistent lighting (no direct source of light);

This would be the standard for all 'Mug Shot' style images that are enrolled in gallery databases, usually captured by police officers within a custody suite or similar. Similar to a ten-print image in fingerprint, this would be high quality and help ensure high confidence matching. Failure to adhere to these standards will result in poor accuracy and higher miss rates (as there are more high scoring false matches).

Probe images will inherently be of lower quality due to nature of law enforcement use of the queries. However, if a high-quality database is maintained, good results can still be expected.

Member States will of course likely have existing image galleries they wish to use which do not comply with the standards outlined above for enrolment. Such images can still be used. However, it is recommended these are separated logically from searches performed of the 'primary' mug shot quality database. This will support increased quality and confidence of matching for known individuals (similar to ten-print in an AFIS). A logical 'Wild' category can be used to enrol images acquired through non-ideal means and used to separate requests. There are multiple ways this could be implemented such as meta-tagging of their images or grouping of images in separate logical data stores.

The Type of Transaction field (TOT) can be used to define a request as a Mug Shot (known individual) or Wild (unknown/wild). TOT is used for current fingerprint exchanges to define Latent or Ten Print search requests. A similar approach could be implemented for 'wild' and 'mug-shot' type gallery enrolments however the key should be protecting and building a high-quality reference database.

Member States were surveyed to understand their existing facial image standards.

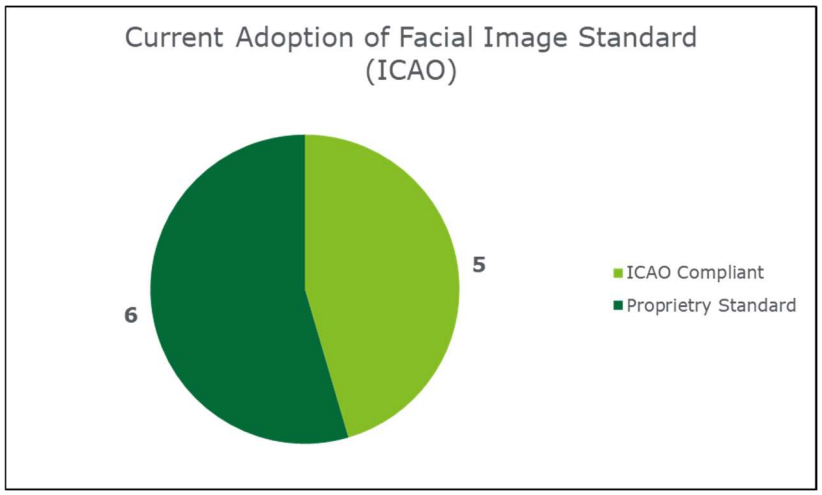


Figure 11 - Current Adoption of Facial Image Standard (ICAO)

Five Member States said they adhere and use the ICAO standards (factors affecting automated matching) for known subjects such as in police custody. 55% use the proprietary quality controls of their chosen platform. However, supplementary information provided with Member State responses indicate many of the quality controls already in place are aligned to the relevant (for automated matching) minimum standards of ICAO, for example, minimum resolution and pose variance.

Candidate List Sizes

A major area of concern is privacy regarding the sharing of data between Member States as each search request will likely produce one or more search results that are not the correct match and unrelated to the investigation.

For example, out of 50 results returned, if only one found to be the correct identity, Member States receive 49 unrelated facial images.

This concern can be resolved in one of three ways:

- Define a maximum limit for all requests. This study recommends 50 however notes feedback from some Member States that they would prefer 100. The study believes that candidate list sizes should be sufficient at 50 if primary mug shot databases maintain good quality, 100 may be better where wild/trace images are combined.
- Put an agreement in place that dictates non-matched data be deleted within a given timeframe. For example, 24 hours. Only confirmed matches should be retained after this time period.
- Allow Member States to define a lower candidate list size in their request, up to a maximum of 50.

Member States were requested to estimate how long they believe would be required to handle the response of a request and verify a results set of 50. 70% believe 48 hours with the remaining Member States believing higher than 48 hours.

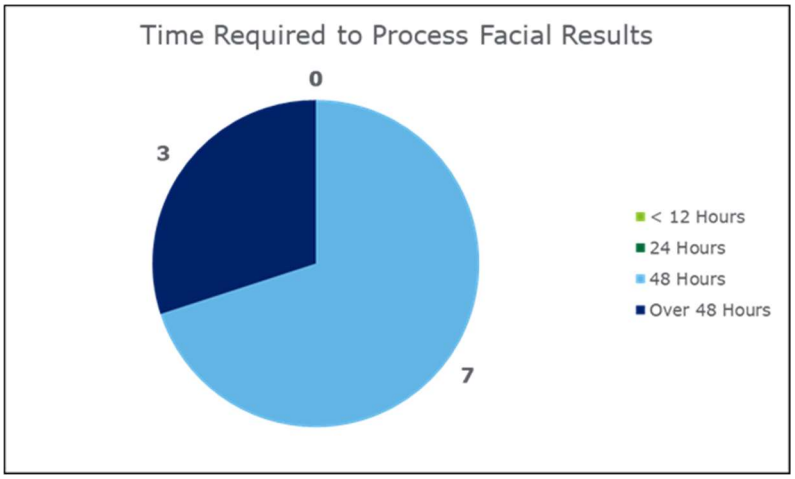


Figure 12 - Time Required to Process Facial Results

Priority-based Scheduling

The addition of facial images to Member State data exchanges will increase substantially the bandwidth requirements of technical and human resources.

As with fingerprint requests, facial image exchanges should be based on daily quote limits. It could also allow a priority-based approach to scheduling search requests. This would allow Member States to control demand better.

The proposed solution would be to adopt a multi-level priority-based approach. Priority levels need agreeing however, examples are:

- Priority Level 1 – request must be processed for example within 1 hour;
- Priority Level 2 – requests must be processed for example within 12 hours;
- Priority Level 3 – requests must be processed for example within 24 hours.

Where possible, requesting Member States should send requests with a priority 3, which would have the largest daily quota. Priority 1 would have the smallest daily quota and

likely be reserved for serious crimes. Daily quotas would need agreeing between Member States.

A 'Priority' field defined on ANSI/NIST-ITL 1-2011 NIST files would allow the transmission of the priority level for each request.

Member States may need to invest significantly to achieve a schedule-based system for incoming requests. However, many will already have such capability with only configuration and minor changes required.

Data Exchange Standards

This study recommends that NIST/ANSI-ITL 1:2011 (2015 update) be adopted as the standard for the exchange of facial image data within Prüm. The key reasons are:

- It represents the minimum standards for quality in ICAO 9303 and the standard Type-10 record definition from 19794-5;
- Provides a high level of interoperable with other ANSI/NIST-ITL based systems and standards such as EBTS and Interpol. Although systems use varying versions of the standard, integration if easily adopted providing systems are implemented correctly;
- Is aligned to the existing standard for the transfer of biometric image data within Prüm.

The general structure and header information for NIST containers are detailed in chapter One above. Facial images will be included as Type-10 records along with any required meta-data. All Type-10 records (face image records) for Prüm would require the following minimum fields:

- **IDC** – the reference to the subject this relates to as defined in the Type-1 record.
- **Image Type** – set to 'FACE' indicating the data type.
- **Dimensions** – the height and width of the image along with other data items for pixel scales.
- **Subject Pose** – supports 'Full Face Frontal', 'Right Profile' and 'Left Profile'.
- **Reference Number** – optional unique identifier for the facial image sample being transmitted.
- **Quality Score** (optional) – can be reserved for future use.

Exchange Packages containing the results of search request transactions will contain up to 50 Type-10 records. Each record will represent a match candidate, it is recommended that the order of the IDC identifier for each Type-10 record should match the rank position. Therefore, the rank 1 candidate will be ICD 1, rank 50 will be IDC 50 etc.

An additional option would be to provide a designated field to provide the match score that is generated by requested Member States. Although Member States will possibly use algorithms from different vendors which implement proprietary scoring metrics, this metric could be useful to requesting Member States to understand the relative confidence of returned match results. This could allow filtering of results to focus on those with the highest confidence and, where results from Member State with the same algorithm are received, to merge results lists into a single ranked list and thus provide operational efficiencies in reviewing top scoring candidates first.

In addition to the above, the interface agreement for Prüm will need to define response standards for when errors occur or data are not suitable for processing.

Based on the existing standard for fingerprint images, errors would be provided as a NIST container with 1 Type-1 and 1 Type-2 record with an error code such as:

- Invalid TCN;
- Insufficient Face Quality;
- Face Not Found;
- Non-valid File Format (multiple codes) ;
- Mandatory Field Missing;
- System Not Available.

The final structure would need to be defined as part of the working group with the above core principles to ensure interoperability.

Usage Reporting

In order to collect statistical data regarding facial image exchanges, Prüm should define a minimum set of usage data items to be stored for all requests and responses exchanged between Member States.

This could allow Member States to understand and report statistics on their search usage, requests received, errors, downtime and various other system metrics. The usage data would be stored locally at each Member State and would support annual reporting to the European Commission.

The above approach is based on the existing de-centralised solution. However, if a central router is adopted (see chapter Four Option 1 –) then these usage data can be captured centrally by the hosting EU agency. This would reduce the cost as databases, software and support will only be needed once rather than for each Member State.

It is proposed that the Prüm ICD be updated to define the minimum data items that should be stored automatically by all Member States (or the central router should it be adopted). The full data dictionary would need to be agreed within the working group, however would likely include the following (at minimum) for each request AND response handled:

- Date\time;
- Type of transaction (mug-shot etc.);
- Number of candidates (responses only);
- Status code (response only) indicating success, error (with reason);
- Number of candidates returned (responses).

4.1.2. Assessment

The adoption of facial recognition platforms will have a wide-ranging impact across all Member States in particular related to technology, cost and impact to security and privacy and implementation. These are covered in the following paragraphs.

Operations and End-users

Introducing an entirely new biometric data type introduces a range of requirements for each Member State to adopt the technical and users skills of using a new type of technology. For these Member States who do not yet have any capability, this will require significant investment. For example:

- Training of existing users would be required to cover the use of facial biometric systems, capability limitations etc. For existing forensic users of facial images this process is not expected to be extensive.

- Member States may need to seek to adopt new Standard Operating Procedures (SOP's) for the capture of facial images and provide necessary training to end-users.
- Increased bandwidth on Member States (higher traffic and larger data sets due to 50 candidates) will result in quotas needing to be agreed between Member States. Member States may also need to consider the impact on network and infrastructure utilisation and possibly upgrade their capabilities where needed.

Member States have been surveyed on existing facial recognition platforms that could be used for serving Prüm requests.

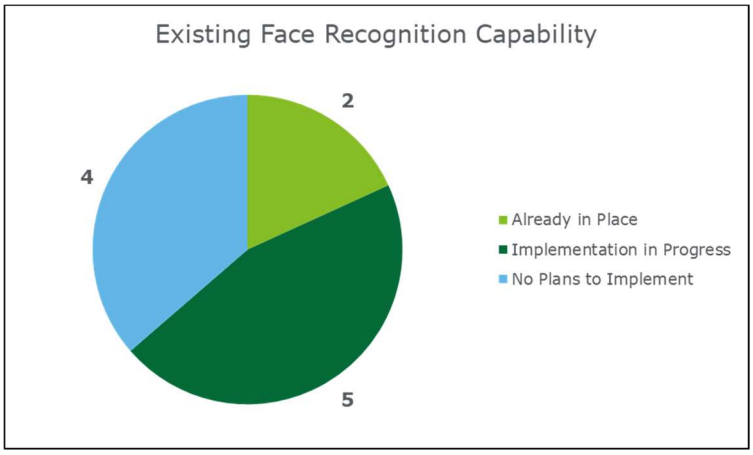


Figure 13 - Existing Face Recognition Capability

67% of Member States who responded indicated they either already have such a system or are in the process of implementing.

Technical and Security

There will be considerable impact on the infrastructure demands of Member States systems serving Prüm requests. Each facial image search can result in up to 50 match candidates in the results. Many requests from multiple Member States could drive high network demand.

All aspects of the data transmission would be governed with existing protocols or those to be defined in next-generation Prüm. The implementation would be the same as for fingerprint and DNA.

Those Member States who do no currently plan to implement any facial recognition technology might face a heavy investment in such technology and its support of Prüm could be needed.

Legal and Data Protection

When consulted, no Member State indicated that there would be serious challenges with exchanging facial images, as long as the exchange is governed in the same manner as fingerprint image data (within the context of law enforcement).

It is true that there are ongoing discussions regarding the accuracy and false positive matches' impact on privacy (innocent people are bothered by the police because of incorrect matching of algorithms), with significant consequences on other fundamental

rights (e.g., gender, age, ethnic discrimination), accompanied or not by negative legal effects for the data subject (suspension or prohibition of social rights, etc.).

However, the use of a rather common type of data, being a facial image, in the limited scope of forensics criminal investigations under the Prüm framework would clearly differentiate this use case from other uses of facial recognition, such as real-time facial recognition for mass identification or identity verification in, for example, border crossing situations. In light of the consultations with the Member States, it appears that, from the law enforcement perspective strictly speaking as meant under Prüm, the inclusion of facial images in the investigations under Prüm could render the candidates' search easier and probably more efficient. This is because the stock of images (image galleries), being available within the national law enforcement authorities is larger than the ones for the fingerprints and DNA. It should not either be underestimated the fact that criminals may not leave any latent-fingerprints in certain cases but they may be detected on a camera. On the other hand, the processing of facial images in this context would require the same deep and accurate scientific expertise through law enforcement agents specialised in this analysis as it is now the case for the fingerprint and DNA analysis. Therefore, the concern that facial images would render easier and would likely generate more "false positives" in relation to the data matching performed on DNA and fingerprint images, to the detriment of the privacy of the individuals concerned, is a wrong perception.

Overall and based on the aforementioned, the transmission of facial images between Member States can be supported although there are some challenges in the context of individuals' fundamental rights described above that should be further assessed in the DPIA.

4.1.3. Conclusion

The study concludes that facial images should be adopted by Prüm and an Interface Control Document (ICD) should be created defining the standards and formats that will be adhered to by Member States when sharing data.

The following points highlight the key conclusions and recommendations.

- **Adopt face images for next-generation Prüm** – facial images should be adopted for data exchange under Prüm and defined in the ICD.
- **24/7 Availability** – Member States should provide 24/7 access to national Facial Recognition systems for requesting Member States.
- **Data Exchange Standard (ANSI/NIST-ITL 1-2011)** – Prüm ICD should define a common XML exchange standard based on ANSI/NIST-ITL 1:2011 (2015 or later) as outlined in section 2.2.
- **Image Standards** – the study strongly recommends the definition of Prüm minimum quality expectations for gallery data in the ICD. Guidance should define which aspects of ICAO (as outlined in section 2.2) are important to automated facial recognition and documented the minimum expectations for Member State galleries. It should be noted this guidance will only be for gallery data and not probes which can be and are expected to be of a much lower quality. Images should not be restricted from use by the quality guidance however, tagging (wild v mugshot, trace v reference etc.) can be enabled for use of TOT based transactions (as per fingerprint exchange).
- **Candidate Lists** – 50 is recommended as the standard candidate list size however requests can allow requesting states to define a maximum up to 50. This is to get a balance of benefit to impact and cost on infrastructure. The study believes that if latest technology is used and primary gallery data is sufficient in quality, high accuracy can be achieved. It should be noted that if data quality (gallery) is not assured then there may be need to have a larger candidate list

size (possibly up to 100). However this should be resisted if possible – doing so will accept and allow a culture of low quality gallery data rather than promoting the need for higher quality.

- **Data Retention Guidelines** – retention periods for non-match data should be defined clearly. The study suggests 24 hours is sufficient time for review. This appears to align with data protection requirements too.
- **Usage Reporting** – Prüm shall define a minimum data set that will be automatically recorded for future reporting. This will include requests received, sent, errors, match hits, match no-hit etc. as to be determined as part of the working group.

Finally, the study has considered the other opportunities and recommendations outlined in the document. The following points describe consideration for architecture options 1 and 4 (central router and web-services).

- **Architecture (Central Router)** – should a central router (SMTP or Web-service based) be implemented, face requests would be packaged up as XML NIST containers and directed to the central router. No changes are expected to accommodate this solution.
- **Architecture (Web-services) –** should a Web-service based integration model be implemented, face requests would be packaged up as XML NIST containers attached to outgoing Web-service calls. No specific changes would be needed for the data exchange format. It would be attached as an XML payload on the outgoing/incoming Web-service calls.
- **Interoperability** – by supporting ANSI/NIST-ITL 1:2011 maximum support for interoperability can be achieved. Alternatively, the Interpol implementation of ANSI/NIST-ITL 1 can be chosen. Compatibility with any system that complies with ANSI/NIST-ITL 1 will be supported with minimal integration effort.

The conclusion is that facial recognition should be adopted regardless of any other changes made and the high-level solution described in this document would remain unchanged. The ANSI-NIST-ITL 1-2011 files would be based on the XML encoding which can be easily incorporated into new Web-services. There is little impact on the message payload implementation.

The cost analysis breakdown is included in the Cost-Benefit Analysis (CBA) accompanying this report.

4.2. *Driving licences*

All Member States are already exchanging driving licence information through the RESPER application.[15] However, RESPER's purpose focuses on supporting driving licence issuing, verification and fraud prevention, and not covering crime-fighting purposes.

4.2.1. Proposal

By including the data set relative to driving licences in Prüm, as laid out in Directive 2006/126/EC,[16] Member States would be able to make Prüm requests on driving licence data items, such as driving licence owner, number and residence, among others. In majority of Member States, law enforcement authorities have access to national driving licence databases.

Driving licence information is relevant in cases of possible fake or invalid IDs, for either corroborating or nullifying the trustworthiness of the documentation and verifying the identity of a suspect.

4.2.2. Assessment

Operations and end-users

As it is a new data category under Prüm, providing training and conducting awareness initiatives for end-users would be essential. These would focus mainly on the new feature's availability, processes, and best practices.

In Prüm searches that return a name as a result, Member States would also be able to search again using the name as an input parameter and receive the corresponding driving licence information. This solution would help maximise the information available. The data structure returned by the lookup would not be changed and would be the same as supplied to other existing authority end users.

The search is done on family name, first name and date of birth or driving license number and the driving license register information is returned to verify the validity of the driving license/ identity of a person and to establish what vehicles the owner is entitled to drive.

Technical and security

From RESPER, the study proposes implementing two features in the EUCARIS Prüm application:

- Search on driving licence number
- Search on the name of the driving licence holder

EUCARIS would support Member States' technical implementation until they would be able to start exchanging data.

[15] https://www.EUCARIS.net/services/resper/

[16] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0126

Given the architecture of EUCARIS, and the user groups having access to the application, it is recommended to grant users of the Prüm application to the RESPER data. This implementation could be performed without involving Member States. If they customized the Prüm application, Member States will need to reflect these changes in their national customized systems.

Even though the new feature would be similar to RESPER, the purpose for searches and the user group able to make queries would be different in Prüm.

Legal and data protection

The legal and data protection impact is similar to the changes proposed in the paragraph on vehicle registration data.

As mentioned above (Operations and end-users), appropriate training to the end-users would be key regarding the data protection aspects too. It would be essential to ensure that the new elements triggering the search (driving license number / driving license holder's name) would be used when there is a "need to know" and through a search approach that respects the rules of data minimisation and proportionality.

Cost implications

Member States would be in charge of covering all costs, equally shared among them. The study foresees minor costs since relevant RESPER features are already developed and in place.

As such, the costs would refer to create an interface between the Prüm and the RESPER application for Prüm users to access the driving licenses data. Member States will have to support the update of their customized application, if any.

At national level, the costs refer to the adaptation of each Member State's national EUCARIS Prüm application. Support and training costs should also be considered.

4.2.3. Conclusion

Including the data items referring to driving licences brings benefits to Prüm data exchanges, since it increases the amount of data available to support criminal investigations.

This data category can be beneficial for complementing searches that returned a person's name, as well as a validity check for suspected fraudulent identity documentation.

On the other side, there might be potential implications, since implementing this new data category would imply technical effort from EUCARIS' experts to copy and adapt the features to the Prüm application, and from the Member States' experts to incorporate the new solution nationally.

Regarding implementation time, copying the RESPER features to the Prüm application would be fast to achieve on a technical level.

In conclusion, including driving licences as a new data category is recommended.

4.3. *Ballistics & firearms*

The discussions held before the adoption of the Prüm Decisions covered the possible exchange of both firearms and ballistic-related data exchanges. At the time, Member States discounted these options due to the lack of accuracy in the matching process and technology readiness.

The technology has evolved, and transnational initiatives have taken place to facilitate the exchange of ballistic and firearm data. The integration of these data modalities in Prüm have been analysed subsequently.

4.3.1. Ballistics

In order to compare ballistic data, Member States require a ballistics identification system to acquire the apprehended evidence, create a profile of the markings that are present in the projectile or cartridge and compare it with other profiles to try to find a match. The match allows to link a particular firearm to a specific crime.

In national systems, the images of markings on bullets and cartridges are compared automatically, and matching profiles are ranked by their level of similarity. The expert using the ballistic identification system then proceeds to manually verify the match to attest for its accuracy.

Current identification systems guarantee a very good matching accuracy, even after multiple firings. Even if the firings do wear out the firearm, the resulting marks remain unique to that firearm.

Including ballistic-related data in Prüm exchanges would allow Member States to automatically correlate their apprehended projectiles and cartridges with firearms used in other crimes in the European Union.

Not only several Member States and interviewed experts mentioned that they were keen on including ballistic data exchanges in Prüm, but there are already some success stories of ongoing data exchanges.

Currently, between Nordic countries, and in the Iberian Peninsula, automated comparison and correlation of bullets and cartridges is taking place. These countries use the same ballistic identification system, *IBIS*, and have agreed upon to this exchange. In addition to using the same systems, the proximity of exchange partners is an influencing factor for making these partnerships possible. As repeat use of ballistics in multiple Member States is expected to be higher in countries located nearby each other.

Extending such solutions to EU-level would be the way to go, if not for an existing hurdle. Currently, there are several ballistics identification systems being used by Member States, and they are not interoperable.

In Europe, the majority of Member States implemented one of three systems, providing the same range of services in terms of ballistic acquisition and comparison:

- **IBIS**[17] – The Integrated Ballistic Identification System is the most used system in the European Union for acquiring, comparing and exchanging ballistic data. It allows for both targeted searches and automatic comparisons of all profiles in the system as soon as a profile is acquired into the system. IBIS is currently the only system that allows for the latter capability. It is also the system chosen by

[17] https://www.ultra-forensictechnology.com/en/our-products/ballistic-identification/

INTERPOL to be used in the INTERPOL Ballistics Information Network (IBIN)[18], a ballistic database to which member countries can compare images of their ballistic data of interest, through their correspondent IBIS. Belgium, Bulgaria, Croatia, Denmark, Ireland, Italy, Netherlands, Portugal, Spain, Sweden and the United Kingdom use this solution;

- **EVOFINDER[19]** - The EVOFINDER ballistic identification system is a network-based system. As such, each member country has a national server enabling the identification, storage and comparison of ballistics data, as well as the access to all servers of other member labs physically connected through communication lines (dedicated or through a VPN). This system does not allow for automatic searches of profiles on the entire network of member labs, but there is an undergoing project aiming at developing this capability. Not having this capability only allows for a reactive approach to ballistic-related investigations, instead of a more proactive one. Belgium, Cyprus, Finland, France, Germany, Hungary, Latvia and Slovakia use this solution;
- **ARSENAL[20]** – ARSENAL is also a ballistic identification system designed to be part of a network, and enabling the comparison of ballistics data. Similarly to EVOFINDER, it only allows for targeted searches, this is, end-users have to request for comparing each profile. There is also a project working on developing an automatic search capability for ARSENAL.

It has to be noted that today the systems developed by the different vendors are not interoperable as they use proprietary protocols and data format. Countries utilising multiple systems cannot automatically exchange data between those systems.

One of the priorities defined by the Council of the EU focuses on illicit firearms trafficking notably in the fight against serious international and organised crime."[21]. Under this priority one ongoing project focuses on trying to harmonise the ballistic information comparison and exchange in Europe, having already identified two possible solutions, and their respective barriers:

- Member States could choose only one system for this exchange. However, this would imply that some Member States would have to invest again in a national system, as well as re-acquire all projectiles and cartridges in their database, as the migration of profiles from one system to the other is not possible;
- Making the existent systems interoperable would be the best course of action, allowing Member States to continue using their preferred systems and avoiding costs with new systems. Unfortunately, the mentioned systems are not interoperable, but studies are taking place to develop a common standard XP3.

In order to confirm the match of ballistic intelligence, one of the following activities have to be carried out:

- When a match occurs, an expert from the country owning the database where the match occurred will have to confirm it manually. This confirmation requires that the requested Member State send a bullet/cartridge to the requested Member State expert, or casting of that bullet/cartridge. This procedure implies an international exchange of either crime evidence or casting of the evidence, requiring legal authorization to perform that exchange and limiting the possibility of having an automated data exchange for ballistic data; or
- At least one of the systems proposed has the possibility for experts to control remotely the requesting Member State's microscope system and verify the

[18] https://www.interpol.int/en/Crimes/Firearms-trafficking/INTERPOL-Ballistic-Information-Network
[19] http://evofinder.com/
[20] http://www.papillonsystems.com/index.php/products/automated-ballistic-identification-system
[21] https://www.europol.europa.eu/empact

match themselves. By accessing remotely and using the other Member States' data, the forensic experts are able to manipulate the ballistic evidence to confirm a hit. This capability does avoid the time consuming process of exchanging evidence, but prevents the use of the system for hit verifications by the requested Member State, during the verification procedure (duplication of acquisition units avoids this issue);

Nevertheless, as the EMPACT project is currently investigating all possibilities and limitations, the study proposes to keep the current ballistic exchanging procedure as it is for the next years, wait for the results of the EMPACT project, and not create a solution for introducing ballistic data exchange in Prüm for now as the best course of action.

If Member States would be adamant in having a short-term solution, deciding on a common vendor' system for ballistic comparison and exchanges for Prüm would be the fastest, most effective and cheapest course of action.

This study does not advocate the choice of a specific ballistic system, but it does defend the inclusion of this data exchange in Prüm.

4.3.2. Firearms

Legal firearms should be registered nationally, in each country's specific database, as licences are required for firearm ownership and use. The registration data set may differ from country to country, but the minimum data set required needs to comply with the Firearms Directive 91/477/EEC, Chapter 2, Article 4.[22]

The data set mentioned includes firearm serial number, type, make, calibre and model, name and address of supplier, supplier serial number and year of production. Member States can search data on other types of firearm-related data through the following international systems:

- **iARMS**[23] – The Illicit Arms Records and tracing Management System is a European Union-funded firearms database managed by INTERPOL. Member countries can "record illicit firearms" and "search to check if they have been reported as lost, stolen, trafficked or smuggled";
- **EIS**[24] – The EUROPOL Information System contains data regarding persons and objects (including weapons) related to crimes and terrorism, and can also be queried by Member States;
- **SIS II**[25] – Some police authorities use the Second Generation Schengen Information System for storing and searching for apprehended and wanted crime-related firearms data.

The European Commission has also promoted the creation of Firearm Focal Points (FFPs) in each Member State, where Member States would centralise the national access to all types of firearm-related information and the communication of firearm-related data with other Member States, through secure channels (SIENA).

[22] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A31991L0477

[23] https://www.interpol.int/en/How-we-work/Databases/Illicit-Arms-Records-and-tracing-Management-System-iARMS

[24] https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

[25] https://ec.europa.eu/home-affairs/content/second-generation-schengen-information-system-sis-ii_en

All points considered, the study does not propose to include firearm-related data exchanges under Prüm for several reasons:

- National databases contain legal firearms registration data, thus not the information needed for investigations on illegal firearms;
- If police do not have the actual firearm, they cannot to trace it back;
- Also, if investigators apprehend a legal firearm and need to find the owner, they could just contact the respective vendor and request that information;
- The most relevant firearms data (illicit, wanted, lost and stolen firearms) is already stored, compared and exchanged in international firearms systems (iARMS, EIS, SIS II);
- As such, the only use case for exchanging this type of data would only be legal firearms that were transferred to another country, not registered in that country and used in crimes.

On a more technical perspective, this exchange is also not advisable, as:

- The format of some data items used for comparing firearms, such as firearm type, make and model can change between vendors and some vendors use the same serial number for different firearms, posing a barrier for harmonising the matching of firearms registration data and ensuring its accuracy;
- This low accuracy would promote false positive matches, which consequently would raise data protection concerns, as registration data includes personal information.

In future, Member States could consider the possibility of using the European Search Portal (ESP) as the default channel for searching and exchanging firearms-related data, as SIS II and EIS will be accessible through the portal.

4.4. *Biographic data*

Member States discussed the possibility to include the automated data exchange of biographic data to facilitate searches for personal information recorded at Member State level. It was mentioned that the ADEP-EPRIS initiative aims to provide this possibility.

In 2017, five Member States launched a pilot project called Automation of Data Exchange Processes - European Police Records Information System (ADEP-EPRIS): France, Finland, Germany, Ireland and Spain, funded by the European Commission. An additional three participated as observers: Hungary, Belgium and Austria.

4.4.1. Proposal

The scope of ADEP-EPRIS is the automation of presently manual, and therefore labour and time-consuming processes for identifying whether certain law enforcement-related data is available in one or several Member States police records databases in order to enable and facilitate the subsequent bilateral or multilateral information exchange. The pilot project aimed at creating a technical system for crosschecking index databases provided by each participant, containing an extract of police records (with pseudonymised biographical data such as family name, surname, any other names/aliases, date of birth, place of birth, gender). The index database is located at each participating Member State. Searches are initiated to target Member States resulting in the indication of a 'hit' or 'no-hit'. In case of a hit, additional data has to be requested using Europol's SIENA (Secure Information Exchange Network Application).

ADEP-EPRIS applies the principle of privacy by design by using pseudonymised data – whereby the identity of persons of interest will not be revealed in the 1st step (hit/no hit reply). It is based on a decentralized architecture and an UMF3 compliant interface, which is planned for the follow-up communication as one major task in the continuation of the pilot project.

One of the requirements to build ADEP-EPRIS was that the development of the solution and its roll-out should be cost-effective. Additionally, already existing IT infrastructure is re-used: the Europol Operations Network (EON, i.e. backbone of the secure telecommunication infrastructure) and SIENA. The EON, running on TESTA, is used as a secured layer for the exchange of information. Every Member State is already connected to the EON. The software, being an open license, is composed of micro-services for the transfer of data and can be adapted to fit every Member States IT infrastructure.

The follow-up procedure is envisaged to be carried out through SIENA, and be UMF-compliant. These measures aim at automating to a maximum the follow-up procedure and leaving the possibility for manual verification where needed. Project officers leading the ADEP-EPRIS initiative are currently looking into measures to reduce to a maximum the need for manual verification whilst ensuring that the appropriate information is being exchanged. Furthermore, in the future the question of supplying the Europol Information System (EIS) with the relevant results from the national indexes will be assessed.[26]

It has been roughly estimated by police officers during an interview that the information that police authorities might look for, are in 70% of instances not available at their counterparts. Those numbers are indicative, given that no study has been done to

[26] ADEP-EPRIS Evaluation Report D3.2_D4.4_D5.5_D6.6_D7.3

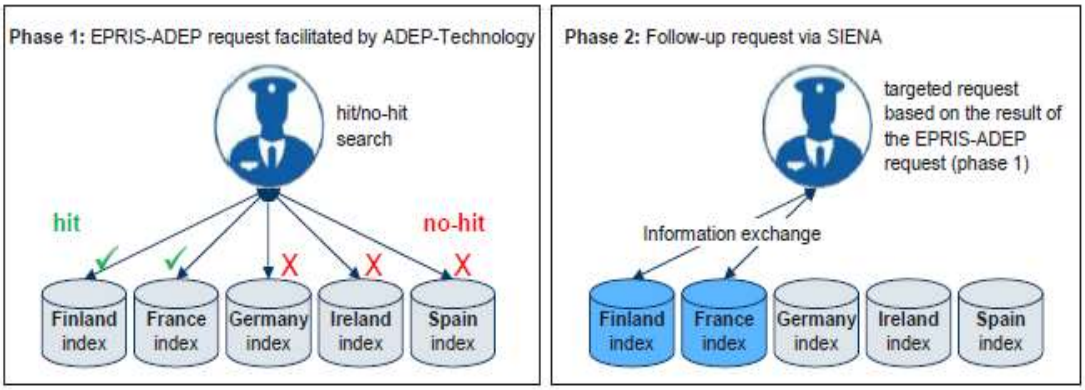
estimate these numbers. However, it does give an understanding of the inefficiently used resources when asking manually for information that is not available.

However, if ADEP-ERPIS becomes operational, police authorities will immediately know if the information is available and in which Member State(s), in order to send targeted SIENA messages only to the Member States concerned, which can make them gain precious time in case of an investigation.

The pseudonymisation of the data as a privacy-by-design principle along with decentralised storage ascertain Member States that their data cannot be automatically accessed.

ADEP-EPRIS can be summarized as follows:

- It is a tool to automate the process of indicating in which Member States' databases the relevant police records could be present;
- The tool aims at reducing the need for manual work: sending information requests by requesting Member State and searching of data in national databases by requested Member States which often leads to "no information" replies;
- In a matter of minutes, requesting Member States are automatically alerted of a hit/no hit for searches on biographic data;
- The searches and decentralized databases are pseudonymised to ascertain the privacy-by-design principle;
- The follow-up exchange of information is UMF compliant and done over SIENA;
- Information can be exchanged with Europol if deemed appropriate by the Member States and if it falls under Europol mandate. All confirmed cases with cross-border dimension falling under Europol mandate should be exchanged with Europol.



Source: ADEP-EPRIS Evaluation Report D3.2_D4.4_D5.5_D6.6_D7.3

Figure 14 - Diagram IT architecture central router

The first pilot project has been deemed successful. In February 2020, the follow-up project was launched, financed by the EU. The follow up project will further develop and refine the software and will establish business processes in order to have a roll-out capable system by the end of the project.

4.4.2. Assessment

Operations and end-users

If a search in Member States' indexes results in a hit/hits, the law enforcement officer should decide which of these hits he/she will follow up with a targeted SIENA request. Some Member States have highlighted that follow-up requests to ADEP-EPRIS searches may cause higher workload in requested Member States. On the other hand, ADEP-EPRIS technology will allow more targeted requests and avoid using scarce resources for "no information" queries. The exact work processes will be tested by the pilot project. Nonetheless, there is a clear desire to automate and streamline the process as much as possible. Nevertheless, law enforcement authorities need to be trained and resources need to be foreseen for possible increase of incoming requests.

Technical and security

Member States will have to provide a consolidated index of biographic data based on data from national databases containing information on police records. For many Member States this will require combining or accessing data from multiple national databases. This increases the technical complexity significantly. The complexity of supporting this requirement will depend on the way Member States organise their existing databases and systems.

Legal and data protection

A feasibility study assessing legal and possibly other aspects will be launched, if deemed necessary, by the European Commission. A DPIA of the ADEP-EPRIS might be required in order to address all relevant data protection aspects resulting from this new information to be exchanged.

Cost implications

The solution is foreseen to be very cost-effective since many already existing components, e.g. Europol Operations Network and SIENA, are used for the communication and exchange of data. The software for exchange and pseudonymisation has already been developed. However, it is expected that significant costs will be incurred through the deployment and ongoing support of the solution at a central EU level and Member States will be required to transfer data to the indexed databases and the creation of relevant user interfaces.

4.4.3. Conclusion

The ADEP-EPRIS project and the Prüm Decisions share common objectives and material scope: cross-border law enforcement cooperation and reduced human labour amongst other.

Therefore, it is recommended to include the automated data exchange of biographic data in the next-generation Prüm, leveraging the ADEP-EPRIS technology. However, it has to be noted that certain working principles still need to be defined, such as the processing of hits.

This page has been left blank intentionally.

5. INTRODUCING A NEW IT ARCHITECTURE

The current Prüm Decisions (2008/616/JHA) specifies that Member States should use the TESTA network for the electronic exchange of DNA data, dactyloscopic data and VRD data. Connections over the network should be set up either by:

- Using the existing national access point or establishing a new national TESTA access point; or by
- Setting up a secure local link from the site where the databases are located and managed by the competent national agency, to the existing national TESTA access point.

The IT architecture is based upon point-to-point integration architecture and there is no existing central technology (systems and databases) available at an EU level which could be used to handle or process Prüm requests. Member States are required to provide access to national level databases for the purposes of serving Prüm requests over this network.

This current IT architecture has been deemed appropriate by several Member State representatives. This can be explained by the fact that the Prüm system is resilient and that once a connection has been established, the automated data exchange works very well. Nevertheless, this IT architecture presents some challenges.

The decentralised architecture has shown that limitations exist when it comes to the coverage of the exchange of biometric data: Prüm bilateral connections are not established between several countries. Around 55% of all possible connections have been established – as some countries are not yet exchanging data between them. Therefore any improvements that would increase adoption (e.g. reduced complexity, lower costs) are highly desirable.

The coverage of operational data exchanges of vehicle registration data (VRD) is 86%. This is mostly due to the architecture of EUCARIS solution which allows every Member State to connect their databases and systems with all participants.

In addition, efforts are being made by the Commission and Member States to make large scale European central information systems, e.g. SIS, VIS, Eurodac, Entry-Exit, ETIAS and ECRIS-TCN, interoperable. By doing so the EU aims at facilitating access to the data contained in the different systems through one single interface the European Search Portal (ESP).

Although the current Prüm de-centralised architecture does not technically prevent an integration with future interoperability solutions, any implementation would be complex due to each exchange needing to be integrated on a one-to-one basis. A more desirable approach would be to have a single centralised component that would allow transferring queries between Prüm participants and if desired, with other EU information systems or interoperability solutions.

5.1. *Assumptions and limitations*

Based on the considerations above, the following areas of improvement should be addressed by the next-generation Prüm.

- Lower complexity and lower cost for implementing exchanges between Member States: This will help drive adoption and allow Member States to integrate with one target end point reducing the complexity of their IT systems and demand on support teams;

- Centralised logging and statistics recording: This will allow accurate information related to requests, responses, errors, etc. to be reported on. This is highlighted in the various biometric topics of this report as useful for the Member State;
- Uptime monitoring and availability at central EU level (e.g. eu-LISA): This would allow Member States to receive insights on the operational status as well as notifications (e.g. in case of downtime);
- Modernised integration protocol allowing quick and consistent implementation across Member State systems.

The study also identified a number of architecture behaviours which are considered to currently work well and would be desirable in next-generation Prüm.

- For data security and privacy reasons, (unencrypted) personal data should not be stored at a central EU level. Any solutions proposed will therefore ensure that no identifiable data is stored or visible at a central level.
- The study recommends that the s-TESTA network remains the secure standard communication infrastructure to support the Prüm exchange of data.
- No changes to the architecture of the EUCARIS system will be required as no significant problems were highlighted by Member States.

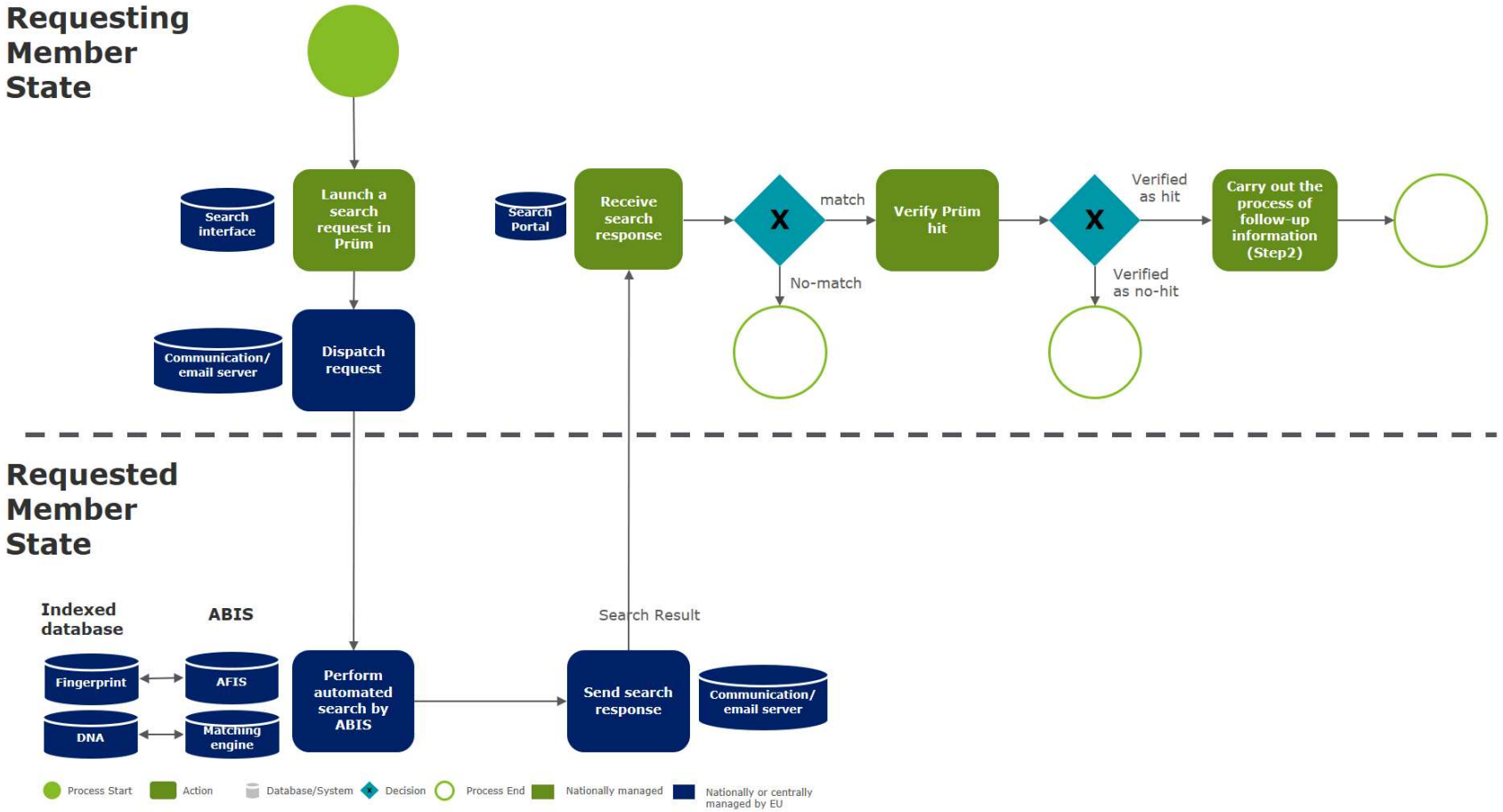
The solution options presented in this section are aligned to these assumptions and limitations.

5.2. ***Assessment***

This paragraph describes the business, stakeholders and technology requirements of the solutions proposed in the following sections.

The assessment and options will focus on the exchange of DNA, fingerprint and other new data categories that could be part of the Next-generation Prüm.

The different architecture options are defined with a focus on business value for Prüm. All current and supporting IT components are presented and analysed to understand how they can be used to facilitate some of the operational processes (e.g. adjudication of a biometric sample or collection of statistics). The business architecture components are defined in manner to support the current nominal data exchange process in Prüm depicted below. Two colours are used in the process, green meaning that the action or IT components can only be managed by a country and blue meaning that the action can be either supported by a country or centrally by a European agency. This is the current work flow.



Source: Deloitte Touche Tohmatsu Services, Inc.

Figure 15 - Prüm current request process and supporting IT infrastructure

In the current IT architecture, Member States are responsible to develop and to set up their IT application to exchange biometric data in a decentralised manner. The European Commission is responsible for maintaining the underlying secure network infrastructure TESTA.

5.2.1. Architecture requirements

Architecture requirements for the Prüm network will serve as a basis to define new options for the IT architecture. The new options will then be evaluated against all requirements in order to retain the best architecture.

The table below provides an overview of these requirements along with their perceived priority using MoSCoW categorisations (Must, Should, Could, Won't):

Table 6 - Architecture requirements 1

Architecture requirements	MoSCoW classification
1. The automated data exchange over the Prüm network must be accessible on a 24/7 basis, and must not be disrupted at any time.	Must have
2. The introduction of new data categories must be supported by the current or proposed architecture.	Must have
3. Architecture shall embed "data protection by design" and "data protection by default" capabilities, at the level of message formats, connection with new IT components and integration of new ways of data handling.	Must have
4. Future architecture will support lower complexity and adoption costs than currently. It will allow Member States to establish connections in an easier and quicker way.	Should have
5. Possibility to re-use already existing IT infrastructure should be preferred.	Should have
6. The harmonization of message format standards should be facilitated communications with other systems.	Should have
7. The possibility to connect new IT components could be considered. The new IT component could serve the Prüm processes in several ways (e.g. reduction of the manual verification).	Could have

5.2.2. Prüm actors

The current actors of the architecture are the participating Member States and the European Commission by providing the TESTA network as messaging infrastructure. In the Next-generation Prüm, new stakeholders such as Europol, mandated EU agency (i.e. eu-LISA) or third countries could integrate with the landscape, if agreed.

5.2.3. Existing Search Interfaces

In order to share data, Member States have developed and established search interfaces at national level. These search interfaces allow users to send and receive requests from their European counterparts via Prüm. The national search portal relies on and is connected to other components (i.e. middleware) for sending and receiving the results.

This component is typically a graphical user interface that allows to launch biometric search queries and return the respective results.

5.2.4. Middleware Components

The middleware is a set of technical components deployed by a Member State to process requests received by other Member States and perform searches against other national database.

In the current architecture, an email server (which is part of the middleware) is responsible for both sending and receiving requests. It is connected to the communication server, which performs the translation of the data, its encryption, and queuing of messages.

In order to start exchanging data, Member States need set up the middleware and make sure that they comply with the data format rules/format of the countries expected to exchange with.

5.2.5. Existing "ABIS"

Member States host multiple databases and matching systems which can collectively be referred to as an ABIS (Automated Biometric Identification System). This includes current DNA and AFIS systems and could include Facial Recognition systems.

Each Member State generally selects different vendors for their underlying ABIS platforms. In addition technology vendors vary between Member States, as the technical needs vary according to the size of the biometric database and the required matching accuracy.

5.2.6. Indexed biometric database

The indexed biometric database is the set of biometric gallery databases that Member States can query in the Prüm context. It both entails the current DNA and fingerprint database and will include any other type of biometric data that can be queried in a two-step approach. The database is called indexed because a reference number (root ID) is provided for every possible match.

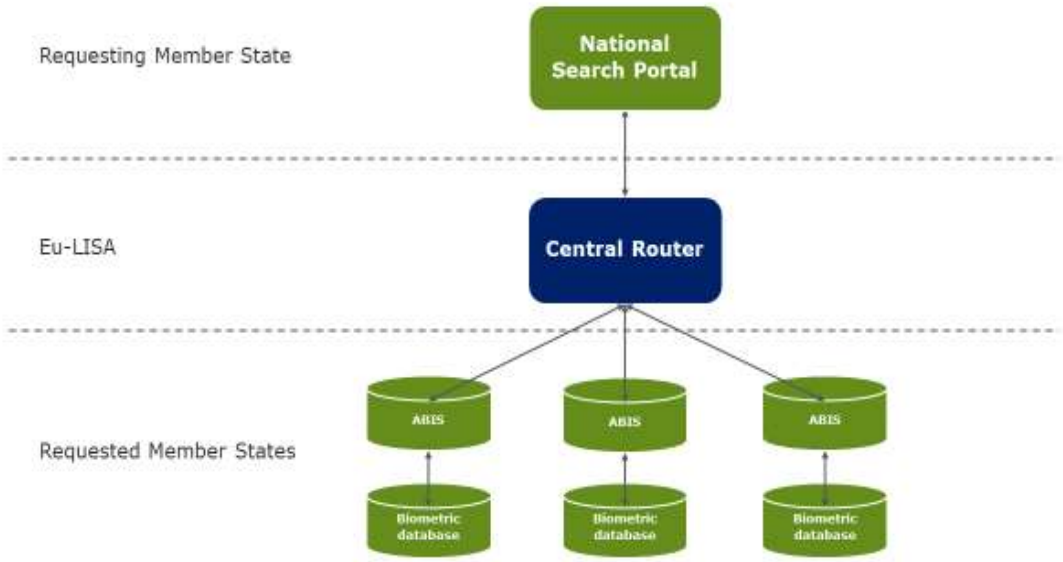
5.3. *Architecture options*

This report presents a set of options that would help the Prüm Decisions to reach their full potential and improve the efficiency of exchanges over the network. The options that are here presented are valid for the biometric data.

5.3.1. Option 1 – Central router (Hub-and-spoke solution)

The first option is a hub-and-spoke solution. This solution was proposed to be analysed in the high-level expert group on interoperability[27].

The first option is based on a decentralized architecture and consists of a central router. This router allows Member States to connect to and to route messages to the respective matching engines of every Member State through one connection.



Source: Deloitte Touche Tohmatsu Services, Inc.

Figure 16 - Diagram IT architecture central router

A solution based upon a central router would involve the following:

- The central router provides a brokering service, receiving and sending Prüm requests between Member States as soon as Member States have set up the connection;
- Requesting Member States connect to the central router and send Prüm compliant XML request files;
- The central router receives the incoming request and extracts originator and destination(s) routing information;
- The central router records statistical information such as counting the number of requests sent, received and errors; including timing details of transactions
- The central router forwards the request on to one or more destination hosts and handles the response (routing) returned by the requesting Member State;
- The central router forwards the responses directly onto the requesting Member State and records statistical usage information for reporting;
- The requesting Member State handles the processing of the responses in the same manner as currently done.

[27] This expert group was set up under Commission Decision C/2016/3780 on information systems and interoperability.

It should be noted that the described solution will work with the existing communication model (SMTP/email servers). However, as described below, a web-service based approach may offer other benefits. This is covered in the recommendations at the end of this chapter.

The following diagram depicts the current situation on the left, and the proposed solution on the right.

Source: Deloitte Touche Tohmatsu Services, Inc.

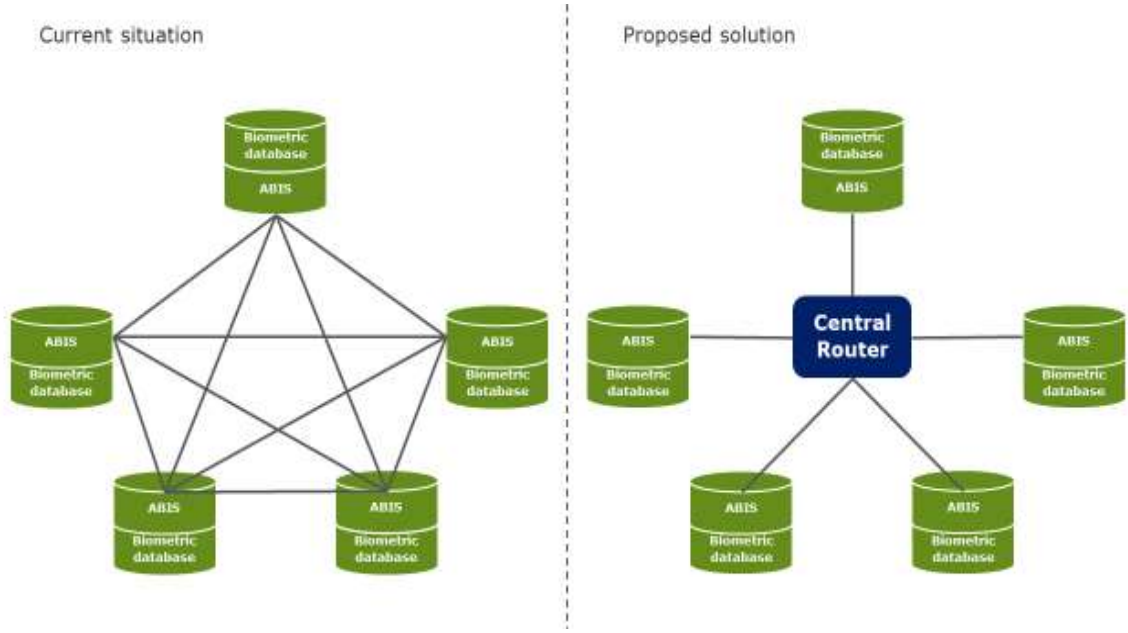


Figure 17 – IT architecture central router topology

The central router could be composed of either a Web Server (proposed) or an Email Server (existing). It would serve as a connecting point between all Member States. The connection to that router would allow to switch from the current mesh topology to a star topology. This will bring several benefits, as follows:

First, if the topology switches from a mesh to a star architecture, the number of connections to establish and maintain from a Member State perspective will drastically be reduced. Even for countries that have already all their connections established, this would be useful given that only one connection should be maintained, and they would not be required to establish bilateral connections with Member States that will join in the future.

Secondly, the star topology would allow for easier integration of other possible EU and/or non EU third party IT systems in the future, such as the interoperability solution that will be further explained in section 6.1.

By having a central router a number of additional benefits, aligned to the architecture requirements, may be achieved. For example:

Statistics hub

Member State needs to report on an annual basis a set of statistics to the European Council. It appears that sometimes the statistics reported by the different Member States diverge as the number of outgoing request by a Member State A do not correspond to the incoming requests to a Member State B. With a central router, statistics on the Prüm exchanges would be easier to produce and more accurate. The collection of data will be done at central level, and will no longer have to be reported by Member States.

The proposed central Prüm router will not have any access to message level data (biometric, biographical etc.). It will only be capable of collecting data including, but not limited to:

- Requests received (by Member State, Type);
- Requests responded (by Member State, Type);
- Errors;
- Response Times.

Additional fields could be included in message headers in order to produce richer reports. These can be agreed ahead of defining the next-generation Prüm interface control document.

Central Pooling/Quota Management

Member States existing fingerprint exchanges are based on a per Member State daily quota. If Member States exceed their quota, they are not able to process further requests until the next day, unless asking for/receiving additional quota based on bilateral agreement.

Having a central router may allow for the centralised monitoring of quotas and/or adoption of a more complex quota management features. This would centralise quota systems currently deployed by each Member State. Note, this is a separate consideration to the priority-based scheduling discussed (but not recommended) for fingerprint in chapter One

Quota and priority-based processing are discussed in the relevant biometric related sections (2.3 & 2.4) of this document.

The central router's main benefit is as a mechanism to help Member States in establishing data exchanges to other Member States. Allowing Member States to integrate with one single end-point using (if Web-services are adopted) easy to use technologies and best practices, will greatly reduce the complexity of Prüm implementation and help ensure a high quality of service and security.

The table below provides a cross reference of the architecture requirements with the solution requirements.

Architecture requirements	Fulfilment of the requirement
1. No disruption of the service	**Yes.** If the connection to the central router is done in a phased approach, meaning that temporally a hybrid situation exists with both the central router and bilateral connections, there should be no disruption in the service.
2. Introduction of new data categories	**Yes.** The central router should be fit to be used for the automated exchange of other data such as facial images.
3. Data protection by design and data protection by default	**Yes.** The central router merely serves as the connecting point between all Member States, with no access to the message level – in other words, ensuring the end-to-end secure transportation of the message. On the other hand, the star architecture could be built in a way that the key "data protection by design" requirements related to data resilience, confidentiality and integrity are known and implemented at the level of *transportation* of messages (e.g., incident management procedures to avoid data leakage in transit, business continuity plan at central router level).

4. Adding new connections	**Yes.** The prime purpose of the central router, is to serve as an interface for Member States to connect their national systems. Member States will still need to put effort to connect to the central router.
5. Re-use of existing IT component	**Possibly.** The router will have to be set up to ensure it appropriately serves the purposes of Prüm. However, if Prüm is linked with the interoperability solutions, the European Search Portal might be used as central router. (Please refer to section 6.1.3)
6. Harmonization of message format	**Yes.** The central router could adapt the Prüm XML format if communications with other systems are needed.
7. Connection of new IT components	**Yes.** It is possible to connect new IT components to the central router that will serve Prüm users in various ways.

Table 7 - Architecture requirements 2

Operations and end-users

By facilitating the connections to the Prüm network, and by having more connections established, more automated data exchanges are expected to be performed. This is a very positive point given that it serves the purpose of Prüm directly. Of course, more exchanges mean more need for manual verification post-match, but this requires less effort to be made than the manual verification without the Prüm network.

If multiple systems are queried simultaneously, all operational systems should still send the automated answers, and temporarily unavailable systems should send an error message.

The search process over the Prüm network will not change for forensic experts should this new IT architecture be implemented.

In order to implement a central router, the best approach would be to recommend a phased approach and avoid any "big-bang". Member States should first establish the connection to the central router, test the connection and exchanges before gradually stopping the search through the bilateral connections.

In terms of timing, this would depend whether the reuse of an existing router could be done, and efficiency of Member States to connect to the router. The study team expects a dedicated router to be used.

Technical and security

The central router offers the chance to queue messages received by Member States and schedule for the delivery to target Member States. Should a Member State system be offline, the central router could follow a retry policy before sending back an error message to the requesting Member State.

The actual network, TESTA, will still be used for this solution. In terms of performance, no issues are to be expected. The router should be robust enough to deal with the forecasted flow of query that will transit once all connections are established. In 2018, about 1.5 million DNA and 380.000 fingerprints search requests were performed. The study expects an increase in searches over the coming years. The router should be able to cope with future requests. Since the matching capabilities are governed at a national level, we do not expect any new problem here from the central router perspective.

An important topic to cover is the need for redundancy or other methods to avoid a single point of failure. If all messages can transit through a single router, no communication can be done if the router is down. A business continuity plan (potentially

involving a redundant/backup solution) should be elaborated by the European agency maintaining the central router to avoid such problem.

All data exchanged through the central router could use a layered encryption model to ensure that only data relevant to each stakeholder (central router and Member States) is accessible. The security proposed for the central router is:

- **Transport Security** – SSL certificates (assuming Web-service based approach is adopted for central router) provides a high level of encryption of requests whilst in-transit. This is in addition to being transmitted over the secure TESTA network.
- **Message Encryption** – the entire message is encrypted using a key that is known to each Member State and the central router only. This is used by the central router to decrypt header information for routing and reporting.
- **Payload Encryption** – the underlying message payload (NIST, DNA, etc.) is encrypted and is accessible with keys known only by sending and receiving Member States.

This layered approach ensures no identifiable data is stored or visible at a central level however information required to handle the request and responses is available but also secured. However, it must be noted that it probably prevents offering any additional biometric services at central level, should these be desired to be implemented.

Further information relating to message structure (header and payload) is detailed below.

Legal and data protection

This architecture will not bring any changes, nor entail any interferences in the way Member States will handle the requests in their own system (decentralised approach). Practically, Member States will continue to be in charge of the data processing operations involved (amongst others, appropriately handling the requests received and operating the matching) as data controllers. The current working principles of the Prüm Decisions will not be modified.

The star topology is compliant per se (as concept and approach) with data protection rules. The measures that are already suggested above (SSL "in transit" encryption, two-layered message encryption) are key to ensure that the applicable data protection requirements are met.

Yet, the following elements should still be considered working further on the solution's implementation:

1) Clarify the role of all actors involved in the architecture as "(joint) data controller" vs. "data processor". The Star model proposes that an additional new agency (i.e. eu-LISA or Europol) performs a well-defined set of automated data-processing operations. It will therefore be necessary to determine the roles and responsibilities of each actor in the whole process and document them (see point 2 below). For example, while the Member States will remain responsible for making the data matching according to their procedures and policies, the party (-ies) supporting the central router will be responsible to ensure the secure transmission of the data over the network and will be the one providing the means of transferring (central router). We understand that as, in all likelihood, the body that will operate the router is an EU agency (i.e. eu-LISA or Europol), the determination of the role of (joint) controller vs. processor may have already been made in the context of other information-sharing activities involving that agency, the European Commission and Member States. Therefore, it is advisable to look at, and if necessary adapt, these precedents to the context of the new Prüm architecture.
2) Review, update or tailor the data protection documentation (policies, data access procedures, data subject rights procedures to mention only a few) maintained at the level of central router but also, at the Member State level (e.g., agencies' data protection records of data processing activities, data protection statements, data handling guidelines to staff, and so on).
3) Define the data processing responsibilities in the new legal instrument.
4) Confirm and if not in place, review and update an incident response plan on how to prevent and react to IT security incidents (e.g., data breaches, leakage) taking into account that the data transmission component of the architecture is now being changed. The incident response plan must also include the procedure adopted for notifying personal data security incidents (e.g., to EDPS and/or Member States in case of high risk).
5) In addition to the measures described above to ensure data confidentiality (layered encryption, etc.), clarify other obligations of the staff of the third entity (-ies) supplying the star model (i.e. eu-LISA or Europol). For example, staff confidentiality obligations in case the staff may have access, inadvertently, to the encrypted data upon transit during testing, maintenance and system upgrades, and training on how protecting those data during those operations.
6) The European Agency, possibly eu-LISA or Europol, will need to receive the legal mandate to set up, and manage the central router.

Cost implications

Several technical changes will have to be implemented for this improvement opportunity to be implemented. Member States will have to set up the necessary middleware that supports the use of web-services. The SMTP servers will have to be used for the transition period until they can be decommissioned. Integration tests with the central

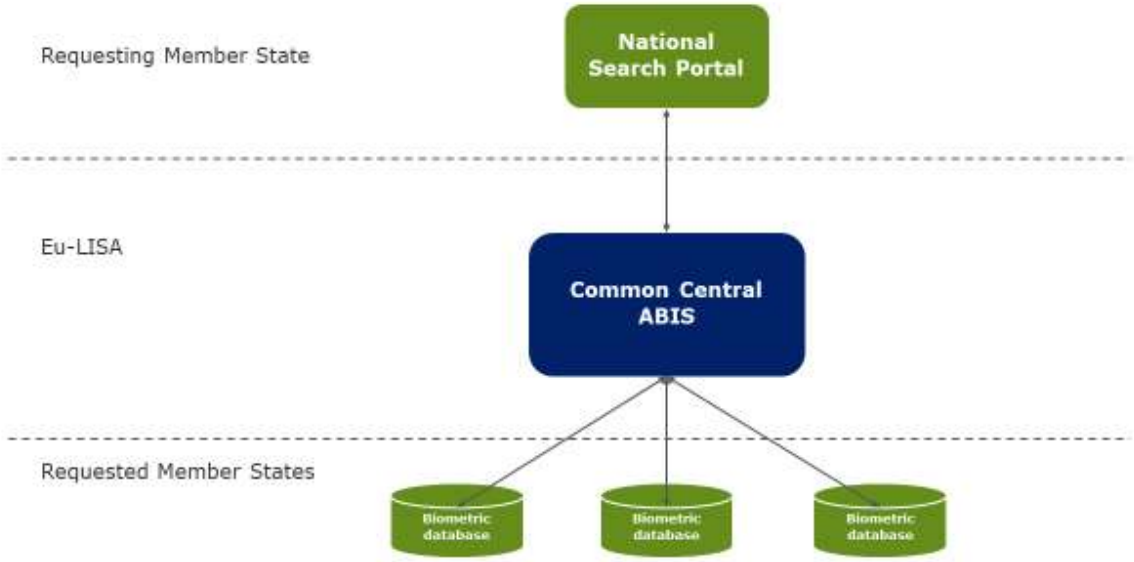
router and end-to-end tests between Member States should be performed to ensure that the new solution works properly. These national infrastructures and processes could be financially supported by an EU budget.

The central router will have to be configured to serve as brokering system between Member States. Furthermore, eu-LISA will have to provide the necessary support to Member States ensure the connection to the router.

5.3.2. Option 2 – Common ABIS matching system

The second option envisaged for the IT architecture remains a decentralised architecture, but with a European ABIS managed at a central level. Member States will still manage their national databases, but all Member States would make use of a common centrally managed ABIS (for the purposes of matching) with direct access to all databases to perform both Prüm and national searches.

This concept could be somewhat compared to FBI's Next Generation Identification programme.



Source: Deloitte Touche Tohmatsu Services, Inc.

Figure 18 – Diagram IT architecture common ABIS

The common ABIS involves the following:

- A central ABIS would be implemented and provide centralised biometric matching to requesting Member States;
- The central ABIS would not store any image data and only biometric template data would be stored in a proprietary format;
- A central portal could be provided to allow Member States to login and perform operations, submit requests and view previous results;
- When a requesting Member State performs a search (resulting in a candidate list), the central ABIS would need to provide response data (finger print images) from the connected national level database.

The purpose of this solution is to provide economy of scale (single central matching engine for all Member States) in relation to the ABIS platform whilst ensuring Member State image data is stored in a decentralised manner.

The main concern for this solution is that every national image should be enrolled in this common ABIS which would lead to a very large gallery size. The biometric images will still continue to be stored in national databases.

In other words, a European Agency would maintain a common ABIS system that would be used for Prüm searches. Member States should be offered the possibility to use the common ABIS for their national searches, to avoid duplication of an ABIS system at European, and one at a national level. The data would still be stored and managed at national level.

With an immediate connection between the ABIS matching system and the national databases, there would be no need for an SMTP email messaging infrastructure for the first step. This would signify that the central router as presented earlier would no longer be necessary. However, national biometric templates need to be stored in the common ABIS for the matching. This means that all fingerprint images will need to be enrolled in the new common ABIS.

By using a common ABIS, it would make sense to also propose a common search interface to perform queries using the ABIS. All those solutions should be managed at a central level. The search through a central ABIS should still be performed in a two-step approach, where a follow-up procedure is needed to share the personal information of a suspect related to the confirmed hit.

Having a common central European ABIS would present the following benefits.

It is estimated that an ABIS should be replaced every 5-8 years. This replacement will depend on the re-evaluation of the expectation of the system requirements. This means that if this technical solution is accepted, thoroughly analysed and put into production, several national ABIS will have to be replaced by then. They will be able to benefit from an economy of scale given that only one ABIS should be bought for all participating countries, and only one should be maintained. Of course, this ABIS should be very robust, as it should be able to deal with much more data and many more requests than the current national ABIS have to deal with.

Furthermore, all Member States would be using the same ABIS and therefore would need to agree the minimum performance, configuration and technical requirements required to accommodate all Member States.

Business requirements	Fulfilment of the requirement
1. No disruption of the service	**Possibly**. Connecting the central ABIS to all national Member States will prove to be very difficult, given that national matching engine are already in place. The guarantee to not have the Prüm process disrupted cannot be given at this stage.
2. Introduction of new data categories	**Yes and No**. The new ABIS can be foreseen to accommodate new data categories such as facial images. However, once the ABIS is up and running, adding new data categories will most likely very difficult to implement.
3. Data protection by design and data protection by default	**Yes.** The architecture already fulfils this requirement (e.g., storage of template data that is not personal data).

4. Adding new connections	**Yes**. Once connection has been made with the central ABIS, all other already connected Member States will be able to query the new joiners' database. However, connecting the ABIS to a new national database will be more complex than linking the current national systems to the central router.
5. Re-use of existing IT component	**Yes**. Although a new separate system could be provisioned, existing platforms such as the shared Biometric Matching Service could be utilised.
6. Harmonization of message format	**Yes.** The central ABIS or communication server should be able to adapt the message format in order to communicate with other systems.
7. Connection of new IT components	**No**. No other IT components should be added to the central ABIS.

Table 8 - Business requirements 1

There are many potential cost benefits and operational improvements that could be gained from a central ABIS platform. It has extensive legal and technical implementation considerations which, along with feedback from Member States, has been used when determining the final recommendations presented below.

Operations and end-users

Adoption of a central shared (criminal) ABIS platform would require Member State users to be re-trained in the use of the set of new software packages. In addition considerable effort would be needed to setup a team to help manage the national data contained within the central system.

The central ABIS is foreseen to deal with fingerprints and facial images, not DNA data. Efforts (made nationally or at central level) to enrol all fingerprint images into templates usable by the central ABIS should be undertaken.

As some Member States will want to retain their national level systems, law enforcement users would need to be trained in the use of multiple systems and workflows.

It would be useful for any central system to provide support for all national languages to ensure that every Member State get usability benefits. Given that the central ABIS will not be stored at national level, a cloud-based login could be foreseen.

In terms of search and adjudication process, no major changes are expected, as the two-step approach will be maintained. However, all forensic experts would make use of the central ABIS, instead of using national systems. This would probably mean for many forensic experts that they should be trained and get familiar with the new ABIS technologies. As the features of a central ABIS would be the same as of the national ABIS, this does not present any major implications.

In terms of data, problems are expected to arise while trying to connect the central ABIS to every national database. Since Member States have been collecting and storing biometric data in different quality, the use of the ABIS with every database might be difficult. Any solution will need to accommodate for gallery images of varying quality and outline common quality metrics for communication (i.e. ESS for DNA, ICAO for faces, and NFIQ2 for fingerprint). Enforced restrictions based on quality will not be suitable due to potential loss of data (unusable lower quality data).

It is important that either the biometric image data stored at national level shall be converted in a readable format by the ABIS or the ABIS should be able to treat all the biometric data whatever the data format or quality. However, poor image quality in the

image gallery will result in poor matching results which will be amplified by the enormous gallery size of a common central ABIS.

It should be noted that this solution involves the storage of biometric templates only at a central level for the purposes of matching. The central ABIS requires a connection to the national level databases in order to return data sets back to the requesting Member State for manual verification.

Technical and security

Connections from the central ABIS to the national databases need to be established and will be much more complex than linking national systems to the central router. This can be explained by the fact that encoded fingerprint are stored in a vendor proprietary data format, meaning they cannot simply be transferred and loaded in a new biometric matching system. Most of the pictures of fingerprints will have to be enrolled in the system again.

The system should be efficient and scalable enough to be able to cope with all national and Prüm requests. The ABIS should ideally be organised in such a way that biometric gallery items are tagged with meta-data allowing for targeting searches. This would allow searches to be performed on individuals where the data originated from a particular Member State. The re-use of the sBMS would be recommended, if this technical solution is opted as a central criminal ABIS.

This will prove to be difficult, due to the organic growth of databases, and different standards that are being used. This will definitely have an impact on the performance of the ABIS and should be further analysed with potential vendors.

The ABIS would be centrally hosted. This would remove the need for a central router as all requests would be send and handled centrally. The ABIS would be managed by a European body with adequate mandate (it could be potentially the eu-LISA). In consequence, the following points should be considered:

- Both the central router and central ABIS should be authenticated in Prüm landscape when exchanging requests/replies with other components. Digital certificates of TESTA Certificate Authority (CA) should be considered. The standard X.509 shall be used to ensure interoperability of the certificates.
- In addition to the encryption at the TESTA network level, an additional layer of encryption at the data level could be implemented to ensure only authorised users have access to the data in clear.
- The central ABIS should encrypt again the requests and launch searches in the target country.
- Restricted access should be granted to central ABIS to perform a search in the national biometric databases
- The central ABIS plays an intermediate role to launch search request(s) and return the results to requestor so it is strongly recommended to not store sensitive data. If this is required for business reasons (statistics etc.), this should be formally agreed with data owners (i.e. countries). In consequence, clear retention periods should be defined and should be properly implemented.
- As matter of principle, the encryption technologies to support the security mechanisms mentioned above should always follow state-of the-art open standards/protocols and relevant compliance requirements in order to be in line with evolution of threat landscape.
- As single point of failure, the central ABIS should consider a redundant setup. An adequate capacity planning and monitoring capabilities should be put in place in order to ensure that service availability requirements are met.

The common security best practices should be properly implemented and managed for the central router and ABIS (e.g. Governance and organisation, Physical security, Access

control, network security, backup and operations, Business continuity and disaster recovery etc.). It is recommended to use and align with known frameworks and standards (i.e. ISO27001) in order to be able to provide comfort to Member States and other relevant Prüm stakeholders.

A European Agency should set up the ABIS, but will require cooperation with each Member State to implement data transfer processes between the ABIS and each national database. The implementation is considered to be technically complex however given the experience of eu-LISA in delivering such platforms, it is expected to be a feasible option. As mentioned earlier, all fingerprint and facial (if included in the Next-generation Prüm) images will have to be enrolled into the central ABIS.

Since every Member State will most likely have a different database setup, the connection to the ABIS and the national database will need to be made with the collaboration of both the European agency and the Member States.

Legal and data protection

Legally, many Member States will have to change their national law to accommodate the possibility to store the biometric templates at central level.

Under the hypothesis that this option is retained, the change from the current status quo (decentralised system) to a centralised matching engine is aligned with personal data protection rules. .

Based on the description of this option, it appears that fingerprint/facial images (or DNA profiles) from the Member States' systems would need to be 'enrolled' into the central engine for the purposes of matching. The engine would then create a 'template' of the reference data (both would be stored) and store with a reference to the Member State being the "owner" of the data. However, biometric templates represent feature extractions of actual biometric samples and obtained in such a way that reversing the extraction process is not possible. Therefore, those templates, in the same way as irreversibly anonymised data, are not in general personal data (unless the extraction process can be reversed). Therefore, no personal data would reside or be stored on the centralized matching engine and, hence, personal data protection laws would not apply in this respect.

Bearing this in mind, it may still be worthwhile looking into the following considerations if this option remains envisageable as they refer to data security in general.

1) Clarify the role of all actors involved in the data processing operations entailed by the matching and the responsibilities or not of those actors with respect to personal data (even if, at the end, no personal data are processed at the level of the Agency).

2) Document the roles defined above (in security documentation and data protection documentation) of both the Member States and the third entity.

3) Prepare or review the data retention schedule: indicatively, minimum/maximum data retention periods, as well as logs retention and data archiving relating to the templates.

4) Prepare and/or review the procedures of the Agency with regard to the protection of data at rest and in transit (such as encryption means).

5) Data access management procedure for both the Agency's staff but also of Member States' forensics teams (in case they have access to the matching engine).

In case the above policies and procedures are already in place, the parties involved may still have to adapt them to the context of this option, as well as the data flows and types of data involved.

1) Logging controls to avoid data exfiltration and unauthorised exposure to data on the central matching engine.

2) Draft the mandate to the European Agency (e.g., eu-LISA) or other third party who will set up and manage the central ABIS.

3) A robust incident response plan managed at centralised level is another important element to consider, in order to prevent data breach incidents and mitigate the consequences of those if they happen.

Cost implications

It is expected that significant cost will be required at a central EU level in order to define and deploy a central ABIS capability that meets the requirements of Prüm and all Member States.

In addition each Member State would be required to establish procedures for transferring and managing data stored in the central ABIS and as such would incur development costs in setting these up, assuming they are automated.

5.3.3. Option 3 – Web-service Communication

The third option presented relates to the adoption of web-service technology as the primary communication protocol for all Prüm requests.

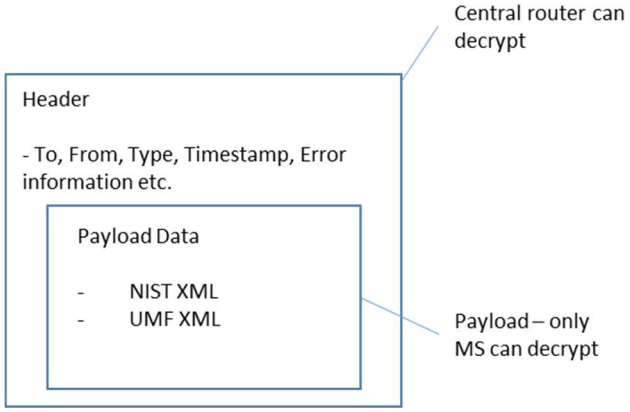
This solution aims to reduce the complexity of implementing data exchanges, make use of modern and secure technology platforms and compliment Prüm technical standards described in the chapters above. See Chapter Two on biometric exchange format and Chapter Three on the UMF.

In order to do so, the current SMTP mail system would be replaced with a new communication system, using web servers. Member State's application would send requests to either a target Member State web-service or, if adopted, the central router as described in section 5.3.1.

The web-service definitions would be defined centrally and be offered to Member States as an ICD and an XSD schema definition which would allow quick and consistent integration by technical teams. This is as currently done for DNA data exchanges in an ICD.

All messages sent via web-services will follow the same general structure and provide capability for enhanced, multi-layer security options.

First, all web-services calls will be invoked via the TESTA network using HTTPS/SSL protocols and encryption. In addition to this, the message is broken into a header and body section. The header information contains data used for routing (if with central router) and the body contains the underlying payload. The payload could be an ANSI/NIST-ITL 1-2011 XML file or a UMF compliant data set depending on the type of call being sent\returned. The diagram below shows how the record is composed.



A key aspect relating to security is that two separate pairs of encryption keys mayl be required if to ensure the central router can only access the header. Payload keys would

then still be shared between Member States (and not the central router) as currently done.

Follow-up Procedure Automation

In addition to the core benefits of adopting Web-service for next-generation Prüm, this solution aims at reducing the lead time for waiting for follow-up information during the second step after hit confirmation. This would result in a single Web-service based model being adopted for all Prüm message exchanges.

1) The following narrative would illustrate the business process of this solution:

2) The forensic expert of Member State A will look for a hit of a DNA stain he found on a crime scene. After querying the national database, he intends to verify if Member State B could have any potential matches, as the investigation has led to believe that this might be possible.

3) The forensic expert sends the query in the regular data format of Prüm to Member State B using the current SMTP email system. After several minutes all potential matches (with appropriate data for manual verification) are sent back to the forensic expert for adjudication. By chance Member State B finds a matching DNA profile, and a hit is then confirmed by the forensic expert.

4) The forensic expert validates the hit through the web-service communication system referring the country and the identification number of the biometric profile.

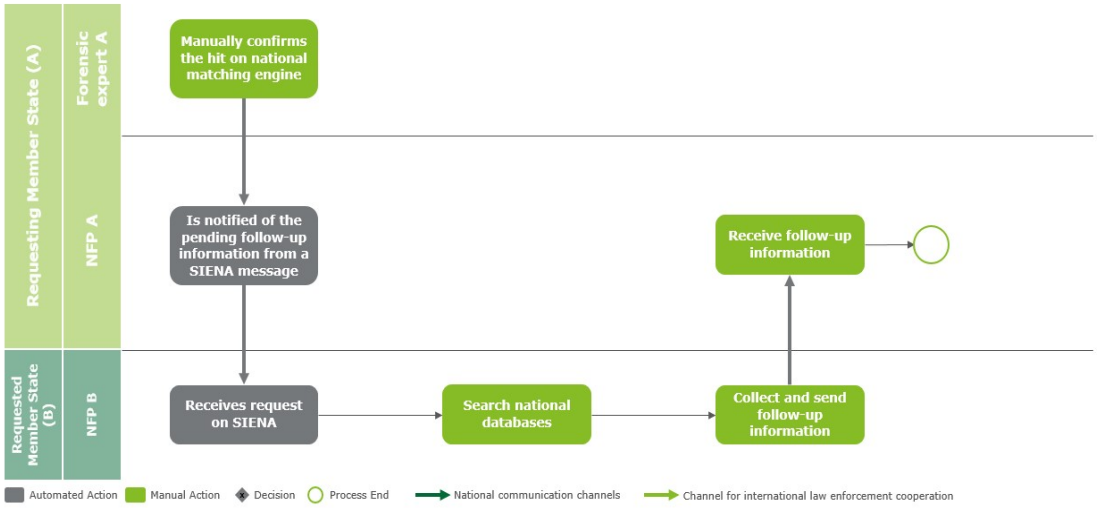
5) The web-service system, connected to the national databases, will trigger the automated retrieval of the minimum data set, using the identification number of the biometric profile.

6) The minimum data set will be forwarded to the requested national NPC, for their manual review and authorisation before controlling release back over the communication channel (e.g. SIENA).

7) The requesting NPC would proceed to forward the minimum data set after reception to the relevant criminal investigator and would request additional information than the minimum data if the investigation demands it.

This means that a new XML message format should be foreseen that would be sent after the adjudication process by the forensic expert. The message would then be automatically created, and include the reference information of the biometric profile. This message would be sent over from the national system using the SIENA communication channel to the requested Member State’s database for triggering the minimum data set.

Web service integration with SIENA



Source: Deloitte Touche Tohmatsu Services, Inc

Figure 19 – web-based communication solution process integrating SIENA

An extra module should be provisioned if a judicial authority needs to provide permission to exchange minimum data set after a verified match. The lead time for providing minimum data set of the suspect can be reduced from weeks to minutes if the process is automated.

With this solution, it is easier to track relevant statistics about match follow-up process that were not collectable in the past. It would be possible to track the time needed to answer specific requests.

The web server platform should be installed in every Member State replacing current SMTP based servers, and be connected to the appropriate IT components for DNA, fingerprint and facial recognition platforms.

The web-service communication system could be using a central router as it is proposed for the automated data exchange. This would avoid that bilateral connections need to be set up. The central router would work in a similar fashion as in the section 5.3.1 "Central router (hub-and-spoke solution)", with the difference that the minimum data set would be exchanged, and no biometric data.

Business requirements	Fulfilment of the requirement
1. No disruption of the service	**No.** The implementation of the web-based data exchange system should be done in a phased approach to avoid the disruption of the service.
2. Introduction of new data categories	**Yes.** Even though its main purpose is not the facilitation of introducing new data categories, this solution should support the automated data exchange of new data categories such as facial recognition.

3. Data protection by design and data protection by default	**No.** The technology will not per se support any data protection by design or by default principles.
4. Adding new connections	**Yes.** The purpose of the web-service approach is allowing easier integration into Member State systems. However, existing systems would be impacted.
5. Re-use of existing IT component	**Possibly.** It is possible to re-use partial already existing IT component, SIENA, for the exchange of data and minimum data set. However, the solution can also be built from scratch.
6. Harmonization of message format	**Yes**. The web-based system could be used to adapt the message format if deemed necessary.
7. Connection of new IT components	**No**. No other IT component should be linked to the web-based data exchange system.

Table 9 - Business requirements 2

Operations and end-users

No specific legal impacts are foreseen. Under more concrete terms, Swedish Framework Decision provides for general principles/requirements and Member States have a discretion to follow and implement them. In order to make the implementation of the web-service a success, Member States need to agree upon the use of this solution for the exchange of the minimum data set.

A similar solution is already being used by a Member State to communicate with 3rd countries (i.e. Austria with the USA). The work process for forensic experts would not change, but National Point of Contact should make use of this application for sending and receiving minimum data set and therefore the latter should responsible for dealing with the exchange of follow-up communication and information.

The web-service communication system should be made available on a 24/7 basis. The front end experience of users is not expected to change as the underlying delivery mechanism is transparent. However, for automation of the follow up process, new user interfaces should be foreseen and therefore users may need to be trained in its use.

Technical and security

Since this option is more an extension/enhancement of the different architecture options described in the previous sections, this analysis focuses more on the key risks introduced by web technology. The findings presented should be considered as extra elements on the top of the findings related to the option to select among the three option previously described.

Based on the Open Web Application Security Project (OWASP) framework, the following risks are identified as the top 10 possible risks for web technology – We included an analysis, how Prüm would be impacted by those risks

Risk Category	Top 10 OWASP risks	Impact on Prüm web component

Input Validation	A1:2017-Injection A4:2017-XML External Entities (XXE) A7:2017-Cross-Site Scripting (XSS)	Lack of input validation in Prüm search web form may involve the risk of injecting malicious script/text that will result in several issues (data loss/corruption, denial of access) sometimes this can lead to complete host takeover.
Access Control	A2:2017-Broken Authentication A5:2017-Broken Access Control	Weak authentication design may lead to gain unauthorised access to the privileged admin account to compromise the system.
Secure development	A3:2017-Sensitive Data Exposure A8:2017-Insecure Deserialization A10:2017-Insufficient Logging & Monitoring	iDevelopment not following best practices (i.e. OWASP) may lead to the disclosure of confidential info (i.e. Biometric info)
Mis-configuration	A6:2017-Security Misconfiguration A9:2017-Using Components with Known Vulnerabilities	Unpatched components/ unprotected files and directories in the Prüm web application may lead to unauthorised access to confidential info (i.e. Biometric info)

Table 10 - Top 10 OWASP risks

The exchange of data should be UMF-compliant to ensure homogeneous answers across Member States. This format is adapted for the exchange of the minimum data set.

Implementation will largely depend on the underlying IT architecture, as this solution will come as an extra feature. Furthermore, the implementation will depend on whether a custom application is created, bought from an IT vendor or if a similar application can be adapted to fit the business requirements of this web-based application.

The performance should be similar to the requirements of the actual Prüm network. Member States should connect their national databases to the web-service communication system, using messaging servers to receive and log the requests for the minimum data set, and then also for sending the information across.

Legal and data protection

The nature of data being exchanged over this solution will not change from what is currently exchanged. Only the means to exchange the data will be different. Therefore an assessment of the solution (DPIA) will be necessary to ensure that the level of security is appropriate and that risks can be identified. In particular, the solution would utilise the same TESTA network as currently used along with layered encryption which protects message payload to the same level as the current solution.

Cost implications

As with the central router changes, significant initial costs may be incurred when Member States update their systems to communicate via Web-services. However, as these costs would be a part of a wider EU-architecture and new standards implementation, the majority of costs would be covered by an EU-budget thus minimising the financial impact for MS.

The ongoing costs of using Web-services is expected to be low given the simpler integration architecture and costs for new Member States joining Prüm would be significantly lower than the existing SMTP based approach.

5.3.4. Conclusion

To conclude on the possible evolution of Prüm architecture, we believe that the best option is to implement a central router architecture together with the web-service communication model (option 1 and option 3). The implementation of a central ABIS or database will be too difficult compared to the efficiency gains. Furthermore, some Member States' representatives expressed a strong feeling against the centralisation of a biometric matching service.

The table below highlights each options alignment to the key architecture requirements.

Criteria	Central router	Common ABIS	web-based system
1. Adding new connections	Yes	Yes	No
2. Re-use existing IT component	Possibly	Yes	Possibly
3. Data protection by design and data protection by default	Yes	Yes	Yes
4. Introduce new data categories	Yes	Yes and No	Yes
5. Connect new IT components	Yes	No	No
6. Harmonise message format	Yes	Yes	Yes
7. No disruption of the service	Yes	Possibly	No

Table 11 - Alignment options to the key architecture requirements

Theoretically, all solutions are eligible to meet the data protection by design and by default requirements in the way they are outlined above. Yet, specific considerations have been identified for all of them.

The centralisation of the ABIS will only help in the matching process (first step), but is technically quite difficult to implement given the potentially enormous amount of records and the current different national processes and solutions.

Moreover, experts have indicated that the effort, required for making legal changes for the centralisation of the ABIS, would be quite high. The operational efficiency gains would not compensate therefore for a change from a decentralized architecture to a centralized one. This solution is not recommended.

In conclusion, it is recommended to change the architecture to implement a central router (option 1) and a web-based data exchange system (option 3) in a phased approach to avoid any disruption of service. The central router should guarantee that no data can be read in clear and should be maintained by a European agency. The web-based data exchange system should also be developed at central level and distributed to Member States for them to configure and implement. It is not recommended to exchange the minimum data set through web-service, but to use the SIENA communication channel.

The use of web-services to exchange the minimum data set as prescribed in section 3.1 set is not recommended for the Single Composite Option as there are significant differences when it comes to the national implementation of databases (centralized vs. decentralized) or the authorities managing the databases and channels are already used for this purpose. The study team recommends the use of Siena as prescribed in section 3.2.

This page has been left blank intentionally.

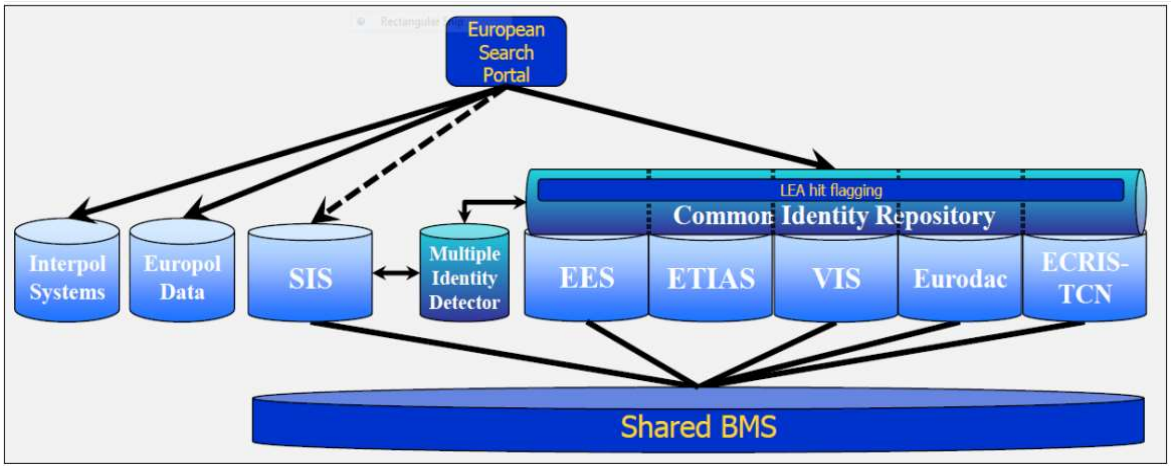
6. ADDING INTEROPERABILITY SOLUTIONS

6.1. *Interoperability solutions*

In May 2019, the European Parliament and the Council adopted regulations 2019/817 and 2019/818 establishing a framework for interoperability between EU information systems for borders and visa and for police and judicial cooperation, asylum and migration.[28] The purpose of the regulations is to ensure that border guards and law enforcement officers have systematic and efficient access to the information they need to perform their duties, thus further closing security gaps.[29]

By making the EU information systems interoperable, police and border officers, among others, will be able to access information much faster than today. Easier information sharing will considerably improve security in the EU, allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat illegal migration. This will be done via:

- A European search portal to allow authorities to search multiple information systems simultaneously, using both biographical and biometric data;
- A shared biometric matching service, which would enable searching and comparing fingerprints and facial images from several system;
- A common identity repository, which would contain biographical and biometric data of third-country nationals available in several EU information systems;
- A multiple identity detector, which checks whether the biographical identity data contained in the search exists in other systems covered, to enable the detection of multiple identities linked to the same set of biometric data.[30]



Source: European Commission

Figure 18 – Interoperability solution 1

Out of the six major EU central information systems[31] that will be made interoperable through the use of central components, five systems store biometric information; fingerprints and facial images. It is estimated that about 300 million persons will be

[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1578995996634&uri=CELEX%3A32019R0817

[29] https://www.eulisa.europa.eu/Newsroom/News/Pages/Political-Agreement-for-Interoperability-between-EU-Information-Systems.aspx

[30] https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/

[31] VIS, SIS, Eurodac, EES, ECRIS-TCN and ETIAS

registered in the Common Identity Repository, the common database for every information system through the interoperability framework. The CIR will contain both biographic and biometric data.

From the perspective of law enforcement access to non-law enforcement EU central systems, the Interoperability Regulations include two relevant articles:

- Article 20 Access to the common identity repository for identification and
- Article 22 Querying the common identity repository for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences.

The interoperability solutions are expected to be implemented by 2023.

Article 20 of the Interoperability Regulations allows a police-officer (following adoption of national legislation) to perform an identification, using the fingerprints/facial-image of a person that is physically present to capture these biometric samples. It can thus not be used for investigations where biometric data (in particular latent-fingerprints) were captured in absence of the person.

The police-officer queries the combination of ESP-CIR-sBMS in order to retrieve the identity-details (names, date-of-birth, gender, travel-document-details, fingerprints and facial-image) if these are recorded in the CIR (consisting of identity data on persons recorded in EES, ETIAS, VIS, EURODAC and ECRIS-TCN).

The co-legislators accepted the fact that the core-data to identify a person (names, date-of-birth, gender, travel-document-details, biometric-samples) be retrieved directly without requiring a second step.

Article 22 of the Interoperability Regulations allows a law-enforcement query towards the data in the CIR (so containing identity data of persons recorded in the EES, ETIAS, VIS, EURODAC. ECRIS-TCN being excluded).

This query requires no ex-ante authorisation but the result will only include a hit/no-hit indicating which source-system (EES, ETIAS, VIS or EURODAC) could contain data concerning the query. In case of a hit, the investigate officers must request full access to the particular records in a second step involving authorisation by a judicial authority. If the officer decides not to request this full access, the reasons must be captured and retained in the national file.

Using the provisions of Article 22 for purposes of a Prum forensic search (in particular latent-fingerprints) would be highly impractical given these particular safeguards.

For the remainder of this document, only the provisions of Article 20 (Police identification) are taken into consideration for a possible integration between Prüm and the ESP-CIR-sBMS.

The interoperability solution currently being designed does not take into account the possible integration of the Prüm network. The high-level expert group on interoperability has recommended the European Commission to investigate if the "hub-and-spoke" model for Prüm (please refer to section 5.3.1 for more information) could serve as a basis for further integration and centralisation for police cooperation. HLEG-Interoperability also recommend investigating whether the Shared Biometric Matching System could replace existing national biometric systems.

The current and the two first aforementioned possible IT architectures (central router and central ABIS), presented in this study, are analysed to determine how they could possibly be integrated the four aforementioned interoperability dimensions, and the associated benefits and implications.

The technical, operational and legal benefits of linking the Prüm network to the interoperability solutions will largely depend on the nature of the chosen IT architecture for Prüm. Nonetheless, some benefits and considerations are valid whatever the Prüm architecture.

Cross-cutting benefits

With major European information systems made interoperable, it can be expected that information exchanges in the EU will become smoother, given that the ESP will technically be able to retrieve information from all EU information systems. Interoperability between information systems will allow the systems to complement each other, help facilitate the correct identification of persons and contribute to fighting identity fraud.

Cross-cutting challenges: data quality

National databases, both with biometrical and biographical data, have been fed over the years without defined or consistent quality standards. This can be explained due to different techniques to store the data, faulty human recording, changing best-practices, operational reasons and others. This is even truer given that 28 Member States have started storing data based on national, and not European legislation.

The automated quality, format and completeness check should be completed at a central level to ensure a minimum level of harmonisation. A balance should be found between strict data quality rules for exchange and end-user flexibility to use the system. By using defined quality standards for biometric data, matching efficiency can be understood and controlled. Given that Member States already possess databases of biometric data and systems for the enrolment of biometric data and that the quality of probes cannot always be ensured, the rules should be flexible enough to not restrict law enforcement officers from using the interoperability solutions.

Cross-cutting challenge: law enforcement access

Law enforcement officers have strict and well-defined access rights and access procedures when it comes to accessing data in the non-law enforcement EU Information Systems. Mechanism are put in place to only access data following strict ex-ante and ex-post procedures often involving a central access-point, a cascade and an ex-ante authorisation.

During the first round of interviews, some Member States pointed out the little added value of integrating the Prüm network to the interoperability solutions because of the specific access-procedures and processes towards primarily non-law enforcement data (EES, ETIAS, VIS, EURODAC). However, for the current and the two new options for the IT architecture (central router and common ABIS) benefits will be presented as from section **Error! Reference source not found.**.

Before analysing the possible interaction of the Prüm system with the interoperability solutions, two concepts that will be used through this documents need to be clarified.

Interoperable: Systems use the same data format and standards in Prüm and the interoperability solutions. Member States can then use the same data format to query both Prüm systems and the interoperability solutions.

Integrated: A hard immediate connection exists between the Prüm network and the interoperability solutions, where data can be exchanged between the two systems.

6.1.1. Assumptions and limitations

It is unlikely that the current Prüm network can be made interoperable or be integrated with other major European information systems without changing its architecture. Linking the current mesh network of decentralized databases with the interoperability components and EU central systems will be inefficient and technically difficult to put in place.

Therefore, if the EU aims for integrating the Prüm network in the interoperability landscape, there is a need to integrate some components of the Prüm IT architecture at central level.

The feasibility of all proposed architectures have been discussed with eu-LISA, the EU agency responsible for the technical design of the IT architecture of EU central systems and interoperability solutions.

6.1.2. Option 1 - central router

Specifically from the Prüm perspective, the link to Article 20 that allows a police officer (in the presence or immediately following the presence of a person) to perform a biometric identification via the ESP, could provide possibilities for further streamlining the law enforcement work processes.

As mentioned, the centralisation of IT components of the architecture is needed in order to facilitate the integration of the Prüm network to the interoperability solution. Therefore the possibility to integrate a Prüm network with a central router (as described in section 5.3.1) to the ESP is the only option to be analysed.

Error! Reference source not found. depicts the possible integration of the Prüm central router with the European Search Portal for the purposes of an identification (ten-print to ten-print or high-quality facial-image).

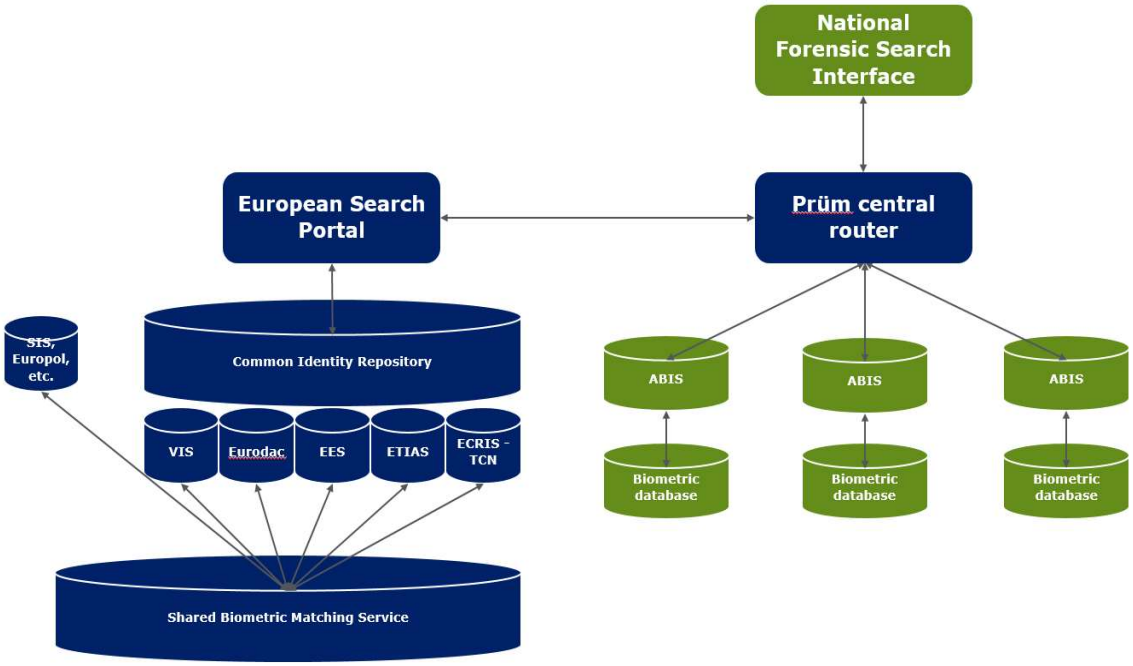


Figure 20 - Diagram of the IT architecture

The search process through the Prüm central router would be very similar to what forensic experts experience today, with the exception that they could target the EU central systems for the purposes of Article 20, to retrieve potential data at the same time.

Operations and end-usersTechnical and security

The new architecture will not have any impact in terms of performance, considering that the European Search Portal and underlying CIR/sBMS components constitute a completely separate infrastructure from the Prüm network.

The considerations for the security of the transaction and the system are the same as for the IT architecture. Please refer to section 5.3.1.

It is advised to use the same standards in terms of data quality and data format than the one used in the interoperability solution for both fingerprints and facial images.

The collection of data statistics could be done over the Prüm central router, which should be centralising the in- and outflow of all Prüm and interoperability requests.

The number of requests sent, the time for providing automatically the data, and the time to answer the follow-up requests can be tracked.

The integration with the interoperability solution is done through the European Search Portal, and no other EU central system or interoperability component(s).

The search would flow from the national forensic search interface to the Prüm central router, then be redirected to one or multiple national forensic search interface and/or the ESP. In case a national forensic system is queried, the system process will be similar. If the ESP is targeted, a query will be launched against the Common Identity Repository, using the sBMS as matching engine.

The European Search Portal should be accommodated to receive and forward SMTP emails, as done over the Prüm network. Alternatively, should a Web-service based approach be implemented as defined in section 5.3.3, the ESP would initiate and receive Web-service calls from the Prüm central router.

Member States should work closely with eu-LISA to ensure their connection to the central router is implemented in line with expectation.

If this solution is chosen, we recommend to first set up a Prüm dedicated router. The connection of the Prüm central router with the ESP through the central router will then be facilitated.

Legal and data protection

Legally, the interoperability solution and the new Prüm legal instrument have to be defined and implemented in order to reflect those technical changes. In the interoperability regulations, Article 20 foresees that the CIR can be queried for cases of serious-crime and terrorism, no additional legal impact is to be foreseen.

For the fundamental rights principles to be respected in this solution, the security of the system should be adequate and risks should be mitigated and only appropriate authorities should have access to the data. A DPIA will most likely need to be performed.

All other requirements are already taken into account by either the Prüm Decisions or the Interoperability solutions regulation.

Cost implications

Please refer to the CBA for the cost estimations.

6.1.3. Option 2 – common ABIS matching system

In order to re-use to the extent possible the components that are or are being developed in the EU, the study team investigated the possibility to make use of the Shared Biometric Matching Service (sBMS) as a possible central ABIS. The concept is comparable to FBI's Next Generation Identification programme. Theoretically, the idea seems very promising. The sBMS is not yet developed, which still make it possible to accommodate the Prüm technical requirements with the Interoperability requirements. Eu-LISA aims at finalizing the interoperability solution project by 2023.

Theoretically, the introduction of a central ABIS would lead to the following benefits:

- A central ABIS would mean that Member States would not need to rely on the capacity of their national systems to send matches, liberating some countries from the need to operate a more expensive ABIS than they need.
- A central ABIS would imply that the matching algorithms would be common and known by the forensic experts, which would allow them to smoothen the matching process.
- If the central ABIS can be used for national queries, instead of their ABIS, Member States could get rid of expensive ABIS, and benefit from economies of scale.

The Prüm network would still make use of the European Search Portal as the message interface for the searches and answers. This means that out of the 4 interoperability components, two would be applicable for this scenario: the European Search Portal and the shared biometric matching system.

For this solution to work, the sBMS should be able to perform the matching for certain (or all) national databases and deal with all type of data format, quality and different storage in the databases.

However, according to the IT architects in charge of the interoperability solution, using the sBMS is most likely to be very challenging given the very high number of templates.

Each Member State will share data with the sBMS by way of "enrolment" into the system. This would require the submission of biometric image data to the ABIS in order for it to encode a template to be used for matching.

This means that if the Prüm network will make use of the sBMS as central matching engine, there is a need to store all national biometric template data and to at least send all biometric image data for enrolment.

The actual sBMS will be designed to match fingerprints and facial images. This means that it should also be able to cope with DNA in the future, if we were to centralise Prüm matching capabilities at European level. This will add a new degree of complexity.

Member States have not expressed the desire to have a central ABIS, as they already possess such capabilities at a national level. Member States might be reluctant to decommission systems for which they have invested.

Operations and end-users

The workflow of using the sBMS as a common ABIS would happen as follows:

- The forensic experts launch the request through the European Search Portal and specifies the country/system(s) he would like to query.
- The search makes use of the sBMS to check in the specified national database and retrieves the potential matches.

These matches would then need to be manually verified by the forensic expert. Once the hit is confirmed, the follow-up procedure could start.

End users would need to adapt to using a new setoff technology tools to serve the purposes of their requests. However these new tools and user interfaces will likely be very similar to the national level applications used for currently processing requests and the impact is expected to be low. Any changes to the existing ESP and sBMS could impact existing users and would need to be considered as part of the implementation.

Technical and security

The sBMS should be able to deal with the varying quality of data stored by each Member State. The sBMS is supposed to match biometric data for five major information systems, adding 28 Member States databases will prove to be difficult. An integration layer should be foreseen between the national databases and the common ABIS so that any change in the databases are can be reflected in the common ABIS.

For the use of a shared ABIS to work, the following would be required.

- Template of the biometric data images would need to be enrolled (stored) into the central ABIS solution. Depending on the selected ABIS, some data migrations may be possible with existing templates however many will need to be enrolled from image data. Storage of the templates only is aligned with the data minimisation requirement and may be considered as an appropriate mitigating control to avoid unnecessary exposure to misuse and confidentiality breaches data that are not any longer placed under the direct control of the Member States.

- Quality and data grouping configuration would be such to ensure data of various quality can be enrolled (minimal Failure to Enrol Rate – FTR). Consideration should be given, for example, to grouping of data based on quality/source of the image data. For example lower quality facial images will significantly impact the FNIR (misses) and FPIR (false matches) of a system, as shown in NIST FRVT.
- A central ABIS would need to be carefully managed and allow both the search of national only data and also globally. I.e. the data is 'binned' (separated). The larger the size of a biometric gallery, the higher the chances of a similar (but false) example existing. This is most significant with face recognition. It is expected that this can be mitigated through proper design of the ABIS solution.

Appropriate technical and organisational measures should be taken to ensure the required level of security to mitigate potential risks, as described in section 5.3.2.

When technical details have been sorted out and the development begins, it is advised to use a phased approach when using the new architecture. The current mesh topology should not be abandoned in a big-bang approach, but gradually abandoned as the sBMS can be used as ABIS. Member States should closely work with eu-LISA to ensure their connection to the sBMS.

Legal and data protection

Member States' legislation would need to allow for the storage of the biometric templates in a central European repository. The Prüm and Interoperability instruments should both be amended to reflect those changes.

Similarly with Option 2 of the architecture discussed above:

1) Clarification of role of (joint) data controller vs. processor. The storage of biometric data images is considered as a 'core' and 'essential' data processing activity and may trigger the qualification of the entity which will provide the central ABIS as joint data controller.
2) National legislation on law enforcement may not allow the transfer for storage outside of the territory or may subject such storage to specific conditions and therefore may need to be changed. In addition, the opinion of the local Data Protection Authority before this option is adopted may be needed.
3) Adequate security measures shall be implemented at the level of sBMS to meet the data confidentiality, availability and integrity requirements. As the system has already been under design, it is expected that such measures are now being defined and developed but they may need review and customisation to the Prüm context.
4) Data segregation requirements (per country) to be implemented on the central ABIS.
5) Data retention and deletion rules would need also to be defined, taking into account national restrictions and needs in this regard.
6) A Data Protection Impact Assessment focussing on the mitigation measures that should be taken to lower the risk of storing those data outside of the direct authority and control of the Member States will be needed.
7) A comprehensive incident response plan shall be designed and if existing, it may be needed to review it and customise it to the Prüm context.

Cost implications

No cost estimates are provided for this opportunity, as this opportunity is not recommended in the study.

6.1.4. Conclusion

It was concluded in section 5.3.4 that the best IT architecture for the Prüm network is a star topology with a central router, and preferably enhanced by a web-service solution to streamline the exchange of minimum data set. This IT architecture could be setup independently of other European Information Systems.

After analysis of the possible integration of the Prüm system with the interoperability solutions, it has been concluded that there is a business case to integrate the ESP for the purposes of Article 20 (Police identifications) to the Prüm network.

Even if the interoperability solutions are mainly designed for border and migration management, law enforcement officers will be allowed to query the Core Business Systems for the purposes stated in Article 20 of the interoperability regulations.

Given the many IT components/systems that compose both the interoperability solutions and the Prüm network, there are several ways to integrate. However, the integration should bring benefits to the law enforcement authorities and should operationally, technically, financially and legally be viable.

The only integration that has been deemed reasonable, is connecting the ESP to the Prüm central router. This will allow simultaneous queries to all biometric data in different systems law enforcement officers have access to, in order to identify an unknown person.

The use of sBMS as matching engine at national level requires the enrolment of all biometric template and a difficult integration.

Biometric data entered in one of the Core Business Systems should not be checked against the Prüm national databases because:

1) There is no legal basis to perform this type of search;
2) National systems do not have the bandwidth to cope with this amount of searches; and
3) The need for manual verification requires extensive human effort.

Deloitte recommends the use of common and interoperable standards for biometric data (ANSI/NIST-ITL 1:2011, 2015 update or later). This will allow national forensic expert to use the same format to search either in Prüm, either in the interoperability solutions without the hassle to convert the biometric file.

6.2. *Integrating new stakeholders in the Prüm landscape*

The consultations with stakeholders led to suggestions that the scope of Prüm could be enlarged in order to include additional stakeholders, such as Europol, Interpol, as well as other third countries. By adding these stakeholders to the Prüm's landscape, their databases would be accessible for the automated exchange of data via Prüm network.

6.2.1. Proposal

The connection of these new stakeholders to the Prüm network would be as follows:

- Europol would have the same technical capabilities as Member States, i.e. putting their biometric database at disposition of Member States to be queried,

with the capacity to also query Member States databases, and receiving a hit/no hit notification;
- Interpol's databases would also be at the disposal of the Member States through Prüm;
- Some third countries (such as the acceding countries, candidate countries and potential candidates) could also be part of the Prüm framework.[32] This would be included with the same technical capabilities as the Member States.

6.2.2. Assessment

This section presents the advanced technical analysis on the possible inclusion of new stakeholders in the Prüm landscape.

Operations and end-users

If Europol is included in the Prüm framework, additional human resources will be needed to address the requests received by the Member States and also launch their searches. Although Europol's databases are relatively small in comparison to the Member States' biometrics databases, it may bring a significant added value as it contains data from third countries, not currently accessible for Prüm searches. Should the options recommended by the study for hit follow-up exchange of data be implemented, Europol would be able to support the Member States throughout the full Prüm workflow.

Concerning Interpol, its databases are also relatively smaller in comparison to the ones of the Member States. Nevertheless, the inclusion of Interpol will likely bring an added value to the Prüm network by providing a single search interface to query Interpol databases via Prüm. The data-protection safeguards and rules on the processing of data as specified by Interpol should be closely analysed. No possibilities for Interpol member countries to query Prüm should be foreseen.

The inclusion of third countries databases would also enlarge the number of databases connected. These would allow for larger scale of searches, as additional countries would make accessible their databases. As for Europol and Interpol, if new third countries join the Prüm network, additional human resources will need to be allocated in order to handle the Prüm's requests.

Lastly, the inclusion of new databases would likely increase the number of data exchanges, entailing additional workload for the Prüm's end users, as well as increasing the manual verifications.

Technical and security

From a technical point of view, the inclusion of Europol will require to connect their databases with the Prüm network, either via a mesh or star topology (depending on the final architecture of the Next-generation Prüm). Besides, in order to avoid any overlap in the data (i.e. duplication of the same data providing from EU Member States and Europol), only Europol's data coming from third countries, and not from Member States, should be made available.

[32] Albania, Austria, Bosnia and Herzegovina, Bulgaria, Hungary, Macedonia, Moldavia, Montenegro, Romania, Serbia and Slovenia are developing a network similar to Prüm for the cross-border exchange and comparison of forensic data.

Likewise, Interpol's connection could also be implemented either via a mesh or star topology. Similarly to Europol's connection, only Interpol's data coming from third countries will be at the disposal of Member States to avoid any type of overlap.

As for the third countries, the databases (biographic and biometric) will need to be set up first, if not done so yet, in order to subsequently connect them to the Prüm network (via a mesh or star topology, depending on the final architecture of the Next-generation Prüm). Besides, the databases and connection will be required to follow the Prüm network standards and requirements.

Legal and data protection

From a legal point of view, international agreements would be necessary between the European Union and the stakeholders willing to join Prüm. As established in Article 218 TFEU, the Council shall authorise the opening of such negotiations, adopt negotiating directive, authorise the signing of agreements and conclude them. These international agreements should replace the current bilateral agreements in place between third countries and some of the EU Member States.

Concerning Europol, being an EU agency, no international agreement will be required as the Regulation (EU) 2016/794, together with respective provision in the future Prüm instrument would provide a relevant legal basis. Taking into consideration that in the context of these transfers, sensitive data is exchanged, Europol based on Article 67 of the Regulation (EU) 2016/794 has to adopt all the appropriate security measures and rules for protecting data confidentiality. In case of classified sensitive information, Europol has to take into account the requirements foreseen in the Decision (2013/488/EU). The concrete provision on Europol's participation must make explicitly clear that no data that has become available to Europol in the context of Prüm exchanges, is transferred to third countries without the permission of Member State(s) concerned.

As for data protection, special attention should be paid to the exchange of personal information with third countries in order to avoid any misuse of personal data. This issue should be clearly addressed in the international agreement signed between the European Union and the third country or Interpol. More specifically, based on the Article 36 of the Law Enforcement Directive, Member States shall provide that a transfer of personal data to a third country may take place where the Commission has decided that the third country in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. The assessment of the adequacy of the level of protection will be assessed and the European Commission will proceed to this assessment taking into account some concrete and mandatory requirements based on the Article 36(2) of the Law Enforcement Directive.

Cost implications

Depending on the IT architecture (mesh or star topology), the financial implications will be different. Concerning the former, i.e. mesh, new stakeholders joining would be required to set up several connections with each of the Member States using Prüm. On the other hand, a star topology would require new stakeholders to establish only one connection. Therefore, this second option is more interesting from a cost view.

In the case of Europol, EU budget needs to be allocated to the agency in order to finance the connection and cover new profiles necessary to handle the Prüm request.

6.2.3. Conclusion

It can be concluded that the inclusion of new stakeholders under the Prüm framework can bring some benefits. Particularly, as the inclusion of Europol will make biometric data from third countries accessible for Prüm searches and as Europol will provide a channel for Prüm follow-up changes via SIENA. As Europol is an EU agency, its inclusion can be more easily regulated in next-generation Prüm legal base.

As for Interpol and third countries, the access to new data is also the main benefit. However, the inclusion of these stakeholders poses some constraints, as international agreements will be needed, and the connections with these external stakeholders would be required to follow Prüm's and European data protection requirements. The study concludes that both options (third countries' and Interpol's participation in Prüm) are feasible, but are rather subject to political decisions.

Overall, one can conclude that Europol should part of the next-generation Prüm, given the clear benefits. On the contrary, the potential benefit of integrating Interpol and third countries is not as clear-cut given the constraints mentioned above. Therefore, the inclusion of these stakeholders is not a priority for the next-generation Prüm.

7. NEXT STEPS

The Advanced Technical Report has highlighted several manners to improve the operational efficiency of the Prüm process end-to-end. Every improvement topic described will not improve the Prüm Decision in the same fashion. In the final report that will be delivered to the European Commission, the preferred Single Composite Option will be presented along with a cost-benefit analysis.

This page has been left blank intentionally.

ANNEXES

Annex 1 – The current Prüm framework for fingerprints

This annex documents the current situation for the exchange of fingerprint data under Prüm in three areas:

- Principles & process – current principles for sharing fingerprint data and the process for communication between Member States;
- Quality & performance – current guidelines for image quality and the current understanding of matching accuracy;
- Exchange standards –available data exchange formats for sharing fingerprint images and adopting a new standard for Prüm.

Principles & Process

The current Prüm Decisions define a framework for sharing data based upon the Interpol Implementation of the ANSI/NIST-ITL 1-2000 standard for the exchange of biometric data (INT-I, Version 4.22b). Core to the exchange of data are the standard principles for sharing data between Member States, these are:

- Will allowing sharing of fingerprint data for criminal investigations
- Requested Member States should process and return results within 24 hours
- Member States should ensure 24/7 availability for the processing of requests
- Data exchanged between Member States must be suitable for use with an AFIS
- Data should be secured with appropriate measures (i.e. encryption)
- Member States will agree on daily search quotas

The current Prüm ICD (Interface Control Document) provides a detailed schema for how data should be structured for both search requests and responses. The following sections detail the key highlights of these definitions.

Support for Different NIST Record Types

The Prüm ICD defines the following types of NIST records that can be included in search requests

- Fingerprint Images (Greyscale), Type-4 Records are supported for the transfer of raw fingerprint images with WSQ compression.
- Minutia Data, Type-9 Records are supported for the transfer of ANSI INCITS 328 complaint feature data.
- Palm/Latent Images, Type-13 Records support the transfer of latent lifted images.

All NIST containers will contain a header record containing information related to the transaction (identifier, crime reference number, date, agency codes etc.).

As of 2019, 23 Member States have implemented fingerprint exchange systems and established connections with other Member States. None of the Member States interviewed have raised any issue with the existing exchange standard.

Finally, the current exchange format is defined using traditional file encoding and not an XML based schema more commonly adopted in modern systems.

Search Requests

All search requests sent by Member States are defined as follows.

- Requires the inclusion of transaction information (Type-1 Record) such as control number (TCN), state country codes, type of transaction (TOT) such as ten-print or latent to latent along with other header information.
- Allows the ability to set the expected number of candidates (ENC) to allow requesting Member States to define a maximum limit for returned candidate lists up to the maximum limits (see below).
- Multiple images (latent) can be sent as part of requests providing they relate to the same crime scene. Match candidates returned in responses will provide a reference to the probe image that resulted in the match. It is noted that feedback from Member States indicated that in fact, multiple latent images from the same crime scene are usually sent in separate requests.
- Allows several optional fields such as 'priority' (Type-1 Record) and 'quality' (Type-4 Record – fingerprint image). It is not known to what level, if it all, these are implemented by Member States.

Member States send requests to other states based on quotas which are agreed on a bilateral basis. These quotas are based on the ability of a country to serve all requests from connected Member States and also their national-level requests.

This overall framework and implementation of data exchanges are, by all accounts, successful and there have been no major problems raised.

It is unclear if the optional fields for Priority and Quality are being used. Suggestion from Member States is generally that they are not. It is the understanding of this study that all requests are sent with the same level of urgency.

As part of early discussion some Member States indicated that quota limits are low and requests often can be delayed due to daily quotas being hit. This can have a significant effect on law enforcement efficiency in the requesting state.

Following this, Member States were asked to indicate the impact daily quotas had on operations, the results are shown below.

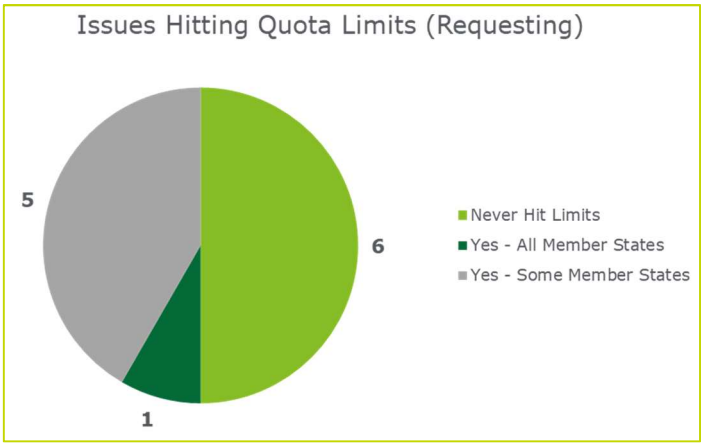


Figure 21 - Impact of daily quotas on operations

This indicates that 50% of the time Member States can hit quota limits when dealing with at least some other Member States. 50% indicate they have no problems with hitting limits however this may be indicative of their usage (number of search requests) rather than low quota limit.

Member States also noted it would be hard to increase quotas due to the impact on infrastructure (IT, networks, and system capabilities) and administration. IT bandwidth is a particular problem for Member States who have a single system that serves national requests and Member States.

Search Responses

Responses to Member States are sent as follows:

- Responses are sent even if no results are found or the request could not be processed. In the event 0 results are found, a Type-2 record is returned indicating a 'no-hit'. A status/error field (ERM) is provided in the case a request cannot be served - for example, due to a system error, image quality or quota exceeded.
- NIST containers are sent for each candidate that is generated in a particular search. Each NIST container contains information relating to the sequence of the returned candidate within the overall candidate list. This is provided through the responders' list field (RL) on the mandatory Type-2 record.
- Ten-Print to Ten-Print searches return a maximum of 1 candidate. This is because a false match against all 10 finger segments is not expected and a match is considered extremely high in confidence and beyond doubt.
- Latent to Ten-Print responses contain a maximum of 10 candidates. Given the lower quality and partial completeness of latent images being searched, the likelihood of similar candidates is higher. No threshold is defined limiting candidates lists, therefore, it is assumed the top 10 ranked candidates are returned each time however Member States may have systems configured with a minimum threshold to remove matches where scores are significantly low (obvious non-match). However this has not been quantified.
- All responses include a Type-1 header record that contains a reference to the original request identifier (TCN) along with a range of other fields for reporting errors, status etc.

This process is well defined and implemented across all currently connected Member States.

A few Member States did indicate issues with candidate list sizes being too small as often a correct match has a lower match score then false match results and/or they fall outside of the top 10 results (latent requests). This is predominantly due to varying quality of images which results in a higher level of false matches.

Member States agreed with this assessment and also that having a common understanding of quality would allow them to filter and sort results in a more efficient manner. There is currently no indication of quality candidates which could be used to assume confidence of a match. Operational improvements could be improved by inclusion of a standard quality metric in all requests/responses.

Current Prüm Quality and Performance Guidelines

Quality

The guidance provided to Member States about fingerprint image quality is loosely defined and includes only the following:

- Image quality must be "usable by an AFIS" and does not state any common minimum level of quality that should be adhered.
- Member States are responsible for checking the quality of images when a request is received and reject it if it does not meet quality requirements. It does not define any particular standards to be adhered to.
- States that images should be scanned and exchanged at 500 DPI as is commonplace most biometric exchange standards. It should be noted however many modern capture devices are capable of image acquisition at 1000 DPI offering a higher resolution of scanned images.
- Defines that fingerprint image data should be compressed using WSQ. This is considered the standard method of image compression.

It is clear that the level of image quality control for Member States is subjective and based on the type and configuration of their AFIS platforms. Each will be interpreting the guidance to a different level. And given the context of law enforcement requests such as for Prüm, is acceptable that lower quality images may be shared. However a common way to describe image quality may be useful to help users determine the confidence of matches.

It is known that some larger Member States can afford to have the image quality (ten-print) reviewed by a forensic user prior to enrolment to the AFIS. Other Member States will rely only on the AFIS quality check performed automatically during enrolment. Some systems may only perform a basic 'sequence' check (check all fingers present and in correct positions) for ten-prints with no quality assessment then being performed.

Accuracy Performance

The study has found that there is no current mechanism or data available for assessing the accuracy level of individual Member States within Prüm.

Through discussions with some Member States, it was clear that there is perceived variance in the accuracy and performance of Member State AFIS platforms. However this is anecdotal and cannot be quantified in any way.

It is expected that the following attributing factors will result in a wide range of accuracy capability across Member States:

- Age of and capability of Member State AFIS platforms range significantly with some having databases which date to the original implementation of Prüm and therefore could be up to 10 years old
- Quality of the ten-print galleries managed by Member States are based on different quality guidelines and some may even operate combined latent and ten-print galleries which possibly could impact the level of performance for some types of transactions

The challenge is that Prüm does not define any level of reporting back to a Member State to record that a match was reviewed and confirmed to be a hit or indeed that results did not contain a true hit.

Providing this type of data along with an indication of match position of true hits within the overall candidate list would be useful to allow the Member State to track hit accuracy of their systems.

This type of reporting capability was discussed with some Member States who identified that whilst this may be useful for some states, others will understand their capability based on their national level requests.

Review of Fingerprint Standards

Exchange Format - ANSI/NIST-ITL 1-2011

ANSI/NIST-ITL 1-2011 is a standard that is defined to provide interoperability between agencies who share biometric data between disparate systems such as those in law enforcement. It describes the file format and quality expectation of data being shared.

A full explanation of ANSI/NIST-ITL 1-2011 is included within section 2.2.2 of this document.

Specific to fingerprint data items this standard defines a very similar field structure to the existing Interpol implementation (INT-I, Version 4.22b) that is described in section 2.2.2.

The ANSI/NIST-ITL 1-2011 standard defines several elements that may offer opportunity within Prüm, these include:

- Vendor Feature Sets – the standards defines fields that are reserved for the transmission of vendor-specific feature sets. Sharing data using feature data (templates) allows agencies who adopt it to realize efficiencies in the way they handle and process data. For example, by transmitting feature data, requested Member States may be able to remove the need to quality assess and encode incoming images and thus reduce computational resource demand significantly. This presents an opportunity to increase the bandwidth of their AFIS systems. It should be noted that any implementation of feature data in any system exchange should always be complementary to image data which should also be included to validate a request by a forensic expert.
- Priority – the standard allows for the use of priority to indicate the processing requirements of each request. It should be noted this field is already defined as part of the existing Prüm data exchange format. This priority field can be used to allow for scheduling of incoming requests based on agreed timescales or SLA's. Within the context of Prüm, this may offer the opportunity to evolve the current process for SLA's to have a tiered approach with different priority levels being recorded within all requests. Although this does change the overall number of requests being sent or received by Member States, it could allow better management of bandwidth in systems that handle both national and Prüm based search requests.

Finally, the current standard for data transmission between Member States is based on a traditional file encoding and does not take advantage of the XML based encoding that is common in many deployments of ANSI-NIST-ITL 1-2011.

Annex 2 – The current Prüm framework for sharing DNA profiles

The current Prüm framework defines a method for sharing DNA profile data on a Prüm specific XML based message structure. This XML schema is defined by the ICD (Interface Control Document) and is also provided as a common XSD across Member States. An XSD is a file that describes an XML scheme and allows easy implementation of data models within software applications.

Prüm defines several core principles for the exchange of DNA profiles, for example:

- MS's should use an existing standard such as ESS or ISSOL for data exchange
- Data should be secured with appropriate measures (i.e. encryption)
- Matches will be communicated if the 2 DNA profiles match at 6 loci
- Matches will be communicated as near-misses if 1 allele is found to be wrong
- Communication of no matches will also be communicated
- Response time required within 24 hours and
- Member States systems must seek to be available 24/7
- Upon analysis of results, requesting Member States should follow up in step 2

This process is aligned to other data types such as fingerprint and describes the core operating agreement of all connected Member States.

A key observation is that the core principals do not include any requirement to report information. It is not clear how such requirements can actually be measured to ensure a consistent level of operation across Prüm Member States.

Concerning the standard loci set, the Prüm framework only states that ESS or ISSOL should be used for data transmission and reporting a match.

DNA Exchange Standards

The current Prüm ICD (Interface Control Document) provides a detailed schema along with XSD (as described) defining how DNA exchanges should operate. In general, requests are supported as follows:

- DNA profiles can contain up to 24 loci and 7 of which are defined based on the ESS.
- For a match to be determined, at least 6 loci of ESS must match between the compared DNA profiles however all available loci should be compared and supplied as part of the request.
- Near matches can also be provided if 1 allele of matching minimum 6 loci is found to be incorrect, this is to accommodate for any input or analysis errors
- Matches, near matches and no matches are all reported back between Member States.
- When matches are received it is the responsibility of the requesting Member State to validate the results and establish Step 2 communication via the local NCP.
- The schema used to transmit data is be XML based encoding aligned to the format in the ICD. It allows the transmission of single requests and batches of multiple DNA profiles (separate requests). The XML schema is not based on any international standard and is specific to Prüm. A Prüm XSD is provided to allow Member States to quickly adopt the standard.

Search requests sent by requesting Member States include the following:

- Header information with fields related to requesting/requested agencies, date and time and unique message identifiers.

- Up to 24 loci to match in the target Member State database, seven of which must be present in the ESS.

Search responses sent by requested Member States include the following:

- Result of the match request and flag indicating if the search was successful.
- Number of DNA profiles that have resulted in a hit along with the full DNA profiles (as available) included in the response.
- A quality value from the requested Member State database indicating confidence.
- A reference to the original request identifier.

Overall the general data exchange format for DNA profiles works as expected and none of the Member States interviewed raised any concerns. In fact, the XML based approach, supported by standard XSD, supports an easy integration approach and is compatible with the latest technologies and standard in communication (Web-service etc.).

The only area raised by the study was the fact that the DNA structure does not align to any international standard and is specific to Prüm. In addition, it is a different structure to the other biometric data items exchanged between Member States.

As outlined in section 2.2 of this document, the study recommends the adoption of ANSI/NIST-ITL 1-2011 (2015 or later) for all existing and new biometric types. The standard supports DNA as Type-18 records. The standard is intended to support the exchange of non-coding regions of DNA and therefore, for example, would not support phenotyping as no identifiable traits should be present in the DNA.

Methods for Searching

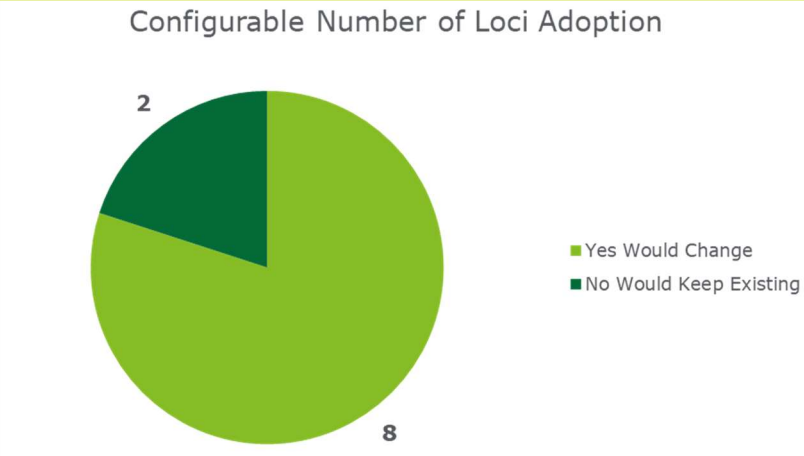
Member States and experts have raised concerns regarding the number of loci used for deciding if a match should be considered a hit.

The first opinion is that, given the ever-increasing size of national DNA databases, the set minimum of 6 loci matches increases the false-positive rate to an unmanageable level and therefore the minimum match threshold should be raised.

The second is that raising the number above this threshold will result in more misses and, given DNA matches are usually reserved for serious crimes, Member States want every possible opportunity to get a hit.

Anecdotal feedback indicates that statistically, 6 matching loci is considered 60-65% accurate. Others have stated that a matching loci level of 7 could decrease false positives by up to 20%.

When surveyed 80% of Member States responded that, if possible, they would increase the required number of matching loci. Many Member States provided significant additional reasoning for why the minimum loci should be higher. It is now considered that most Member States prefer increasing the match threshold.



Configurable Number of Loci Adoption

The number and type of loci recorded by Member States are known to vary mainly due to the following:

- Many DNA profiles are old and collected with dated/different technology (CODIS vs non-CODIS). Therefore a number of loci available is low and the Member State often has no defined way to attempt to re-analyse the DNA profiles.
- Adherence to a standard set. Other than the 7 loci required by Prüm from the ESS model, there are no defined full loci set that Member States should adhere to for recording DNA of persons and matching of stains.
- Member States may have different sizes and diversity of their national databases where 6 loci is an adequate number for their national needs. Member States who have much larger databases have a much higher level of loci stored for DNA profiles
- Member States with large human resources can handle processing of results containing higher false matches and therefore a low number of loci may be acceptable. This allows larger result sets to be further analysed in a laboratory and thus ensure the lowest possible miss rates (i.e. use low threshold and check all results). Other Member States do not have the resources required to check the number of false-positives returned with the same low loci matching threshold.

It is clear that the arguments are valid for both opinions and realistically there can be no one size fits all given that Member States technology, process, database sizes and resources vary significantly. Similar to candidate list sizes for fingerprint needing to be large enough to suit all variabilities in accuracy performance, DNA match thresholds need to be low enough to gain the same support.

The common consensus of the few Member State is that the number of loci should be increased but they agree there is no one size fits all. Therefore a way to have different agreed matching thresholds could be useful.

Annex 3 – Facial recognition, standards and technology

Automated facial recognition technology has been in development for over three decades and has seen accelerated growth in recent years with an ever-increasing level of adoption in law enforcement, public safety and intelligence.

The rise of smartphone technology and the commercial use of biometrics has driven public awareness and opinion. This combined with the increasing use of automated surveillance facial systems has rightly raised several questions on technology maturity/readiness, limitations, benefits and their impact.

This annex provides an overview of (i) common use cases of facial recognition and description of common technical components; (ii) facial image and exchange standards – a description of the international standards governing the exchange of facial images and quality restrictions; and (iii) facial recognition technology and accuracy – a detailed review of current accuracy capabilities of facial recognition technology used to determine the suitability for including facial images within Prüm exchanges

Facial Recognition Overview

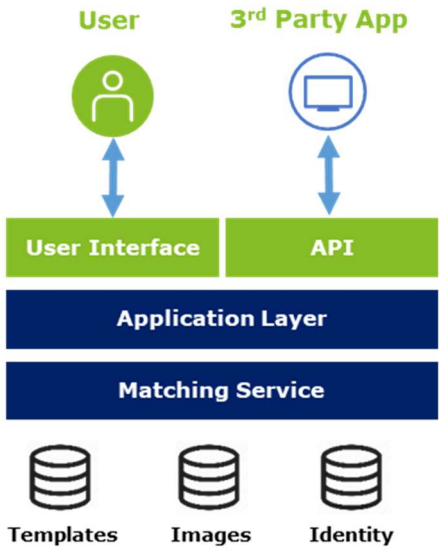
As with other biometric modalities such as fingerprint and iris, facial recognition provides three primary methods to allow the full or partial automation of searching and confirming an individual. These are:

- **Verification (1:1)** – involves the comparison of 2 probes to generate a match score which indicates the algorithms confidence level (how similar). A strict threshold is usually configured allowing the automation of hit/no-hit. Verification is usually used in highly controlled environments where a high-level of quality in both images can be assured.
- **Identification (1: N, threshold**) – involves performing a 1: N search with a high confidence threshold configured in order to identify the rank 1 hit in the target gallery.
- **Investigational (1:N, no threshold**) – often referred to as Rank, Investigational or Forensic based identification, this involves the searching of a probe template against a gallery of N previous enrolled templates with a very low threshold or none at all (T = 0). The search is configured to return the top X match candidates in order of descending match score. This rank list (candidate list) is returned to the user for adjudication.

Each approach to FR deployment is useful for different use cases depending on the requirements and required confidence of the system. The following diagram provides an example overview of where different use cases require different implementations.

Note: investigational/forensic matching is the relevant use case for Prüm.

Although facial recognition systems vary significantly in their technical architecture and implementation between vendors, they all generally have the same high level logical architectural components:



These components are described as follows:

- **Image Repository** – a database or directory of images containing raw facial images that are or will be 'enrolled' into the target facial recognition system.
- **Template Repository** – a database of proprietary templates, created during 'enrolment' of facial images into the target facial recognition system.
- **Matching Service** – hosts the vendor's algorithm and handles match requests for 1:1, 1:N etc. Systems may have multiple instances of this component depending on database sizes and bandwidth requirements.
- **Application Layer** – vendor-specific software platform and architecture that provides, for example, the core feature, request orchestration and access control etc. Modern platforms often adopt a service-based architecture which allows for highly scalable deployments.
- **User Interface** – one or more user interfaces that allow users to manage the system and use facial platform feature such as enrolment of images, image quality assessment, reporting, identification/verification and system monitoring.
- **Application Programmable Interface (API)** – provides an interface that allows 3rd parties to create custom software applications and system integrations primarily for enrolment of images and processing match requests. Modern platforms commonly provide this as a Web-service Interface.

Standards

As with other biometric modalities, several international standards are defined for the quality and exchange of facial images. The following paragraphs describe the relevant standards for the quality of facial image data and the interoperability of data between systems.

ICAO 9303 (Part 9)

ICAO 9303 provides guidelines for the deployment of Machine Readable Travel Documents (MRTD). Part 9 defines the minimum standards for supporting biometric identification and the electronic storage of data on MRTD's.

These standards ensure a minimum level of image quality to ensure they are suitable for verification by either a human actor such as border official or for use in automated facial recognition such as an airport eGate.

For facial images the standard defines the following:

- Image files are provided with 300 DPI
- Face resolution should be a minimum of 90 pixels between eyes
- Image sizes will ideally be ~640 Kb in size
- Images will be provided in JPEG or JPEG 2000 formats
- Full frontal pose
- Issuing states should define facial ornaments allowed

It should be noted this standard also defines fingerprint and iris standards however only facial is mandatory, due to the need to support manual human adjudication. It also defines a maximum retention period of 10 years (before requiring an update) in order to ensure a good level of similarity still exists between the reference image and current true representation.

Finally, the standard discusses a range of processes, technical approaches and use constraints with regards to facial recognition however these cover the operational aspect of deployment within border control and are outside the scope for this study.

The ICAO 9303 standards for facial images for use by automatic matching or human are widely adopted within the industry and have been used in border control for over 30 years.

ISO/ISE 19794-5:2005

ISO/IEC 19794 provides biometric data exchange standards that apply to a range of identity management systems that use biometrics across all industries.

The standard is intended to provide the base level of standards which are also used to define several other specific ISO/IEC biometric system standards which are outside of the scope of this study.

The core framework is covered in ISO/IEC 19794-1:2006 which describes general usage guidance on biometric data items and naming conventions. It also defines the scope of the overall standard which includes:

- Fingerprint (Images, Minutia and pattern)
- Face Images
- Iris Images
- Signature Images

ISO/IEC 19794-5:2005 provides the standards specific guidance for the capture and storage of face images to support manual human adjudication and the processing by automated facial recognition systems.

It defines the requirements of the scene, photo capture, and digital processing and file format specifications for facial images, such as:

- 1.2 to 2.5 metre distance between camera and subject

- 0 degrees pose on all angles (roll, yaw and pitch)
- Consistent lighting and control of environmental factors
- Neutral expression, open eyes, minimal occlusion etc.
- Consistent with ICAO 9303 face image specifications

For face images, the standard defines hierarchical definitions for increasing requirements in quality based on 'Basic', 'Frontal' and 'Full Frontal' face types with 'Full Frontal' defining minimum image quality requirements for both human adjudication and reliable automated facial recognition.

All face types are defined with the same face record format which is based upon the Common Biometric Exchange Formats Framework (CBEFF) that defines standards for biometric data structures and encoding. The CBEFF data structure defined in ISO/IEC 19794-5:2005 contains the following blocks:

- CBEFF Header – header information detailing the version and type
- Facial Record Header – meta-data related to images stored
- Facial Record Data – image meta-data and raw image data
- CBEFF Signature – a signature that finalises the data structure

The Facial Record Header contains information related to the enclosed record such as version number, length of data (bytes) and a number of face images it contains. The Facial Record Data contains the facial images themselves along with meta-data relating to each one. This includes:

- Facial Information – flags for gender, eye colour, hair colour and expression and pose angles.
- Feature Points – a collection of feature points such eyes, nose etc. and their X and Y coordinates within the enclosed image
- Image Information – the type of image, width, height, and source and capture device information along with a quality indicator flag.
- Image Data – the raw image data encoded as JPEG or JPEG 2000

It should be noted that the quality indicator provided in the Image Information block is provided for future use when a standardised quality assessment metric is decided.

As mentioned, the Full Frontal image type is the relevant face quality definition for images intended to be used for human and automated recognition and this type inherits from the Frontal and Basic face types.

For the Basic face type, ISO/IEC 19794-5:2005 defines the following to be adhered by all sub-types:

- JPEG or JPEG 2000 encoding must be used
- For facial header, the version, length and number of faces must be used
- For facial information, the length and number of features must be used
- For image information, the type, height and width must be used
- For image information, the face type should be set to 0 (Basic)

For Frontal face type, ISO/IEC 19794-5:2005 defines the following to be adhered by all sub-types. This is in addition to those defined for Basic type.

- Pose will be within +/- 5 degrees in all angles (roll, yaw and pitch)
- Expression data field shall be used (smile, neutral, frown etc.)
- Shoulders are square to the camera and image is "portrait style"

- Lighting must be equally distributed up/down and left/right
- Shadows should be minimal with no dark areas in eyes and face
- There should be no hot-spots produced from sources of direct light
- Eyeglasses should be worn if normal for use by the subject
- Balanced image exposure, no saturation of light/dark
- Focus and field-of-view depth should be clear for the subjects face area
- Colours should be balanced with no red-eye and white light from devices
- Image should have a 1:1 aspect ratio (pixels per inch equal for X and Y)
- 24-bit colour saturation should provide 7 bits of intensity after conversion to greyscale
- For image information, the face type should be set to 1 (Frontal)

For Full Frontal face type, ISO/IEC 19794-5:2005 defines the following to be adhered by all sub-types. This is in addition to those defined for Basic and Frontal types.

- The horizontal alignment of the nose and mouth shall be centred
- Image to head width ratio should be 7:5
- Head height should be no more than 80% of the image's height
- Width of the head should be a minimum of 180 pixels or 90 between the eyes
- For image information, the Face Type should be set to 2 (Full Frontal)

In addition to these technical aspects of the standard definitions for face images, ISO/IEC 19794-5:2005 also provides significant guidance on best practices for capture that should be followed by users to ensure compliance with the relevant minimum standards.

ANSI/NIST-ITL 1-2011 (2015 update)

ANSI/NIST-ITL 1-2011 is a standard that is defined to provide interoperability between agencies who share biometric data between disparate systems such as those in law enforcement. It describes the file format and quality expectation of data being shared.

A full explanation of ANSI/NIST-ITL 1-2011 is included within section 2.2.2 of this document.

Specific to facial images, Type-9 records allow the transmission of 1 or more example to be sent between agencies based on the ICAO 9303 and ISO/IEC 19794-5:2005 quality standards.

Accuracy

The facial recognition industry has undergone a large transformation in recent years largely due to advancements in Artificial Intelligence (AI) and Deep Learning (DL) techniques enabled through enormous amounts of reference data that is accessible to technology vendors for 'training' of their algorithms.

The National Institute for Standards and Technology (NIST) has been assessing facial recognition algorithm accuracy for over 15 years, most notably through the Face Recognition Vendors Test (FRVT) which analysis the raw matching accuracy of FR algorithms and capability of the technology in different scenarios. These tests highlight the capability of facial matching algorithms in terms of Miss Rate – how often algorithms fail to miss correct matches when configured to produce a certain likelihood of a false match being produced (threshold). This indicates both the overall performance level facial recognition technology and the comparative performance of each vendor.

FRVT is considered the 'gold-standard' of benchmarking and includes most of the top industry vendors. It was previously run in 2014 using databases of up to 1.6 million and

was recently re-run in 2018 and expanded to database sizes of 12 million. FRVT tests the raw accuracy of FR algorithms for the following use cases:

- Identification – threshold-based 1:N (high confidence, R1)
- Investigational – rank-based, non-threshold 1:N (Rank-1 and Rank-50)

For forensic law enforcement use cases such as Prüm, the most relevant test results are 'Investigational'. FRVT reports the 'Miss Rate' of each algorithm for each test case with a 'Miss' being recorded when a match, known to be in the database, does not appear in the top 50 results.

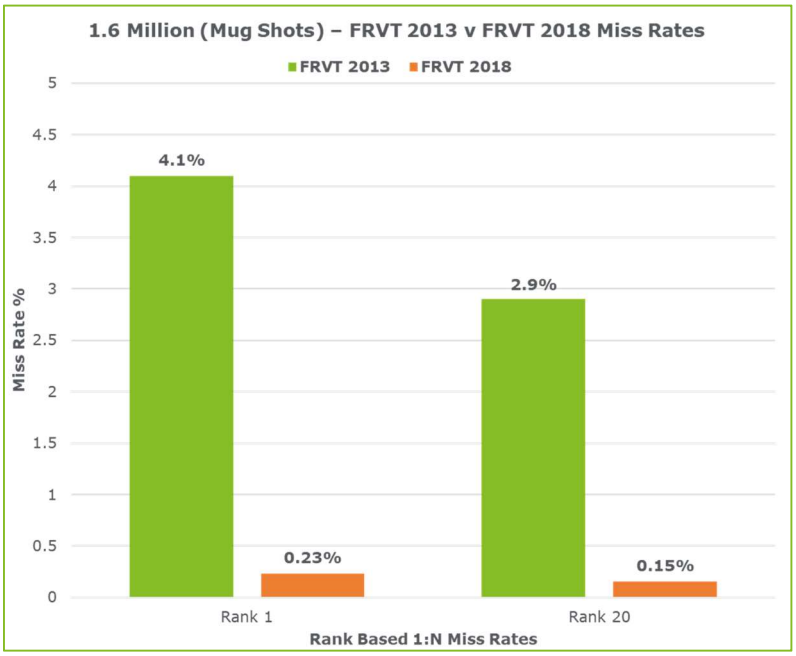
Important: the main large database tests performed by NIST are based on 'mug shot' data which roughly complies with ICAO 9303 and ISO/IEC 19794-5:2005 standards for 'Full Frontal' images. Other tests are performed with images taken in the 'wild', 'webcam' and surveillance. It is important to note that the tests only demonstrate accuracy when rigid quality controls are applied, this is noted throughout the following section.

Current Accuracy Compared to 2013 FRVT

FRVT 2013 demonstrated that for the purposes of forensic based use cases, facial recognition was at a level suitable for use on databases up to 1.6 million. Raw accuracy tests using Mug Shot (ICAO) standard facial images produced Miss Rates (FNIR) as low as 4.1% for Rank-1 based testing and 2.9% for Rank-20.

To demonstrate the general industry improvements over the 4 years between tests, NIST performed a re-run of the previous 2013 test cases using the latest 2018 algorithms.

The following chart shows the accuracy (Miss Rates) of the best performing vendor of 2014 (NEC) against the most accurate from 2018. The FRVT 2014 test used a 1.6 million Mug Shot face gallery and performed 50,000 mated searches.



1.6 Million (Mug Shots)

The following observations can be made based on these results.

- Miss Rates for Rank-1 results have decreased to 0.23% in 2018 which is equal to 115 misses from the 50,000 mated searches compared to 2,050 misses in 2014 at 4.1%.
- Miss Rates for Rank-20 results have decreased to 0.15% in 2018 which is equal to 75 misses from the 50,000 mated searches compared to 1,450 misses in 2014 at 2.9%.
- In 2018 99.77% of all matches returned the correct match in the Rank-1 position compared to only 95.9% in 2014.

It is clear that the raw accuracy improvements between top-performing vendors since 2014 is significant and that when using databases sizes of up to 1.6 million mug shot quality images, Rank-20 lists can offer a 99.85% hit rate.

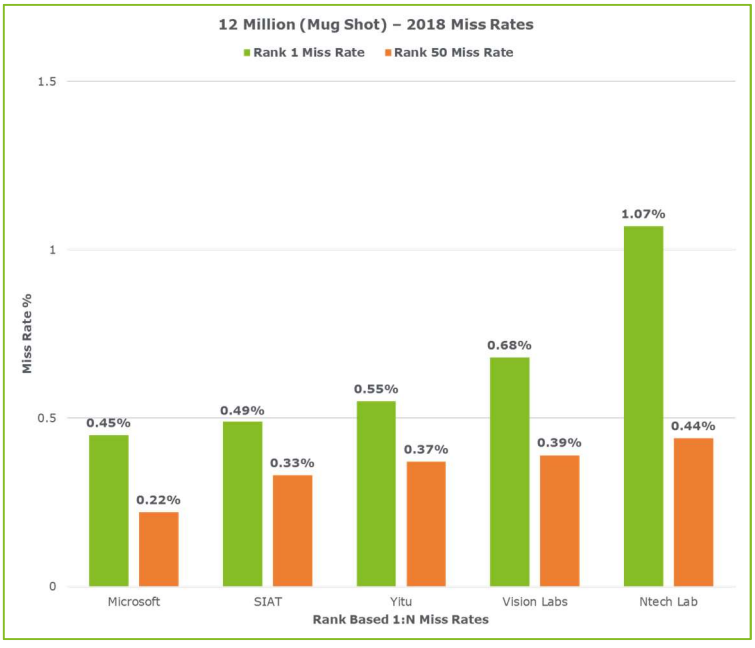
The high accuracy shown for Rank-1 indicates high confidence results and adjudication time saving as the correct match is usually in the 1st position of the results which ensures quick human adjudication time.

FRVT 2018 provided extensive testing relating to raw accuracy, the impact of age, database size and quality as described in the following sections.

Current Raw Accuracy

FRVT2018 expanded the raw accuracy test using Mug Shot data with a database as large as 12 million.

The chart below shows the raw accuracy (miss rates) of the top 5 performing vendors in FRVT 2018. It shows Rank 1 and 50 results on a gallery of 12 million images with results generated using 154,000 search requests.



12 Million (Mug Shot)

The following observations can be made based on these results.

- All algorithms achieved < 0.5% miss rate which equates to approx. 770 missed matches from ~154,000 mated requests.

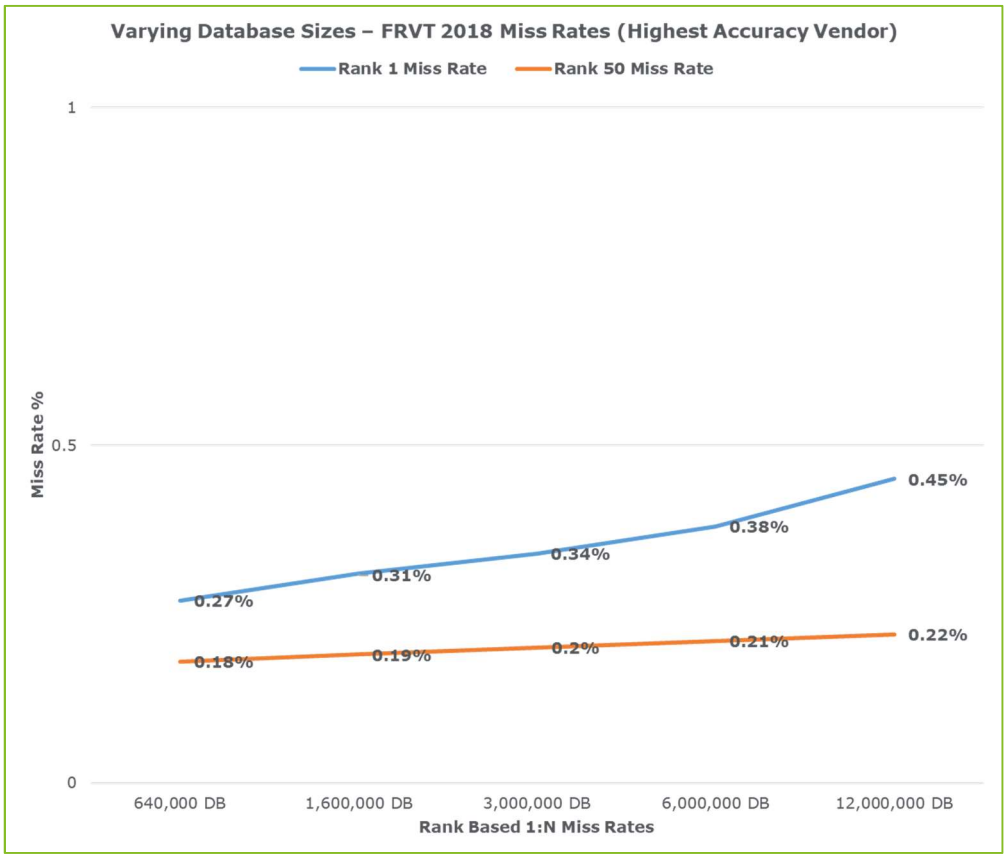
- The top vendor almost achieved the same miss rate at Rank-1 as the 5th most accurate algorithm at Rank-50.
- That the correct match usually shows in the rank 1 position, for example with the vendor with the best accuracy, 99.55% of the time and only 0.23% of the correct matches appeared in positions 2-50.

The results show that even with very large databases of law enforcement style mug shot images, very high accuracy is achieved by all of the top 5 vendors.

In particular, for Rank-50 results which is ideal for forensic use cases. Not only is it accurate but 99.55% of the time the correct match is in position 1 of the candidate list improving adjudication time for users.

Impact of Database Size

The next chart below shows the Miss Rates of the top-performing vendor in FRVT 2018 across a range of database sizes. It shows ranked results (1 and 50) on databases of 640K, 1.6M, 3M, 6M and 12M gallery records with results generated using 154,000 mated searches.



Varying Database Sizes

These results show, that for the top-performing vendor:

- Rank-50 Miss Rates are hardly effected by database size with only a 0.04% increase between the smallest and largest galleries. This is the equivalent of 20 extra misses from the 154,000 requests.

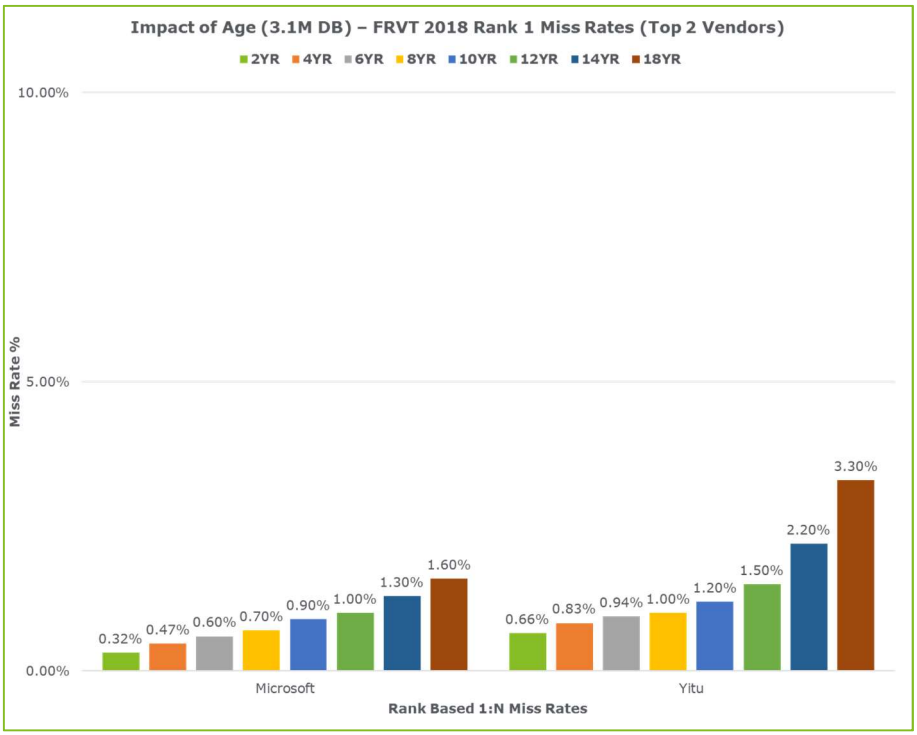
- Rank-1 Miss Rates increase slightly more but only show a 0.18% increase between the smallest and largest galleries. This is equivalent of 90 extra misses.

It should be noted that FRVT 2018 has a documented error rate where several probe images were found to be invalid. This is calculated as ~0.18% by NIST and is not corrected in the reported results. In theory, the lowest Miss Rate possible would, therefore, be 0.18% which was almost achieved in the 640K DB test and can be considered almost a 0% Miss Rate.

This shows that for forensic use cases current modern algorithms are highly resilient to database size and growth providing the gallery image quality is consistent with the minimum ICAO 9303 and 19794-5 requirements.

Impact of Age

FRVT 2018 investigated the impact of age on accuracy of matching. This is important in forensic cases where the enrolled gallery image may have been enrolled many years prior to a subsequent search being requested. The following graph shows the results of age for the 2 vendors with the overall highest accuracy.



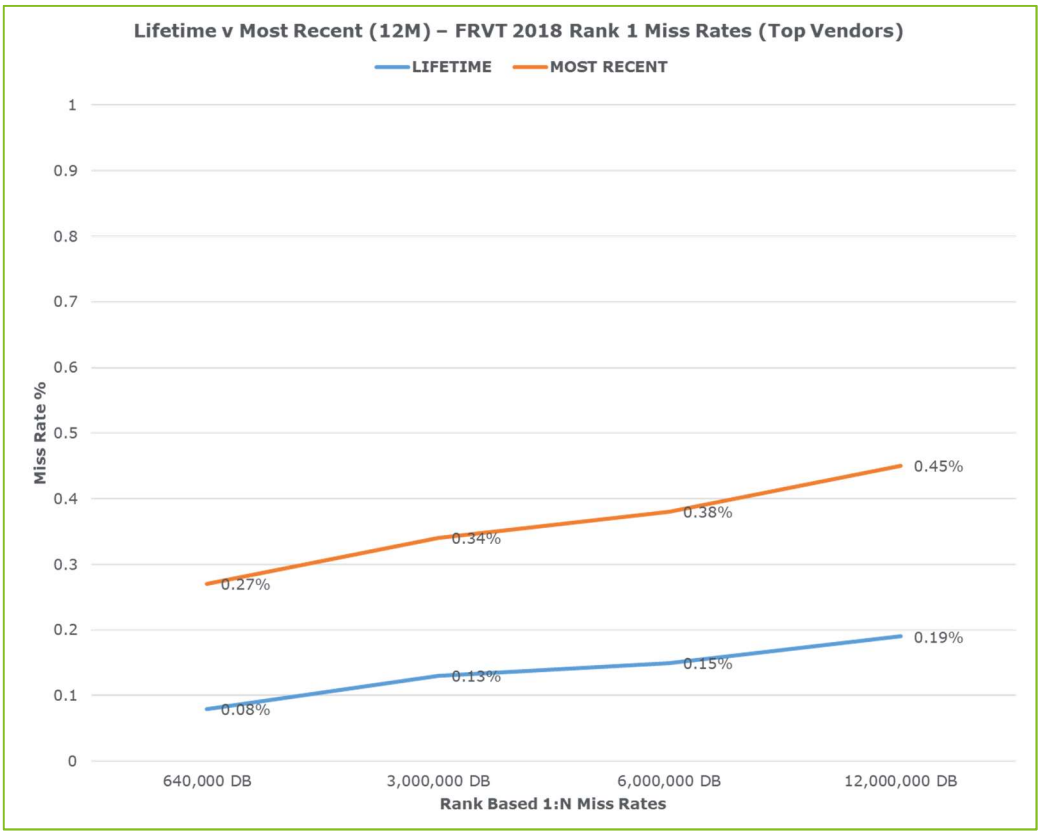
Impact of Age (3.1M DB)

The following observations can be made based on these results.

- There is a gradual increase in Miss Rates with both vendors exceeding 1% at around the 10-year point
- Miss Rates on a 3.1M DB for 18 years age difference is now lower than those seen in 2014 in the 1.6M DB primary mug shot test

This shows that top algorithms are highly resilient to age on databases up to up 3M with the most accurate achieving a 98.4% hit rate on images differing by 18 years.

In addition to this, NIST also tested the impact of having multiple (lifetime) images enrolled for a subject. It should be noted that all previously discussed results are based on 'most recent' enrolment. The following chart shows a comparison between Miss Rates 'most recent' enrolment vs all 'lifetime' enrolments.



Lifetime v Most Recent (12M)

This Miss Rates demonstrated when multiple images are enrolled for gallery subjects are significantly lower. The benefit of having multiple images of an individual in the gallery, providing they meet a minimum ICAO 9303 based standard, cannot be questioned even for large database sizes of up to 12 million (26 million images for lifetime testing).

Impact of Image Quality

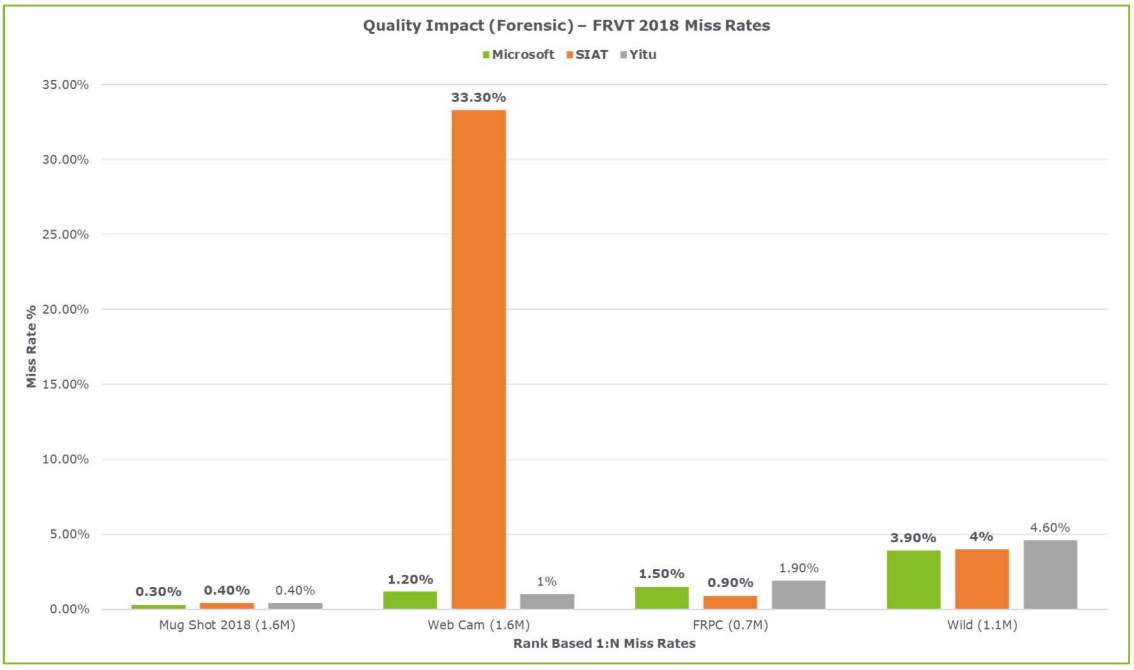
In addition to standard Mug Shot data testing and to investigate the impact of varying gallery quality on the accuracy, NIST also tested Miss Rates for several other data sets as follows:

- **Mug Shot Data** – as with other tests this is a gallery of 1.6M gallery images that conform to best practice within law enforcement and aligned to standards defined in ANSI/NIST-ITL 1-2011.
- **Web Cameras Data** – a data set of 1.6M Web Camera sourced images. All images are low in resolution at around 240x240 pixels.
- **Face Recognition Prize Challenge (FRPC) Data** – is a data set of 0.7M high-quality mug shot data aligned to ICAO (Visa Standard) tested with 79K probes of limited quality and mostly sourced from CCTV type video footage.

- **Wild Data** – a data set of 1.1M gallery unconstrained images sourced from various locations such as photojournalism. Images suffered from high variance in quality, pose angles and occlusions. Probes were also 'Wild'.

Within the context of Prüm, FRPC data set tests are highly relevant as they include Mug Shot quality enrolments and poor quality probes taken from investigational scenarios.

The following graph shows the Rank-1 miss rates of the top 3 algorithms across the data sets described above.



Quality Impact (Forensic)

It should be noted that the comparison of results across these varied data sets are not a true like-for-like comparison as each database varies in size. However, the following observations can still be made.

- As shown in previous raw accuracy test, high-quality Mug Shot data compliant to ANSI/NIST-ITL 1-2011 Type-10 record definitions provides the best overall accuracy.
- Wild images suffer the worst for accuracy given the high degree of variance in pose angles, unconstrained subjects and occlusions photo editing. The most accurate algorithm produced 3.6% more misses then Mug Shot test even with a smaller database of 1.1M.
- FPRC (high-quality gallery and low-quality probes) performs well with low Miss Rates however this is with a gallery of 0.7M.

This shows us that:

- Good Quality Gallery + Good Quality Probe = Best Accuracy
- Good Quality Gallery + Low Quality Probe = Good Accuracy
- Low Quality Gallery + Low Quality Probe = Lower Accuracy

In summary, where a gallery database is known to be good quality (ICAO type), the impact to matching accuracy is minimal when using lower quality probes (within reason).

This demonstrates the importance of protecting the quality of gallery data and ensuring that data of different quality should be isolated where necessary especially when the source of probes means that quality will inherently be lower.

It also demonstrates that the tolerance for probe quality levels need not be as strict as gallery images (providing they adhere with the above standards) to get beneficial results from matching.

These varying results in accuracy based on image quality are an important factor and most relevant to Prüm data exchanges where a large percentage of gallery images are expected to be mug shots with probes likely to range in quality (surveillance, social media images, mug shot images etc.)**.**

FRVT 2018 Review Conclusion

Overall FRVT 2018 shows that several vendors have reached a level of capability that and resilience to data size and quality than shown in previous tests and it is obviously a major milestone has been reached in the general capability of facial recognition for forensic use cases.

The following key considerations are drawn from this accuracy review and should be considered by Member States considering the implementation of facial recognition platforms.

- **Vendor Capability** – there is a broad range of accuracy across the industry in particular with the ability to handle lower quality of data. With ICAO 9303 standard mug shot images used for galleries, high accuracy can be achieved by many vendors, where image quality varies only a handful can achieve high confidence results.
- **Database Size and Growth Expectations** – with good quality mug shot databases the top vendors all show resilience to large databases, especially for forensic Rank-50 matching. Well implemented solutions can expect to achieve < 1% on databases far exceeding 20 million.
- **Gallery Image Quality** – for high accuracy results in forensic use cases, primary galleries should be kept to a high standard aligned to 19794-5, Type-10 records. Lower quality images can still play a role for forensic use however these should have separate galleries to not impact the performance of primary data sets.
- **Probe Image Quality (Cross Domain)** – for highest accuracy matching, ICAO 9303 'mug shot' images should be used. However, providing the gallery images adhere to the standard, many of the top algorithms are resilient to lower quality probes such as those taken from surveillance. Therefore, even probes of low quality can produce results of sufficient accuracy for forensic use cases, providing primary galleries are of a sufficiently high quality.
- **Rank List Size** – for the top 5 vendors the difference between Rank 1 and Rank 50 is small and therefore demonstrate high accuracy. For other vendors, there is a larger gap but still consistently good results with Rank 50.
- **Impact of Age** – 5 top algorithms performed well with < 3% miss rates at 10 years and < 4% at 18 years. Many more vendors performed well up to 10 years and then dropped off significantly to miss rates between 10-20%. However, testing of the use of lifetime images for subjects showed large increases in accuracy and should be considered.
- **Algorithm Bias** – future versions of FRVT will focus specifically on the impact of bias in gender and ethnicity. This testing will provide much-needed transparency across the industry and should be subject to review at the relevant time. This may find differences in performance for algorithms which train data on images collected in specific geographical regions.

For several vendors, facial recognition algorithm accuracy and ability to scale are such that they could be highly effective if added to Prüm, providing a certain quality and design considerations were adhered to. Further to this, given the accelerated rate of improvements shown in the last four years, capabilities are expected to increase more over time.

Within the context of Prüm, it is important to note that Member States with existing facial recognition technology may not observe this same level of performance. This would be due to not having access to their FR vendor's latest algorithms and/or having quality control measures which are not aligned to the findings of the FRVT report. These Member States therefore would need to consider their technology and operational processes in order to achieve the performance indicated in this study.

Annex 4 – Database custodian and NCP per country

Country	Database custodian (1st step)	NCP for the follow-up information exchange procedure (2nd step)
Austria	General Directorate for the Public Security - Criminal Intelligence Service	Federal Ministry of Interior - Criminal Intelligence Service
Belgium	**For DNA:** National Institute for Criminalistics and Criminology **For FP:** Federal Police – Belgium Judicial Police – Forensic Directorate Department for Judicial Identification	**For DNA:** Federal Public Prosecutor's Office **For FP:** Federal Police
Bulgaria	Research Institute of Forensic Sciences	Ministry of Interior, International Operational Cooperation Directorate – Prüm and Swedish Initiative Unit
Croatia	Ministry of Interior - General Police Directorate - Forensic Science Centre 'Ivan Vučetić' - Department of Biology and Fibers	Ministry of Interior - General Police Directorate - International Police Cooperation Department (SPOC)
Cyprus	**For DNA:** Molecular Genetics Dept. B & Laboratory of Forensic Genetics - The Cyprus Institute of Neurology & Genetics **For FP:** Ministry of Justice and Public Order - Cyprus Police Headquarters - Fingerprints Department of Criminalistics Services	Ministry of Justice and Public Order - Cyprus Police Headquarters - European Union & International Police Cooperation Directorate
Czech republic	Institute of Criminalistics Prague	Police Presidium of the Czech Republic - International Police Cooperation Division
Denmark	Danish National Police - Police Operations Branch - Communication Centre	Danish National Police - Police Operations Branch - Communication Centre
Estonia	Estonian Forensic Science Institute	Police and Border Guard Board - Intelligence Management and Investigation Department - Law Enforcement Intelligence Management Bureau (SPOC)
Finland	National Bureau of Investigation - Forensic Laboratory	National Bureau of Investigation - Communications Centre
France	DCPJ/SDPTS/SCIJ/FNAEG	SCCOPOL : Unité de coordination et d'assistance Prüm (UCAP) - DCPJ/DRI/SCCOPOL
Germany	Bundeskriminalamt	Bundeskriminalamt

Greece	Hellenic Police - Forensic Science Division For DNA: Subdivision of Biological and Biochemical Examinations and Analyses - National DNA Database Section For FP: Crime Scene Investigation Department	Hellenic Police Headquarters (HQ) - International Police Cooperation Division / SIRENE Bureau
Hungary	Hungarian Institute for Forensic Sciences - Department of Genetics	International Law Enforcement Co-operation Centre
Latvia	State Police - Forensic Service Department	State Police - International Cooperation Bureau - Central Criminal Police Department
Lithuania	Lithuanian Police Forensic Science Centre **For DNA:** Identification Department - Biological Analysis Division **For FP:** Forensic Registration Subdivision of the Identification Department Dactyloscopic Analysis Division	Lithuanian Criminal Police Bureau - International Liaison Office
Luxembourg	Service de Police Judiciaire - Direction	**For DNA:** Parquet Général du Luxembourg - Cité Judiciaire – Bâtiment CR **For FP:** Service de Police Judiciaire - Direction
Malta	Forensic Science Laboratory (FSL) - Police General Headquarters	International Relations Unit - Police General Headquarters
Netherlands	**For DNA:** Netherlands Forensic Institute (NFI) - Unit DNA database **For FP:** Netherlands Police - Central Intelligence Services - National Forensic Service Centre - Fingerprint department	**For DNA:** Netherlands Prosecutor Service - National International Legal Request Centre (LIRC)) **For FP:** Netherlands Police - Central Division - Central Intelligence Services
Poland	Central Forensic Laboratory of the Police (CFLP) **For DNA:** Biology Department **For FP:** Fingerprint Examination Department	National Police Headquarter - International Police Cooperation Bureau
Portugal	**For DNA:** National Institute of Legal Medicine **For FP:** Forensic Science Laboratory of the Criminal Police (Polícia Judiciária)	**For DNA:** National Institute of Legal Medicine **For FP:** Interpol National Central Bureau, Europol National Unit and SIRENE Office
Romania	Ministry of Internal Affairs - General Inspectorate of the Romanian Police - National Forensic Science Institute	Ministry of Internal Affairs - General Inspectorate of the Romanian Police - International Police Cooperation Centre
Slovakia	Ministry of Interior of the Slovak Republic, Presidium of the Police Force, Institute of Forensic Science **For DNA:** Biology and Genetic Analyse Department **For FP:** Department of fingerprint identification	Ministry of Interior of the Slovak Republic, Presidium of the Police Force, International Police Cooperation Bureau, SPOC (Single Point of Contact)

Slovenia	Ministry of the Interior - Police, General Police Directorate - National Forensic Lab	General Police Directorate – Criminal Police Directorate – Division for International Police Cooperation
Spain	Operator NSIS	División de Cooperación Internacional - Oficina SIRENE or Centro Nacional de Comunicaciones Internacionales
Sweden	National Forensic Centre - NFC	The Swedish Police Authority - National Operations Department - International Division

This page has been left blank intentionally.

Annex 5 – Firearm-related databases per country

Firearm-related databases in Member States, and management and access rights of law enforcement authorities

Country	Managed and directly accessible	Not managed and directly accessible	Not managed and not directly accessible
Already exchanging Prüm data			
Austria	Firearms		
Belgium		Firearms	
Bulgaria	Firearms tracing		
Croatia	Stolen/missing firearms	Firearms register	
Cyprus	Firearms		
Czech Republic	Firearms	Firearms tracing	
Denmark	Firearms tracing (IBIS), firearms		
Estonia	Firearms licences, firearms classification		
Finland	Firearms licences		
France		Firearms owners, persons prohibited from purchase or possession	
Germany	Alerts concerning arms and explosives		
Hungary	Firearms register		
Latvia			
Lithuania	Wanted weapons register	Weapons in civil circulation register	
Luxembourg		Firearms register	
Malta	Weapons licences, arms/weapons		
Netherlands	Holders of legal firearms permits, shooting incidents and tracings (IBIS)		

Poland	**Lost firearms, issued firearms licences**		
Portugal	Weapons, firearms registration data, explosives, ammunition		
Romania	Arms, arm bearers, operations with arms and ammunition, explosives		
Slovakia	Firearms	Firearms tracing	
Slovenia		Firearms tracing	
Spain	Firearms identification, firearms owners		
Sweden	Firearms tracing, firearms		
Not yet exchanging Prüm data			
Greece	Weapons stolen, lost, misappropriated or found, used on national territory		
Iceland			
Ireland	Firearms register		
Italy	Firearms		
Liechtenstein			
Norway	Firearms licences		
Switzerland			Firearms data and firearms owners
United Kingdom	Firearms tracing, firearms		

Source: Manual for Law Enforcement Information Exchange (January 2018), a document from the Presidency of the Council of the European Union to DAPIX (Working Party on Information Exchange and Data Protection

Annex 6 – Preliminary list of improvement opportunities

Please refer to the Intermediate Report delivered in March 2019 for additional information on the preliminary list of improvement opportunities.

Improving existing data exchanges regarding DNA and fingerprints

General

Opportunity 1.1 – Adapting the purpose of Prüm

Opportunity 1.2 – Sharing database content description

Opportunity 1.3 – Implementing evolving technical requirements

DNA

Opportunity 1.4 – Increasing the current standard of six loci for DNA comparisons

Opportunity 1.5 – Using the likelihood ratio for confirming a match

Opportunity 1.6 - Introducing targeted familiar searching techniques

Opportunity 1.7 – Combining common loci, likelihood ratio, familiar searching and high chromosome markers

Opportunity 1.8 – Defining search schedules per Member States

Fingerprints

Opportunity 1.9 – Algorithm and matching procedures benchmark assessment

Opportunity 1.10 – Decrease, increase or eliminate daily search quotas

Opportunity 1.11 – Pre-select highly probable candidates

VRD

Opportunity 1.12 - Expanding EUCARIS searches for the purpose of investigating traffic offenses

Opportunity 1.13 - Including an empty result message when there is no response

Opportunity 1.14 – Adding new search functionalities

Opportunity 1.15 - Including new mandatory items in EUCARIS data set

Streamlining and improving the efficiency of the match follow-up procedure for DNA and fingerprints

Opportunity 2.1 - Setting a Universal Message Format (UMF 3)

Opportunity 2.2 - Defining a preferred communication channel

Opportunity 2.3 – Fully automate the Prüm process

Opportunity 2.4 - Semi-automate the follow-up procedure option#1

Opportunity 2.5 - Semi-automate the follow-up procedure option#2

Opportunity 2.6 – Automate the follow-up procedure for high-quality matches

Opportunity 2.7 - Introducing an urgency degree label

Opportunity 2.8 - Creating training opportunities

Opportunity 2.9 - Providing further technical support

Opportunity 2.10 – Supplementary intelligence

New data categories in Prüm

Opportunity 3.1 - Facial images

Opportunity 3.2 - Driver licences

Opportunity 3.3 - Firearms & ballistics

Opportunity 3.4 – Tattoos

Opportunity 3.5 - Iris & voice

Opportunity 3.6 – EPRIS-ADEP – biographic data

New architecture of Prüm information exchanges

Opportunity 4.1 - Simple Messaging router

Opportunity 4.2 - Simple Messaging router with harmonized data format

Opportunity 4.3 - Central router with a Shared Biometric Matching Service

Opportunity 4.4 - A common central European database

Opportunity 4.5 – Update of the security technical requirements

Opportunity 4.6 – Security accreditation

Linking the Prüm network to central EU information systems and interoperability solutions in the area of Justice and Home Affairs

Opportunity 5.1 - Common Identity Repository

Opportunity 5.2 - Shared Biometric Matching Service

Opportunity 5.3 - EUROPOL/INTERPOL/3RD COUNTRIES

Annex 7 - List of stakeholder interviews

#	Stakeholder	Entity	Interviewees	Type	Date	Place	Topics discussed
1	**General Secretariat of the European Council**	**General Secretariat of the European Council**	**Georg Biekoetter and team**	Introductory interview	17-01-2019	Brussels	Assessment of Prüm's current state. Brainstorming on improvement opportunities and priorities for NG Prüm
2	**Austria**	**Federal Ministry of the Interior**	**Dr. Reinhard Schmid**	Introductory interview	23-01-2019	Phone interview	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
3	**Finland**	**National Police Board**	**Anssi Kangas and team**	Introductory interview	29-01-2019	Helsinki	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
4	**Sweden**	**Swedish Police Authority**	**Kristoffer Müller and team**	Introductory interview	30-01-2019	Stockholm	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
5	**France**	**Ministry of the Interior**	**Muriel Sylvan and team**	Introductory interview	31-01-2019	Paris	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
6	**Czech Republic**	**Institute of Criminalistics**	**Pavel Kolár and team**	Introductory interview	04-02-2019	Prague	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm

7	**eu-LISA**	**eu-LISA**	**Stephan Brandes, Ana Maria Ruginis Andrei and team**	Introductory interview	05-02-2019	Strasbourg	Assessment of Prüm's current state. Brainstorming on improvement opportunities and priorities for NG Prüm
8	**United Kingdom**	**Metro Police**	**Shazia Khan and Hillary Brown**	Introductory interview	06-02-2019	Phone interview	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
9	**Europol**	**Europol**	**Krzysztof Klebek and team**	Introductory interview	07-02-2019	The Hague	Assessment of Prüm's current state. Brainstorming on improvement opportunities and priorities for NG Prüm
10	**Netherlands**	**Ministry of Justice and Security**	**Dominique Lenssen and team**	Introductory interview	08-02-2019	The Hague	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
11	**Romania**	**Permanent Representation of Romania to the EU**	**Cristian Manea and team**	Introductory interview	13-02-2019	Bucharest	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
12	**Germany**	**Bundeskriminalamt**	**Sandro Dicker, Robert Lorenz and team**	Introductory interview	14-02-2019	Frankfurt	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
13	**Latvia**	**Latvian State Police**	**Aleksandra Tukisa and team**	Introductory interview	18-02-2019	Phone interview	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm

14	**Belgium**	**Belgian Federal Police**	**Marc Vervaenen and team**	Introductory interview	20-02-2019	Brussels	Assessment of Prüm use and satisfaction. Brainstorming on improvement opportunities and priorities for NG Prüm
15	**Netherlands Forensic Institute**	**Netherlands Forensic Institute**	**Dr. Meuwly**	Expert consultation	04-04-2019	Phone interview	Assessment of the feasibility of introducing in Prüm biometric-related improvements presented at the first workshop
16	**EUCARIS**	**EUCARIS Secretariat and EUCARIS Operations**	**Idske Dijkstra and Herman Grooters**	Expert consultation	23-04-2019	Phone interview	Assessment of the feasibility of introducing in Prüm VRD-related improvements presented at the first workshop
17	**ENFSI**	**ENFSI R&D**	**Ülar Lanno and Ivar Prits**	Expert consultation	26-04-2019	Phone interview	Assessment of the feasibility of introducing in Prüm biometric-related improvements presented at the first workshop
18	**eu-LISA**	**eu-LISA**	**Sandra Nunes and team**	Expert consultation	29-04-2019	Phone interview	Assessment of the feasibility of introducing new architecture and interoperability solutions in Prüm
19	**EPRIS ADEP project team**	**EPRIS ADEP project team**	**Sandro Dicker**	Expert consultation	07-05-2019	Phone interview	Assessment of the feasibility of introducing EPRIS ADEP data in Prüm exchanges

20	**Fingerprint Focus Group**	**Fingerprint Focus Group**	**Reinhard Schmid and team**	Expert consultation	10-05-2019	Phone interview	Assessment of the feasibility of improving Prüm fingerprint-related improvement opportunities and choosing match follow-up communication channel
21	**ENFSI**	**ENFSI Fingerprint Working Group**	**Aldo Mattei**	Expert consultation	14-05-2019	Phone interview	Assessment of the feasibility of introducing in Prüm fingerprint-related improvements presented at the first workshop
22	**Council Legal Service**	**Council Legal Service**	**Melpo-Menie Josephides**	Expert consultation	16-05-2019	Phone interview	Assessment of the feasibility of extending Prüm's use cases and available administrative data
24	**Portugal**	**National contact point**	**Luis Pebre and team**	Expert consultation	16-05-2019	Lisbon	Assessment of Prüm use and identification of DNA and Firearms experts
25	**UMF**	**Europol UMF representative**	**Bogdan-Victor Catrina**	Expert consultation	17-05-2019	Phone interview	Assessment of the feasibility of implementing UMF format in Prüm exchanges
26	**ENFSI**	**ENFSI DNA Working Group**	**Sander Kneppers and team**	Expert consultation	20-05-2019	Phone interview	Assessment of the feasibility of introducing in Prüm DNA-related improvements presented at the first workshop

27	**eu-LISA**	**eu-LISA**	**Ana Maria Ruginis Andreo and team**	Expert consultation	20-05-2019	Phone interview	Assessment of the feasibility of introducing new architecture and interoperability solutions in Prüm
28	**General Secretariat of the European Council**	**General Secretariat of the European Council**	**Georg Bieköetter and team**	Expert consultation	22-05-2019	Phone interview	Assessment of the feasibility of improving Prüm's technical standards and match follow-up process automation
29	**Portugal**	**Public Safety Police - Firearms department**	**Pedro Moura**	Expert consultation	24-05-2019	Lisbon	Assessment of the feasibility of introducing firearms & ballistics data exchanges in Prüm
30	**Portugal**	**National Institute of Legal Medicine**	**Ana Margarida Bento and Pedro Brito**	Expert consultation	24-05-2019	Coimbra	Assessment of the feasibility of introducing in Prüm DNA-related improvements presented at the first workshop
31	**DNA Expert Group**	**Bundeskriminalamt**	**Sandro Dicker and team**	Expert consultation	03-06-2019	Phone interview	Assessment of the feasibility of improving Prüm's technical standards and choosing the match follow-up communication channel
32	**Switzerland**	**Federal Department of Justice and Police**	**Roman Blaser and team**	Expert consultation	03-06-2019	Phone interview	Assessment of the feasibility of introducing facial image data exchanges in Prüm
33	**DG HOME**	**DG HOME**	**Richard Rinkens**	Expert consultation	04-06-2019	Brussels	Assessment of the feasibility of automating Prüm's match follow-up process automation, architecture and interoperability

34	**Council Legal Service**	**Council Legal Service**	**Melpo-Menie Josephides**	Expert consultation	11-06-2019	Phone interview	Assessment of the legal feasibility of all improvement opportunities of the study
35	**DG Home**	**Organised crime – Firearms group (Unit D3)**	**Emmanuel Vallens**	Expert consultation	18-06-2019	Phone interview	Assessment of the feasibility of introducing firearms data exchanges in Prüm
36	**EUCARIS**	**EUCARIS Operations**	**Herman Grooters**	Expert consultation	19-06-2019	Phone interview	Assessment of the feasibility of introducing driving licences data exchanges and new EUCARIS features in Prüm

This page has been left blank intentionally.

Annex 8 – References

Council of the European Union, Council Decisions 2008/615/JHA, June 2008

Council of the European Union, Council Decisions 2008/616/JHA, June 2008

Council of the European Union, Council Framework Decision 2009/905/JHA, November 2009

Council of the European Union, Council Framework Decision 2006/960/JHA, December 2006

European Parliament and Council, Data Protection Police Directive 2016/680, April 2016

European Parliament and Council, General Data Protection Regulation 2016/679, April 2016

LIBE Committee by Dr Victor TOOM, Marie Curie Research Fellow, Cross-border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision, June 2018

DG JRC, Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II), 2015

European Commission, High Level Expert Group in Information Systems and Interoperability, May 2017

European Commission, Proposal for a Regulation on establishing a framework for interoperability between EU information systems, December 2017

European Parliament and Council, Establishing a framework for interoperability between EU information systems, June 2018

eu-LISA, Future Architecture for Interoperable IT Systems at eu-LISA, Impact Assessment and Migration and Integration Plan, October 2017

eu-LISA, Shared Biometric Matching Service (sBMS), April 2018

University of Leiden, The light's at the end of the funnel, November 2015

European Commission, Fingermark and face automatic recognition technologies for their implementation in the Schengen Information System (SIS), June 2018

UKPFE, United Kingdom Prüm Fingerprint Evaluation Project, 2012

Council of the European Union, Manual on Law Enforcement Information Exchange, 2016

Council of the European Union, Manual on Law Enforcement Information Exchange, 2018

DAPIX, DAPIX Summary of the discussions, December 2018

DAPIX, DAPIX Summary of the discussions, November 2018

DAPIX, DAPIX Summary of the discussions, July 2018

DAPIX, DAPIX Summary of the discussions, September 2011

DAPIX, Statistics and reports on automated data exchange, March 2016

DAPIX, Statistics and reports on automated data exchange, February 2017

DAPIX, Prüm statistics and reports, May 2016

DAPIX, Prüm statistics and reports, July 2016

DAPIX, Prüm statistics and reports, May 2017

DAPIX, Permanent Representation of Portugal, March 2013

DAPIX, Next-generation Prüm Discussion paper on developing Prüm, November 2018

DAPIX, Next-generation Prüm Discussion paper on developing Prüm, October 2018

DAPIX, Next-generation Prüm Discussion paper on developing Prüm, September 2018

DAPIX, Implementation of the provisions on information exchange of the Prüm, November 2018

DAPIX, Implementation of the provisions on information exchange of the Prüm, October 2018

DAPIX, Implementation of the provisions on information exchange of the Prüm, October 2012

DAPIX, Implementation of the provisions on information exchange of the Prüm, May 2016

DAPIX, Implementation of the provisions on information exchange of the Prüm, April 2018

European Parliament, Stepping up of cross-border cooperation, April 2017

European Network of Forensic Science Institutes (ENFSI), Evaluation of new commercial STR multiplexes that include the European Standard Set (ESS) of markers, May 2012

Principal Forensic Services - Dr Gillian Tully & Dr Susan Pope, Statistical study on Prüm, September 2014

Kammi Schmeer, Stakeholder Analysis Guidelines

Future Group, First meeting of the Future Group, May 2007

DAPIX, Roadmap to enhance information exchange and information management, October 2017

Filipe Santos and Helena Machado, Patterns of exchange DNA data in the EU, April 2017

Filipe Santos, Overview of the implementation of the Prüm Decisions, November 2016

eu-LISA, IT in the service of a more open and secure Europe, 2014

DAPIX, Renewed Information Management Strategy (IMS), October 2016

eu-LISA, eu-LISA Strategy 2018-2022, 2017

"Europol, Europol's contribution on its short-term activities in the implementation of the Roadmap on information exchange and interoperability, July 2016"

UK - Home Office, Prüm Business and Implementation Case, November 2015

European Commission, TESTA Next-generation, June 2018

German delegation, Universal Message Format (UMF) 3, March 2016

Europol, UMF Europol brochure

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

DR-02-20-311-EN-N

Publications Office
of the European Union

doi: 10.2837/1710
ISBN 978-92-76-18456-0