STUDY

For the LIBE committee

European Parliament

Interoperability of Justice and Home Affairs Information Systems

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Policy Department for Citizens' Rights and Constitutional Affairs

Directorate General for Internal Policies of the Union

PE 604.947- April 2018

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Interoperability of Justice and Home Affairs Information Systems

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, at the request of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), primarily assesses the Commission's December 2017 proposals for a Regulation on establishing a framework for interoperability between EU Justice and Home Affairs information systems. The study first analyses the relationships between the information systems in the current and proposed implementation before assessing the key elements of the Commission's proposals, including the concept of interoperability used, the problem definition and objectives and the proposed solutions, as well as the implementation, fundamental rights and data security implications.

PE604.947 EN

ABOUT THE PUBLICATION

This study was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and was commissioned, overseen and published by the Policy Department for Citizens' Rights and Constitutional Affairs.
Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.
To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to:
poldep-citizens@ep.europa.eu

Research Administrator Responsible

Dr Udo Bux
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@ep.europa.eu

Editorial Assistant

Monika Laura LAZARUK

AUTHORS

Mirja GUTHEIL, Optimity Advisors
Quentin LIGER, Optimity Advisors
James EAGER, Optimity Advisors
Yemi OVIOSU, Optimity Advisors
Daniel BOGDANOVIC, Optimity Advisors

With the support of Professor Katrin NYMAN-METCALF, Estonian e-Governance Academy and Tallinn University of Technology; Dr Niovi VAVOULA, Queen Mary, University of London; Jeremy COLLINS, Optimity Advisors; and Carolin Möller, Optimity Advisors.

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in April 2018

This document is available on the Internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
BMS	Biometric Matching System
C-SIS II	Central Second-Generation Schengen Information System
CEAS	Common European Asylum System
CIR	Common Identity Repository
CJEU	Court of Justice of the European Union
CRRS	Central Repository for Reporting and Statistics
CS-VIS	Central System VIS
CTC	Counter-Terrorism Centre
DNA	Deoxyribonucleic Acid
DPA	Data Protection Authority
EASO	European Asylum Support Office
ECRIS	European Criminal Records Information System
ECRIS-TCN	European Criminal Records Information System Third Country Nationals
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
eIDAS	Electronic Identification Authentication and trust Services
EIF	European Interoperability Framework
EP	European Parliament
ESP	European Search Portal
ESTA	Electronic System for Travel Authorization
ETIAS	European Travel Information and Authorisation System
eu-LISA	The European Agency for the operational management of large-scale IT Systems in the area of freedom, security and justice
Eurodac	European Dactyloscopy database

FRA	European Union Agency for Fundamental Rights
FRONTEX	European Border and Coast Guard Agency
HLEG	High-Level Expert Group
ICT	Information Communication Technology
JHA	Justice and Home Affairs
LEA	Law Enforcement Access
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MID	Multiple-Identity Detector
N-SIS II	National Interface Second-Generation Schengen Information System
NI-VIS	National Interface VIS
NUI	National Uniform Interface
Prüm	Prüm Convention – Schengen III Agreement
sBMS	shared Biometric Matching System
SIRENE	Supplementary Information Request at the National Entries
SIS II	Second-Generation Schengen Information System
SLTD	Stolen and Lost Travel Documents
TCN	Third-Country National
TDAWN	Travel Documents Associated with Notices
UMF	Universal Message Format
VIS	Visa Information System

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Interoperability of JHA information systems: History and context

Discussions on the interoperability of EU Justice and Home Affairs (JHA)[1] information systems began in the wake of 9/11[2] and continued through the 2000s. Primarily driven by terrorist attacks on EU territory – the 2004 Madrid bombings and the 2005 London bombings – these discussions resulted in the 2005 Commission Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs.[3] However, criticism from prominent stakeholders, such as the European Data Protection Supervisor (EDPS), ensured these discussions did not progress. The criticism was concentrated on two issues: the **definition** of interoperability; and the consideration of the potential personal **data protection implications.**[4]

In the following decade, limited activity was undertaken with regard to interoperability, although significant developments took place in relation to the EU JHA information systems environment, including, for example, the establishment of VIS[5], SIS II[6] and ECRIS.[7]

Following further terrorist attacks on EU soil – namely, the 2015 Paris attacks and the March 2016 Brussels attacks – discussions on interoperability received fresh impetus. As a result, 2015–2017 saw significant political weight placed behind the drive to implement the interoperability of JHA information systems through the publication of, *inter alia*: multiple Council Conclusions[8]; a Council Roadmap[9]; and a 2016 Joint Statement of EU Ministers for Justice and Home Affairs[10].

Building on this focus and the calls of the Council, the Commission published its 2016 Communication on stronger and smarter information systems for borders and security.[11] This Communication presented 'four dimensions'[12] of interoperability and established a High-Level Expert Group (HLEG) on Information Systems and Interoperability to explore the legal, technical and operational aspects of these four dimensions. In June 2017, following the final report of the HLEG, the **Commission announced its intention to present a legislative proposal on interoperability.**[13]

On 12 December 2017, the European Commission published its proposals for a Regulation on establishing a framework for interoperability between EU information systems.[14] The proposals, produced as two separate but very closely related legislative proposals, aim to implement four main solutions.

---

1 Due to its frequent use in the Commission's proposals, the term 'Justice and Home Affairs' (JHA) has been used instead of the Area of Freedom, Security and Justice (AFSJ).

2 Council of the European Union, Document 13176/01 (24.10.2001).

3 COM(2005) 597 final (24.11.2005).

4 EDPS (2006) Comments on the Communication of the Commission on interoperability of European databases.

5 Council Decision 2004/512/EC.

6 Regulation (EC) No 1987/2006 (Border control cooperation); Council Decision 2007/533/JHA (Law enforcement cooperation); Regulation (EC) No 1986/2006 (Cooperation on vehicle registration).

7 Council Framework Decision 2009/315/JHA; and Council Decision 2009/316/JHA.

8 Council of the European Union, Document EUCO 28/15 (18.12.2015); Council of the European Union, Document EUCO 34/16 (15.12.2016).

9 Council of the European Union, Document 9368/1/16 (06.06.2016).

10 Council of the European Union, Document 158/16 (24.03.2016).

11 COM(2016) 205 final (06.04.2016).

12 Ibid, p. 14.

13 COM(2017) 261 final (16.5.2017).

14 Proposals for a Regulation on establishing a framework for interoperability between EU information systems: COM(2017) 794 final, Brussels, 12.12.2017; and COM(2017) 793 final, Strasbourg, 12.12.2017.

- The **European Search Portal (ESP)** would enable the simultaneous query of multiple JHA information systems using (both biographical and biometric) identity data (Central-SIS, Eurodac, VIS, the future EES, and the proposed ETIAS and ECRIS-TCN systems, as well as the relevant Interpol systems and Europol data) (Chapter II).
- The **shared Biometric Matching Service (sBMS)** would enable the querying and comparison of biometric data (both fingerprint and facial images) across EU information systems by generating and storing mathematical representations of the biometric data (SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN) (Chapter III).
- The **Central Identity Repository (CIR)** would be a shared component for storing the biographical and biometric identity data of third-country nationals, spanning Eurodac, VIS, the future EES, and the proposed ETIAS and ECRIS-TCN systems (Chapter IV).
- The **multiple-identity detector (MID)** would check whether queried identity data exists in more than one system and allow a mechanism for investigating and verifying the linked identity data (data held in the CIR as well as SIS) (Chapter V).

In addition, the proposed Regulations aim to implement a:

- **Two-step process for law enforcement access to non-law enforcement information systems** for the purpose of prevention, investigation, detection or prosecution of terrorism and other serious criminal offences (Article 22):
  - 'Hit-flag functionality' of the CIR would allow law enforcement authorities to determine which information systems hold a record on an individual, without visibility of the underlying data.
  - Subsequently, the law enforcement authority would have the opportunity to individually request access to each system that contains data in line with the existing rules and procedures, as established in the Regulations of each information system.
- **Central repository for reporting and statistics (CRRS):** this repository would enable the creation and sharing of reports with anonymised statistical data from across the information systems for policy, operational and data quality purposes (Article 39).
- **Universal Message Format (UMF):** the UMF would be a standardised technical language to describe and link data elements, thereby allowing easier integration and interoperability between EU and Member State information systems (Article 38).

The proposals also introduce the concept of **automated data quality control mechanisms** (Article 37). Such mechanisms include the implementation of automatic validation rules when inputting data and the establishment of common data quality indicators and minimum quality standards. Although Article 37 establishes that these will be developed and details the related roles and responsibilities, the core of these mechanisms is still to be developed.

Current and proposed JHA information systems

With regard to the current implementation, it is key to note that **each of the JHA information systems was established – or has been proposed – for a specific purpose** within a particular institutional context. Though the primary purposes of each system remain distinct, there are clear trends with regard to:

i. The **broadening of system scope over time**. For instance, Eurodac has been expanded to include wider migration purposes and law enforcement purposes.
ii. **Increasing overlap between the ancillary purposes of the systems**, primarily in relation to law enforcement access. For example, the identification of 'illegally staying third-country nationals' is now common across Eurodac, SIS II, VIS and EES.

The additions of functions and purposes to the distinct information systems can lead to a **blurring of the boundaries between immigration control and internal security**.

Considering the **data collected by each system, they primarily, but not exclusively, relate to third-country nationals**. This has potential implications for the interoperability proposals, as certain solutions aim to solely target third-country nationals but incorporate databases that include EU nationals. Furthermore, there is **significant overlap across the systems in relation to the biographical and biometric identity data collected**; and, beyond identity data, there are significant overlaps in the data collected by VIS and EES, as well as EES and ETIAS. As many travellers would be in EES and at least one other of these information systems, interoperability between these systems has been included in the respective legislative proposals.

Regarding the challenges facing the existing systems, there are a **number of cross-cutting issues**. Those most prominently highlighted include:

- fragmentation of the EU's data architecture;
- effective risk management and protection of data subject's rights;
- poor data quality; and
- heterogeneous use across the Member States.

Interoperability proposals: Definition of interoperability

The **concept of interoperability is considered to be positive by the vast majority of stakeholders, when implemented appropriately**. The linking of distinct information systems to improve the efficiency of operations for end-users, while strictly regulating access rights and fully respecting the protection of personal data, can be a significantly beneficial endeavour. What interoperability is not intended to deliver is new modes of storage, new processing of personal data beyond the purposes of each system or new access rights.

In the Commission's legislative proposals on establishing a framework for interoperability between EU information systems, however, **the definition appropriated for the concept of interoperability is not explicitly stated and not sufficiently elaborated, as most prominently highlighted by the EDPS**. The roots of the definition can be clearly traced back to the field of e-Government, but the application requires much greater clarity on how the concept of interoperability – in particular, the notions of legal, semantic, operational and technical interoperability – has been applied to the creation and design of the solutions.

Therefore, the **biggest challenge facing the proposals is that, in reality, they do not establish a framework for interoperability, but instead propose technical solutions, some of which are compatible with the concept of interoperability, some of which are not**. Furthermore, the understanding of interoperability appears to be based on the solutions conceived as opposed to the solutions being developed based on a clear, transparent and agreed understanding of interoperability. However, interoperability needs to be clearly defined, including its outer limits, otherwise it may become a flexible concept and a moving target.

Additionally, the proposals would benefit from increased clarity and transparency on the following cross-cutting issues:

- **Use of presumptive terminology** that consistently asserts the necessity of the proposals with limited supporting evidence.
- **Limited consultation exercise**, particularly with regard to the data protection and fundamental rights implications of the proposals.

Problem definition and needs

The problem definition highlights the following two principal problems with the current situation:

i. Information in the existing databases is not always complete, accurate and reliable.

ii. End-users do not always have fast, systematic access to all the information they need to perform their tasks. In some cases, existing rights to access the various systems in accordance with EU legal instruments are not exercised in full because of a 'lack of technical and practical means at a national level'.[15]

It is clear that the second problem can be addressed by interoperability, but further clarity is required on how interoperability can improve the completeness, accuracy and reliability of data. The proposed measures to improve data quality and the operation of the CIR, sBMS and MID could contribute to addressing the first need, but they introduce new access rights, new processing of personal data and new modes of access.

Additionally, the problem definition highlights two principal problem drivers. The **differences between the drivers are not clearly explained and these drivers suggest that a lack of interoperability is fostering the abovementioned problems**. In reality, it is those individuals tasked with inputting data who drive the completeness, accuracy and reliability of the data in each system.

Furthermore, the different information systems were intentionally developed separately based on the specific purposes of each system and in line with the data protection principle of purpose limitation[16]; and the needs articulated in the proposals often lack supporting evidence.

Objectives

The **proposals establish various sets of objectives, for which the links are not clearly explained**. The explanatory memorandum presents general, Treaty-based objectives and specific objectives, and Article 2 of the legislative text presents further objectives.

Furthermore, the general objectives detailed in the explanatory memorandum bring together migration and internal security objectives. As previously highlighted by the EDPS, this can lead to a **conflation of migration management and management of internal security, as well as blurring the boundaries between the two policy areas** with almost interchangeable use of the terms in relation to the JHA information systems. Furthermore, it should be clearly stated that, for most information systems covered by the proposals (not SIS II or ECRIS-TCN), security-based objectives are also ancillary.

In the explanatory memorandum supporting the proposals, four specific objectives are also defined. These **objectives introduce significant new purposes to the existing JHA information systems environment**. The detection of multiple identities and the facilitation of identity checks of third-country nationals on the territory of a Member State, for instance, are both significant new objectives for the existing and planned JHA information systems. Furthermore, both of these new objectives have a strong security element and limited relevance to the objectives of the existing and planned JHA information systems.

Article 2 of the proposals presents the objectives of the legislative text. Paragraph (1) simply lists the general objectives of the existing and planned information systems, thereby **equating the distinct systems and their objectives**.

---

[15] Impact Assessment accompanying the proposal for a Regulation on establishing a framework for interoperability between EU information systems, p. 9.

[16] General Data Protection Regulation (GDPR), Article 5(1).

Solution purposes and design

The **European Search Portal (ESP) could be a very successful innovation that will likely lead to improved operational efficiency**. Furthermore, no significant aggregation of data is possible and no additional information systems are developed. As such, the ESP will contribute to the achievement of specific objective one (i.e. to facilitate fast, seamless, systematic and controlled access by authorities) and could be implemented without data protection implications. Where the protection of personal data could become a challenge is in the development of the delegated acts related to the user profiles and the maintenance of existing access rights. These should be developed with significant data protection input.

Lastly, further clarity is required on the extent to which owners of Interpol data will be notified of searches relevant to their data. It is not clear, for example, whether the owner of the Interpol data is notified that a search has taken place.

The **shared Biometric Matching Service (sBMS)** will likely contribute to achieving the objectives to which it is intended to contribute through the storage and use of mathematical representations of biometric data to support the ESP, the CIR and the MID. However, the sBMS constitutes a new database and therefore does not conform to an appropriate definition of interoperability. Furthermore, greater clarity is required on whether the mathematical representations (i.e. biometric templates) stored by the sBMS constitute personal data.

However, regardless of whether the mathematical representations are personal data or not, it is clear that the sBMS can add value in identifying multiple identities across the information systems. What is not recognised, reflecting the limited options explored in the impact assessment, is that the sBMS would also bring value without the other interoperability components. **The sBMS would still be able to determine multiple identities across all systems except for ETIAS, when the detection of multiple identities will be based on the comparison and consultation of biometric data.** Considering the implications of implementing the CIR and MID, this represents a potential alternative implementation option.

The **Central Identity Repository (CIR)** will likely contribute to the achievement of its purpose and the related objectives. In particular, it will greatly facilitate the identification of third-country nationals on EU territory, it will support the functioning of the MID in detecting and verifying multiple identities across the systems and it will facilitate the streamlined process for law enforcement access to non-law enforcement databases. However, the establishment of the CIR is the most invasive dimension of interoperability – as conceived by the Commission – and raises privacy and data protection concerns in numerous respects:

First, the **text on its architecture is unclear as to whether it will constitute a separate database**. Furthermore, the proposals explicitly state that the CIR is not a new database, while calling it a 'repository' and using terms such as 'stored' and 'storing'.[17] This is further supported by the legislative text, which discusses the CIR in the same manner as the current and planned information systems (see, for example, articles 9, 11 and 14). In the light of the above, the **CIR does not seem to constitute an interoperability solution and if so, this should be declared and processed as such**.

Furthermore, **the CIR will act as a database** when facilitating the identity checks by law enforcement personnel of third-country nationals on the territory. As such, its operation is akin to the creation of a new database that: provides new access rights to the personal data collected across the information systems; equates all types of third-country nationals; and constitutes a major purpose change for the personal data collected across all the systems. Furthermore, this purpose change is related to the ancillary purposes of the systems, which

[17] Proposal for a Regulation on establishing a framework for interoperability between EU information systems, 2017/0352 (COD) and 2017/0351 (COD), p. 7, paragraph 3.

further calls into question its proportionality. Finally, the proposals do not adequately detail or evidence the current challenges and problems that are reportedly necessitating this new purpose.

The existing mechanisms of law enforcement access to VIS have faced criticism. The judgments in both *Digital Rights Ireland* and *Watson* stated that independent or judicial authorities should be responsible for the verification of the conditions of access to VIS, rather than central access points or verifying authorities, which are permitted to be within the same organisation that is gaining access to VIS. With this in mind, it is clear that the two-step approach detailed in the interoperability proposals relaxes these conditions further, generating the following challenges:

- It will be possible for law enforcement to have a finding without any authorisation, as the absence of a record across the information systems (i.e. no flags on an identity) would be a finding;
- The knowledge provided by the hit-flag functionality – i.e. which database an individual is in – negates the current conditions for access, provides law enforcement with access to new information and equates all third nationals from across the distinct systems.

As such, the **CIR introduces the most significant changes compared to the current implementation** and represents the most significant threat to the protection of personal data and the right to privacy in this context.

The **multiple-identity detector (MID)** will likely support the purposes it is set out for and contribute to the achievement of the objectives established. However, it does not constitute an interoperability solution in line with an appropriate definition of interoperability. This is because it creates new data in the form of links and identity confirmation files; and it provides new access rights to those individuals who encounter a yellow link.

Furthermore, the purpose of the MID to combat identity fraud is not supported by the legal basis for Eurodac. The inclusion of Eurodac data would require a further amendment to the purpose of the information system.

The additional elements proposed by the proposals are also not interoperability solutions. However, the consistent implementation of the UMF and the development of a CRRS are valid endeavours that will add value without additional implications.

1. INTRODUCTION AND METHODOLOGY

Recent terrorist attacks across the EU Member States, and the perceived threat posed by terrorists travelling through routes of irregular migration before remaining undetected in the Schengen area, have prompted discussion at the EU level about the need for deepening cooperation and increased information sharing to ensure the safety and security of EU citizens.[18] Furthermore, the number of non-EU nationals travelling to the EU has increased significantly in recent years,[19] thus necessitating efficient measures and mechanisms to manage EU external borders.[20]

Although there are numerous existing centralised and decentralised JHA information systems, as well as additional systems in the legislative pipeline, the Commission has highlighted information gaps caused by the complexity and fragmentation of these systems.[21]

Following repeated calls from the Council,[22] in 2016 the Commission published its Communication on stronger and smarter information systems for borders and security.[23] This Communication presented 'four dimensions'[24] of interoperability and established a High-Level Expert Group (HLEG) on Information Systems and Interoperability to explore the legal, technical and operational aspects of these four dimensions. In June 2017, following the final report of the HLEG, the Commission announced its intention to present a legislative proposal on interoperability.[25]

On 12 December 2017, the European Commission **published its proposals for a Regulation on establishing a framework for interoperability between EU information systems.**[26]

Within this context, Optimity Advisors, in collaboration with independent experts Professor Katrin Nyman-Metcalf and Dr Niovi Vavoula, has developed the present report on the '*Interoperability of Justice and Home Affairs Information Systems*', as commissioned by the European Parliament Policy Department on Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. This introductory chapter presents the structure of this report before providing overviews of the study scope and study methodology.

---

[18] COM (2016) 205 final Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security.

[19] EPRS (2017) European information systems in the area of justice and home affairs: An overview.

[20] COM(2016) 205 final (06.04.2016).

[21] Ibid.

[22] See, for example: Council of the European Union, European Council meeting (17 and 18 December 2015) Conclusions, Document EUCO 28/15 (18.12.2015); Council of the European Union (2016) European Council meeting (15 December 2016) Conclusions, Document EUCO 34/16 (15.12.2016); Council of the European Union (2016) Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, Document 9368/1/16 (06.06.2016); Council of the European Union, Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016, Statements and remarks 158/16 (24.03.2016).

[23] COM(2016) 205 final (06.04.2016).

[24] Ibid, p. 14.

[25] European Commission (2017) Seventh progress report towards an effective and genuine Security Union. COM(2017) 261 final (16.5.2017).

[26] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, Brussels, 12.12.2017; Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 793 final, Strasbourg, 12.12.2017.

1.1. Structure of the report

The structure of this report is as follows:

Chapter 1. Presents the structure of the report, the material and geographical scope of the study and the methodological approach.

Chapter 2. Provides an overview of each existing and proposed JHA information system within the scope of the study, before comparatively analysing:

- the objectives, purposes and data collected by the systems
- the use of, and access to, the systems
- the key challenges faced by the current implementation.

Chapter 3. Assesses the Commission's proposals for a Regulation on establishing a framework for interoperability between EU information systems, covering:

- the concept of interoperability and its development in EU Justice and Home Affairs, and wider EU, policy
- the problem definition and objectives, as well as the design and purposes of the solutions, as detailed in the Commission's proposals
- the implementation, fundamental rights and data security implications.

Chapter 4. Builds on the above chapters, outlining the conclusions of the study.

In addition, the following appendices are included:

- **Appendix 1:** a profile summary for each of the six information systems covered by this study, namely:
  - Visa Information System (VIS)
  - European Dactyloscopy (Eurodac) database
  - Second-Generation Schengen Information System (SIS II)
  - Entry/Exit System (EES)
  - European Travel Information and Authorisation System (ETIAS)
  - European Criminal Records Information System for third-country nationals (ECRIS-TCN)
- **Appendix 2:** a bibliography.
- **Appendix 3:** a list of stakeholder organisations interviewed for the study.

1.2. Scope of the study

This study aims to achieve three key objectives, as described below, which relate to: i) the current and proposed JHA information systems, and ii) the Commission's proposals for interoperability.

Current and proposed Justice and Home Affairs information systems

Objective 1: Provide a detailed analysis of the overlap between JHA information systems,[27] including the existence of duplicate or triplicate data records throughout existing information systems and planned new databases, such as the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS).

Objective 2: Map the use of, and access to, existing JHA information systems by various EU and national agencies[28] and examine the patterns of use by these agencies.

Proposed interoperability and its implications

Objective 3: Provide a detailed analysis of the proposed methods for interoperability. Under this objective, the focus is placed on analysing, to the extent possible, the European Commission and HLEG proposals on the topic of interoperability.

1.3. Study methodology

The methodology used for this study comprises descriptive, comparative and legal analysis techniques, in combination with expert opinion, to analyse the qualitative and quantitative data collected through the following means:

- **Desk research** assessing information published at the EU level and in the Member States covered;
- **Interviews** covering European institutions, as well as national-level stakeholders in the Member States covered (a list of stakeholders interviewed can be found in Appendix 3);
- **Expert workshop**, held in London in February 2018, with study experts Professor Katrin Nyman-Metcalf and Dr Niovi Vavoula.

The first-level outputs of the research methods were the summary profiles, presented in Appendix 1, which detail key information on the different JHA information systems covered by the study. On the basis of these profiles, the further desk research, interviews and the expert workshop, the analyses have been conducted in order to achieve the study objectives and answer the study's research questions.

[27] Regarding the coverage of JHA information systems, this report focuses on the six existing and proposed information systems directly impacted by the Commission's proposals, namely VIS, Eurodac, SIS II, EES, ETIAS and ECRIS-TCN.

[28] In order to understand the use of the JHA information systems by national-level authorities, desk research and interviews were conducted in a selection of Member States. Research was conducted in Estonia, France, Germany, Greece, Italy and Sweden, taking into account the following sampling criteria: i) Member State geography and size; ii) border control systems; iii) criminal justice and information system implementation needs/particularities; and iv) use of the different databases.

2. CURRENT AND PROPOSED JHA INFORMATION SYSTEMS

Section 2.1 gives an overview of each of the six EU JHA information systems covered by the study. Section 2.2 presents a comparative assessment focusing on the purpose and objectives of the different information systems, as well as the data collected and held by the different information systems and the access rights. Section 2.3 discusses the overarching challenges and the specific challenges faced in relation to each system.

2.1. Overview of JHA information systems

This section provides a general overview of each of the EU JHA information systems examined in this study by answering the following questions:

- What are the functions of each system?
- What are the stated purposes of each system?
- What has been the Commission's rationale for establishing/proposing each system?
- What is the technical structure of the system?
- How is the system used in practice by authorities granted access to the data?

Visa Information System (VIS)

The Visa Information System (VIS) is a centralised database containing information on visa applicants who require a short-stay visa to enter the Schengen area. Council Decision 2004/512 provided the legal basis for the establishment of a common identification system for visa data, while Regulation 767/2008[29] defines the purpose, functionalities and responsibilities of the VIS, which are to establish the conditions and procedures for the exchange of visa data between Member States, and the facilitation and management of the visa applications and the decisions related to them. As a multi-purpose tool, the system has the overarching purpose of 'improving the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States'.[30] Within this purpose, the VIS aims at:

a) facilitating the visa application procedure;
b) preventing 'visa shopping';
c) facilitating the fight against fraud;
d) facilitating checks at external border crossing points and within national territory;
e) assisting in the identification of persons that do not meet the requirements for entering, staying or residing in a Member State;
f) facilitating the implementation of the Dublin mechanism for determining the Member State responsible for the examination of an asylum application and for examining such applications; and
g) contributing to the prevention of threats to Member States' internal security.

The central system VIS (CS-VIS) has two components, a VIS central database (located in Strasbourg, France, with a back-up site in Sankt Johann im Pongau, Austria) with alphanumerical searching capabilities, and an Automated Fingerprint Identification System (AFIS) that compares new fingerprints against those in the database and returns a hit/no-hit response, along with matches. The national interfaces (NI-VIS) are located at all external

[29] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

[30] VIS Regulation, Article 2.

border crossing points of each Schengen state and at consulates in non-EU countries. The national interfaces enable competent authorities of the participating Member States to process data on visas issued, revoked, annulled, extended or refused. VIS also has a communication infrastructure that links national systems and consulates in third countries.

The primary data used for verification and identification are 10 fingerprints and a scanned/digital photograph, both of which are required to be registered for persons wishing to apply for a visa into the Schengen area. While other alphanumeric data are necessary for the visa application process, the VIS makes use of biometric data for identification and verification purposes.

When a Schengen visa application is lodged and when a decision is taken on the application, the information is registered in the VIS by the visa authorities of the competent Schengen states. Access to VIS data is granted to authorised staff of national visa authorities responsible for entering, amending or deleting data when 'examining and for taking decisions on visa applications or for decisions whether to annul, revoke or extend visas, including the central visa authorities and the authorities responsible for issuing visas at the border'.[31] The information is centrally stored and cross-referenced at border crossings against the visa holder for verification by external border control authorities.[32] Biometric information for new applicants for a Schengen visa at an EU consulate remains valid in the system for five years after the expiration of the visa.

Upon the arrival of third-country nationals to the Schengen area competent border authorities can perform two types of searches, both carried out using the separate Biometric Matching System (BMS):

- A check that the fingerprints scanned at the border crossing point correspond to the fingerprints associated with those attached to the visa to establish the validity of a claimed identity (one-to-one check).
- An identification search at the border crossing post that compares the fingerprints of any person who may not, or may no longer, fulfil the conditions for the entry to, stay or residence on the territory of the Member States with the contents of the entire database (one-to-many check).

Box 1: Key concept: Centralised and decentralised systems

In the context of the EU information systems, a **centralised system** refers to one where the data are held in a central database. Through secure communication infrastructure, Member States can connect and send information to or receive information from the central system via national interfaces located within designated authorities. In contrast, a **decentralised system** is where information is held in national databases, and upon request can be transferred to other Member States along secure communication infrastructure.

[31] VIS Regulation. Article 4(3).

[32] Ibid, Article 18(1).

Eurodac

Eurodac has been the EU asylum fingerprint database since 2003.[33] Its primary purpose, set out in the Eurodac Regulation,[34] is to assist application of the Dublin III Regulation[35] that lays down rules for determining which Member State is responsible for examining an asylum application. The main reason why Eurodac was created was to determine whether an asylum applicant had previously applied for asylum in another Member State, thus preventing 'asylum-shopping'.

The Eurodac system comprises a central database in which data are processed for the purpose of comparing the fingerprints taken by participating States, and a communication infrastructure between the central system and the national access points of Member States.[36]

Each Member State is required to fingerprint all applicants for international protection and those apprehended whilst attempting to cross a border irregularly over the age of 14 and to transmit the data to Eurodac within 72 hours of the irregular crossing.[37] When an asylum-seeker or third-country national has been found to be present illegally in a Member State, then that Member State may consult Eurodac to determine whether the individual has previously sought international protection in another Member State or has previously been apprehended when trying to irregularly enter the EU. However, these fingerprints are not currently stored. Thus, the Eurodac holds fingerprints on two categories of persons:

- individuals who have applied for international protection; and
- individuals from irregular border entries.

Fingerprint data is required to be erased from Eurodac once those present in the database acquire EU citizenship. The 2000 Eurodac legislation[38] did not provide for law enforcement authorities to request fingerprint comparisons; however, the scope of Eurodac was expanded with Regulation (EU) No 603/2013 providing new functionalities for granting access to national law enforcement bodies and Europol.[39] Competent national law enforcement bodies and Europol are only permitted to consult Eurodac data for the purposes of preventing, detecting or investigating terrorist offences and other serious crimes referred to in Articles 1 to 4 of Framework Decision 2002/475[40] and Article 2(2) of Framework Decision 2002/584[41]

---

[33] Council Regulation (EC) No. 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national.

[34] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

[35] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person

[36] Regulation (EU) No 603/2013, art 4.

[37] Irregular migration refers to non-EU/EEA nationals or stateless persons entering without valid documents.

[38] Council Regulation (EC) No 2725/2000.

[39] http://www.eulisa.europa.eu/Publications/Reports/2017-088_2016%20Eurodac%20Annual%20Report.pdf. For further information see Niovi Vavoula, The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?' in Céline Bauloz and others (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Brill 2015).

[40] Article (1): Terrorist offences and fundamental rights and principles; Article (2): Offences relating to a terrorist group; Article (3): Offences linked to terrorist activities; Article (4): Inciting, aiding or abetting, and attempting.

[41] Offences listed within the scope of the European arrest warrant.

respectively. The lists of the designated authorities, and the operating units within the designated authorities, are maintained by each Member State.[42]

The 2016 proposal for recasting the Eurodac Regulation which is in the trialogue phase is expected to extend the scope of the Regulation to include the possibility for:

i. Member States to store and search data of third-country nationals or stateless persons who are not applicants for international protection so that they can be identified for return and readmission purposes.

ii. Member States to take and transmit fingerprints and a facial image of all three categories of persons and makes sure that Member States impose these obligations on applicants of international protection and third-country nationals or stateless persons so that they are aware.

iii. Storage of personal (biographical) data of the data-subject such as the name(s), age, date of birth, nationality, and identity documents, as well as a facial image.

iv. Storage and comparison of fingerprint and facial image data of all three categories of data.[43]

Second-Generation Schengen Information System II (SIS II)

The second-generation Schengen Information System (SIS II) supports external border control and law enforcement cooperation in the Schengen states. It enables competent authorities to enter and consult alerts on certain categories of wanted or missing persons and objects. Furthermore, it provides instructions on what to do when the person or object has been found. As a prime compensatory measure for the abolition of internal border control, the purpose of the SIS II is

> 'to ensure a high level of security within the EU's area of freedom, safety and justice, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of the Treaty relating to the movement of persons in their territories, using information communicated via this system'.[44]

SIS II is composed of a system (C-SIS II) and national interfaces (N-SIS II) in each participating Member State that are connected via communication infrastructure. Member State alerts are registered in C-SIS II and broadcast in real-time to SIS II participating Member States, who themselves maintain a 'partial' or 'full' copy of the C-SIS II database. Each Member State operating SIS II is required to establish a Supplementary Information Request at the National Entries (SIRENE) Bureau responsible for providing supplementary information on alerts, validating alerts on persons wanted for arrest and acting as the point of communication with the Member State that issued the alert when a match has been received.

The scope of SIS II is defined by three legal instruments. First, Regulation 1987/2006 provides for border guards and visa issuing and immigration authorities to insert and consult

---

[42] Regulation (EU) No 603/2013, Art. 5.

[43] Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast).

[44] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen area.[45] Second, Council Decision 2007/533 enables competent authorities to register and check alerts on persons or objects related to criminal offences, as well as on missing persons.[46] Third, Regulation 1986/2006 allows vehicle registration services to check the legal status of the vehicles presented to them for registration.[47]

Alerts are inserted on to the system by competent authorities (which is dependent upon the nature of the alert issued) of Member States on third-country nationals to be refused entry or stay; persons wanted for arrest or surrender purposes, persons sought to assist with a judicial procedure; missing persons; persons and objects for discreet checks or specific checks; and objects sought for the purpose of seizure or use as evidence in criminal proceedings.[48]

Entry/Exit System (EES)

The Entry/Exit System (EES) will electronically register the time and place of entry, exit and refusal of third-country nationals admitted for a short stay to the territory of Schengen Member States and will automatically calculate the duration of their authorised stay.

In November 2017, the Regulation establishing an EES and amending the Schengen border code in relation to the EES was adopted.[49] This system is anticipated to be fully operational in 2020 with the **aim of ensuring systematic and reliable identification of overstayers; the strengthening of internal security and the fight against terrorism by permitting law enforcement authorities access to travel history records**.[50] The EES will abolish passport stamping and instead a record of all cross-border movements of third-country nationals will be created via the collection of alphanumeric and biometric (fingerprints and facial recognition) data to strengthen the fight against irregular migration and ease the border crossing time for the large majority of 'bona fide' third-country travellers.

The EES will consist of a central system, operating a computerised central database of biometric and alphanumeric data, a National Uniform Interface in each Member State, and a secure and encrypted Communication Infrastructure between the EES central system and the National Uniform Interfaces. The EES Regulation is envisaged to be interoperable with the VIS via secure communication channel. In particular, border authorities using the EES to consult the VIS to retrieve visa-related data will be able to create and update entry/exit records or refusal of entry records; to enable the border authorities to verify the validity of the visa and the identity of the visa holder by directly searching the VIS with fingerprints at the borders where EES is operated; and to enable the border authorities to verify the identity of visa-exempt third–country nationals against the VIS by using fingerprints. This interoperability also allows the border and other authorities using the VIS to directly consult the EES from the VIS for the purposes of examining visa applications and of taking decisions

[45] Ibid.

[46] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

[47] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second-Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates.

[48] Ibid.

[49] Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[50] http://www.consilium.europa.eu/en/press/press-releases/2017/11/20/entry-exit-system-final-adoption-by-the-council/.

relating to those applications, and of enabling visa authorities to update the visa-related data in the EES in the event that a visa is annulled, revoked or extended.

EES data may be used as an identity verification tool in cases where the third-country national has lost/destroyed his or her documents or where designated authorities are investigating a crime through the use of fingerprints or facial images and wish to establish an identity. The Commission also outlined that EES data is intended to facilitate the construction of evidence by tracking the travel routes of a person suspected of having committed a crime or who is the victim of crime.[51]

European Travel Information and Authorisation System (ETIAS)

The European Travel Information and Authorisation System (ETIAS) is a proposed information system with the intention of improving the security at the EU's external border by pre-screening individuals travelling from visa-exempt countries to the Schengen area. It will function in a similar manner as the US ESTA. Given that the number of visa-exempt third-country nationals to the Schengen countries is expected to increase from 30 million in 2014 to 39 million by 2020,[52] it was deemed necessary to assess and manage the potential irregular migration and security risks represented by third-country nationals visiting the EU in a manner that is in line with the EU's visa liberalisation policy.[53] Under this new system, third-country nationals from visa-exempt states will undergo an electronic security check prior to arriving in Schengen Member States that will grant sufficient information for the relevant authorities in the EU to determine whether the individual poses a security, irregular migration, or public health risk.

The data that would be required in the ETIAS before entry could be authorised includes names and date of birth, citizenship information, education and work experience and the initial EU country of entry. Background and eligibility questions will inquire about the third-country national's medical condition, previous travels to war countries, history of deportations and/or refusals of entry and/or visa rejections, as well as criminal records. Information provided by applicants will be automatically cross-referenced against other EU and international databases. If there are no hits or no requirement for further analysis, a valid authorisation can be issued and will allow its holder to stay in the Schengen area for a period of up to 90 days in any given 180-day period and would be valid for three years from the date of issuance or until the expiry date of the passport, whichever comes first.[54]

The ETIAS would be made up of the ETIAS Information System, the ETIAS Central Unit and the ETIAS National Units for all participating States. It would also include a secure communication infrastructure between the central system and the National Uniform Interfaces. It would also include a public website and a mobile app for mobile devices as an interface for applicants. The system will also include an e-mail service; a secure account service enabling applicants to provide additional information and/or documentation, and a

[51] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

[52] Technical Study on Smart Borders, European Commission, DG HOME, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm Visa liberalisation dialogues have been concluded with a number of countries in the EU's neighbourhood (Commission proposals presented on Georgia, Ukraine, Turkey and Kosovo).

[53] Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624.

[54] https://www.etiaseurope.eu/news/etias-applications-changes/

carrier gateway if deemed necessary; and a web service to enable communication between the central system and external stakeholders.

In terms of the ETIAS central system, a mandate would be given to the European Border and Coast Guard Agency (Frontex), and the central system would be integrated in the national border guard infrastructures. The ETIAS Central Unit Frontex would be responsible for reviewing the information in applications that were automatically rejected during processing by verifying that the data recorded in the application file corresponds to the data triggering a hit, before forwarding the alert or hit to the relevant Member States. Eu-LISA would be responsible for developing the ETIAS information system and ensuring its technical management.

European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)

In its current form, the European Criminal Records Information System (ECRIS) is a decentralised system that permits the designated central authorities of Member States to electronically exchange data with other Member States, upon request and using a standardised format. It was established in 2012 with a view to **facilitating the exchange of information on criminal records throughout the EU**. The setting up of the ECRIS became necessary as national courts passed sentences on individuals without prior knowledge of possible previous convictions in other EU Member States. This lack of information led to inadequate judgments that did not consider the criminal history of a person and meant that measures were not instigated to prevent a similar crime being committed again.[55]

In view of this, the ECRIS was created to improve the exchange of information between participating countries on:

- criminal proceedings against a person;[56]
- recruitment procedures with regard to posts involving direct and regular contact with children and;[57]
- information exchange for any other purpose according to national law.[58]

Obligatory data that must be exchanged via ECRIS includes general information on the convicted person; information regarding the nature of the conviction; information on the offence giving rise to the conviction; and information on the contents of the conviction.

ECRIS works efficiently with regard to EU nationals based on the principle that when a Member State convicts a non-national EU citizen, it is required to send information as soon as possible, including any updates, on the conviction to the Member State(s) of nationality. The Member State of nationality is responsible for the single repository of all conviction information for an individual and is obliged to update all information received so that it is in a position to provide a complete overview of its own nationals' convictions, regardless of where those convictions were handed down.

---

[55] https://e-justice.europa.eu/content_criminal_records-95-en.do

[56] Implementing Council Framework Decision 2008/675 on taking account of previous convictions in new criminal proceedings against the same person.

[57] As required by Article 10 of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography.

[58] Such as recruitment procedures, naturalisation procedures, asylum procedures, firearm licence procedures, and child adoption procedures.

The current ECRIS configuration requires Member States to send 'blanket requests' to all Member States for information on third-country nationals and, as such, through 2016 and 2017, the Commission developed two proposals related to the identification of third-country nationals through ECRIS (ECRIS-TCN):

i. A proposal for a Directive as regards the exchange of information on third-country nationals. This proposal aims to amend Council Framework Decision 2009/315/JHA and replace Council Decision 2009/316/JHA.[59]

ii. Proposal for a Regulation (accompanying the above Directive) establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCNs) to supplement and support ECRIS. This proposal aims to amend eu-LISA's founding Regulation, requiring them to provide a **centralised system** for third-country nationals.[60]

Under the proposed new centralised system to be developed, ECRIS-TCN should contain only the identity information of third-country nationals convicted by a criminal court within the European Union, such as alphanumeric data, fingerprint and facial images to the extent they are recorded in the national criminal records databases data in accordance with Framework Decision 2009/315/JHA, as amended by the proposed Directive. Data to the centralised component of ECRIS would be input by central authorities designated under Framework Decision 2009/315/JHA, to be amended by the Commission's proposal, under the responsibility of eu-LISA. Member States are to have hit/no-hit access (see Box 2) to the centralised system under the Commission's 2017 proposed Regulation.

Box 2: Key concept: Hit/no-hit

A **hit/no-hit system** allows searches based on partial information. The search term(s) are compared against profiles held in any given system. A 'hit' means there is a positive match between the search term(s) and the information held in the database. In some cases, a 'hit' will allow the competent authority to access further information related to the individual/object, while in other cases the 'hit' provides the requesting authority with reasonable grounds to obtain further data held by a Member State.

[59] Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS) and replacing Council Decision 2009/316/JHA.

[60] Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011.

2.2. Comparative assessment of JHA information systems

Building on the above understanding of each information system and the further detail provided on each in Appendix 1, this section presents a comparative assessment of the JHA information systems covered by this study. In particular, comparisons are given of the purpose, objectives, data collected and held, access rights and challenges.

Purpose and objectives of JHA information systems

Table 1 summarises a selection of the information in section 2.1 regarding the presently defined primary and ancillary purpose(s) of each of the six JHA information systems examined, as well as the Commission's rationale for establishing / proposing each system.

Table 1: Current primary and ancillary purpose(s) of six EU JHA information systems and Commission's rationale for establishing / proposing each system

	Eurodac	SIS II	VIS	ECRIS	EES	ETIAS
Primary Purpose	To serve the implementation of the Dublin Regulation, determining the EU Member State responsible for examining an application for international protection	To ensure internal security in the Schengen area in the absence of internal border checks by exchanging information between Member States	To improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto	To facilitate the exchange of information on criminal records throughout the EU	To improve the management of external borders, prevent irregular immigration and facilitate the management of migration flows in the Schengen area	To identify any risks associated with a visa-exempt visitor travelling to the Schengen area
Ancillary purpose(s)	To identify illegally staying third-country nationals and those who have entered the European Union irregularly at the external borders, with a view to using this information to assist a Member State to re-document a third-country national for return purposes. To assist in detecting and decreasing crime and terrorism	The return of third-country nationals who do not fulfil or no longer fulfil the conditions for entry, stay or residence in the Member States	To assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States. To help determine the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national. To facilitate the prevention, detection or investigation of a terrorist offence, or other serious criminal offences.	Not applicable	To strengthen internal security and the fight against terrorism by permitting law enforcement authorities access to travel history records To ease the crossing for the large majority of 'bona fide' third-country travellers	To facilitate the prevention, detection or investigation of a terrorist offence, or other serious criminal offences

	Eurodac	SIS II	VIS	ECRIS	EES	ETIAS
Commission's rationale for the system's establishment/ proposal	To determine whether an asylum applicant had previously applied for asylum in another Member State, thus preventing 'asylum shopping'	To compensate for the abolition of internal border controls	a) facilitating the visa application procedure; b) preventing 'visa shopping'; c) facilitating the fight against fraud; d) facilitating checks at external border crossing points and within national territory; e) assisting in the identification of persons that do not meet the requirements for entering, staying or residing in a Member State; f) facilitating the implementation of the Dublin mechanism for determining the Member State responsible for the examination of an asylum application and for examining such applications; and g) contributing to the prevention of threats to Member States' internal security.	To address the problem of national courts passing sentences without prior knowledge of possible previous convictions in other EU countries. The current ECRIS configuration requires Member States to send 'blanket requests' to all Member States for information on third-country nationals, making the exchange of criminal record information on TCNs inefficient	The anticipation of increased numbers of travellers and in response to security concerns regarding the control of EU external borders	The competent border and law enforcement authorities have little information on visa-exempt third-country nationals as regards risks they may pose before their arrival at the Schengen border

Each of the **six JHA systems was established/proposed to address a very specific set of initiatives within a particular institutional context**. These systems have their own objectives, purposes, user groups and legal bases.[61] Though the primary purpose of each system is distinct from the others, there is some overlap in their presently defined ancillary purposes. For instance, one of the common ancillary purposes among Eurodac, SIS II, VIS and EES is the identification of 'illegally staying third-country nationals'. Furthermore, the 'facilitation of the prevention, detection or investigation of a terrorist offence, or other serious criminal offences' is a cross-cutting ancillary purpose of VIS, Eurodac, EES and the ETIAS.

An observation to be made about the currently established systems is the broadening of their scopes over time to serve purposes beyond those defined at their initial inception. For instance, Eurodac was created with the purpose of facilitating the Dublin system but its purpose was expanded to include 'wider migration purposes' and law enforcement purposes.[62] Furthermore, the SIS was initially established as a means of ensuring internal security within the Schengen area by exchanging law enforcement alerts between Member States but, on the basis of the Commission's proposal,[63] it will have an additional function to facilitate the removal of third-country nationals who are no longer lawfully allowed to reside in the Member States. Furthermore, ECRIS-TCN has been proposed as a means to fill the 'TCN gap' in the current ECRIS system where the storage of criminal records information on third-country nationals is inefficient.[64] Though this is not necessarily an evolution in the primary purpose of the ECRIS (to exchange criminal data between the Member States), ECRIS-TCN will constitute a centralised database as opposed to the decentralised structure of the current ECRIS and would function as a supplement to the information currently in ECRIS[65] and hence an extension of its scope.

Thus, there appears to be a convergence in the ancillary purposes of the current JHA systems towards the facilitation of law enforcement functions and migration control. Interestingly, the Regulation for the EES and the proposal for ETIAS both define one of the ancillary purposes of each system as being the facilitation of law enforcement functions, further demonstrating the trend of increased law enforcement access to non-law enforcement databases.[66,67] One could argue that there is an element of the foreshadowing of interoperability in the way in

[61] Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration).

[62] Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast).

[63] Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU.

[64] Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011.

[65] Ibid.

[66] Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624

[67] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011.

which the scopes of the systems have evolved over time. It is also to be noted that the consecutive additions to the functions and purposes of the databases in question blur the boundaries between immigration control and law enforcement.

Data collected and held by JHA information systems

Table 2 provides a framework for comparing the different types of data collected and held by each of the six JHA information systems examined by this study. Firstly, it is noteworthy that the systems primarily collect, or are intended to collect, data on third-country nationals – with the exception of SIS II, which contains alerts also in relation to EU nationals. Another exception involves the VIS, which may contain data on EU nationals in cases when sponsors of visa applications are EU nationals. Finally, the ECRIS-TCN may include convictions on dual citizens (both third-country nationals and EU nationals). Secondly, there is notable overlap in the data collected or intended to be collected, with the overlaps between VIS and EES as well as between EES and ETIAS being particularly significant. This is attributed to the fact that each of these systems serves the purpose of facilitating border management. However, a person coming to the EU for a short-term stay is unlikely to be in all three systems but **would certainly be in two** (one of which will necessarily be the EES) depending on whether they hold the nationality of one of 60 visa-exempt countries or not. This forms part of the justification for the envisaged interoperability between the VIS and EES, as well as the proposal for the interoperability between the EES and ETIAS. Finally, nearly all the information systems hold biometric data, as well as alphanumeric biographical data (though on different categories of TCNs). This is particularly interesting when considering the implications of interoperability between the systems and the detection of multiple identities.

Table 2: Data collected and held by six EU JHA information systems

	Biometric data	Alphanumeric data										
	Biometrics	Travel information					Personal information				Other information	
Characteristics of TCNs included	Fingerprints, facial images, etc.	Country of origin (EU and / or Non-EU)	Place of entry	Dates / Times of entry / exit	Purpose of travel / stay (work, study, leisure)	Travel history	Biographical data (name(s), sex, nationalities held, passport information, etc.)	Socioeconomic data (occupation, level of education, etc.)	Criminal record / history (EU and/or Non-EU)	Medical information	Information related to applications for entry / asylum (status of application, ref. numbers, etc.)	Law enforcement alerts (alerts on overstayers, stolen goods, etc.)
oApplicants for international protection/ Irregular migrants	**Eurodac:** Fingerprints Facial images	**Eurodac:** Member State of origin					**Eurodac:** Name(s), sex, age, POB/DOB, identity documents				**Eurodac**	
Persons convicted of a crime in the EU	**ECRIS-TCN:** Fingerprints, Facial images						**ECRIS-TCN:** Name(s), sex, identity document numbers		**ECRIS-TCN**: EU Criminal record			
Wanted or missing persons	**SIS II:** Fingerprints, Facial images						**SIS II:** Name(s), sex, age, POB/DOB, identity documents, nationality(ies), aliases					**SIS II**[68]

[68] Whether the person concerned is armed, violent or has escaped, Reason for the alert, Authority issuing the alert.

Characteristics of TCNs included	Fingerprints, facial images, etc.	Country of origin (EU and / or Non-EU)	Place of entry	Dates / Times of entry / exit	Purpose of travel / stay (work, study, leisure)	Travel history	Biographical data (name(s), sex, nationalities held, passport information, etc.)	Socioeconomic data (occupation, level of education, etc.)	Criminal record / history (EU and/or Non-EU)	Medical information	Information related to applications for entry / asylum (status of application, ref. numbers, etc.)	Law enforcement alerts (alerts on overstayers, stolen goods, etc.)
Persons coming for a short-term stay	**EES**: Fingerprints, Facial images **VIS:** Fingerprints, Facial images	**EES** **ETIAS** **VIS**	**EES** **ETIAS**	**EES**	**VIS**	**ETIAS**[69]	**EES:** Name(s), nationality(ies), passport number **ETIAS**: Name, sex, nationality(ies) contact details (home address, e-mail, phone number), first names of parents **VIS:** Name(s), sex, age, POB/-DOB, identity documents, nationality(ies)	**ETIAS:** Level of education, current occupation	**ETIAS:** Disclosure of non-EU criminal convictions	**ETIAS**[70]	**VIS:** Status of application, Reference number	

*Note: JHA systems **colour-coded in red** represent where data are not necessarily available*

*Note: JHA systems **colour-coded in green** represent information systems/data collected that has yet to be operationalised/has been proposed*

[69] Whether applicant has travelled to a war or conflict zone in the last 10 years and where / when.

[70] Disclosure of whether the applicant has been subject to any disease with epidemic potential or other infectious or contagious parasitic diseases.

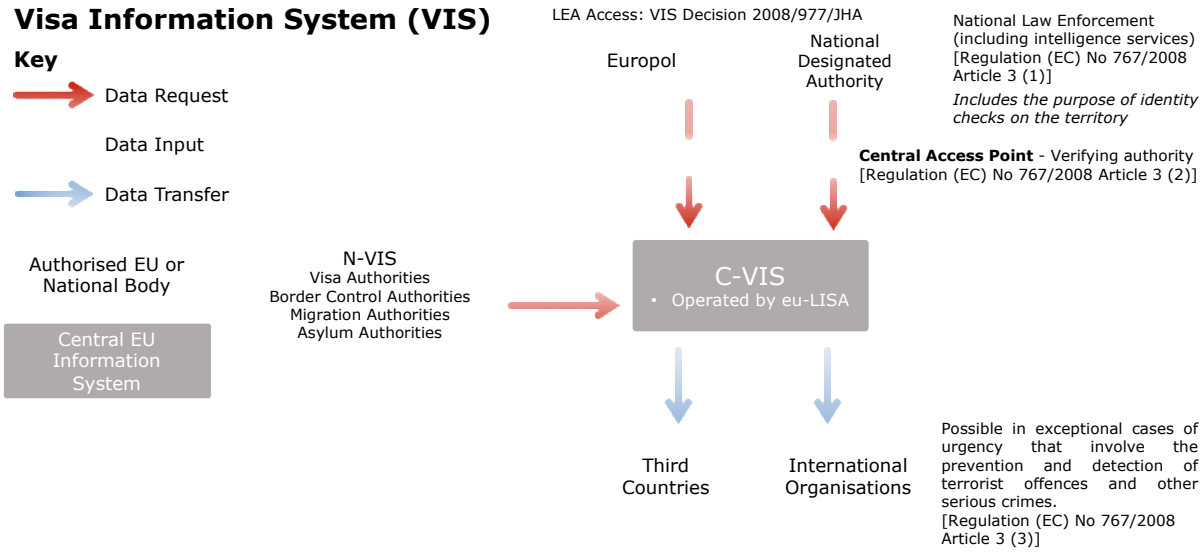
Access rights for each JHA information system

This section explains access rights to the databases in question and distinguishes between the **primary** and **secondary users** of each information system. A **primary user** is one who uses the system to carry out its **primary purpose**. **A secondary user** is one who uses the system to carry out its **ancillary purpose(s) (as defined above)**.

VIS: VIS access is granted to a wide range of authorities so long as the data are required for the performance of their tasks in accordance with those purposes and are proportionate to the objectives pursued. Visa authorities are the primary users of VIS and use it to exchange visa data between Member States as well as to facilitate and manage visa applications and the decisions related to them. Immigration authorities are secondary users of VIS and may have access to VIS data in order to verify the identity of a person and check the authenticity of the visa,[71] while asylum authorities may enter the fingerprints of an asylum seeker to help determine the merits of asylum claim or for Dublin-related purposes.

Furthermore, national 'designated authorities' are also secondary users of VIS and may access the VIS data of an individual if, on a case-by-case basis, there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Access is obtained through a reasoned written request to the national central access point, which acts as an independent verifying body that determines whether the conditions for the request for access have been met. Transfers of VIS data to third countries or international organisations is possible in exceptional cases of urgency that involve the prevention and detection of terrorist offences and other serious crimes, and records of transfers must be maintained and made available to DPAs. Europol may also access the system within the limits of its mandate and when necessary for the performance of its tasks.

Figure 1: Illustration of access rights under VIS



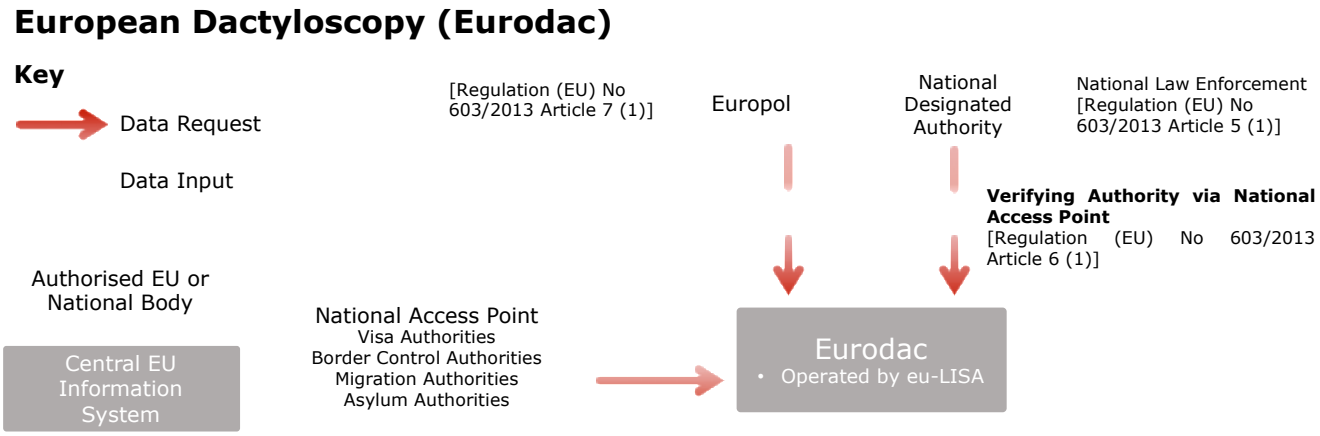
Eurodac: The primary users of Eurodac are **asylum authorities** who use the system when examining applications for international protection in a Member State. Article 5 in the Eurodac Regulation outlines the legal definition of '**Designated authorities**' who are authorised to request comparisons with Eurodac data by individual Member States and who comprise the group of secondary users of the database. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist

[71] Including on the territory of a Member State (i.e. not at an external border).

offences or of other serious criminal offences. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security. These designated authorities must submit a reasoned written or electronic request to the verifying authority via the National Access Point. The verifying authority, which can be within the same organisation that has made a request for Eurodac data but should act in an independent manner, is a safeguard to ensure strict compliance with the conditions for access.[72] If the conditions for the request are met, the National Access Point will process the request transmitted by the verifying authority to the Eurodac central system. The condition of access for designated authorities must be case-specific, connected to situations or person associated with a terrorist offence or other serious criminal offence, including the victims of such offences. Furthermore, access is only granted if searches in Member States' national databases or searches in the VIS database have not provided any matches.[73] Law enforcement authorities, secondary users of the system, are also permitted to conduct searches of Eurodac based on latent fingerprints; that is, fingerprints that are left on a surface and discovered at a crime scene.[74]

Europol, another secondary user of the system, can be granted access to Eurodac if there is an overriding public security concern and where the use of the system is justified to be proportionate. Furthermore, the Member State that recorded the Eurodac data is required to authorise the processing of data by Europol.[75]

Figure 2: Illustration of access rights under Eurodac



SIS II: SIS alerts are only accessible to authorised users within competent authorities, such as national border control, police, customs, judicial authorities, visa authorities, and authorities issuing residence permits,[76] who form the group of primary users of the system. Furthermore, such authorities are only permitted to access the SIS data that is necessary for the performance of their tasks. Europol and the national members of Eurojust have the right to access and to directly search data entered in SIS II according to Articles 26, 32, 34 and 38 of the SIS II Decision.[77]

[72] Regulation (EU) No 603/2013.

[73] Jones, C (2014). 11 Years of Eurodac, Statewatch.

[74] As mentioned in Recital 14 of the recast Regulation, the use of latent fingerprints is a 'fundamental facility for police cooperation'.

[75] Eurodac Regulation (n 3) Article 21(3).

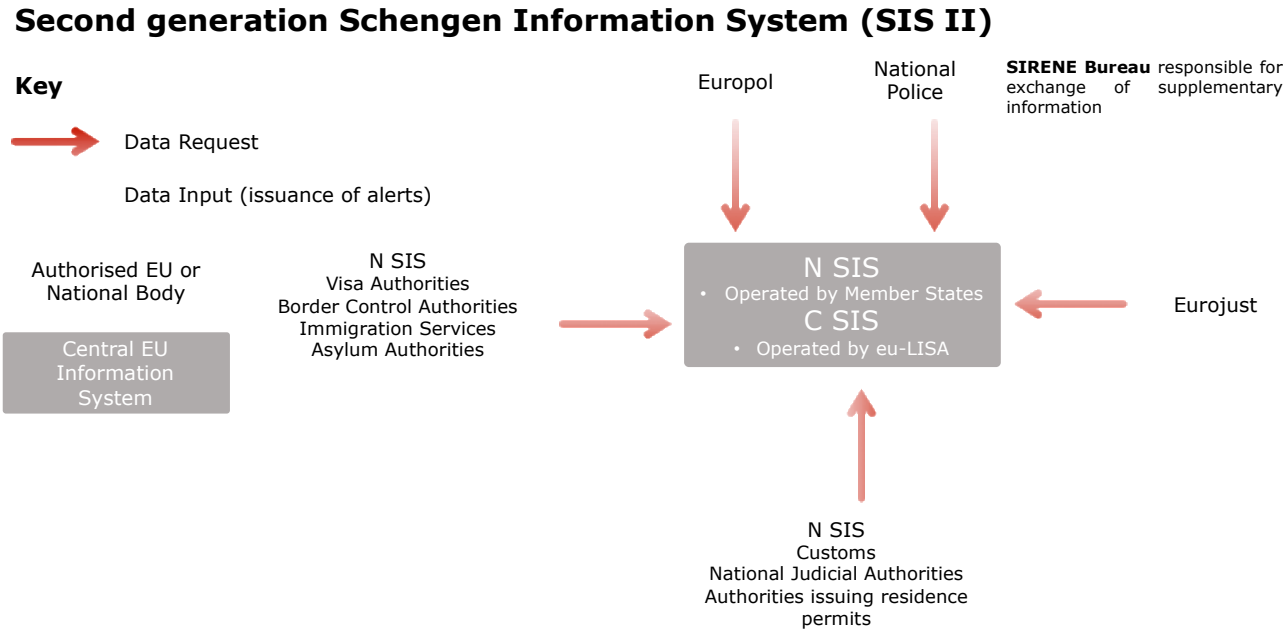
[76] Article 27 SIS II Regulation.

[77] Commission Implementing Decision (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second-generation Schengen Information System (SIS II) (notified under document C(2015) 326).

SIS II is a hit/no-hit system reducing the chances of a prejudice. In the event that an officer's search returns a 'hit', the issuing Member State must be contacted immediately via the SIRENE bureau of the Member State that executed the alert so that an appropriate decision can be taken in line with national and European laws.

Furthermore, it has been proposed that data processed in SIS and the related supplementary information pursuant to 'Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals' may be transferred or made available to a third country in accordance with Chapter V of Regulation (EU) 2016/679 with the authorisation of the issuing Member State, only for the purpose of identification of and issuance of an identification or travel document to an illegally staying third-country national in view of return.[78]

Figure 3: Illustration of access rights under SIS II



EES: The primary users of EES will be the border authorities in each Member State who use the system to carry out border management functions. Among the secondary users of the system, the EES data will be available to the 'designated authorities' of Member States that are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences, and to Europol subject to the existence of evidence or reasonable grounds to consider that the consultation of the EES data will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.[79] Europol is due to have access to EES within the framework of its tasks, and data processing by the organisation will be monitored by the European Data Protection Supervisor (EDPS) to ensure full compliance with applicable data protection rules. At the national level, access will be

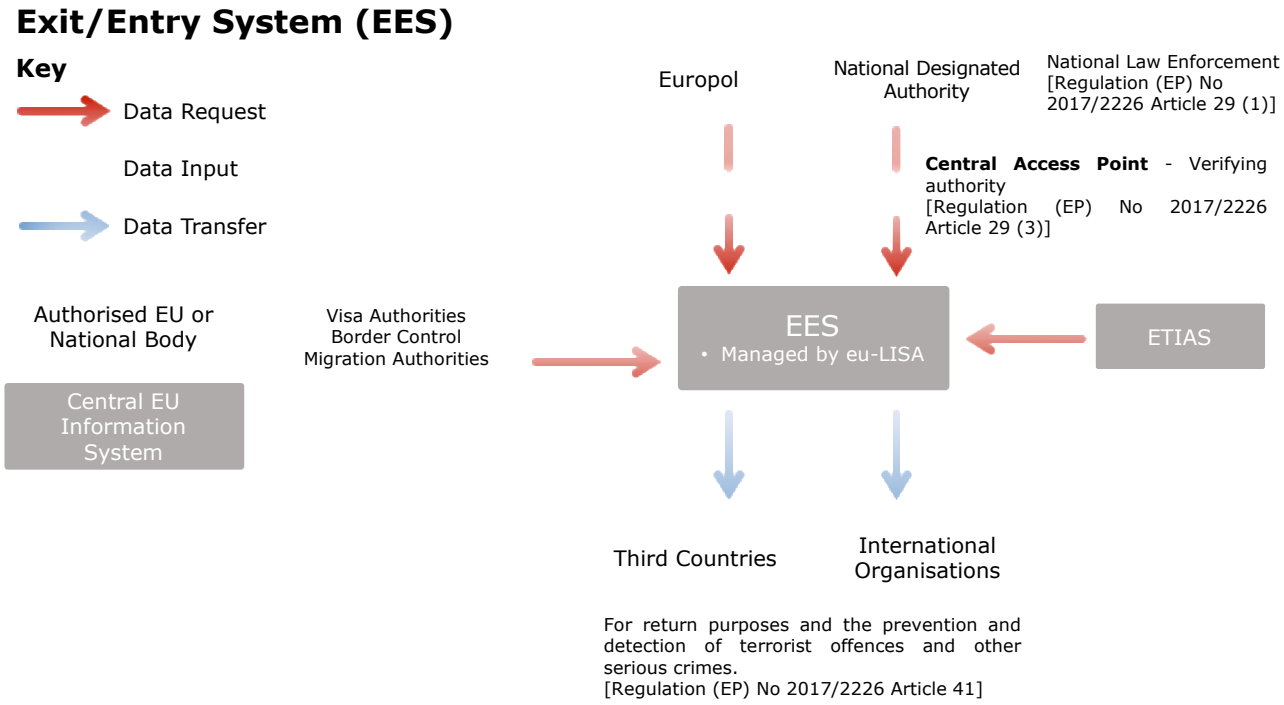
[78] Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals, 2016/0407.

[79] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

granted to operating units within 'the designated authorities' via a central access point. The central access point will be an independent body entrusted to effectively verify whether the designated authority has met the conditions for a proportional request, such as a public security concern, and has strictly complied with the terms of the Regulation.

As in the case for the proposal for SIS II, the transfer of personal data in the EES to third countries is only permitted for the purpose of identification of and issuance of an identification or travel document to an illegally staying-third-country national in view of return.[80]

Figure 4: Illustration of access rights under EES



ETIAS: It is proposed that access will be granted to competent authorities designated by the Member States. National border guards would interact with ETIAS only for purposes of verifying that the travelling third-country national has received travel authorisation by the system. If and when an application is rejected during the automated application process the ETIAS Central Unit Frontex and designated national visa authorities would have access to third-country national applicant data in the process of examining the application and manually deciding on travel authorisation. Furthermore, the proposal foresees access to the personal data held in the ETIAS system by national law enforcement and Europol for the purpose of countering terrorism and serious and organised crime. The conditions of access for designated authorities of ETIAS are equivalent to those of EES, with the inclusion of a requirement for Europol data to be queried prior to access being given to the ETIAS database.[81]

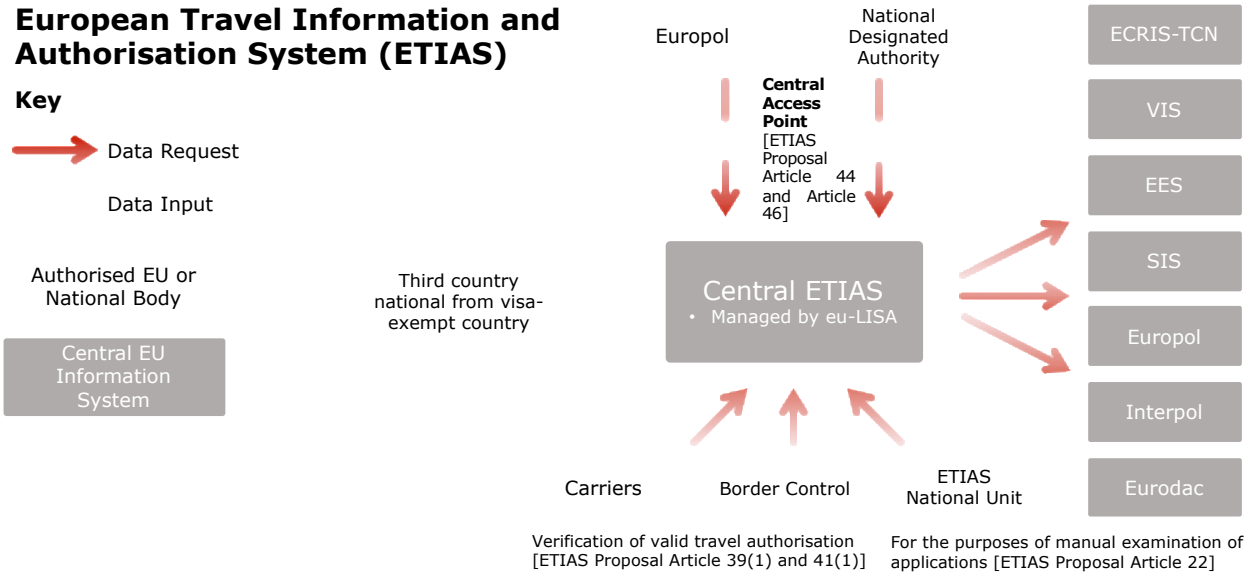
Based on these descriptive profiles, the **comparative table** shown in Figure 5 has been developed. As the figure shows, the entities with most extensive access across the different systems are the national border control, immigration / asylum and visa authorities – all these entities have access to Eurodac, VIS, SIS II and will have access to EES. Law enforcement

[80] Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals.

[81] Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624.

stakeholders, at both the national and EU levels, have access, but only for specific purposes and under certain conditions, which are not identical in all cases. Additional stakeholders, including customs officers, judicial authorities, vehicle registration authorities, Eurojust, the Central Authority for Criminal Records and international organisations have access to specific information systems or access under specific circumstances.

Figure 5: Illustration of access rights under ETIAS



ECRIS and ECRIS-TCN: Data in ECRIS is stored by a Member States' Central Authority for Criminal Records. Applications are made by the judicial authorities of Member States to see an individual's criminal record, due to involvement in criminal proceedings, that the Member State of nationality is obliged to disclose. The ECRIS Regulation provides that a Member State's Central Authority for Criminal Records may release data to non-judicial authorities. Between 2014 and 2016, 81% of all requests made to ECRIS were for the purpose of criminal proceedings while 19% were for 'other purposes'. Included in 'other purposes' was the release of ECRIS data to competent administrative authorities that are responsible for giving permits to carry weapons, authorities responsible for nationality applications, and those responsible for employment vetting, particularly in the case of professional or voluntary activities involving direct or regular contact with children.[82] It is proposed that Europol and Eurojust should have direct access to ECRIS-TCN. As part of the proposal a central contact point would be established at Eurojust for third states requiring information on a convicted third-country national.[83]

[82] Report from the Commission to the European Parliament and the Council (2011) concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States.

[83] Ibid.

Figure 6: Illustration of access rights under ECRIS-TCN

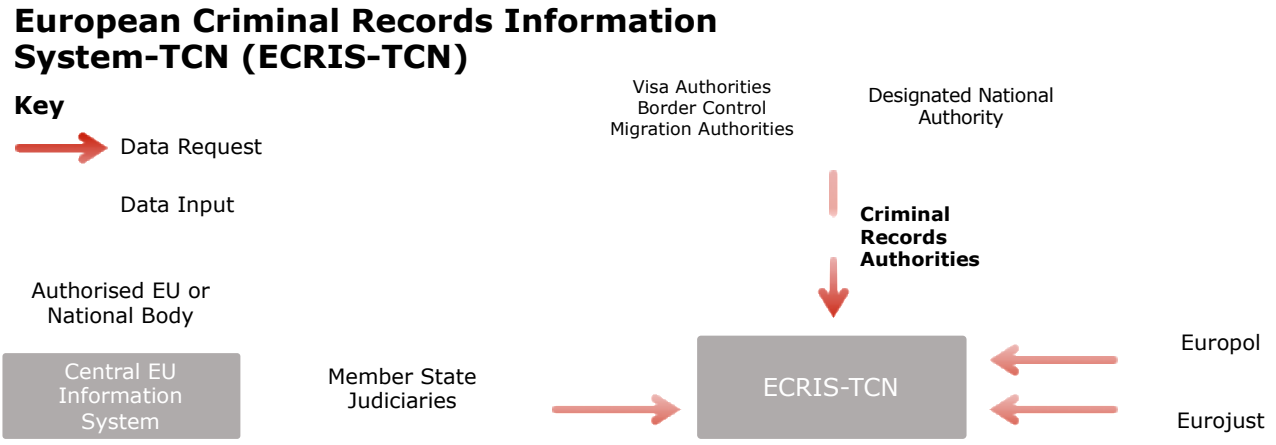


Table 3: Comparative overview of access rights across the six existing and proposed JHA information systems

Entity	Eurodac	VIS	ECRIS-TCN	ETIAS	SIS II	EES
National law enforcement authorities	Yes: to check against latent fingerprints	Yes: preventing, detecting and investigating terrorist and criminal offences	No	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes	Yes: preventing, detecting and investigating terrorist and criminal offences
National border control	Yes	Yes	No	Yes: only for verification purposes	Yes	Yes
Immigration authorities	Yes	Yes	Yes: may apply to criminal records authorities for access	No	Yes	Yes
Asylum authorities	Yes	Yes	Yes: may apply to criminal records authorities for access	No	Yes	No
Customs officers	No	No	No	No	Yes	No
Judicial authorities	No	No	Yes: apply for access to criminal records data of an individual undergoing criminal proceedings	No	Yes	No
Visa authorities	Yes	Yes	Yes: may apply to	Yes: in the event of	Yes	Yes

Entity	Eurodac	VIS	ECRIS-TCN	ETIAS	SIS II	EES
			criminal records authorities for access	rejection after automated application process		
Vehicle registration authorities	No	No	No	No	Yes	No
Europol	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes: preventing, detecting and investigating terrorist and criminal offences	Europol and Eurojust would have access to ECRIS-TCN but not ECRIS in its current format	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes	Yes: preventing, detecting and investigating terrorist and criminal offences
Eurojust	No	No		No	Yes	No
Central Authority for Criminal Records	No	No	Yes: storage of criminal records data	No	No	No
Private organisations	No	No	Yes: if appropriate, can apply to view the criminal history of EU nationals during recruitment	No	No	No

2.3. Challenges: Current and proposed JHA information systems

This section presents overarching and system-specific challenges related to the functioning of Eurodac, VIS and SIS, as well as the limitations of the systems that have been communicated by competent authorities at the national level.

The siloed structure of the current EU JHA systems was initially attributable to the distinct institutional, legal and policy contexts in which these systems were developed. The preference towards their compartmentalisation has been maintained in order to protect the fundamental rights, in particular privacy and data protection, of the third-country nationals whose data are collected, stored and further processed. However, as outlined in the Commission's 'Overview of information management in the area of freedom, security and justice' this compartmentalisation inevitably comes with the price of a lower degree of information sharing,[84] whereby '[i]nformation is stored separately in various systems that are rarely inter-connected. There is inconsistency between databases and diverging access to data for relevant authorities.'[85] One of the consequences of this fragmentation is the **inability to link multiple identities**, which is seen as a serious limitation in the way in which the systems are currently set up. The inconsistency and **fragmentation can also**

[84] Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice, Brussels, 20.7.2010, COM(2010)385 final

[85] Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security, Brussels, 6.4.2016 COM(2016) 205 final.

result in efficiency losses for the end-user, who has to consult many databases and receives partially overlapping information. This can cause delays and lengthy processes, which is detrimental to the individuals concerned.

Related to the above, the Commission has highlighted the fact that **end-users of the systems do not always have fast, systematic access to all the information they need to perform their tasks**. In some cases, for example, existing rights to access the various systems in accordance with the respective EU legal instruments are not exercised in full because of a 'lack of technical and practical means at a national level'.[86] One of the fundamental concerns regarding Eurodac, for instance, is that there is an assumption that asylum procedures are applied homogeneously and are of a certain standard in all Member States, but in practice this is not the case. Despite the harmonisation efforts of the Common European Asylum System (CEAS), differences remain in the asylum procedures, reception conditions and integration capacity of EU Member States.[87] This may have implications for the application of the Dublin Regulation, as the identity and motivation of migrants may be undetermined upon entry into the EU due to the said differences in standards.

The challenges facing SIS II have been laid out in the Commission's 2016 Report on the evaluation of the second-generation Schengen Information System (SIS II).[88] To begin with, a major issue for SIS II is **poor data quality**. The evaluation identified that 'Member States sometimes enter incorrect or incomplete data (for instance, an incomplete name or a name instead of a document number)'.[89] Furthermore, 'new categories of alert or the new functionalities (fingerprints, photographs, European Arrest Warrant, links, misused identity extension) are not fully implemented and displayed to the end-users, contrary to the SIS II legal instruments'.[90] Poor data quality can significantly diminish the effectiveness of the system, as end-users may not have all the relevant information on a case at their disposal. This can have major implications for the EU.

Furthermore, the evaluation states that 'certain Member States and Member States' **authorities do not query SIS II systematically** when they query their national police or immigration databases, which means that they need to search SIS separately with an additional transaction which does not always happen'.[91] As a result, there is the potential for delays in law enforcement authorities accessing highly time-sensitive information or even being entirely oblivious to 'hits' on the SIS.

As with SIS II, **data quality is a significant hurdle for VIS**, where 'problems with data quality mostly stem from sub-optimal application of the legal provisions'.[92] Moreover, the **use of VIS for asylum and law enforcement purposes is currently very fragmented**

---

[86] Impact Assessment accompanying the proposal for a Regulation on establishing a framework for interoperability between EU information systems, p. 9.

[87] Evaluation of the Dublin III Regulation DG Migration and Home Affairs Final report, 2015.

[88] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, 2016.

[89] Report from the Commission to the European Parliament and the Council on the evaluation of the second-generation Schengen Information System (SIS II) in accordance with art. 24(5), 43(3) and 50(5) of Regulation (EC) No 1987/2006 and art. 59(3) and 66(5) of Decision 2007/533/JHA, 2016.

[90] Ibid.

[91] Report from the Commission to the European Parliament and the Council on the evaluation of the second-generation Schengen Information System (SIS II) in accordance with art. 24(5), 43(3) and 50(5) of Regulation (EC) No 1987/2006 and art. 59(3) and 66(5) of Decision 2007/533/JHA, 2016.

[92] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, 2016.

across the Member States where, for instance, 'the possibility for fingerprint searches is not yet used'.[93] Again, this lack of consistency among the Member States in harnessing the system to its full capacity could have major implications for the EU.

While this is not the primary focus of this report, it has been acknowledged that there are potential privacy risks associated with the existence of large-scale information systems[94] and that 'the collection and use of personal data in these systems has an impact on the right to the privacy and the protection of personal data, enshrined in the Charter of Fundamental Rights of the European Union'.[95] A significant challenge in this respect is the **effective risk management and protection of data subjects' rights**. The more databases there are, the more potential risks there may be relating to personal data, for example with incorrect data and data not updated in some databases. In addition, the generalised surveillance of movement, which seems to encompass all third-country nationals, is a key privacy issue.

[93] Ibid.

[94] Vavoula, N (2018) *Immigration and Privacy in the Law of the EU – The Case of Databases* (Brill Nijhoff, forthcoming 2018).

[95] Ibid.

3. INTEROPERABILITY OF JHA INFORMATION SYSTEMS

Building on the assessment of existing and proposed JHA information systems presented in chapter 2, this chapter discusses the Commission's legislative proposals on establishing a framework for interoperability between EU information systems.[96] These proposals comprise the following four solutions:

i. **European search portal (ESP):** a centralised single-search interface capable of simultaneously querying multiple systems (C-SIS II, Eurodac, VIS, the future EES and the proposed ETIAS and ECRIS-TCN systems, as well as relevant Interpol systems and Europol data).

ii. **Shared Biometric Matching Service (sBMS):** this component would enable the querying and comparison of biometric data (fingerprints and facial images) from several central systems (in particular SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN).

iii. **Common identity repository (CIR):** the repository would be a shared technical component for storing biographical and biometric identity data of third-country nationals recorded in Eurodac, VIS, the future EES, and the proposed ETIAS and ECRIS-TCN.

iv. **Multiple-identity detector (MID):** this component would check whether queried identity data exists in more than one of the systems connected to it.

Prior to discussing these proposed solutions in greater depth, this chapter presents the concept of interoperability and its appearance and evolution in European Union policy (section 3.1) before discussing the problem definition, objectives and solutions (section 3.2). Section 3.3 analyses the implications of the proposals, considering the implementation implications as well as the fundamental rights, data protection and data security implications.

3.1. Concept of interoperability and its development in EU policy

Discussions on the interoperability of EU Justice and Home Affairs information systems began in the wake of 9/11[97] and were primarily related to whether VIS (being negotiated at the time) could be made interoperable with SIS[98]. Although VIS and SIS were not made interoperable at this time, discussions on the matter continued. After the 2004 Madrid bombings, for instance, the European Council called on the European Commission to 'submit proposals for enhanced interoperability between European databases and to explore the creation of synergies between existing and future systems'.[99] Calls of this nature were further echoed by The Hague Programme[100] and Council Declaration of 13 July 2005 following the

[96] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, 2017/0352 (COD); Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

[97] Council of the European Union, Document 13176/01 (24.10.2001).

[98] European Commission (2001) Development of the Schengen Information System II, COM(2001)720 final, 18.12.2001, p. 8.

[99] Council of the European Union, Declaration on combating terrorism, Document 7906/04 (29.03.2004).

[100] The Hague Programme: strengthening freedom, security and justice in the European Union, 10 May 2005.

7/7 London bombings[101]. Alongside these discussions, the EU has long pursued the goal of interoperability in other policy areas. This section presents the concept of interoperability; first, as developed in relation to other policy areas (section 3.1.1) and second, as specifically developed in relation to JHA information systems (sections 3.1.2 and 3.1.3).

3.1.1. Interoperability in EU digital public services

The issue of interoperability has most prominently been discussed in relation to digital public services,[102] but has also been raised in relation to many other policy fields, including: eHealth; social affairs: education, science and research; state and society; economy and labour; infrastructure; and taxes and customs.[103] Box 3 presents the EU approach to interoperability in relation to digital public services as an example of the extensive work done in this area.

Box 3: EU approach to interoperability in digital public services

Interoperability of e-Government services is discussed via the European Interoperability Framework (EIF). The EIF was initially published in 2004 and has been subsequently updated in 2010 and 2017; the latter update following calls in the EU's Digital Single Market Strategy.[104]

Although the subject matter is different, much of the EIF is relevant to the implementation of an interoperability model for JHA information systems. In particular, the extensive work conducted by the EU in this field has **resulted in the development and refinement of guiding principles for, as well as a definition of, a model for interoperability.**

The Digital Single Market Strategy states that 'interoperability means ensuring effective communication between digital components like devices, networks or data repositories'.[105] Building on this, the most recent EIF, adopted on 23 March 2017, defines interoperability as 'the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems'.[106]

Alongside this definition, the EIF articulates that an interoperability model should include a clear **governance framework** that requires transparency on 'institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability'.[107] Within this governance structure, the EIF states that interoperability should be considered and specified with clarity at the following **four layers**:

[101] Council of the European Union, Declaration condemning the terrorist attacks on London, Document 11116/05 (Presse 187).

[102] European Commission (2017) New European Interoperability Framework: Promoting seamless services and data flows for European public administrations.

[103] Kubicek, H. and Cimander, R. (2005) Interoperability in Government. A survey on information needs of different EU stakeholders. *European Review of Political Technologies*, No. 3, pp. 1–17, December 2005.

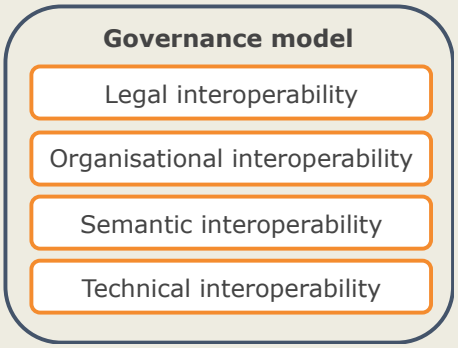
[104] European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe {SWD(2015) 100 final}.

[105] Ibid.

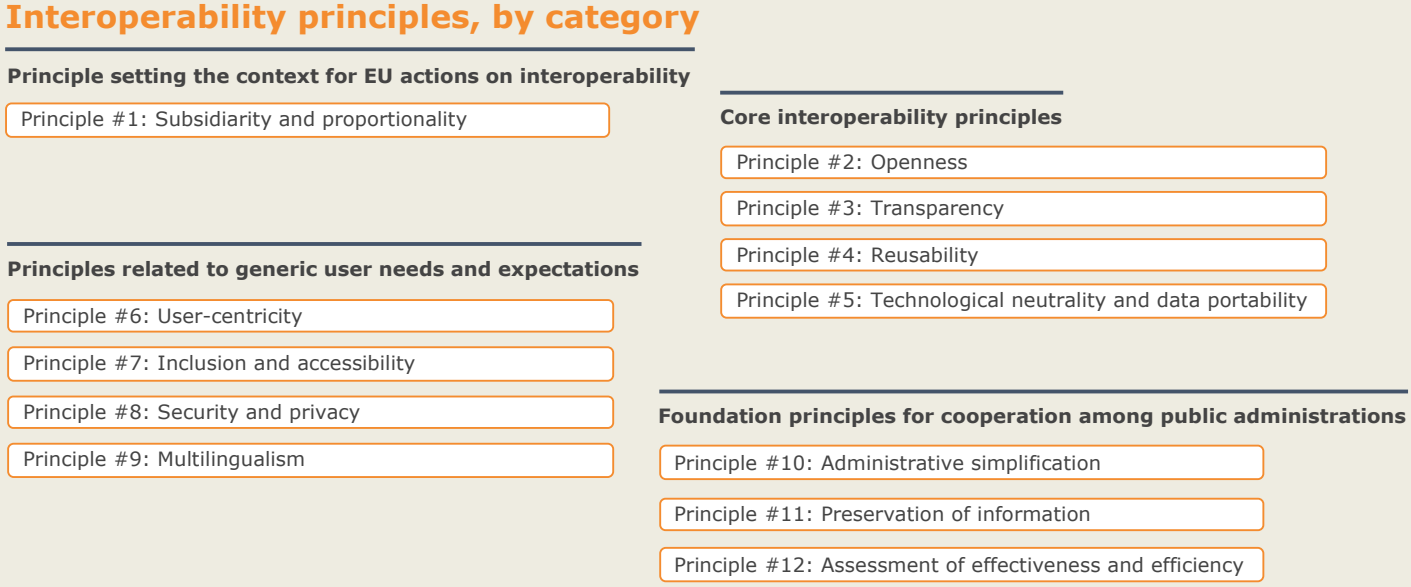
[106] European Commission (2017) New European Interoperability Framework: Promoting seamless services and data flows for European public administrations, p. 5.

[107] Ibid, pp. 27–28.

1. **Legal interoperability:** this layer should define the EU- and national-level legislative instruments that intersect with the area in which interoperability is to be implemented, identify barriers to interoperability and present appropriate legislative amendments.
2. **Organisational interoperability:** this layer should define the processes, responsibilities and expectations necessary to ensure the successful implementation of interoperability, including their alignment across different entities and the organisational relationships between those entities. This aims to ensure the requirements of the user community are met.
3. **Semantic interoperability:** this layer should define the mechanisms to ensure the semantic and syntactic compatibility of the data and information across different systems.
4. **Technical interoperability:** this layer should define how the applications and infrastructures of the systems and services will be interconnected, including data integration and interconnection services, interface specifications and secure communication protocols.



Furthermore, the EIF details **12 interoperability principles** that should guide the design of the governance framework and the approach to each of the four layers.



An additional example at the Member State level, which is closely tied to the EIF, is the e-Government interoperability framework developed and implemented in Estonia, as detailed in Box 4.

Box 4: Member State interoperability example: e-Government in Estonia

Estonia – one of the most advanced Member States in relation to the interoperability of e-Government services – implements a framework for interoperability that strongly mirrors the EIF. In its IT Interoperability Framework, the Estonian Department of State Information Systems describes interoperability as 'the ability of information systems and of business

processes they support to exchange data and share information and knowledge'.[108] Furthermore, it discusses three angles of interoperability: the organisational, the semantic and the technical; and details many of the principles highlighted by the EIF.

As can be seen, a significant amount of effort has been invested in developing the concept of interoperability in the context of digital public services across the EU. Many elements, including the four layers of interoperability and most of the principles of interoperability, however, are not context-specific, however, and should be considered in the application of interoperability in relation to other policy areas. In view of this, the following sections detail the evolution of discussions and the understanding of the concept of interoperability in the EU JHA context, linking back to the EIF, where relevant.

3.1.2. Interoperability in the Justice and Home Affairs context

In November 2005, the Commission published its Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs.[109] Focusing on the operation of SIS, VIS and Eurodac, the Communication first identifies existing shortcomings before briefly presenting ideas for the further development of existing and planned systems.

The discussions on interoperability consider how centralised databases can 'more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime',[110] while ensuring the continued protection of fundamental rights – in particular, privacy and personal data protection.

Furthermore, the 2005 Communication presented the concept of interoperability using the definition prescribed in the 2004 EIF.[111] Specifically, it defined the concept as 'the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge'.[112] Without discussing the applicability of this definition to the JHA context, the Communication further states that **interoperability is a technical concept and not a legal or political concept**.[113]

The EDPS[114] and legal scholars[115] criticised the 2005 Commission Communication. De Hert and Gurtwirth,[116] for instance, expressed concerns over what they saw as a **presentation of technological changes as an acceptable policy without due critique, particularly with regard to the political and social dimensions**. The Communication was described as a 'wish list compiled to serve the interest of one single good, viz. (assumed) efficiency in security and crime fighting',[117] with other vital elements not sufficiently presented; such

[108] Department of State Information Systems, Ministry of Economic Affairs and Communications. Estonian IT Interoperability Framework.

[109] COM(2005) 597 final (24.11.2005).

[110] Ibid, p. 2.

[111] European Interoperability Framework for Pan-European eGovernment Services, Office of Official Publications of the European Communities, 2004, point 1.1.2.

[112] European Commission (2005) Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. COM(2005) 597 final (24.11.2005), p. 3.

[113] Ibid, p. 3.

[114] EDPS (2006) Comments on the Communication of the Commission on interoperability of European databases. Brussels, 10 March 2006.

[115] See, for example: De Hert, P. and Gurtwirth, S. (2006) Interoperability of Police Databases within the EU: An Accountable Political Choice? *International Review of Law Computers and Technology*, Vol. 20, Nos 1&2, pp. 21–35.

[116] Ibid, p. 32.

[117] Ibid, p. 32.

elements, in particular, relate to the definition of interoperability and the impact on fundamental rights, most prominently the protection of personal data.[118]

These concerns are further echoed by the EDPS, who noted that:

- Regarding the **definition of interoperability**: 'the EDPS regrets that the concept of interoperability is not given an unambiguous and clear meaning' and the EDPS 'does not fully share the view that interoperability is a technical rather than a legal or political concept';[119]
- Regarding **privacy and personal data protection**: 'the protection of personal data has not been explored sufficiently as an inherent part of the improvement of the interoperability of relevant systems'.[120]

Although discussed at various points in the decade following the 2005 Communication, limited policy proposals related to the interoperability of JHA information systems were developed.[121]

3.1.3. Interoperability of JHA information systems: from discussions to actions

Following the November 2015 Paris attacks, discussions on interoperability in the field of Justice and Home Affairs received fresh impetus. The Council's Conclusions of 18 December 2015 noted the 'urgency of enhancing relevant information sharing',[122] including through the interoperability of JHA information systems – a view further stressed through the Joint Statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016.[123]

Responding to these calls, on 6 April 2016 the Commission published its Communication on stronger and smarter information systems for borders and security.[124] This Communication details the following perceived shortcomings of the existing implementation of JHA information systems:

- **partial utilisation** of the systems by Member State and EU agencies;
- **technical and functional limitations**, such as poor use of biometric data and low data quality;
- **persistent gaps in the EU informational architecture**, particularly since certain categories of persons are not sufficiently covered by existing schemes (e.g. visa-exempt third-country nationals or long-stay visa holders);
- a **complex legal and policy landscape** governing the various European information systems, given that not all EU Member States are connected to all existing systems; and

[118] Ibid.

[119] EDPS (2006) Comments on the Communication of the Commission on interoperability of European databases. Brussels, 10 March 2006.

[120] Ibid, p. 4.

[121] Council of the European Union, Council Conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal immigration, Document 6975/10 (01.03.2010), point 20, p. 7.

[122] Council of the European Union, European Council meeting (17 and 18 December 2015) – Conclusions, Document EUCO 28/15 (18.12.2015).

[123] Council of the European Union, Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016, Statements and remarks 158/16 (24.03.2016).

[124] COM(2016) 205 final (06.04.2016).

- overall **fragmentation of EU data management architecture** and limited interoperability between information systems.

To address these shortcomings, the Commission proposed three strands of measures:

i. measures to **improve the implementation** of existing JHA information systems;

ii. measures to **implement additional**, new JHA information systems; and

iii. measures to **improve the interoperability** of existing, and new, JHA information systems.

The Communication did not explicitly define interoperability but described the concept as the 'ability of information systems to exchange data and to enable the sharing of information'.[125] This description clearly mirrors the EIF and Estonian definitions of interoperability.

Additionally, the Communication informs the reader that 'one can distinguish **four dimensions of interoperability**, each raising legal, technical and operational issues':[126]

1. a **single search interface** to query several information systems simultaneously and to produce combined results on one single screen;
2. the **interconnectivity of information systems** where data registered in one system will automatically be consulted by another system;
3. the establishment of a **shared biometric matching service** in support of various information systems; and
4. a **common repository of data** for different information systems (core module).

However, the Commission provides no explanation for the creation of these four dimensions, with no reference to these dimensions in previous documentation and no apparent theoretical parallels with the concept of interoperability as described by the EIF, as discussed in section 3.1.1 above. In order to explore the legal, technical and operational aspects of these four dimensions, a High-Level Expert Group (HLEG) on Information Systems and Interoperability was established. The work of the HLEG is described further in Box 5.

Box 5: High-Level Expert Group on Information Systems and Interoperability

On 17 June 2016, the **High-Level Expert Group on Information Systems and Interoperability** (HLEG) was established.[127] It comprised authorities from all Member States and three Schengen associated countries (Liechtenstein, Switzerland and Norway), as well as relevant EU agencies (eu-LISA, European Union Agency for Fundamental Rights (FRA), European Border and Coast Guard Agency (Frontex), European Asylum Support Office (EASO) and Europol) and EU bodies / institutions (Counter-Terrorism Centre (CTC) and the EDPS). The General Secretariat of the Council and the Secretariat of the LIBE Committee attended the HLEG as observers.

The **overarching objective** of the HLEG was 'to contribute to an overall strategic vision on how to make the management and use of data for border management and security more effective and efficient, and to identify solutions to implement improvements'[128]. More

[125] Ibid, p. 14.

[126] Ibid.

[127] Commission Decision of 17 June 2016 setting up the High-Level Expert Group on Information Systems and Interoperability (2016/C 257/03).

[128] European Commission (2016) High-Level Expert Group on Information Systems and Interoperability: Scoping Paper, June 2016, p. 2.

specifically, the HLEG was called to explore each of the following four challenges, in the period June 2016 to June 2017:[129]

- to improve the **implementation** and use by Member States of existing systems;
- to make **existing systems** more effective, process-oriented and user-friendly;
- to consider the development of **new systems** to address identified gaps in the present information system landscape; and
- to develop an **interoperability vision** for the next decade that reconciles process requirements with data protection safeguards.

Furthermore, the following guiding points were highlighted:

- Information systems should be **complementary**. Overlaps should be avoided, and existing overlaps should be eliminated. Gaps shall be appropriately addressed.
- A **modular approach should be pursued**, making full use of technological developments and building on the principles of privacy by design.
- Full **respect of all fundamental rights** of both EU citizens and third-country nationals should be ensured from the outset in line with the Charter of Fundamental Rights.
- Where **necessary and feasible, information systems should be interconnected and interoperable**. Simultaneous searches of systems should be facilitated, to ensure that all relevant information is available to border guards or police officers when and where this is necessary for their respective tasks, without modifying existing access rights.

Following five meetings, the HLEG delivered its Final Report[130] in May 2017. Regarding the HLEG's core task of examining various options for interoperability, the Final Report focused on three of the abovementioned dimensions of interoperability: i) a single-search functionality; ii) the shared biometric matching service; and iii) the common identity repository.

In relation to the second of the original four dimensions, the HLEG determined that the interconnectivity of systems 'should only be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system'.[131]

Through 2016 and 2017, significant additional weight was placed behind the drive to implement interoperability of information systems. For instance, the 'Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area',[132] published just prior to the establishment of the HLEG, reflects the recommendations of the Commission's Communication. In addition, the topic received coverage in President Juncker's September 2016 State of the Union address[133] and

[129] High-level expert group on information systems and interoperability. Final report. May 2017. Ref.Ares(2017)2412067 – 11/05/2017.

[130] Ibid.

[131] Ibid, p. 27.

[132] Council of the European Union (2016) Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, Document 9368/1/16 (06.06.2016).

[133] State of the Union 2016 by Jean-Claude Juncker, President of the European Commission, 14 September 2016.

the Council Conclusions of December 2016,[134] while it was included as the first key area of focus in the Commission's Fourth progress report towards an effective and genuine Security Union.[135]

Building on the work of the HLEG, and its recommendations in relation to the three potential solutions for improving interoperability, as highlighted above, the Commission, in its 'Seventh progress report towards an effective and genuine Security Union',[136] published on 16 May 2017, **announced its intention to present a legislative proposal on interoperability**. Subsequently, in June 2017, the European Council[137] invited the Commission to prepare draft legislation enacting the recommendations of the HLEG. Through the remainder of 2017, the Commission: developed an inception impact assessment,[138] published on 26 July 2017; conducted its consultation process, which included the development of at least three technical studies related to the feasibility of the different solutions, multiple hearings with the LIBE Committee and the public consultation; and developed its legislative proposal. In addition, this timeframe saw the publication of the proposal for extending the mandate of eu-LISA.[139]

On 12 December 2017, alongside the 'Twelfth progress report towards an effective and genuine Security Union', the **Commission presented the following two legislative proposals**, which together aim to establish a framework for interoperability between EU information systems:

- Proposal for a Regulation on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration); and
- Proposal for a Regulation on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC (VIS Decision), Regulation (EC) No 767/2008 (VIS Regulation), Council Decision 2008/633/JHA (regarding law enforcement access to VIS), Regulation (EU) 2016/399 (Schengen Borders Code) and Regulation (EU) 2017/2226 (EES Regulation).

The proposals do not explicitly define the concept of interoperability, but describe it as the ability 'to exchange data and share information *so* that authorities and competent officials have the information they need, when and where they need it'.[140] Besides the similarities between this indirect definition and the definitions of the EIF, the proposals on establishing a framework for interoperability suggest limited consideration of the EIF in terms of the layers beyond the technical. This focus on the technical and the omission of an explicit definition mean that the proposals cannot clearly present how the objectives and implementation of the proposed solutions would achieve interoperability in line with the concept, as understood across EU and Member State policy. In view of this, this study evaluates the proposals in accordance with a working definition of interoperability based on the linking of distinct information systems to improve the efficiency of operations for end-users, while strictly

[134] Council of the European Union (2016) European Council meeting (15 December 2016) – Conclusions, Document EUCO 34/16 (15.12.2016).

[135] European Commission (2017) Fourth progress report towards an effective and genuine Security Union. COM(2017) 41 final (25.01.2017).

[136] European Commission (2017) Seventh progress report towards an effective and genuine Security Union. COM(2017) 261 final (16.5.2017).

[137] European Council (2017) European Council meeting (22 and 23 June 2017) – Conclusions, Document EUCO 8/17 (23.06.2017).

[138] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3765711_en

[139] Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011.

[140] Proposal for a Regulation on establishing a framework for interoperability between EU information systems. {SWD(2017) 473 final} – {SWD(2017) 474 final}, p. 1.

regulating access rights and fully respecting the protection of personal data. In line with this working definition, this study considers that interoperability should not deliver new modes of storage, new processing of personal data beyond the purposes of each system or new access rights.

Interoperability in future and proposed systems: EES and ETIAS

In addition to the new solutions, described above, the Commission has included steps to improve the interoperability of JHA information systems in the Regulation establishing an Entry/Exit System (EES), the proposal to revise Eurodac and the proposal to establish a European Travel Information and Authorisation System (ETIAS).

Regarding **EES**, the adopted text envisages interoperability with VIS through a connection and direct access between the central systems of both JHA information systems.[141] Such a connection would reportedly enable border control authorities to consult VIS through EES for the following purposes:[142]

- retrieve and import visa-related data to create or update an individual file;
- verify the validity and authenticity of a visa;
- verify whether a citizen from a visa-exempt third country has previously been registered in VIS; and
- utilise fingerprint data to verify the identity of a visa holder.

The revised **Eurodac** allows for future interoperability with other JHA information systems but it is not explained how such interoperability would be implemented.[143] In relation to both EES and Eurodac, stakeholders have raised concern with how they 'seem to pre-empt future developments without a proper assessment of their impact'.[144]

For **ETIAS**, the Commission's proposal describes interoperability with many existing and planned systems, including EES, VIS, SIS II, Eurodac, the proposed ECRIS for third-country nationals, Europol data, as well as Interpol's Stolen and Lost Travel Documents (SLTD) and for Travel Documents Associated with Notices (TDAWN).[145] In a similar way as with EES and Eurodac, concerns have been raised about the inclusion of interoperability in the ETIAS proposal. A recent European Parliament study, for instance, notes that the ETIAS 'proposal does not specify any rules on how interoperability will be ensured, which model will be preferred and how it may be embedded in ETIAS'.[146] The study goes on to warn that the inclusion of interoperability in the ETIAS Regulation could lead to a legitimisation of the principle of interoperability without proper scrutiny.[147]

---

[141] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[142] European Parliament (2017) European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection. Study for the LIBE Committee, pp. 35–40.

[143] Recast Eurodac Regulation.

[144] European Parliament (2017) European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection. Study for the LIBE Committee, p. 37.

[145] Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624.

[146] European Parliament (2017) European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection. Study for the LIBE Committee, p. 37.

[147] Ibid, p. 38.

3.2. Proposals for interoperability of JHA information systems

This section first discusses the problem definition and the needs articulated by the proposals (section 3.2.1), before detailing the objectives of the proposals (section 3.2.2) and the solutions designed to establish a framework for interoperability between JHA information systems (section 3.2.3).

3.2.1. Problem definition

The European Commission identifies two principal problems as justification for the need for interoperability between the EU border and security information systems:

- Information is not always complete, accurate and reliable.
- End-users do not always have fast, systematic access to all the information they need to perform their tasks. In some cases, existing rights to access the various systems in accordance with EU legal instruments are not exercised in full because of a 'lack of technical and practical means at a national level'.[148]

Interoperability of the EU information systems can directly address the problem of end-users gaining access to data that they are legally permitted to access. Interoperability can also help to systemise the manner in which authorities access data that is required for the effective completion of their tasks across the EU and provide harmonisation across Member States in this respect. Insufficient data and poor data quality has been highlighted in both VIS[149] and SIS[150] evaluations, and also in the FRA report on the fundamental rights and interoperability of EU information systems[151]. To this end, the Commission has proposed the introduction of data quality standards to improve the data quality within the information systems, but it is important to understand that interoperability in itself does not lead to improvement in the completeness, accuracy, and reliability of data.[152]

Further, the Commission identifies two principal problem drivers:

- a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots;
- a complex landscape of differently governed information systems.[153]

The separation of the different information systems into 'silos' has arisen as a result of the incremental development of policy in the area, and further maintained partly on the basis of the principle of purpose limitation of data. As described above, each information system has a distinct legal basis and a clear purpose, and access rights to these systems are reflected accordingly. While the elimination of 'blind spots' is desirable for effective border

[148] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, p. 9.

[149] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation.

[150] Report from the Commission to the European Parliament and the Council on the evaluation of the second-generation Schengen Information System (SIS II) in accordance with art. 24(5), 43(3) and 50(5) of Regulation (EC) No 1987/2006 and art. 59(3) and 66(5) of Decision 2007/533/JHA.

[151] Fundamental rights and interoperability of the EU information systems: borders and security.

[152] http://library.ahima.org/doc?oid=107104#.Wo6b7pNJYXo

[153] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, pp. 9–12.

management and effective security, the nature of the 'blind spots' should be clearly articulated and understood in the context that the data are to be collected for specified, explicit and legitimate purposes as outline in Article 5(1)(b) of the General Data Protection Directive. The challenge is to understand where the silos and 'blind spots' are beneficial for data protection purposes and where they lack such qualities and instead cause harm to proper data processing.

3.2.2. Objectives of the proposals

The proposals contain various sets of objectives. General objectives of the initiative are derived from Treaty-based goals:

- to improve the management of the Schengen external borders;
- to contribute to the internal security of the European Union.

It has been highlighted both by the EDPS[154] and in an initial appraisal of the impact assessment by the European Parliamentary Research Service[155] that **combining migration objectives with internal security aims blurs the boundaries and conflates migration management with management of internal security**. This conflation is potentially exacerbated when contextualised with the fight against terrorism, which is highlighted from the first sentence of the proposal's explanatory memorandum.[156] This can inadvertently lead to equating short-stay travellers, migrants, asylum seekers, irregular migrants and criminals.

The outlined objectives included in the explanatory memorandum are the specific objectives of the interoperability initiative and are directly related to the proposed technical solutions derived from the HLEG:

1. ensure that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have **fast, seamless, systematic and controlled access** to the information that they need to perform their tasks;
2. provide a solution to **detect multiple identities** linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of bona fide persons and **combating identity fraud**;
3. facilitate **identity checks of third-country nationals**, on the territory of a Member State, by police authorities; and
4. facilitate and **streamline access by law enforcement authorities** to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.

Objective 1 is consistent with the direct definition of interoperability. Interoperability can facilitate **fast, seamless, systematic and controlled access** for authorities that require information to aid their decision-making, while maintaining a high regard for data protection rights and the purpose limitation of the data. For example, the 2016 VIS Evaluation demonstrated that Member States do not uniformly consult VIS for Dublin purposes although it is reported to have a positive impact on the application of the Dublin III Regulation.[157] Ideally, interoperability would change workflows to allow end-users easy access to the

[154] FRA (2017) Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice.

[155] EPRS (2018) Interoperability between EU information systems for security, border and migration management.

[156] 'In the past three years, the EU has experienced an increase in irregular border crossings into the EU, and an evolving and ongoing threat to internal security as demonstrated by a series of terrorist attacks.'

[157] Commission Staff Working Document. Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation.

information that they are entitled to, while simultaneously creating homogeneity across the Member States to allow for uniform migration and asylum management in accordance with EU Regulations. The proposed European Search Portal (ESP) solution directly relates to the realisation of this objective.

Objective 2 is aimed at providing a solution to **detect multiple identities** across the different centralised EU information systems. The proposal asserts that there is a problem of third-country nationals having multiple identities across the EU information systems that refer unlawfully to different people. The problem of multiple identities linked to the same set of biometric data across the different systems was also identified as a challenge in interviews carried out with various Member State level stakeholders. In this respect, the objective directly aims to resolve a need that persists due to the current architecture of the systems. The driver of this problem is said to be the fragmentation of the EU information systems, with the solution being to **connect them so that multiple identities linked to the same set of biometric data can easily be detected. Thus, the objective does not necessarily relate to the *interoperability* systems but rather to the *interconnectivity* of the information systems.**

The achievement of this objective is anticipated to improve accuracy and reliability of data across the EU systems for use by end-users; combat multiple identities, document and identity fraud by eliminating blind spots that result from incomplete information; and improve internal security. **However, the extent to which third-country nationals with multiple identities exist across the different information systems to justify this interoperability solution is not clearly articulated**. An estimate of third-country national multiple identity use appears in Annex 4 of the Impact Assessment in the section on the Summary of Costs and Benefits where it is stated that 'at least 500 000 third-country nationals use multiple identities for various reasons'.[158] The Commission's document states these to be 'very cautious estimates', but does not provide any reasoning as to how they arrived at this figure. The MID, supported by the CIR and the sBMS, is the proposed solution that has been designed to address the challenges of multiple identities across the EU information systems.

Objective 3 is aimed at facilitating **identity checks of third-country nationals** on the territory of a Member State. The proposals justify the objective by asserting the difficulties that competent authorities have in identifying a third-country national in the territory of a Member State who 'cannot or is not willing to present his/her passport, identity card or other identity document'.[159] The necessity of the objective is further justified in the proposal because Member States do not keep registers on third-country nationals present for a short stay, whereas such registers exist for nationals and residents. Failure to properly identify a person means that 'actions or decisions on that person may be misplaced or may not be possible, which is a major concern in the context of, inter alia, ensuring internal security, contributing to the prevention of irregular migration or respecting the right to asylum'.[160]

The proposals would allow competent authorities to query VIS, Eurodac, SIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN using the alphanumeric or biometric data of a third-country national. This is to aid identification of persons in the event of emergencies,

[158] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

[159] Ibid.

[160] Ibid.

for investigations into criminal activity that does not reach the threshold of serious crime,[161] or in other situations that are unrelated to migration management where national authorities cannot currently access the information systems to identify a third-country national on the territory.[162]

Presently, police are authorised to use biometric data to query the SIS for the purposes of identifying or verifying the identity of a third-country national on the territory of a Member State.[163] Furthermore, competent authorities are permitted to carry out checks within the territory for the purpose of verifying the identity of the visa holder and/or the authenticity of the visa and/or whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled.[164] To this end, as far as we have been able to ascertain, the Commission has not previously indicated a necessity to identify third-country nationals within the Schengen area, only referencing the need to establish 'specific provisions in relation to the intensity and frequency' of identity checks at internal borders.[165] It would have been helpful if the proposals were accompanied by **an analysis, or estimate, of the frequency with which successful or failed identifications of third-country nationals occur, and an assessment of the current identification procedures that are in place**, if any, in various Member States. In this regard, the proposals could have articulated more clearly why the existing capabilities for identity checks within the territory of the Member States are inadequate, and why there is a need to extend beyond the currently accessible databases to include, for example, Eurodac. Finally, it may not be appropriate to suggest such potentially far-reaching new powers in proposals on interoperability, as **the new checks are not just a question of improved interoperability between existing systems but add new purposes for use of the systems.** The ESP, sBMS and the CIR solutions put forward in the Commission's proposals will facilitate identification checks on the territory of a Member State.

Objective 4 is intended to facilitate and **streamline access by law enforcement authorities** to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism. This will necessitate amending the conditions and procedure of access for law enforcement to EU information systems. The current 'cascade' mechanism requires that designated Member State authorities first conduct a search of their national databases (and consult the fingerprint dataset with the Automated Fingerprint Databases of other Member States under the "Prüm" Decision, i.e. 'Prüm check', if they intend to access Eurodac and, in future, the EES) before they may be granted access to a central EU information system. The requesting authority must specify that the conditions explicitly prescribed in relation to each database are met when submitting a reasoned request to the verifying authority/central access point justifying the necessity of access for each individual system in the 'cascade'.

[161] 'Serious criminal offences' means offences that correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

[162] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

[163] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) Article 27.

[164] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). Article 19.

[165] Commission Recommendation of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area.

The proposals seek to introduce a two-step approach known as a 'hit-flag functionality' instead of the 'cascade' mechanism of access. For the purposes of preventing, investigating, detecting or prosecuting a serious crime and terrorism offence, **law enforcement would be able to query the information systems in parallel using biometric or biographical data and receive a notification, or 'hit-flag'**, indicating the presence or absence of data on a third-country national. The second step will permit full access to the data contained in the EU information systems, subject to the conditions and procedures laid down in the respective legislative instruments that govern such access.

In its April 2016 Communication,[166] the Commission acknowledged the need to optimise the existing tools for law enforcement purposes, without compromising data protection requirements. That is, the current 'cascade' mechanism was designed as such to limit undue access to systems and fulfil data protection obligations. The justification for the proposal of streamlined access rights through a first check on all systems at once is the 'considerable amount of administrative burden' that the 'cascade' mechanism causes. Access by law enforcement to non-law enforcement information systems is thus presented as a prohibitive process that may cause 'delays' and 'increases the data flow potentially leading to data security risks'.[167] Furthermore, the 'cascade' requires that the designated authority must end its query once information is found in one system. However, this does not mean that the next or even a later system would not contain valuable information for the purposes of their investigation. The difficulty of law enforcement agencies' access to non-law enforcement databases that they are legally permitted to access was also highlighted during interviews with various Member State level stakeholders. In France for instance, law enforcement authorities only request data from Eurodac 'a few dozen times per year', given the operational difficulties in using the 'cascade' mechanism.

Interestingly, the results of the survey conducted as part of the most recent VIS evaluation indicated that 'all the responding Member States consider that the central access point is easily accessible for the designated authorities', and, of the few respondents that provided general comments, '[t]hree Member States reported that the access procedure is adequate or sufficient', while '[o]ne Member State considered that the conditions for access are set at a high level, which prohibits the use of VIS to prevent, investigate or detect less serious offences'. The 2016 VIS Evaluation states that 18 of the 26 eligible Member States accessed VIS for law enforcement purposes and that use of the system was low, and ultimately could not conclude whether this was due to its recent availability to law enforcement, the potentially prohibitive access conditions or the limited efficacy in this regard.[168]

Eu-LISA's annual report on the 2016 activities of Eurodac[169] noted that 326 print and latent-print searches were performed by seven Member States for the purpose of prevention, investigation, detection or prosecution of terrorism and other serious criminal offences. This low number of law enforcement searches in Eurodac perhaps indicates that demand for access to Eurodac is low and that there is no necessity for streamlined law enforcement access; alternatively, it could be an indication that the burden for access to this system is

[166] Communication from the Commission to the European Parliament and the Council. Stronger and Smarter Information Systems for Borders and Security. 6.4.2016.

[167] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

[168] The VIS Law Enforcement Access (LEA) Decision (Council Decision 2008/633/JHA of 23 June 2008) became applicable in September 2013 and by December 2015 (the end of the reporting period) most of the 16 Member States that had used the VIS for law enforcement purposes had only been doing so for a few months according to the 2016 VIS Evaluation. In this context, the VIS evaluation should be interpreted cautiously.

[169] Annual report on the 2016 activities of the Eurodac central system, including its technical functioning and security pursuant to Article 40(1) of Regulation (EU) No 603/2013.

presently too high. Streamlined law enforcement access is to be facilitated by the CIR and sBMS interoperability solutions.

Article 2(1) of the proposal describes the high-level general objectives, as enshrined in the Treaty, which include:

a) to improve the management of the external borders;

b) to contribute to preventing and combating irregular migration;

c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States;

d) to improve the implementation of the common visa policy; and

e) to assist in examining applications for international protection.

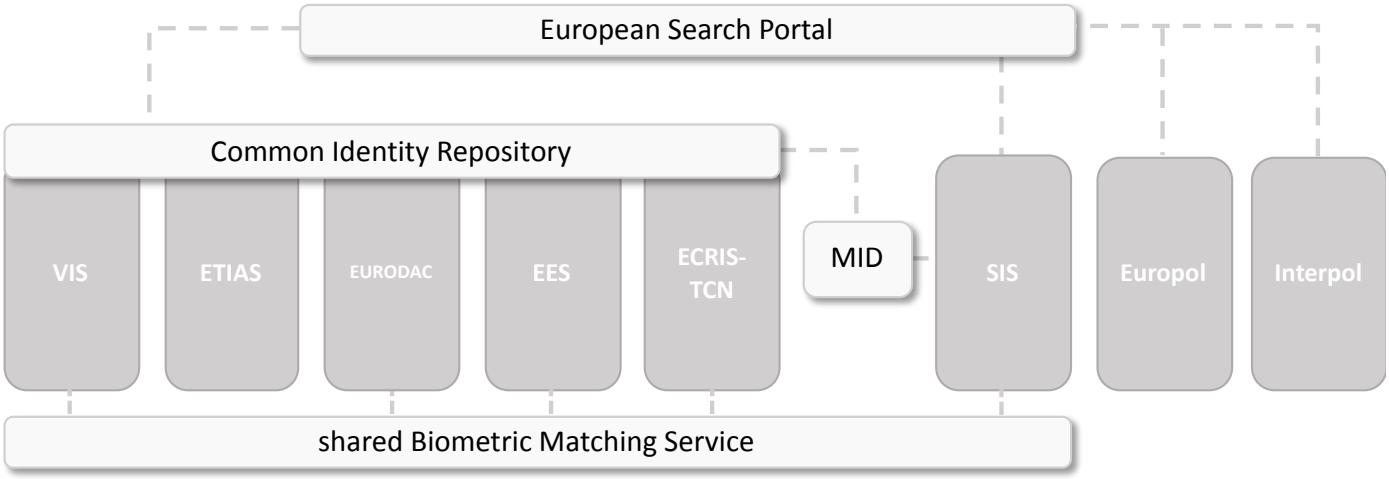
These objectives **directly mirror the purposes of the underlying systems** covered by the interoperability proposal and again **demonstrate how the objectives of the proposal conflate border management, applications for international protection and the maintenance of internal security.** Each underlying system aligned to the above purposes was created with specific limits but instead Article 2(1) merges these distinct purposes under the auspices of interoperability. The wide scope of the objectives as laid out in Article 2(1) is problematic because they allow elements to be introduced into the proposal that do not necessarily relate to interoperability. This is reflected in the generalised reasoning of the Commission which anticipates that 'interoperability' will improve border management, improve internal security and even improve public trust, without providing clear causal links and sufficient evidence for these claims.[170]

[170] Interoperability between EU information systems for security, border and migration management (2018). European Parliamentary Research Service.

3.2.3. Proposed solutions

This section details the proposed solutions for establishing interoperability, as presented in the Commission's proposals. Figure 7 illustrates how the four solutions relate to the existing JHA information system architecture.

Figure 7: Overview of the proposed solutions for interoperability



European Search Portal (ESP)

The European Search Portal is intended to serve as 'message broker' for the end-user that would enable the simultaneous query of multiple systems[171] using both biographical and biometric identity data. The solution would enable 'fast, seamless, efficient, systematic and controlled access to all information that they need to perform their tasks' and would only retrieve the information that corresponded to the legal access rights of a specific user. This **fulfils a direct definition of interoperability** whereby the end-user is not necessarily granted additional access rights, and there is no requirement for an aggregation of data and no requirement for the creation of additional systems or databases. Operational efficiency, which is at the core of IT interoperability,[172] can be achieved via provision of a single point of access that would grant automatic access without the requirement to request data, with the added potential of creating harmonisation across the EU. One of the current challenges highlighted in eu-LISA's most recent Eurodac report is the perceived lack of trust between Member States, leading to delays and low transfer rates. The systemisation of processes may help to engender trust across Member States, leading to improved operational efficiencies.

The proposals lay out provision for eu-LISA to **create the access profiles for each category of user**, and it should be made clear that **access rights should be granted in accordance with the access rights provided for by the respective legal instruments that govern the underlying systems**. Further, in line with the commitment outlined in the proposals to adhere to data integrity best practices, the introduction of a system that automatically tracks the modification (and potential manipulation) of any data transactions would be welcome. In addition to the proposed logging of access, a qualified electronic timestamp could be incorporated into these interoperability proposals to enhance trust and ensure data integrity such that it has legal effect as outlined in Article 41 of the eiDAS

[171] Central-SIS, Eurodac, VIS, the future EES, and the proposed ETIAS and ECRIS-TCN systems, as well as the relevant Interpol systems and Europol data.

[172] 'The aim of the IT interoperability framework is to increase public sector efficiency in Estonia by improving the quality of services provided to citizens and enterprises both at the Estonian and the EU level.'

Regulation.[173] A qualified electronic timestamp would enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

Shared Biometric Matching Service (sBMS)

The shared Biometric Matching Service would enable the searching of biometric data (fingerprints and facial images) from the centralised EU information systems.[174] Whereas at present each existing central system has its own dedicated, proprietary search engine for biometric data, the shared biometric matching service would provide a common platform that **permits simultaneous searching of the databases, thus improving the technical and operational efficiency of performing searches**. The proposals indicate that the biometric data are exclusively retained by the underlying systems and the sBMS would create and store a mathematical representation of the samples (i.e. templates). The Commission asserts that the sBMS will support the role of the CIR and the MID, and by doing so will provide a solution to detect and combat identity fraud but also to prevent situations in which bona fide persons are mistaken for others. **Thus, the sBMS solution contributes to the realisation of all four operational objectives outlined in the proposals.**

Article 12(1) of the proposal states that the sBMS will be 'storing biometric templates'[175] – implying the creation of a new database – that will be used to query the existing biometric data of the underlying systems (the CIR). If this is the case, it should be clearly articulated in the proposal, as the concept of interoperability should not be confused with the setting up of additional systems aggregating data in existing compartmentalised systems. There is further contention regarding whether the storage of biometric templates constitutes the storage of personal data (see Box 6). Despite this, the sBMS appears to be a component that *facilitates* direct interoperability of the systems. There appears to be value in the sBMS even independent of the other proposed solutions for improving the workflows of end-users that use these systems, whereby they will have the provision to biometrically cross-reference necessary information in different databases for the effectively fulfilment of their duties. It is foreseen that identity checks made on the territory of a Member State will make use of the data stored in in the sBMS; however, **the proposals could be more explicit with regard to which authorities and in which other contexts the sBMS will be utilised**.

As previously discussed, one of the key challenges in the current centralised systems is the substandard quality of data that is input. The proposals highlight that the successful implementation of the sBMS is predicated on 'appropriate data quality standards' being in place.[176] This is to avoid the risk of a higher rate of false positive errors in the event of inadequate implementation of data quality standards. Indeed, it is the minimum requirements of fingerprint quality that will determine whether the data quality across the systems will improve, rather than interoperability by itself. In view of the data quality challenges identified by the Commission in relation to VIS and SIS II and the possibility that low-quality fingerprints will be collected when visa-exempt nationals are registered in the EES, the possibility of false matches undermining the effectiveness of interoperability is high.

---

[173] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[174] SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN system.

[175] Proposal for a Regulation of the European Parliament and of the council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

[176] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

The operational and technical challenges underpinning the existing and forthcoming systems should be addressed before or alongside the deployment of interoperability solutions.

Considering this minimum requirement, it should also be borne in mind that lesser-quality data, including fingerprints, input into SIS can be necessary for police to effectively conduct their investigations. One Member State highlighted that there will be technical difficulties in creating a universal matching service that can accurately compare across the different types of fingerprint data, given that there are different starting points of the fingerprint data depending on the different systems (i.e. 4 flat for VIS, 10 rolled for Eurodac, latent fingerprints in SIS).

Finally, the proposals should provide more **clarity on whether facial templates will also be included** in the shared Biometric Matching Service.

Box 6: Conclusions on biometric templates as personal data

The **categorisation of biometric templates**, such as the mathematical representations discussed in the Commission's interoperability proposals, has been the subject of much debate in the EU academic and policy community over the past 10–15 years.

A range of Dutch authors, for instance, concluded that under certain conditions a template of biometric data should not be considered personal data, stating that 'on the basis of a template alone, a person is not identified or identifiable'[177] because finding the person based on the template would require unreasonable effort.

Other academics have suggested that such templates do in fact constitute personal data. Kindt,[178] for instance, argues this point, concluding that biometric templates are personal data and 'need as much protection as [captured biometric] samples'[179]. In reaching this conclusion, Kindt conducted an extensive analysis of the Article 29 Working Party opinions on the topic.

In its 2003 document on biometrics,[180] the Article 29 Working Party states that 'measures of biometric identification or their digital translation in a template form [are] in most cases […] personal data',[181] However, the document further stated that it was also possible for templates not to be considered as personal data.

In 2011, the EDPS gave an opinion on the EU project 'TrUsted Revocable Biometric IdeNtitiEs' (Turbine) and stated that pseudonymisation of biometric data via the creation of 'encrypted irreversible derivatives' (i.e. biological templates) enhances the protection of an individual because it is considered technically impossible to derive the biometric identity from the template.[182] The EDPS went on to state that

> 'although the biometric identity (or template) could not independently lead to disclosure of information relating to a person, it may nevertheless lead to the identification of this person within the framework of the biometric system operation (e.g. during access control) in combination with other personal data kept in the system for the same person (e.g. full name). In this sense, the biometric identity [as it is produced and used by the Turbine project] also constitutes personal data'.[183]

Article 9(2) of The European Data Protection Regulation permits the processing of personal data if

> 'processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and

[177] Van Kralingen, R., Prins, C and Grijpink, J. (1997) *Het lichaam als sleutel. Juridische beschouwingen over biometrie*, Alphen aan den Rijn/Diegem, Samson BedrijfsInformatie Bv, pp. 31–33.

[178] Kindt, E. J. (2013) *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. pp. 94–100.

[179] Ibid, p. 99.

[180] Article 29 Data Protection Working Party (2003) Working Document on Biometrics, WP80, 1 August 2003.

[181] Ibid.

[182] Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development – Turbine (TrUsted Revocable Biometric IdeNtitiEs). 1 February 2011, p. 4.

[183] Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development – Turbine (TrUsted Revocable Biometric IdeNtitiEs). 1 February 2011, p. 5.

specific measures to safeguard the fundamental rights and the interests of the data subject'.[184]

In the light of the ambiguity regarding the nature of templates, it is all the more problematic that the sBMS will store them, as this essentially constitutes processing of personal data, thus bringing into scope the protective principles of data protection and the fundamental rights limitations in processing personal data as articulated by the Strasbourg and Luxembourg Courts.

[184] General Data Protection Regulation (GDPR)

Common Identity Repository (CIR)

The Common Identity Repository will be a shared component of biographical and biometric identity data and provide a unified view of third-country nationals recorded in Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system. The data in this system will contain the biographical data,[185] travel document number, fingerprints and facial image that are originally contained in the underlying systems.

Article 17(1) states that CIR is established for the purposes of:

- facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system]
- supporting the functioning of the multiple-identity detector
- facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime.

The explanatory memorandum of the proposal states that '[t]he establishment of the CIR is necessary to enable effective identity checks of third-country nationals, including on the territory of a Member State',[186] and the impact assessment goes a step further and states that 'the key objective of the common identity repository is to enable the correct identification of a third-country national present in the territory of the Member States regardless of the identity and the central system used'[187]. The CIR is also anticipated to support the streamlining of access by law enforcement to non-law enforcement systems by making it possible to query the identity data of all the underlying systems simultaneous as part of the 'hit-flag functionality'. **Thus, the CIR solution contributes to the realisation of all four operational objectives outlined in the proposals.**

As previously stated, the extent to which the identification of third-country nationals presently represents a challenge to Member State authorities in the territory of the Member States is not addressed within the proposal or the accompanying impact assessments. Nor is there an indication of the current procedures in Member States if an EU citizen or third-country national refuses to identify themselves. Instead, it is stated that 'Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for third-country nationals'. The proposals do not elaborate on this challenge, even though it is deemed to be a 'key objective'. Without this information clearly presented it is difficult to conclude whether the creation of a large-scale repository that includes basic identity data of essentially all third-country nationals within the scope of databases is proportionate for the stated objective of identifying individuals.

The use of the CIR for the correct identification of a person by competent authorities would require changes to the ancillary purposes of Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS. This would necessitate re-architecture/re-design of the underlying databases to create a primary function in pursuit of fulfilling secondary objectives. The EDPS reflection paper noted that the underlying information systems had been built for

[185] Last name, first name, gender, date of birth.

[186] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, p. 7.

[187] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, p. 21.

purposes other than combating identity fraud and highlighted that the new use facilitated by the CIR would run the 'risk of "function creep" (i.e. a widening of the use of a system or a database beyond the purpose(s) for which it was originally intended)'.[188] That means, for example, that the data in Eurodac collected to assist in examining applications for international protection will also be used to perform identity checks on the territory of the Member States. As already highlighted, there appears to be a convergence of the ancillary purposes of the current JHA systems towards the facilitation of law enforcement functions, and the purposing of the CIR for identity checks on the territory of Member States can be perceived as a continuation of this trend.

Small-scale surveys commissioned by the Fundamental Rights Agency engaging officers at consulates and border crossing points suggest that inaccurate/incorrect/out of date personal data in Eurodac, VIS and SIS II is 'sometimes' encountered.[189] Highlighted factors that can affect the reliability of the alphanumeric data in a given system included cases where documents are not provided by a person, incorrect transcription of names into the Latin alphabet and increased workload of staff inputting the data. In this regard, the CIR, as part of supporting the correct identity verification of individuals with the MID, may represent an effective tool for reducing data errors within the systems as automatic comparisons between databases can assist with the systematic identification of data errors. However, interoperable systems can also have the effect of multiplying the negative effects of inaccurate data of bona fide persons.

In a similar same-small scale survey, approximately half of the border guards reported that they had experienced a case in which the fingerprints of an individual were not found in VIS, although the data should already have been in the system.[190] Data quality errors such as these imply that the current systems have some inherent important challenges that the Commission's interoperability proposals will not necessarily address. As a result, further training and stricter data input/quality processes and protocols will be just as important as interoperability solutions in addressing the challenges faced by end-users of the current and proposed EU information systems.

Critically, the **proposals are lacking clarity as to how the CIR will function technically**. The proposal explicitly states that the CIR is not a new database, but rather a shared technical component between all the systems that would store and search the biographical data across all the central systems. However, the use of terms such as 'store' and 'storage' throughout the proposal and the accompanying impact assessment implies the creation of a new database that will store the data of all third-country nationals.[191] In a section on the compatibility with previous initiatives with regard to how the solutions were developed, the proposal states, '[i]t became clear afterwards a distinction had to be made between the CIR as the database of identities and a new component that identifies multiple identities linked to a same biometric identifier (MID)'.

This may have been simply a semantic error, but confusion could be avoided if there was greater clarity on the technical functionality of the CIR. What is clear is that the CIR will have 'database-like' functionality that will permit querying of the identity data of all third-country

[188] EDPS (2017) Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice.

[189] Fundamental rights and the interoperability of EU information systems: borders and security (2017). Fundamental Rights Agency.

[190] Fundamental rights and the interoperability of EU information systems: borders and security (2017). Fundamental Rights Agency.

[191] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, p. 29.

nationals within the underlying systems. The outcome of accessibility to identity data of third-country nationals would be the same. This would not be, to our understanding, consistent with the *direct definition* of interoperability, but instead would represent a restructuring of the technical architecture to facilitate checks on third-country nationals. **The restructuring creates a conflation of the specific purposes of the different systems and leads to their convergence under the auspices of security**. The CIR would, in effect, create a new system from existing systems and appropriate the data from each system for alternative purposes; that is, identification of third-country nationals on the territory of Member States, identification of individuals with multiple identities, and streamlined law enforcement access. Finally, the CIR will include data of individuals that are linked to criminal behaviour or illegal border crossing, as well as bona fide persons (included in Eurodac and VIS). It should be explained that interoperability will not lead to the mixing up of these categories. The logical separation of the different categories of data subjects is critical for the fulfilment of the legal purposes of the underlying Regulations.[192]

If indeed it is the intention of the Commission to have the basic biographical and biometric data of almost all categories of third-country nationals stored within one system and to make them available for a variety of purposes under the 'umbrella purpose' of preserving EU internal security, this should be explicitly stated, justified and argued rather than bypassing the compartmentalised approach to databases through interoperability. With the establishment of the CIR, the proposal seems to create a catalogue of a wide range of third-country nationals irrespective of the legitimacy of the reasons behind their initial registration in a system.

Multiple-Identity Detector (MID)

The multiple-identity detector would check whether the queried identity data exists in the information systems included in the CIR and SIS, and then create and store links between the data. It is said to have a dual purpose of 'facilitating identity checks for bona fide travellers and combating identity fraud'. As outlined in Article 27(1) the MID will be launched automatically when:

- an individual file is created or updated in EES;
- an application file is created or updated in VIS;
- an application file is created or updated in ETIAS;
- an alert on a person is created or updated in the SIS.

Automatic verification using the MID will result in a no-hit if the data does not match with data already in the underlying databases covered by the CIR or SIS. If there are similarities between the identity data across the different systems, the MID will create links that will be stored in an identity confirmation file. A white link will indicate that the identity data in another system corresponds legitimately to the same person in another information system. A yellow link will be created when linked data share the same biometric data but different identity data or when the identity data is similar but not similar enough to be classified as a white link.

Yellow links are then to be manually verified and access to the identity confirmation file with references to the underlying systems that contains linked identities is proposed to be granted to:

[192] CM1802 Comments (2018) on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM (2017) 794. Meijers Committee.

- border authorities when creating or updating an individual file in EES;
- competent authorities creating or updating an application file in the VIS;
- the ETIAS Central Unit and the ETIAS National Units when carrying out a manual assessment;
- SIRENE Bureau of a Member State when creating an alert in accordance with SIS II border checks.

Users are to manually verify links, designating them white to indicate that the linked identities refer to the same person legally; green indicating that linked data refers to legally distinct persons; or red which indicates that the identity data refers unlawfully to the same person and is to be followed up according to national law or EU law.

Although the problem of fragmented EU information architecture was identified by the HLEG as being a driver in the multiple identities that may be present across the JHA information systems, the MID solution was not designed by the HLEG and was not identified in prior documentation.[193] It is justified as the only possible solution for addressing multiple identities between the CIR and SIS due to the technical complexity of migrating third-country national biographical data from SIS into the CIR. Thus, the MID is seen as a solution to link the identity data in SIS to the identity data in the CIR.

An identified gap in the current structure of the JHA systems is the inability to detect multiple identities. **The proposed MID solution (together with the CIR and sBMS) would directly meet the stated objective of detecting multiple identities across the different systems linked to the same biometric data.** In doing so, there is the possibility that the end-users involved with border and migration management will be better equipped to perform their tasks, given that there would be a systemised mechanism for detecting multiple identities that arise as a result of data input errors or identity fraud.

As previously mentioned, the proposals do not explore in depth the extent of the problem of multiple identities, due to data errors or identity fraud, across the various systems. The MID will introduce new processing of data and also **new types of data** with the creation of coloured links between identities. The proposals also envisage new access rights granted to authorities that are to manually verify newly linked identities, but it is difficult to assess the necessity or proportionality of the proposed changes without further indications of the scale of the problem.

Member State interviews highlighted challenges for the automatic procedures that determine whether identity data can be considered identical or similar (which are to be developed in accordance with Article 28(5)), as well as the significant training that will be required for all staff responsible for verifications. In this regard, the proposals do not provide sufficient clarity for manual identification processes which need be clearly articulated (e.g. the exact procedure after a red link has been created).

The proposals expect that those responsible for the manual verification of identities will be those at the second line for border management and visa applications. This could conceivably cause delays in the processing of visa applications and at external borders if the verification period takes more time than anticipated. SIRENE Bureaux of Member States are already having to 'prioritise workloads and disregard the mandatory 12-hour response time [for

[193] Commission Staff Working Document. Impact Assessment, Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, p. 23.

exchange of requested supplementary information], which has brought several SIRENE Bureaux to the limits of efficient operation', according to the SIS II evaluation.[194] It would have to be ensured that the verifications workload was not in excess of the resource that the bureaux have at their disposable. It is also currently unclear whether the information contained in a given identify confirmation file, namely the identity data of all linked persons, will be sufficient to resolve yellow links.

Law enforcement access to non-law enforcement databases

Article 22 of the proposal sets forth the conditions for streamlined law enforcement access to the EU non-law enforcement databases for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences.

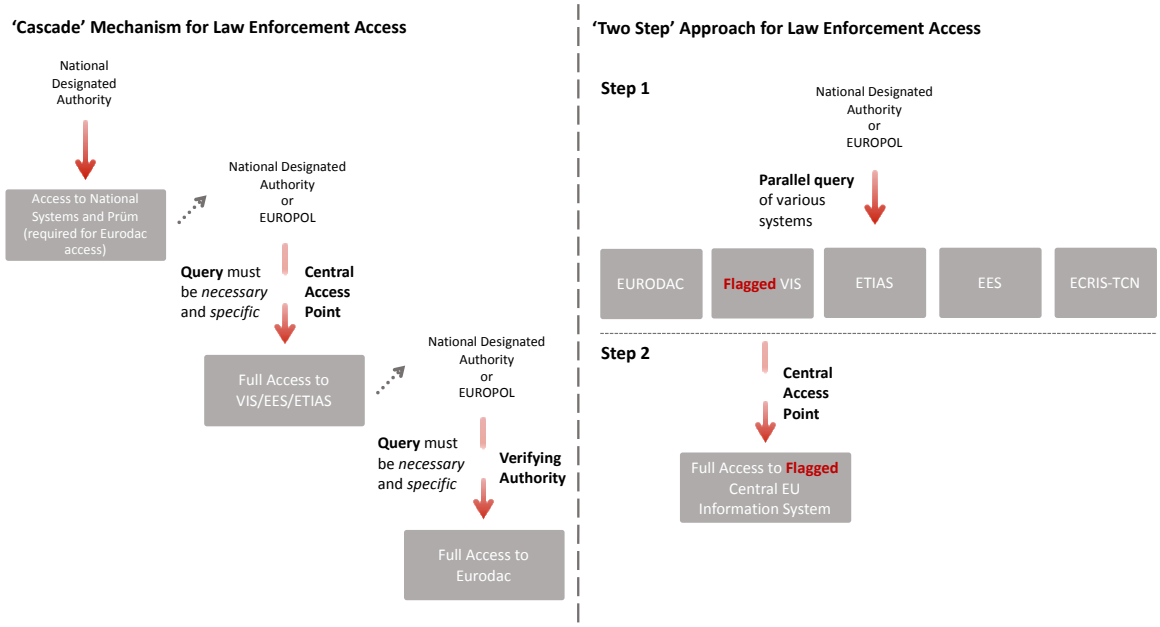
In the first step, law enforcement agencies would be able to query the CIR and obtain a reply in the form of a reference indicating which of the information systems contains data that matches the search query (referred to as the hit-flag). In the second step, to obtain full access to the data contained in the relevant EU information system, the same conditions and procedures laid down in the respective legislative instruments governing the rights to such access would apply (i.e. justification of necessity and specificity).

This proposed 'two-step' approach involves new data processing (hit/no-hit) and a significant change in the conditions of access to personal data. The flagging after a hit would reveal previously unknown information about an individual (e.g. that the individual is a Schengen visa holder or has applied for international protection). It would facilitate the bypassing of the measures that systemise necessity and grant rights to new information, where **the existence of a 'hit' or 'no-hit' is a finding in itself,** without the requirement for fulfilment of conditions of access at initial step. **In this respect the solution links directly to the objective of providing streamlined access by law enforcement to non-law enforcement databases,** where the current 'cascade' mechanism has been described as causing too great an 'administrative burden'.[195] In light of the new access rights, the proposals could provide further clarity as to whether intelligence services are included within the definition of designated authorities, and under what circumstances this functionality would be granted.

[194] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) Article 27.

[195] Impact Assessment accompanying the Proposals for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems.

Figure 8: Existing and proposed mechanisms for law enforcement access



The keeping of logs that identify the user is intended to ensure that new access rights are not used improperly. However, in light of the proposed relaxation of rules governing *ex-ante* authorisation to new information on an individual, it is worth reviewing the current access processes. The 'cascade' mechanism of access was designed as a safeguard for the protection of personal data. Further, the attribution of designated authorities and central access points, in the context of VIS, was designed as an additional data protection safeguard. In a survey conducted during the VIS evaluation, only 16 of the 19 responding countries had designated a central access point. Only 14 of them indicated that they had designated the relevant competent authorities. Furthermore, two of the responding countries, one of which was a regular user of VIS data for law enforcement purposes, stated that the relevant authorities had not been designated, as is required by the VIS Decision. This demonstrates that perhaps the current data protection safeguards are not sufficiently robust. **An adoption of the 'two-step approach' could arguably lead to a further reduction of data protection safeguards if it is not well designed and possible safeguards are not properly applied**.

It is worth noting that in the same reporting period Member States only initiated 52 urgent requests (there were a total of 26,629 requests) whereby VIS central access points are able to process a request immediately under Article 4(2) of the Decision. All of these were justified by the *ex-post* verification, perhaps suggesting that law enforcement agencies currently have adequate capability to access at least the VIS rapidly with the existing access mechanisms.

In any case, even the current conditions of law enforcement access to VIS and Eurodac (and consequently the EES and ETIAS) raise concerns as regards their compatibility with the pronouncements of the CJEU in the *Digital Rights Ireland* and *Watson* judgments requiring that access should be authorised:

> 'by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned

request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions'.[196]

As a result, it is arguable that this new streamlined approach of law enforcement access through interoperability raises even more proportionality concerns, as it shows blunt disregard of the case law of the CJEU.

Identity checks

Identity checks have also been suggested as a means to combat identity fraud within Member States' territory by eliminating obstacles to identity verification by competent authorities. However, under the current proposals the MID would not be launched during identity checks. This raises the question whether an identifying officer will be presented with all the identities linked to an individual. Further, even with a new system in place that is capable of identifying individuals using their biometrics, refuse to identify themselves, in a similar way as with the situations which are given as the apparent justification for the proposed solution. It would be helpful if more clarity could be provided with regard to the procedures and practical implications of such scenarios.

Additional components

The Commission also outlined additional supporting components for interoperability:

- **Universal Message Format (UMF)** – establishes a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home Affairs.
- **Central Repository for Reporting and Statistics (CRRS)** – established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes managed by eu-LISA.
- **Automated data quality control** – automated data quality control mechanisms and common data quality indicators developed by eu-LISA.

The Commission has not provided many details on these additional components, but they appear to directly address the challenges that are faced by end-users of the current systems, namely with regard to data quality. Both the UMF and the data quality proposals will be critical for the successful introduction of interoperability solutions, as the proposals suggest. The minimum data quality standards for EU information systems should carefully consider the requirements of SIS, where data are sometimes expected to be of a lower quality as an investigation is initiated. The CRRS proposal is welcomed as there is value in monitoring the overall functioning of the EU information systems. As outlined in the proposals, particular care must be taken to ensure that all data are anonymised.

[196] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Ireland* (08.04.2014) para 62.

Table 4: Summary table: Objectives and solutions in the context of interoperability

	Direct Interoperability?	Additional Purposes?	Additional Access Rights?
Objectives			
Fast, seamless, systematic and controlled access for end-users to perform their tasks	Yes, consistent with a direct definition of interoperability whereby controlled access to relevant systems will provide operational efficiencies.	None required.	Does not require granting of additional access rights. Technical configuration proposed to only permit access to data that users already have access to.
Detection of multiple identities	Proposed new capability as a result of interoperability/ interconnection of information systems.	Requires changes to the purposes of the underlying databases.	Verifying authorities to be granted access rights to identification data of third-country nationals.
Identity checks on third-country nationals	Proposed new capability as a result of interoperability/ interconnection of information systems.	Requires changes to the purposes of the underlying databases.	Access to SIS is currently permitted for the purposes of identity checks on third-country nationals. Access to VIS is currently permitted to identify/verify visa holders on the territory. Upon fulfilment of conditions, access rights to identity data of all underlying systems will be extended to designated competent authorities.[197]
Streamlined access by law enforcement authorities to non-law enforcement information systems at EU level	Proposed new capability as a result of interoperability/ interconnection of information systems.	No changes required. Secondary purpose of law enforcement access already present in legislation of underlying systems (except SIS where LEA is covered by primary purpose).	Hit-flag functionality will permit law enforcement knowledge of whether data of individual is present in a specific underlying database without the requirement to demonstrate necessity or specificity of the query (i.e. a change in the conditions of access).

[197] Directive 2016/680 Article 3(7) 'competent authority' means:(a) any public authority competent for 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; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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).

	Direct Interoperability?	Additional Purposes?	Additional Access Rights?
Solutions			
European Search Portal	Yes. Interoperable systems will permit end-users to send simultaneous queries and receive data from various information systems into a single user interface.	No changes required to the purposes of the underlying systems.	No additional access rights.
Shared Biometric Matching System	Facilitates interconnection/interoperability of the systems. Will provide a common platform that permits standardised communication of the centralised systems, thus improving technical and operational efficiency of searches.	Requires changes to the purposes of the underlying databases to facilitate use of biometrics for identification/verification of individuals on the territory of a Member State.	A biometric match after identity query on the territory of the Member State would grant the competent officer access to the identity data of a third-country national present in the CIR.
Common Identity Repository	Consolidation of all identity data across the systems; logically separated repository not necessarily consistent with direct interoperability.	Will require the purposes of all the underlying systems to include identification and identity verification of third-country nationals.	Access rights granted to competent authorities conducting identity check.
Multiple Identity Detector	Not direct interoperability. Will be a new component that connects CIR with SIS II to process identity data and create new types of data (i.e. coloured links).	The ancillary objectives of the underlying systems may have to be adapted to permit data to be used for identity verification purposes.	Verifying authorities to be granted access to rights to identification data. Access rights granted to authorities investigating red links.
Universal Message Format	Assists with the implementation of standardised information exchange between systems, facilitating effective interoperability of the systems.	n/a	n/a
Automated Data Quality Control	Not related to interoperability.	n/a	n/a
Central Repository for Reporting and Statistics	Not related to interoperability.	n/a	n/a

3.3. Proposals for interoperability: Implications

Building on the details of the proposals, this section discusses the implications of the legislative proposals. Firstly, it presents the implementation implications (section 3.3.1), covering the cost implications and cost-efficiency calculations, the timelines proposed for implementation, implementation at the Member State level and the roles and responsibilities of eu-LISA. Section 3.3.2 discusses the fundamental rights, data protection and data security implications of the proposals.

3.3.1. Implementation implications

Considering the complex policy and legislative environment surrounding the EU's JHA information systems, the proposals for interoperability require clarity of focus with regard to their implementation. This section examines the proposals for the implementation of interoperability, including the assessments of the costs and cost-efficiency of the proposals, the timelines and roll-out plans, the Member State level implementation and the roles and responsibilities of eu-LISA.

Costs and cost-efficiency

The costs of implementation are to fall to the EU budget and the Member State authorities operating the information systems. The costs of implementation are discussed in Box 7, then the economic impacts and cost-benefit analyses presented in the impact assessment are detailed.

Box 7: Interoperability proposals: Budgetary implications

As detailed in section 4 of the Commission's proposals, the **budgetary implications** cover both the current Multiannual Financial Framework (until 2020) and the subsequent seven years (2021–2027). The proposals foresee budgetary allocations of EUR 424.7 million over nine years for the:

i. development, integration, maintenance and operation of the four interoperability components and the CRRS by eu-LISA;

ii. data migration to the sBMS and the CIR;

iii. update of the national uniform interface (NUI) by eu-LISA;

iv. integration of Member State national systems with the NUI; and

v. training on the use of interoperability components by end-users.

The allocations by stakeholder, as presented in the proposals (pp. 20–21), are shown below:

Stakeholder	Budgetary allocation by activity
eu-LISA	**EUR 225.0 million** • EUR 68.3 million for delivery of the five interoperability components (incl. CRRS) • EUR 56.1 million for maintenance to 2027 • EUR 25 million for sBMS data migration and NUI elements • EUR 18.7 million for upgrading and operating ECRIS-TCN in high-availability mode (from 2022)
Member States	**EUR 136.3 million** for changes to national systems and end-user training
Europol	**EUR 48.9 million** for upgrading Europol's IT systems
Frontex	**EUR 4.8 million** for a specialist 1-year MID link verification team
CEPOL	**EUR 2.0 million** for preparation and delivery of training
DG HOME	**EUR 7.7 million** for staff and costs related to the development period and the additional tasks related to the UMF
Total	**EUR 424.7 million**

As can be seen from the table in Box 7, section 4 of the proposals does not fully disaggregate the allocations across any of the stakeholder groups. For instance, the proposal only details how EUR 168.1 million of the EUR 225 million allocated to eu-LISA is to be spent. Furthermore, the Legislative Financial Statement does not clearly explain the full eu-LISA allocation. Section 3.2.2.4 details the appropriations highlighted in the above table plus additional figures of: EUR 3.502 million for meetings; EUR 1.01 million for updates to the NUI; and EUR 1.735 million for updates related to increased network traffic. Subsequently, section 3.2.3.4 explains the appropriations for human resources (EUR 48.344 million). However, this leaves EUR 2.348 million of the overall figure unspecified. This figure is similar to the amount apportioned under title 2, which covers 'additional office space for the temporary hosting of the contractor teams in charge of the development, maintenance and operations tasks', but does not match exactly and is not specifically labelled.

Furthermore, as they are presented from different perspectives, it is not possible to evaluate the links between the appropriations discussed in the Legislative Financial Statement and the costs of the interoperability solutions, as detailed in the impact assessment (section 7.3.1 and Annex 4).

With regard to the **economic impacts** of the proposals, the impact assessment concludes that they will positively impact tourism, airports, seaports and carriers, driven by the assumed contributions of the proposals to: i) improving the security of the EU; and ii) speeding up border control processes. As discussed in section 3.2 of this report, the causal link between the interoperability proposals and increased security 'appears to lack more concrete explanations and evidence',[198] bringing into question the contribution of the first point to positive economic impacts in these areas.

Furthermore, the second positive impact is based on the assumption that the verification of individuals via CIR and MID would minimise disruption for legitimate travellers with bona fide or resolved multiple identities. However, the proposals present no indications or evidence on the extent to which legitimate travellers have multiple identities. It is clear that such travellers would be positively impacted (following the resolution or acceptance of their multiple identities). What is not clear is the scale of this positive impact. This is particularly challenging in light of the existing data quality issues experienced by certain databases (e.g. SIS II and VIS), as stated above.

Additionally, it is not considered that the additional collection and storage of information on third-country nationals, if perceived as excessive by those individuals, may have a negative impact on tourism.

Regarding the **cost-benefit analyses**, the main text of the impact assessment lacks clarity on a few key elements and the presentation of both the cost and benefit calculations faces a number of challenges. Most importantly, clarity could be improved by including the assumptions on which the calculations are based and the confidence margins of the calculations in the main text – at present, they are only found in Annex 4 of the impact assessment. Furthermore, the costs to the Member States and Europol have been grouped with no explanation as to why this presentation choice has been made.

Considering the costings, first, it is noted that they rely strongly on the results of the technical feasibility studies, which, at the time of writing, have not all been fully published, thereby limiting this study's ability to comment. Second, the costings are determined on the basis of 'a lot of approximations'[199] and, third, clarity is required on the discussions on the confidence

[198] European Parliamentary Research Service (EPRS) (2018) Interoperability between EU information systems for security, border and migration management. Briefing: Initial Appraisal of a European Commission Impact Assessment.

[199] Impact assessment, pp. 15, 17.

of the analysis in the cost estimates. At present, the terminology used – 'confidence margin' – appears to conflate the concepts of confidence intervals and margins of error. Considering the first concept (confidence intervals), the Commission is stating that they are 20–25% confident that their estimates are correct; under the second concept (margins of error), the Commission is stating that the costs could be up to 25% higher or lower than the estimate presented. It is likely that the latter is the intended concept, but clarification is required.

Considering a margin of error of 20–25%, the costs determined as EUR 169.8 million could, in reality, be as little as EUR 127.35 million or as much as EUR 212.25 million.

The benefits face similar challenges with precision and accuracy, with the impact assessment again recognising that the figures are the result of 'a lot of approximations'.[200] Further clarity is also required on the following issues:

- **Evidence supporting assumptions:** in the case of the assumptions regarding: i) the number of training sessions per person per annum[201] and ii) the number of multiple identities in existence across the information systems,[202] the supporting evidence is not transparently cited. It is therefore not possible to validate these assumptions and place reliance on them,
- **Saved cost of identification of multiple identities:** the impact assessment estimates that the 'systematic identification of multiple identities'[203] will deliver EUR 50 million in savings per year. The basis for this estimate is another estimate – that 500 000 third-country nationals in SIS, VIS and Eurodac are using multiple identities. This statement, considering the challenges detailed above, presents significant limitations in terms of its accuracy and precision. Using this figure, the saving estimate is generated by comparing a baseline scenario to the foreseen situation following the implementation of the interoperability solutions. However, the activities assumed in the baseline scenario are not evidenced, leading to a potentially unrealistic saving estimate. Firstly, the accuracy and the precision of the estimated number of multiple identities, as highlighted above, lacks concrete evidence. Secondly, the baseline scenario assumes that, every year, 500 000 multiple identity cases are detected and handled. However, no evidence of this caseload has been presented and it is not clear whether, in the situation that all 500 000 multiple identities are resolved, the same number of cases would appear in each of the following years.

Implementation timelines

Regarding the timelines for implementation, presented in the Legislative Financial Statement accompanying the proposals, the first key assumptions are that development of the solutions will be able to start at the beginning of 2019, with completion by the end of 2023. Considering the complexity of the policy and legislative environment surrounding the legislative proposals for interoperability, and the inter-reliance between the component parts, progress against the timeline needs to be closely monitored. Considering, for instance, how the establishment and roll-out of the SIS II suffered delays and additional costs, the estimations of implementing the interoperability solutions may not represent a realistic timeline.

Furthermore, although the Commission prepared the interoperability proposals quickly – as evidenced by the short turnaround time between the delivery of the Regulatory Scrutiny

[200] Ibid.

[201] The impact assessment (p. 14) states in its explanation of calculating the assumption: 'the size of end-user population having to be trained is estimated taking the number of end-users of border management systems in Schengen countries (about 1.5 million) and considering one out of seven needs to be retrained annually'. The source for the figure of one in seven is not presented.

[202] The annexes supporting the impact assessment (p. 59) cite the experiences of a number of Member States.

[203] Annex 4 supporting the impact assessment, p. 17.

Board's 'positive with reservations' opinion on 8 December 2018 and the publication of the proposals on 12 December 2017 – its future timelines rely on the quick work and progress of the co-legislators on these complex proposals in a complex policy and legislative environment, with many documented challenges. This phase also needs to be monitored closely.

Finally, given the heterogeneity of the Member States' current implementation and use of the JHA information systems, it will be important for the Commission to establish clarity on Member State implementation measures in relation to the implementation of interoperability.

Member State implementation

A key point raised throughout the interviews conducted for this study relates to the need for every Member State to implement and use the information systems and interoperability solutions to the same level to achieve the full benefits.

As mentioned above, an important step is the design of a Member State implementation plan and a more comprehensive understanding of the actions required of the Member States. However, interviewees at both the EU and Member State levels consider that the implementation activities to be undertaken at the Member State level will not raise significant challenges.

Some potential challenges have been identified, which could impact the implementation of standard processes and use of the information systems across the Member States and the heterogeneity of the benefits achieved across the Member States. The impact assessment highlights the following development and implementation challenges:

- **technical integration** of the three components with existing systems, processes and technology in Member States;
- **operational integration** of the three components in the workflows of the use of existing systems;
- **migration of historical data** (for sBMS only). Further to this point, without the publication of the technical study on the sBMS, Member State representatives struggle to envisage the feasibility of the sBMS concept, particularly considering the different ways in which the information systems collect biometrics;
- **development complexities** of the multiple-identity detector (MID);
- **integration of the MID** in existing systems, processes and workflows, both at the central level and at the level of Member States, entailing new, additional responsibilities and activities for authorities that may already be strained.

Considering the lack of a Member State implementation plan, it is not explained how these challenges will be addressed.

Another issue, not within the scope of the proposals, but a potential challenge nonetheless, is the availability and accessibility of handheld biometric scanners across the law enforcement agencies of the EU Member States. Following the development of the CIR, and the implementation of the practice of police authorities conducting identity checks, discrepancies in the availability of handheld biometric scanners will mean that significantly different benefits are achieved across the Member States.

Finally, the engagement of the Member State experts in the development of the delegated acts (Article 8(2) and Article 9(7)) will be necessary for the achievement of uniform use, processes, data quality and benefits across the Member States.

Box 8: Key concept: Delegated acts

As determined in preamble paragraph (63), and in accordance with Article 290 TFEU, the Commission has the delegated responsibility to supplement certain technical aspects of the Regulations with **detailed delegated acts**. In line with the Interinstitutional Agreement on Better Law-Making of 13 April 2016, the delegated acts should be the result of appropriate consultations with the European Parliament and the Council, as well as Member State experts. These proposals govern the development of delegated acts through Article 63 and stipulate the need to create delegated acts on the following elements:

- **Article 8(2):** the profiles for the users of the ESP in accordance with their access rights;
- **Article 9(7):** the content and format of the ESP replies.

Eu-LISA's role and responsibilities

The proposals require amendments to the eu-LISA Regulation. Given that the eu-LISA Regulation was already under negotiation in the European Parliament and the Council,[204] the legislative amendments required by these proposals cannot be specifically established. A significant challenge in this regard is that **the proposal to amend eu-LISA's mandate was not accompanied by an impact assessment**.

EU-level stakeholders consider that the eu-LISA appropriations are suitable. However, it has been mentioned that the budget includes limited consideration of the need for management roles. For instance, the human resource budget appropriations do not allocate any funds for general coordination or HR roles.

Furthermore, considering chapter VII of the interoperability proposals, no data protection specialists are programmed to be involved until 2023, when one will be allocated. There is also no reference to the allocation of data security specialists and no discussion on how such expertise will be incorporated into the development, maintenance and operational processes.

Finally, during the development phase, eu-LISA will be required to provide regular reports on the state of play. However, the post-development monitoring and evaluation mechanisms suggested by the proposals – after four years and then every subsequent four years – appear to be too infrequent. This is particularly true when considering the current reporting requirements for the centralised JHA information system (e.g. technical functioning reports for SIS and VIS, annual reports for Eurodac). Such a monitoring and evaluation schedule will not provide eu-LISA with an opportunity to monitor real-world implementation and react accordingly.

3.3.2. Fundamental rights and data security implications

The interoperability proposals not only introduce new tools to make the use of the current and proposed JHA systems more efficient, but they also introduce new functions that envisage the adoption of 'new ancillary purpose[s] of Eurodac, VIS, the future EES'.[205] The proposals seek to introduce new data processing and grant new access rights to authorities which will have **implications on fundamental rights, in particular related to the right to private life (Article 7 of the Charter) and the right to personal data protection**

[204] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011, 29 June 2017.

[205] Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, p. 14.

(Article 8 of the Charter) including data security, as enjoyed by third-country nationals.

Fundamental rights and data protection

New methods for the storage, processing and accessibility of personal data have implications for the right to private life and to the **protection of personal data**, though the proposals mention that interoperability will respect the principles of data protection by design and by default.[206] The EDPS has stated that before such principles can be instigated it is a requirement that 'necessity and proportionality of processing are first established'.[207]

In its report regarding the interoperability of the EU information systems, the EU Agency for Fundamental Rights (FRA) highlighted both the risks and opportunities that the proposed measures would present in relation to fundamental rights. It is important to note that the stated aim of the interoperability proposals are to enhance security, and they are thus envisaged to contribute positively towards the protection of people's **right to life (Article 2 of the Charter).** However, the report emphasised the requirement for safeguards to ensure data quality and preserve the data for use in line with what was originally intended. Such safeguards include the prevention of unauthorised access and the sharing of data with unauthorised authorities; logging of access and usage by authorised users; the implementation of minimum quality standards; and ensuring the right to effective remedy and the practical possibility to rebut false assumptions and inaccurate data held by the relevant authorities.

Sufficient protection must continue to be given to the storage and use of biometric data. FRA's report on interoperability recommends that sBMS should not store, but only match, data.[208] However, the proposals imply that the sBMS will indeed store biometric templates of fingerprints (and potentially facial images). If this is the case, it needs to be clarified that a new database with biometric data will be created – an element which goes against the compartmentalisation of information systems and thus against the *direct definition* of interoperability. In order for the sBMS to operate in line with interoperability, it should be ensured that the necessary precautions are taken to ensure that this new component does not constitute the mass storage of personal data. In *M.K. v. France*, the ECtHR concluded that retention of fingerprints solely for the reason of preventing future identity theft would, in practice, justify the storage of information on the entire population, which would clearly be excessive.[209] There is a question regarding whether the judgment would also be relevant to the consolidation of biometric templates of nearly all third-country nationals within the EU for the purposes of identifying multiple identities across the systems. On this point, it is imperative that there is a clear legal provision that permits the template to be used beyond the initial use for which the data was collected (i.e. template generated from fingerprints in Eurodac being repurposed for identity checks at the national territory beyond the determination of whether the person has applied for international protection elsewhere).

Biometrics, such as fingerprints, have proven to be an effective method of authenticating an individual's identity which have consequently improved the reliability of the EU central information systems. The interoperability proposals anticipate an increased reliance on biometric data for identification and verification of the status of third-country nationals. Due

[206] The CJEU understands the rights to private life and to the protection of personal data as interrelated through the hybrid creation of the right to private life with regard to the processing of personal data. This approach is also favoured in this report, even though the Commission proposal makes reference to the right to personal data only.

[207] EDPS (2017) Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice.

[208] FRA (2017) Fundamental rights and the interoperability of EU information systems: borders and security.

[209] ECtHR, M.K. v. France, No. 76100/13, 18 April 2013, para 40.

to their non-cancellable nature[210] and the difficulties in disputing false matches related to biometric data,[211] it is imperative that processes are established to minimise data entry errors[212] so as to be compliant with the **right to good administration (Article 41 of the Charter)**; and that sufficient redress mechanisms are in place to give individuals the right to effective remedy, as has been highlighted by the EDPS.

The broader availability of data can in itself have both positive and negative implications on the right to an effective remedy. The creation of bona fide green links in the MID has positive consequences for third-country nationals in the EU. However, the timeframes for the redress of red links might be considered too long and the consequences for failure of Member States to redress red links are not elaborated upon. The proposals seek to substantially decrease the use of multiple/false identities within the JHA information systems. This will provide authorities with more certainty regarding an individual's identity and positively affect the **right to asylum (Article 18 of the Charter)** and the **prohibition of refoulement (Article 19 of the Charter)**. However, safeguards should be put in place for those seeking international protection who have sought entry into the EU using a false identity, so as not to have an undue effect on the right to asylum.

The **two-step approach for streamlined law enforcement access** would mean that the designated authority is enabled to obtain information from the flag (the initial step) that may influence decision-making. For example, a flag that an individual is in Eurodac may give the officer clues about the individual that he is not entitled to know, for instance that most likely the person has applied for international protection and that potentially they belong to a vulnerable group of individuals. This new knowledge is no longer necessarily restricted to the querying officer's specific task, and thus would contravene the purpose limitation of the data. The requesting authority would no longer be required to demonstrate the *necessity* to access the identity data, nor would they be required to demonstrate that the information would aid in the investigation of **a specific case, but rather they would have access on a routine basis**. The existence of a 'hit' is a finding on its own and should be covered by the conditions of access, otherwise the requirement of having to link the comparison of the data with a specific case is circumvented and nullified. The proposed logging of queries at the level of the individual may prevent excessive use simply based on the increased possibility of accessing the data, whereby the weakening of *ex ante* controls must be accompanied by significant strengthening *ex post* controls. Under the current 'cascade' mechanism the querying officer would be granted access to all of the information contained within the underlying system upon being granted access. Full access to the data may not have been necessary had the officer only been aware of the identity information. The two-step approach may therefore be more protective as it may restrict full access to data.

The new interoperability proposals increase the likelihood that authorities would become aware of **data input errors and inaccuracies** in alphanumeric data. This has positive implications for the fundamental rights of third-country nationals in the various databases specifically in the context of the right to privacy and to the protection of personal data. However, it may be the additional components to the proposal, namely the universal message format and the proposed data quality measures, that will improve data quality across the systems rather than the linking of the systems. The importance of these additional

[210] Biometrics are not able to be reissued if compromised or misused

[211] Kaamara was detained longer than lawfully permitted due to a false fingerprint match with another person. England and Wales High Court (Administrative Court), Kamara v Secretary of State for the Home Department, [2013] EWHC 959 (Admin), 26 April 2013.

[212] According to public servants interviewed as part of FRA's project on biometrics, a more frequent problem is that the data profile of another person has been attached to the fingerprints, both in relation to Eurodac and VIS.

components must not be overlooked as part of the interoperability proposals. Poor data quality not only impacts operations but, in the context of interoperability, it may lead to the proliferation of inaccuracies throughout multiple systems – presenting a genuine risk to the privacy and personal data protection.

The processing of children's personal data must be considered in the context of the **rights of the child (Article 24 of the Charter)** and must also comply with Article 7 and Article 8 of the Fundamental Rights Charter. Special protection is to be granted to children as stipulated in the EU data protection *acquis*. In the case of *S. and Marper*, the ECtHR emphasised that blanket retention of biometric data by law enforcement authorities of persons not convicted of a crime may be especially harmful for children, given their special situation and the importance of their development and integration in society.[213]

Retention of a child's data in migration and asylum databases can therefore severely impact their lives, especially given that they would have had no choice in the decision to migrate or flee. The proposed interoperability solution, namely the CIR, offers the potential for law enforcement to obtain additional data potentially beyond the purpose limitation of its use, despite the particular vulnerability of children. The presence of children in the proposed ECRIS-TCN for criminal offences related to migration or as a consequence of trafficking may lead to severe prejudice later in life, thus leading to disproportionate consequences due to events beyond their control.

Furthermore, there is a **limitation with regard to the use of biometric data with children**. The ongoing physical development of a child means that fingerprint and facial data that may remain in the system for up to 10 years may not be reliable as time passes (i.e. the margin of error for children may be higher than for adults). False matches may have a disproportionate effect on the child, including **right to liberty and security, and the right to asylum**. Thus, there should be an effective procedure to account for the development of children.

Interoperability of the EU information systems can also be used as a tool for effective child protection. Missing children are frequently encountered at border crossing points, but border guards have stated that challenges exist in such situations.[214] When consulting SIS alerts on missing children the data may be inaccurate or incomplete, hindering the ability to identify a child. Furthermore, not all Member States issue SIS alerts for every reported missing child. With the appropriate connections of databases and the necessary safeguards in place to permit access in these specific situations, interoperability may contribute to the effective protection of vulnerable children. That being said, interoperability alone would be insufficient to enable the protection of children in this respect. A holistic approach that included border staff training and clearly defined procedures that may involve child protection services would also be necessary.

The proposed **identity checks on the territory of the Member States** for the purposes of police investigations that do not reach the threshold of serious crimes has the potential to negatively impact several Fundamental Rights of the EU Charter.

The proposal potentially increases the risk of discrimination of third-country nationals on the basis of racial or ethnic origin, infringing on **the right of non-discrimination (Article 20 of the Charter)**. The proposal's intention to extend the use of interoperable systems to permit identity checks on third-country nationals may increase the possibility of stopping

[213] ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras 124–125.
[214] FRA (2017) Fundamental rights and the interoperability of EU information systems: borders and security.

third-country nationals for checks, which can be construed as inherently discriminatory.[215] The proposals anticipate that such security measures would 'generate increased public trust by ensuring that the… design and use [of interoperable systems] increases the security of EU citizens'.[216]

The Racial Equality Directive (2000/43/EC) states that discrimination occurs 'where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin'. A pertinent question is whether there is a difference between access rights granted to law enforcement to national non-law enforcement databases that contain EU citizens compared to the proposed streamlined access to EU non-law enforcement databases that contain non-EU citizens, entailing the risks of racial discrimination. The necessity and proportionality of any potential differential treatment should be clearly outlined.[217]

The Meijers Committee, in its comments on the interoperability proposal, describe the position taken by the CJEU where

> 'such differentiation was in breach of the right to non-discrimination in relation to data protection rights, including the principle of purpose limitation – Huber v. Germany, in which the CJEU dealt with the differential treatment between nationals and EU citizens living in Germany with regard to the central storage and multiple use of personal data in an aliens administration, including the use for law enforcement purposes.'[218]

Identity checks on the territory may also unduly affect irregular migrants, who may not seek healthcare, report crime (even if they are the victim) or seek education for their children due to fears of identification and removal from the Member State. Thus, undue identity checks on third-country nationals will also impact the **liberty and security of the person (Article 6 of the Charter)**, potentially compromise the **integrity of the person (Article 3 of the Charter)** and could foreseeably lead to the expulsion of individuals, contravening the **prohibition of collective expulsion (Article 19 of the Charter)**. Logging of searches performed by competent authorities including the querying officer, and the requirements that a third-country national must be present during the search, are welcome safeguards to discourage unlawful use.

Data security

The proposals recognise in several locations that the CIR and MID 'will need to be protected for data security issues in the same way as the other central systems'. Article 42(1) states that 'both eu-LISA and the Member State authorities shall ensure the security of the processing of personal data' with necessary measures that they shall adopt to ensure the security of the interoperability components outlined in Article 42(3). It is welcomed that the proposal highlights the necessity of a security plan, a business continuity plan and a disaster recovery plan. However, the technical specifications for enhanced data security are not outlined. It may be useful to adopt ENISA's guidelines on the appropriate use of qualified

[215] Meijers Committee. CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM (2017) 794.

[216] COM (2017) 794, p.17.

[217] Meijers Committee. CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM (2017) 794.

[218] *CJEU Huber v. Germany*, C-524/06, 16 December 2008, para 78–79.

electronic timestamps[219] based on the eIDAS Regulation[220] to ensure the validity and integrity of data within the JHA systems.

There are, however, data security risks related to the interoperability systems and the proposed new uses. The proposal recognises procurement and technical challenges related to the 'Member States needing to purchase and customise handheld biometric terminals and connect them to their national police systems'; however, it does not address the potential data security risks that may accompany the increased availability and use of portable handheld devices that are connected to the JHA systems.

The portable devices with access to the underlying systems must have robust measures to prevent unauthorised access due to inappropriate use contrary to the legal access rights granted, and also to prevent the potential physical loss of such devices. The envisaged increase in portable devices would mean an increased number of access points to the data in the underlying systems, and further, the wireless nature of the access would have to be sufficiently secure. It could be argued that linking the systems and increasing the accessibility of data to be edited could potentially increase the opportunity for malicious editing. It should be reiterated that due to the considerable changes in the way that data will flow, there must be sufficient measures to protect personal data in the storage and communication channels from potential attacks. This again highlights the benefits of incorporating qualified timestamps as data are created and updated, and the requirement for robust data security measures.

The proposals suggest that the 'two-step approach' would lead to a reduced transfer of information between authorities as requests for access to the underlying systems would only be made after confirmation that an individual's data was present in the databases. This may represent a means by which the proposed streamlined access for law enforcement to the non-law enforcement databases may reduce data security risks. However, the first step of initially querying the systems without obtaining prior authorisation may also lead to routine comparisons against the data stored therein.

Finally, there are ongoing discussions regarding a formal working relationship between eu-LISA and ENISA. There have only been a few instances of cooperation between eu-LISA and ENISA to date regarding the interoperability proposals. The benefits of formalising such a relationship may be beneficial when exploring the data security risks that interoperability may bring.

Evaluation and monitoring

Eu-LISA is to submit a report on the functioning of the interoperability solutions four years after the outlined plans have been put in place, and every four years thereafter. However, in the interests of consistent evaluation of the desired and undesired outcomes of interoperability, eu-LISA should consider producing a report sooner than the initial four-year time period stated, and with a regularity that is in line with published reports on other systems (i.e. yearly).

The impact assessment states that the 'General Data Protection Regulation, with Regulation (EC) 45/2001 and, where relevant, Directive (EU) 2016/680 apply to the processing of personal data carried out for the purpose of interoperability by the Member States and by the EU institutions, bodies and agencies involved, respectively', without providing further clarification as to the boundaries between the applicability of each system. This is all the

[219] ENISA (2016) Security guidelines on the appropriate use of qualified electronic timestamps.
[220] Regulation (EU) 910/2014.

more necessary since the interoperability proposals are framed under the auspices of security, which would trigger the application of Directive (EU) 2016/680.

The keeping of logs as proposed in Article 24 of the proposal is an important and welcome tool to control access to data files. However, there are some doubts regarding whether the retention period of the logs is sufficient to be able to evaluate errors and potential misuse of the systems. Furthermore, the mandate for eu-LISA would be extended significantly by the proposals. It is important that there are some assurances that eu-LISA will have sufficient capacity to fulfil all its obligations, including the safeguards proposed for monitoring and evaluation. The interoperability solutions could inadvertently make information accessible to greater numbers of end-users. We have already noted in this report that in some instances Member States have not faithfully followed the conditions for law enforcement access to VIS[221] and therefore it is welcomed that the proposals set out to log access and queries to the system at the level of the user. This level of granularity that goes beyond simply logging the 'authority' that accessed the system is a stronger safeguard that may further discourage misuse. While the proposals outline the legal limits for access and the monitoring of use, they do not elaborate on the procedures in the event that there is a suspicion of unauthorised use. It might provide clarity if the Commission could outline the reporting procedures in the event of suspicion of misuse. Finally, given the proposed expansion of its role in managing and evaluating the centralised EU information systems, it may be of benefit if there is a DPA embedded in eu-LISA.

[221] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation.

4. CONCLUSIONS AND OBSERVATIONS

In this context, the **concept of interoperability is considered to be positive by the vast majority of stakeholders, when implemented appropriately**. The linking of distinct information systems to improve the efficiency of operations for end-users, while strictly regulating access rights and fully respecting the protection of personal data, can be a significantly beneficial endeavour. What interoperability is not intended to deliver is new modes of storage, new processing of personal data beyond the purposes of each system or new access rights.

In the Commission's legislative proposals on establishing a framework for interoperability between EU information systems, however, the definition appropriated for the concept of interoperability is not explicitly stated and not sufficiently elaborated, as most prominently highlighted by the EDPS and summarised in Box 9.

Box 9: Definition of interoperability in the legislative proposals

Definition of interoperability in relation to JHA information systems

The proposals indirectly describe the concept of interoperability as the ability 'to exchange data and share information so that authorities and competent officials have the information they need, when and where they need it'.[222]

This definition closely reflects those published in the 2005[223] and 2016[224] Commission Communications on the topic of interoperability, which both received criticism from the EDPS:

Commenting on the 2005 Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs,[225] the EDPS noted that 'the concept of interoperability is not given an unambiguous and clear meaning', and said the EDPS 'does not fully share the view that 'interoperability is a technical rather than a legal or political concept'.[226]

Commenting on the 2016 Communication on stronger and smarter information systems for borders and security,[227] the EDPS notes that the Commission's work focuses on interoperability as a technical concept, without fully considering whether the data exchange is 'necessary, politically desirable or legally possible'.[228] As such, the EDPS calls for a clear and unambiguous meaning for interoperability and suggests that existing assumptions result in a misaligned focus for the proposed general objectives.

[222] Proposal for a Regulation on establishing a framework for interoperability between EU information systems. {SWD(2017) 473 final} – {SWD(2017) 474 final}, p. 1.

[223] European Commission (2005) Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. COM(2005) 597 final (24.11.2005).

[224] European Commission (2016) Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security. COM(2016) 205 final (06.04.2016).

[225] European Commission (2005) Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. COM(2005) 597 final (24.11.2005).

[226] EDPS (2006) Comments on the Communication of the Commission on interoperability of European databases. Brussels, 10 March 2006.

[227] European Commission (2016) Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security. COM(2016) 205 final (06.04.2016).

[228] EDPS (2006) Comments on the Communication of the Commission on interoperability of European databases. Brussels, 10 March 2006, p. 6.

Moreover, this lack of an explicit definition suggests that the proposals and their precursor Communications define interoperability in relation to the solutions, as opposed to creating and defining the solutions based on a clear and unambiguous understanding of the concept of interoperability in this context.

This conclusion is supported by the finding that, in the 2016 Communication and subsequent publications, there is limited explanation of how the proposed interoperability solutions were conceived.

The roots of the definition can be clearly traced back to the field of e-Government, as the definition mirrors those used in both the European and Estonian e-Government Interoperability Frameworks. However, e-Government is an area that encompasses an extensive variety of different types of information systems, services, users and modes of access and thus requires a broad definition. This broad definition supports a framework that should guide the design and implementation of context-specific interoperability. The layers of interoperability and the principles of interoperability that comprise the core of these frameworks are therefore more pertinent to the design and development of an interoperability solution than the definition.

In view of this, much greater clarity is recommended on how the concept of interoperability – most importantly, the layers and principles – has been applied to the creation and design of the interoperability solutions presented in the legislative proposals on establishing a framework for interoperability between EU information systems. Therefore, the **biggest challenge facing the proposals is that, in reality, they do not establish a framework for interoperability, but instead propose technical solutions, some of which are compatible with the concept of interoperability, some of which are not**. And, as mentioned above, the understanding of interoperability appears to be based on the solutions conceived as opposed to the solutions being created based on a clear, transparent and agreed understanding of interoperability. With this in mind, interoperability needs to be clearly defined, including its outer limits, otherwise it may become a flexible concept and a moving target.

Furthermore, these challenges persist through key elements of the proposals and contribute to the relatively straightforward validation of the necessity and proportionality of the solutions. As detailed below, there are challenges facing the following core elements:

i. the **problem definition and needs** articulated by the proposals;

ii. the **objectives and purposes** detailed for the proposed solutions; and

iii. the **design** of the solutions.

Additionally, the proposals would benefit from increased clarity and transparency, including on the following cross-cutting issues:

- the use of presumptive terminology that consistently asserts the necessity of the proposals with limited supporting evidence;
- linked to the above, the limited consultation exercise, particularly with regard to the data protection and fundamental rights implications.

Problem definition and needs

The problem definition highlights the following two principal problems as justification for the need for interoperability between the EU information systems:

i. Information is not always complete, accurate and reliable.

ii. End-users do not always have fast, systematic access to all the information they need to perform their tasks. In some cases, existing rights to access the various systems in accordance with EU legal instruments are not exercised in full because of a 'lack of technical and practical means at a national level'.[229]

It is clear how the second problem will be addressed by interoperability, but it is not clear – considering an appropriate definition of interoperability that does not deliver new access rights, new processing of personal data or new modes of access – how interoperability can improve the completeness, accuracy and reliability of data. This is particularly relevant given that the data quality is primarily governed by the mechanisms for inputting the data into each system, which rely on processes and actions of the Member State authorities.

The proposed measures to improve data quality and the operation of the CIR, sBMS and MID could, as detailed in the proposals, contribute to addressing the first need, but they introduce new access rights, new processing of personal data and new modes of access that are not aligned to an appropriate definition of interoperability.

Additionally, the problem definition highlights two principal problem drivers:

i. a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots; and

ii. a complex landscape of differently governed information systems.

The differences between these drivers are not clearly explained and they suggest that a lack of interoperability is driving the abovementioned problems. In reality, as mentioned above, it is the individuals tasked with inputting data who drive the completeness, accuracy and reliability of the data in each system and, as recognised above, access rights are sometimes not exercised due to a 'lack of technical and practical means at a national level',[230] not at the EU level. Furthermore, the different information systems were intentionally developed separately based on the specific purposes of each system and in line with the data protection principle of purpose limitation.[231]

As discussed below in relation to each solution, the needs articulated in the proposals often lack supporting evidence.

Objectives

The proposals establish various sets of objectives: the explanatory memorandum presents general, Treaty-based objectives and specific objectives, and Article 2 of the legislative text presents further objectives. As a first point, the proposals lack clarity on the relationship between these different objectives.

The general objectives detailed in the explanatory memorandum bring together migration and internal security objectives. As previously highlighted by the EDPS, this can lead to a conflation of migration management and management of internal security, as well as a blurring of the boundaries between the two policy areas and almost interchangeable use of the terms in relation to the JHA information systems. Furthermore, it should be clearly stated that, for most information systems covered by the proposals (i.e. not SIS II or ECRIS-TCN), security-based objectives are also ancillary.

[229] Impact Assessment, p. 9.
[230] Impact Assessment p. 9.
[231] Article 5(1) GDPR.

In the explanatory memorandum supporting the proposals, four specific objectives are also defined. These objectives introduce significant new purposes to the existing JHA information systems environment. The detection of multiple identities and the facilitation of identity checks of third-country nationals on the territory of a Member State, for instance, both introduce significant new objectives to be achieved using the existing and planned JHA information systems. Furthermore, both of these new objectives have a strong security element and limited relevance to the objectives of the existing and planned JHA information systems.

Article 2 of the proposals presents the objectives of the legislative text. Paragraph (1) simply lists the general objectives of the existing and planned information systems, thereby equating the distinct systems and their objectives.

Solution purposes and design

The **European Search Portal (ESP)** could be a very successful innovation that will likely lead to improved operational efficiency. Furthermore, no significant aggregation of data is possible and no additional information systems or databases are developed. As such, the ESP will contribute to the achievement of specific objective one (i.e. to facilitate fast, seamless, systematic and controlled access to authorities) and could be implemented without data protection implications. Where the protection of personal data could become a challenge is in the development of the delegated acts. As highlighted above, the delegated acts, in particular the user profiles to be developed under Article 8(2), will play an important part in ensuring that existing access rights are respected – it is recommended that the development of these delegated acts be closely monitored and should make significant use of data protection specialists.

Finally, further clarity is required on the extent to which owners of Interpol data will be notified of searches relevant to their data. Article 9(5) states that the 'data used […] to launch a query is not shared with the owners of Interpol data', leaving the question open as to whether data other than the data used to initiate the search is shared. For example, is the owner of the Interpol data notified that a search has taken place?

The **shared Biometric Matching Service (sBMS)** will likely contribute to achieving the desired objectives through the storage and use of mathematical representations of biometric data to support the ESP, the CIR and the MID. However, the sBMS constitutes a new database and therefore does not conform to an appropriate definition of interoperability.

Furthermore, the academic and EU communities have formulated differing conclusions over the years on whether the mathematical representations stored (i.e. biometric templates) constitute personal data. However, regardless of whether or not the mathematical representations are personal data, it is clear that the sBMS can add value in identifying multiple identities across the information systems. What is not recognised, reflecting the limited options explored in the impact assessment, is that the sBMS would also bring value without the other interoperability components. In the case that the CIR and the MID are not implemented, it seems **the sBMS would still be able to determine multiple identities across all systems except for ETIAS**, when the detection of multiple identities is based on the comparison and consultation of biometric data. Considering the implications of implementing the CIR and MID, detailed below, this represents a potential alternative implementation option.

The **Central Identity Repository (CIR)** will likely contribute to the achievement of its purpose and the related objectives. In particular, it will greatly facilitate the identification of third-country nationals on EU territory, it will support the functioning of the MID in detecting and verifying multiple identities across the systems and it will streamline the process of law enforcement access to non-law enforcement databases for the investigation, detection or

prosecution of serious crime. However, the establishment of the CIR is the most invasive dimension of interoperability – as conceived by the Commission – and raises privacy and data protection concerns in numerous respects.

The text on its architecture is unclear as to whether it will constitute a separate database. The full technical study supporting the feasibility of the CIR has, at the time of writing, not been published, which means it is not possible to clarify the exact nature and functioning of the CIR. Furthermore, the proposals explicitly state that the CIR is not a new database, but rather a shared technical component. However, calling it a 'repository' and the use of terms such as 'stored' and 'storing' throughout the descriptions of the CIR, imply the creation of a new database that will store the identity data of all third-country nationals.[232] This is further supported by the legislative text, which discusses the CIR in the same manner as the current and planned information systems (see, for example, articles 9, 11 and 14). In the light of the above, the CIR does not seem to constitute an interoperability solution and, if this is the case, it is recommended that the CIR should be declared and processed more appropriately.

Regardless of whether the CIR is technically a database, it will act as one when facilitating the identity checks by law enforcement personnel of third-country nationals on the territory. As such, its operation is akin to the creation of a new database that: provides new access rights to the personal data collected across the information systems; equates all types of third-country nationals; and constitutes a major purpose change for the personal data collected across all the systems. Furthermore, this purpose change is related to bolstering the ancillary purposes of the systems, which further calls into question its proportionality. Finally, the proposals do not adequately detail or evidence the current challenges and problems that are reportedly necessitating this new purpose.

The current mechanisms of law enforcement access to VIS have faced academic criticism. The judgments in both *Digital Rights Ireland* and *Watson* stated that independent or judicial authorities should be responsible for the verification of the conditions of access to VIS, rather than central access points or verifying authorities which are permitted to be within the same organisation that is gaining access to VIS. With this in mind, it is clear that the **two-step approach** detailed in the interoperability proposals relaxes these conditions further, generating the following challenges:

- It will be possible for law enforcement to have a finding without any authorisation, as the absence of a record across the information systems (i.e. no flags on an identity) would be a finding.
- The knowledge provided by the hit-flag functionality – i.e. which database an individual is in – negates the current conditions for access, provides law enforcement with access to new information and equates all third nationals from across the distinct information systems.

As such, the CIR introduces the most significant changes compared to the current implementation and, as such, represents the most significant threat, in particular to the protection of personal data and the right to privacy in this context.

The **multiple-identity detector (MID)** has a dual purpose of 'facilitating identity checks for bona fide travellers and combating identity fraud'. The functioning of the MID as described will likely support these purposes and contribute to the achievement of the objectives established. However, it does not constitute an interoperability solution in line with an appropriate definition of interoperability. This is due to the fact that:

[232] Proposal for a Regulation on establishing a framework for interoperability between EU information systems, 2017/0352 (COD) and 2017/0351 (COD), p. 7, paragraph 3.

i. the MID results in the creation of new data in the form of links and identity confirmation files; and

ii. the MID provides new access rights to those individuals who encounter a yellow link.

Furthermore, the purpose of the MID to combat identity fraud is not supported by the legal basis for Eurodac. The inclusion of Eurodac data would require a further amendment to the purpose of the information system.

The additional elements proposed by the proposals are also not interoperability solutions. However, the consistent implementation of the UMF and the development of a CRRS are valid endeavours that will add value without additional implications.

Implementation implications

Considering the complex policy and legislative environment surrounding the EU's JHA information systems, the implementation plan for interoperability needs to be clear and transparent.

However, the proposals present limited detail on **implementation**, particularly at the Member State level. In terms of the overarching implementation timelines presented, progress needs to be consistently monitored, as required by the complexity of the policy and legislative environment and the inter-reliance between the component parts. At the Member State level, it is recommended that a detailed implementation plan is developed. The Commission has foreseen a number of development and implementation challenges – including those related to the technical integration of the interoperability solutions and the migration of historical data for sBMS – without providing details of how these challenges will be addressed.

Where further detail is presented, for example in relation to the financial implications of the proposals, a number of challenges have been identified in areas that require further clarification.

Regarding the **budgetary implications**, for instance, the appropriations detailed in the Legislative Financial Statement differ in perspective from those presented in the impact assessment. This prevents any cross-referencing of values across the two outputs. Furthermore, the appropriations for eu-LISA are not clearly detailed. The main text of the proposals only details how EUR 168.1 million of the EUR 225 million allocated to eu-LISA is to be apportioned, and the Legislative Financial Statement, although more comprehensive, leaves EUR 2.348 million unspecified. It is recommended that this be clarified.

The impact assessment also highlights positive **economic impacts** – namely, that the implementation of the interoperability proposals will positively impact tourism, airports, seaports and carriers due to improved EU security and speedier border control processes. However, as detailed earlier, the causal link between the interoperability proposals and increased security has been called into question due to a lack of 'concrete explanations and evidence'[233] and, although the verification of individuals via CIR and MID would minimise disruption for legitimate travellers with bona fide or resolved multiple identities, there is no indication of the extent of this positive impact. Furthermore, the proposals do not consider that, if the new modalities introduced by the interoperability proposals are perceived to be excessive by the third-country nationals subject to them, it could have a negative impact on tourism.

[233] European Parliamentary Research Service (EPRS) (2018) Interoperability between EU information systems for security, border and migration management. Briefing: Initial Appraisal of a European Commission Impact Assessment.

Furthermore, it is clear that the **cost-benefit analysis** requires clarification on a number of issues. Primarily, these issues relate to the reliability of the cost and benefit estimates, which are based on 'a lot of approximations'.[234] The impact assessment estimates the one-off costs at EUR 169.8 million with a 20–25% 'confidence margin'. Firstly, this terminology appears to conflate the concepts of confidence intervals and margins of error. Considering the first concept (confidence intervals), the Commission is stating that they are 20–25% confident that their estimates are correct; under the second concept (margins of error), the Commission is stating that the costs could be up to 25% higher or lower than the estimate presented. It is likely that the latter concept is intended, but clarification is required. In any case, a margin of error of 20–25% means that the one-off costs determined as EUR 169.8 million could, in reality, be as little as EUR 127.35 million or as much as EUR 212.25 million.

Regarding the benefits, the evidence supporting key assumptions, such as the number of training sessions per person per annum and the number of multiple identities in existence across the information systems, is not transparently cited. It is therefore not possible to validate these assumptions.

Furthermore, there are logical challenges facing the benefits linked to the saved cost of identification of multiple identities, which are stated as EUR 50 million per year. This figure, however, is based on an assumption that 500 000 third-country nationals across SIS, VIS and Eurodac are using multiple identities. Using this figure, the saving estimate is generated by comparing a baseline scenario to the foreseen situation following the implementation of the interoperability solutions. However, the activities assumed in the baseline scenario are not evidenced, leading to a potentially unrealistic saving estimate. Firstly, the accuracy and the precision of the estimated number of multiple identities lacks concrete evidence. Secondly, the baseline scenario assumes that, every year, 500 000 multiple identity cases are detected and handled. However, no evidence of this caseload has been presented and it is not clear whether, in the situation that all 500 000 multiple identities are resolved, the same number of cases would appear in each of the following years.

More importantly, as detailed in the conclusion of the impact assessment, this saving of EUR 50 million is the primary detail determining that, from a cost/benefit point of view, 'option 3 is therefore more favourable then option 2'.[235]

[234] Impact assessment, pp. 15, 17.

[235] Impact assessment, pp. 51–52.

APPENDIX 1: INFORMATION SYSTEM SUMMARY PROFILES

This appendix contains the summary profiles for each of the six EU JHA information systems covered in this Interim Report. Each summary profile contains information on: the type of system; the purpose and objective of the system; the scope of the system; the data collected and held by the system; the size of the system; the relevant data retention specifications; the data input process; the access rights; the relevant data protection regulatory framework; the participating states; the cost of the system; the roles and responsibilities of EU bodies; the data storage and security specifications, where available; and the challenges faced or anticipated.

The different information systems are presented in the following order:

- VIS
- Eurodac
- SIS II
- ECRIS
- EES
- ETIAS

Visa Information System (VIS)

Table 5: Information system summary profile: VIS

VIS	
Type of system	**Centralised** system with communication infrastructure linked to national systems and consulates in third countries. The VIS is composed of two systems: the VIS central database and an Automated Fingerprint Identification System (AFIS).
Purpose and objectives of system	• to facilitate the visa application procedure; • to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; • to facilitate the fight against fraud; • to facilitate checks at external border crossing points and within the territory of the Member States; • to assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States; • to facilitate the examinations of asylum applications; • to contribute to the prevention of threats to the internal security of any of the Member States.

Scope of system	The VIS Regulation covers the conditions and procedures for the exchange of data between Member States on applications for short-stay visas and on the decisions taken in relation thereto, including the decision whether to annul, revoke or extend the visa, to facilitate the examination of such applications and the related decisions **Visa applicants (TCNs)**, as well as (indirectly) **EU citizens** who are hosts/sponsors of a visa applicant. Exceptions: • Children under the age of 6; • Persons for whom fingerprinting is physically impossible; • Heads of state or government and members of a national government with accompanying spouses, and the members of their official delegation, when officially visiting; • Sovereigns and other senior members of a royal family, when officially visiting.
Data collected and held by system	• Application number; • Information on the status of the application; • Authority with which the application has been lodged; • Names, sex, and place, date and country of birth; • Current nationality and nationality at birth; • Information concerning the travel document; • Place and date of the application; • Type of visa requested; • Details of the persons issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, namely: a) in the case of a natural person, the name and address of the person, or b) in the case of a company or other organisation, the name and address of the company and the nationality of the contact person within that company/organisation; • Main destination and duration of the intended stay; • Purpose of travel (tourism, business, visit friends/family, cultural, sports, official reasons, medical visit, study, transit, airport transit, other); • Intended date of arrival and departure; • Intended border of first entry or transit route; • Residence; • Current occupation and employer and, for students, name of school; • Parents' names (for minors); • Photograph; and • Full set of fingerprints. In accordance with the Common Consular Instructions, fingerprinting is compulsory for visa applicants over the age of 12.

Size of system	In 2014 VIS processed approximately **8.5 million visas**[236]
Data retention specifications	**5 years** maximum. Automatic deletion of the data if applicant acquires nationality of a participating state.
Data input process	Data input by visa authorities of the participating states.
Access rights	a) Visa, immigration and asylum authorities. b) Competent authorities responsible for carrying out checks at external border crossing points in accordance with Schengen Border Code. c) Designated authorities dealing with terrorist offences and other serious criminal offences, in specific cases only. d) Europol (within the limits of its mandate and when necessary to perform its tasks). e) Third countries or international organisations (under specific circumstances) **Type of searches in the VIS** Searches in the VIS are limited to specific data, for example: • surname, first names, sex and date, place and country of birth; • current nationality and nationality at birth of the visa applicant; • type and number of the travel document; • purpose of travel, and intended date of arrival and departure; • intended border of first entry or transit route; • fingerprints; • type of visa and number of the visa sticker; • details of the person who has issued an invitation for the visa applicant, etc. If the search using any of the above data is successful, the authorities may in addition access other data, such as photographs.[237]
Relevant data protection regulatory framework	Mix of EU and national data protection rules. National supervisory authorities in each contracting state shall monitor the lawfulness of the processing of VIS data on their territory. EDPS shall monitor the activities of the EU personnel managing VIS.

[236] Report on the technical functioning of VIS, eu-LISA, 2014.
[237] EUR-Lex, Rules for access to the EU's Visa Information System (VIS).

Participating states	All Schengen states: EU22 (Denmark has decided to opt in) + Non-EU Member States: Norway, Iceland, Switzerland and Liechtenstein United Kingdom and Ireland have opted out. Each Schengen state is responsible for the development, management and operation of its national system.
Cost of the system	The Commission was in charge of the development of the central database, the national interfaces and the communication infrastructure between the central VIS and the national interfaces. Their development was funded by the EU budget (the cost amounted to **EUR 151 million between 2005 and 2011**).[238]
Roles and responsibilities of EU bodies	As of December 2012, the database manager for VIS is the **European agency for the operational management of large-scale IT systems** in the area of freedom, security and justice, located in Tallinn, Estonia. **EDPS** has special role in checking data protection rules of central database.
Data storage and security specifications, where available	'The protection of personal data related to individuals processed by the VIS at central system level is monitored by the European Data Protection Supervisor (EDPS) in close cooperation with eu-LISA's Data Protection Officer (DPO). Quality of data stored in the CS-VIS and data subjects' rights, as per the legal provision, are ensured by the Member States.'[239] 'The VIS security and continuity risk management strategy covers all layers of the security spectrum: physical security, personnel security, network security, operating systems security, application security, business continuity and data security, in accordance with the relevant security principles and standards of the European Commission and good practices from ISO27001 standard.'[240]
Challenges	**Data quality**: 'problems with data quality mostly stem from sub-optimal application of the legal provisions.'[241] The use of VIS for asylum and law enforcement purposes is currently very fragmented across the Member States, where for instance, 'the possibility for fingerprint searches is not yet used.'[242] Again, this lack of consistency amongst the Member States in harnessing the system to its full capacity could have major security implications for the EU.

[238] COMMISSION STAFF WORKING DOCUMENT Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation

[239] VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008.

[240] *Ibid.*

[241] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, 2016.

[242] *Ibid.*

European Dactyloscopy (Eurodac)

Table 6: Information system summary profile: Eurodac

Eurodac[243]	
Type of system	**A centralised** system (composed of a Central Unit, and a Business Continuity Plan and System), a communication infrastructure between the central system and each Member State's National Access Point that provides an encrypted virtual network dedicated to Eurodac data.
Purpose and objectives of system	The purpose of Eurodac is to assist in determining which Member State is to be responsible for examining an application for international protection lodged in a Member State by a third-country national or a stateless person. Allow for Member States' designated authorities and the European Police Office (Europol) to request the comparison of fingerprint data with those stored in the central system for law enforcement purposes under strict conditions.
Scope of system	a) Applicants for asylum (at least **6** years of age) b) Persons apprehended in connection with the irregular crossing of borders coming from a third country c) third-country national or stateless persons found illegally staying in a Member State (only for comparison purposes)
Data collected and held by system	• Member State of origin, place and date of the apprehension; • fingerprint data (full 10 fingerprints and 4 control images); • sex; • reference number used by the Member State of origin; • date on which the fingerprints were taken; • date on which the data were transmitted to the Central Unit; • operator user ID; and where applicable: • the date of the arrival of the person concerned after a successful transfer; • the date when the person concerned left or was removed from the territory of the Member States; • the date when the decision to examine the application was taken.

[243] eu-LISA, (2016) 'Eurodac – 2015 Statistics'; and Recast Eurodac Regulation.

Size of system	According to the latest statistics (2016), Eurodac has processed **1,018,074** fingerprints of applicants for international protection, and **370,419** fingerprints of migrants apprehended irregularly crossing borders.[244] Furthermore, **252,559** fingerprints of irregular residents have been transmitted for comparison. Storage capacity (amount of data the system can store) – **7 million records** Processing capacity (amount of data the system can process per hour) – **1,500** transactions per hour
Data retention specifications	a) Data shall be stored in the central system for **ten years** from the date on which the fingerprints were taken. Data relating to a person who has acquired citizenship of any Member State before the ten-year time point shall be erased. b) Data relating to a third-country national or stateless person 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing shall be stored in the central system for **18 months** from the date on which his or her fingerprints were taken. The data is to be deleted before then if the person has been issued with a residence document; if the person has left the territory of the Member States; or if the person has acquired the citizenship of any Member State.
Data input process	Data entered by National asylum authorities
Access rights	National authorities dealing with asylum requests. In some Member States, however, Eurodac is operated partly or entirely by national police services. Requests by law enforcement to consult Eurodac data are permitted 'in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences'.
Relevant data protection regulatory framework	Designated authorities may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in Eurodac but must first query national fingerprint databases, the automated fingerprinting identification systems of all other Member States and the Visa Information System. Eu-LISA keeps records to be used only for the purposes of data protection monitoring. Data protection Directive 95/46/EC is additionally applicable. The EDPS is the competent data protection authority to monitor activities concerning Eurodac. Central Unit National data protection authorities supervise collection and use of data at Member State level.
Participating states	Recast Regulation applies to all EU Member States (except Denmark – has a separate agreement to apply original Eurodac Regulation) plus Norway, Iceland, Switzerland and Liechtenstein.
Cost of the system	'One off cost of EUR 29.872 million includes costs for the technical upgrade and increased storage and throughput of the central system. It also consists of IT-related services, software and hardware and would cover the upgrade and customisation to allow searches for all categories of data covering both asylum and irregular migration purposes. It also reflects the additional staffing costs required by eu-LISA.'[245]
Roles and responsibilities of EU bodies	Database manager is the **European Commission**. As of December 2012, the database manager for Eurodac is the **European agency for the operational management of large-scale IT systems** in the area of freedom, security and justice, located in Tallinn, Estonia. **EDPS** has special role in checking data protection rules of central database.

[244] eu-LISA, 'Eurodac – 2015 Statistics' (2016) 5.

[245] European Commission, Brussels, 4.5.2016 COM(2016) 272 final 2016/0132 (COD).

Data storage and security specifications, where available	Data Storage Eu-LISA responsible for 'the best available and most secure technology and techniques, subject to a cost-benefit analysis'[246] for the central system. Security specifications Eu-LISA 'shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with Eurodac data. This obligation shall also apply after such staff leave office or employment or after the termination of their duties.'[247]
Challenges	Assumption that asylum procedures are adequate and of a certain standard in all Member States. This has implications for internal security, as the identity and motivation of migrants may be undetermined upon entry into the EU due to said differences in standards. Implications of the recast Eurodac Regulation on data protection/privacy. 'The European Association for the Defence of Human Rights (AEDH) found that the Eurodac [recast Regulation] significantly exceeded the initial scope of Eurodac and introduced coercive forms that are not necessarily accompanied by adequate safeguards.'[248]

[246] REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013, Article 4.

[247] *Ibid.*

[248] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Stronger and Smarter Information Systems for Borders and Security, Brussels, 6.4.2016 COM(2016) 205 final.

Second-Generation Schengen Information System (SIS II)

Table 7: Information system summary profile: SIS II

SIS II	
Type of system	SIS II provides for a computerised exchange of information and comprises: • a central system (C-SIS II) located in Strasbourg and operated by eu-LISA in Strasbourg that holds all data alerts; • a national system (N-SIS II) located in each member state and operated by the competent authorities within them; • a communication infrastructure between C-SIS and N-SIS. National interfaces do not hold the data directly, but Member States may choose to maintain a full or partial national copy of the C-SIS II database as part of the N-SIS II. SIRENE is an additional component of the system that permits the exchange of any supplementary information and the coordination of activities connected to SIS II alerts.
Purpose and objectives of system	The primary purpose of the SIS is to help preserve internal security in the Schengen states in the absence of internal border checks: 'To ensure a high level of security within the EU's area of freedom, safety and justice, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of the Treaty relating to the movement of persons in their territories, using information communicated via this system.'[249]
Scope of system	The scope of the SIS is defined in three legal instruments: 1. Regulation (EC) No 1987/2006 (Border control cooperation) gives provision for SIS to allow border guards and visa issuing and migration authorities to input and check alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen area. 2. Council Decision 2007/533/JHA (Law enforcement cooperation) gives provision for SIS to support police and judicial cooperation by permitting competent authorities to create and check alerts on missing persons and on persons or objects related to criminal offences. 3. Regulation (EC) No 1986/2006 (Cooperation on vehicle registration) gives provision for SIS to allow vehicle registration services to check the legal status of the vehicles presented to them for registration. The types of alerts that can be inserted into the system are as follows: a) Third-country nationals to be refused entry or stay (Article 20, Regulation 1987/2006); b) Persons wanted for arrest or surrender purposes (Article 26, Council Decision 2007/533); c) Missing persons (Article 30, Council Decision 2007/533); d) Persons sought to assist with a judicial procedure (Article 34, Council Decision 2007/533); e) Persons and objects for discreet checks or specific checks (Article 36, Council Decision 2007/533); and f) Objects sought for the purpose of seizure or use as evidence in criminal proceedings (Article 38, Council Decision 2007/533).

[249] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

Data collected and held by system	The following data may be stored in the SIS on any specific person: • last name(s), forename(s), maiden name(s), and alias(es); • special permanent physical characteristics; date and place of birth; sex; photographs; fingerprints; palm prints; nationality or nationalities; • details on whether the person concerned is armed, violent or has escaped; • reason for the alert; the type of offence; authority issuing the alert; a reference to the decision giving rise to the alert; action to be taken; • link(s) to other alerts issued in SIS II.
Size of system	On 31 December 2016, there were in total 70,827,959 alerts in SIS II.[250] The largest number of alerts concern lost or stolen documents (over 39 million) and stolen vehicles (about 5 million). There is said to be capacity for up to 100 million alerts without the requirement for technical change.[251]
Data retention specifications	Date retention is governed by Articles 44 and 45 of Council Decision 2007/533 which states that Alerts should not be kept in SIS II longer than the time required to fulfil the purposes for which they were supplied. All alerts on persons are to be reviewed within a maximum of 3 years following the alert entry. This timeframe is reduced to 1 year if the alert was issued as part of a discreet check. Member States are obliged to erase the alerts if the review deems it necessary to do so. Member States also have the authority to extend the period of review following a comprehensive individual assessment, should it prove necessary for the purposes for which the alert was issued. Extensions are communicated to CS-SIS and statistics regarding the number of times the retention periods of alerts has been extended are kept. All alerts on objects that are subject to seizure or are to be used as evidence used in criminal proceedings are to be kept for a maximum of 10 years. All alerts on motor vehicles, ships, aircraft and containers, for the purposes of specific control and discreet surveillance, based on a request from the competent authorities of national security, public order or a judicial authority, could be retained for a maximum of 5 years from the date they have been entered. SIS II alerts shall automatically be erased after a specified storage period in case of no necessity for their further storage.
Data input process	Information is input by Member States via the national interfaces, NI-SIS.
Access rights	The SIS is only accessible to authorised users within competent authorities, such as national border control, police, customs, judicial, visa and vehicle registration authorities. Furthermore, such authorities are only permitted to access the SIS data that is necessary for the performance of their tasks. Limited access is granted to Europol and Eurojust to carry out certain types of queries on specified alert categories.

[250] SIS II – 2016 Statistics (2017). eu-Lisa.

[251] http://europa.eu/rapid/press-release_MEMO-13-309_en.htm

Relevant data protection regulatory framework	The Member State that entered the alert is responsible for its content. The national Data Protection Authorities monitor the application of data protection rules in their respective territories, while the European Data Protection Supervisor monitors the application of the data protection rules for the SIS managed by eu-LISA. National and EU-level data protection authorities meet approximately twice a year to ensure coordinated end-to-end supervision.
Participating states	The SIS is in operation in 30 European countries, including 26 EU Member States (Ireland and Cyprus are not yet connected to SIS) and 4 Schengen Associated Countries (Switzerland, Norway, Liechtenstein and Iceland). There exist limitations on the use of SIS in some EU Member States. As Bulgaria, Romania and Croatia are not yet part of the area without internal border checks there are still some restrictions regarding their use of Schengen-wide SIS alerts for the purposes of refusing entry into or stay in the Schengen area. When these countries become part of the area without internal border checks, the restriction to their use of SIS will be lifted. The United Kingdom operates SIS but as it has chosen not to join the Schengen area, it cannot issue or access Schengen-wide alerts for refusing entry or stay into the Schengen area.[252]
Cost of the system	At the end of February 2013, the total budgetary commitments made by the Commission on the SIS II project since 2002 amounted to EUR 167,784,606.[253]
Roles and responsibilities of EU bodies	Each Member State that uses SIS is responsible for setting up, operating and maintaining its N-SIS and its national SIRENE Bureau. The EU Agency for large-scale IT systems, eu-LISA, is responsible for the operational management of SIS and the communication infrastructure. The European Commission is responsible for the general oversight and evaluation of the system, including the correct application and implementation of its legal framework. The SISVIS Committee, comprising technical and operational experts from the Member States and chaired by the Commission, facilitates the exchange of best practice ideas between Member States to harmonise operational procedures for the purpose of optimising the use of SIS.
Data storage and security specifications, where available	Analysis of SIS II architecture indicates that there have been no incidents where data at the central level were at risk of compromise. Security of Central SIS II was said to be 'highly effective' in a 2016 security audit.[254]
Challenges	An issue for SIS II outlined in a SIS II evaluation to Parliament was poor data quality, where 'Member States sometimes enter incorrect or incomplete data (for instance, an incomplete name or a name instead of a document number).' Furthermore, 'New categories of alert or the new functionalities (fingerprints, photographs, European Arrest Warrant, links, misused identity extension) are not fully implemented and displayed to the end-users, contrary to the SIS II legal instruments'. This would serve to diminish the effectiveness of the system as end-users may not have all the relevant information on a case at their disposal. The report also highlighted data privacy/protection issues surrounding the collection and storage of data in SIS II, particularly with regard to compliance with the EU data protection reform.[255]

[252] European Commission, Migration and Home Affairs, Schengen Information System, accessed 8/12/12. https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[253] http://europa.eu/rapid/press-release_MEMO-13-309_en.htm

[254] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of the second-generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA.

[255] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of the second-generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA.

Entry/Exit System (EES)

Table 8: Information system summary profile: EES

EES	
Type of system	The EES would involve the systematic recording of the time of entry and exit of passengers crossing the EU external borders and the provision of alerts to authorities when third-country nationals overstay in the EU. The EES will consist of a central system, operating a computerised central database of biometric and alphanumeric data, a National Uniform Interface in each Member State, and a secure and encrypted communication infrastructure between the EES central system and the National Uniform Interfaces.
Purpose and objectives of system	**Primary purpose:** To improve the management of external borders, prevent irregular immigration and facilitate the management of migration flows in the Schengen area. **Ancillary purposes:** • To strengthen internal security and the fight against terrorism by permitting law enforcement authorities access to travel history records. • To ease the crossing for the large majority of 'bona fide' third-country travellers.
Scope of system	All **non-EU citizens** travelling to the EU.
Data collected and held by system	• Alphanumeric data including: name, nationality and passport number, • Fingerprints, • Photographs, • Time, • Place of entry, • Length of authorised short stay.
Size of system	**More than 350 million** (based on annual figures of international tourist arrivals in EU27).
Data retention specifications	The retention time for stored data is **five** years.
Data input process	National border, visa and migration authorities.
Access rights	Designated competent **visa** and **border authorities** at consular posts and at border crossing points. **Access by law enforcement authorities** could be allowed in clearly defined cases (particularly when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences).
Relevant data protection regulatory framework	The European Data Protection Supervisor and the national data protection authorities are set to be in charge of supervision for data processing.

Participating states	Schengen area
Cost of the system	Amount required for development, integration of the existing national border infrastructures in Member States with the EES, and expenses related to operations in the Member States is **EUR 480 million.**[256]
Roles and responsibilities of EU bodies	Database manager is the **Large-scale IT Agency** in Tallinn. Data processing would be supervised by the **European Data Protection Supervisor.**
Data storage and security specifications, where available[257]	Member States are responsible for ensuring the security of the data before and during the transmission to the National Uniform Interface. Each Member State is responsible for ensuring the security of the data it receives from the EES. Each Member State shall, in relation to its national border infrastructure, adopt the necessary measures, including a security plan and a business continuity and disaster recovery plan, in order to: a. physically protect data, including by making contingency plans for the protection of critical infrastructure; b. deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purposes of the EES; c. prevent the unauthorised reading, copying, modification or removal of data media; d. prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data; e. prevent the unauthorised processing of data in the EES and any unauthorised modification or deletion of data processed in the EES; f. ensure that persons authorised to access the EES have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only; g. ensure that all authorities with a right of access to the EES create profiles describing the functions and responsibilities of persons who are authorised to enter, amend, delete, consult and search the data and make their profiles available to the national supervisory authorities referred to in Article 49 and to the national supervisory authorities referred to in Article 52(2) without delay at their request; h. ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment; i. ensure that it is possible to verify and establish what data has been processed in the EES, when, by whom and for what purpose; j. prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the EES or during the transport of data media, in particular by means of appropriate encryption techniques; k. monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation.
Challenges	There are concerns over data collection practices with respect to EES and whether collecting biometrics of every visitor to the Schengen zone is necessary to accomplish the ultimate purpose of this system when it is fully operational. The EDPS would first stress that from the point of view of Articles 7 and 8 of the Charter the processing of personal data entailed under the proposed EES is significant and intrusive.[258]

[256] http://data.consilium.europa.eu/doc/document/PE-47-2017-INIT/en/pdf

[257] Regulation of the European Parliament and of the Council: establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011.

[258] Opinion 06/2016: EDPS Opinion on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System.

European Travel Information and Authorisation System (ETIAS)

Table 9: Information system summary profile: ETIAS

ETIAS	
Type of system	Centralised system consisting of an information system, a central unit and national units. Will be managed by the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice eu-LISA.
Purpose and objectives of system	**Primary purpose:** • To identify any risks associated with a visa-exempt visitor travelling to the Schengen area. **Ancillary purpose:** • To facilitate the prevention, detection or investigation of a terrorist offence, or other serious criminal offences.
Scope of system	Each citizen from the 60 visa-free countries (to enter the Schengen area) needs to hold a valid ETIAS prior to boarding. Once issued, a valid authorisation will allow its holder to stay in the Schengen area for a period of up to 90 days in any 180-day period and it is **valid for 3 years** from the date of issuance or until the expiry date of the passport, whichever comes first.
Data collected and held by system	• Biographical data, including the applicant's nationalities (if more than one) and the first name(s) of the applicant's parents; • data concerning the travel document; • contact details (home address, or at least city and country of residence), email and phone number; • socioeconomic data (education level and field, current occupation); • Member State of first entry; • in the case of applications filled in by a person other than the applicant, biographical details of that person, details of the firm or organisation, contact details of the intermediary and relationship to the applicant; and • answers to a set of specific questions related to whether the applicant has been subject to any disease with epidemic potential or other infectious or contagious parasitic diseases; his or her criminal convictions; any stays in a specific war or conflict zone over the last ten years and the reasons for the stay; and whether the applicant has been subject to any decision requiring him or her to leave the territory of a Member State or any other country or any return decision issued over the last ten years. • IP address from which the application was submitted.
Size of system	**PwC estimates 30 million**[259]
Data retention specifications	Article 47(1) of the Proposal for ETIAS foresees that each ETIAS application file will be stored in the system: a) for the validity period of the granted authorisation, b) for the following five years from the last entry record of the applicant stored in the EES, or c) for the following five years from the last decision to refuse, revoke or annul the travel authorisation.

[259] PwC Report: European Travel Information and Authorisation System (ETIAS), 2016.

Data input process	Citizens of the 60 visa-free countries
Access rights	ETIAS proposal foresees access to ETIAS data for private entities (at this stage carriers) and public bodies (at this stage border authorities at the external borders and law enforcement authorities of the Member States and Europol).
Relevant data protection regulatory framework	The European Data Protection Supervisor and the national data protection authorities are set to be in charge of supervision for data processing.
Participating states	EU Schengen states
Cost of the system	According to the Commission, ETIAS will be financially self-sustaining. It is estimated that the costs for developing it will amount to EUR 212.1 million, while the average annual operations costs, to be covered by the revenue from fees, will be EUR 85 million.
Roles and responsibilities of EU bodies	1. The European Coast and Border Guard Agency shall be responsible for: a. the setting up and operation of the ETIAS Central Unit; b. the automated processing of applications; c. the screening rules.[260] 2. 'Before being authorised to process data recorded in the ETIAS Central System, the staff of the ETIAS Central Unit having a right to access the ETIAS Central System shall be given appropriate training about data security and data protection rules, in particular on relevant fundamental rights.'[261] **Europol:** • Europol shall ensure processing of the queries referred to in Article 18(2)(j) and (4) and accordingly adapting its information system. • Europol shall be responsible for the establishment of the ETIAS watch list pursuant to Article 29. • Europol shall be responsible for providing an opinion following a consultation request pursuant to Article 26.[262]
Data storage and security specifications, where available	N/A

[260] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, 2016.

[261] Ibid.

[262] Ibid.

Challenges	EDPS has stated that 'The establishment of ETIAS would have a significant impact on the right to the protection of personal data, since various kinds of data, collected initially for very different purposes, will become accessible to a broader range of public authorities (i.e. immigration authorities, border guards, law enforcement authorities, etc.).'[263] The EDPS raises concerns over a lack of transparency in how ETIAS determines the possible risks posed by an applicant and specifically the use of health data in assessing this risk.

[263] EDPS (2017) Summary of the Opinion of the European Data Protection Supervisor on the Proposal for a European Travel Information and Authorisation System (ETIAS), 2017.

European Criminal Records Information System for Third-country Nationals (ECRIS-TCN)

Table 10: Information system summary profile: ECRIS

ECRIS[264]	
Type of system	**Decentralised –** criminal records are stored solely in national databases and exchanged between the designated central authorities of Member States, upon request, using a standardised format, through the S-TESTA common communication infrastructure. Data must be exchanged within short deadlines of 10 or 20 days. **ECRIS-TCN:** Through 2016 and 2017, the Commission has developed two proposals related to the identification of third-country nationals through ECRIS: i. Proposal for a Directive as regards the exchange of information on third-country nationals. This proposal aims to amend Council Framework Decision 2009/315/JHA and replace Council Decision 2009/316/JHA.[265] ii. Proposal for a Regulation (accompanying the above Directive) establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCNs) to supplement and support ECRIS. This proposal aims to amend eu-LISA's founding Regulation, requiring them to provide a **centralised system** for TCNs.[266]
Purpose and objectives of system	Efficient information exchange for the purposes of: i. criminal proceedings against a person (implementation of Council Framework Decision 2008/675 on taking account of previous convictions in new criminal proceedings against the same person); ii. recruitment procedures with regard to posts involving direct and regular contact with children (required by Article 10 of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography); and iii. any other purpose according to national law (for example, recruitment procedures, naturalisation procedures, asylum procedures, firearm licence procedures, child adoption procedures etc.).
Scope of system	National-level databases holding criminal records data. **ECRIS-TCN:** The 2016 and 2017 Commission's proposals for ECRIS-TCN establish a centralised system covering third-country nationals and stateless persons (TCN).

[264] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States; Council Framework Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA; and http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm. This table presents information on both the current implementation of ECRIS and the proposed ECRIS-TCN.

[265] Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA.

[266] Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011.

Data collected and held by system	Data that can be exchanged through ECRIS is separated into three types, as follows: • **Obligatory information:** a. information on the convicted person (full name, date of birth, place of birth (town and State), gender, nationality and – if applicable – previous name(s)); b. information on the nature of the conviction (date of conviction, name of the court, date on which the decision became final); c. information on the offence giving rise to the conviction (date of the offence underlying the conviction and name or legal classification of the offence as well as reference to the applicable legal provisions); and d. information on the contents of the conviction (notably the sentence as well as any supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence); • **Optional information:** a. the convicted person's parents' names; b. the reference number of the conviction; c. the place of the offence; and d. disqualifications arising from the conviction; • **Additional information:** a. the convicted person's identity number, or the type and number of the person's identification document; b. fingerprints, which have been taken from that person; and c. if applicable, pseudonym and/or alias name(s). In addition, the central authority may transmit any other information concerning convictions entered in the criminal record. **ECRIS-TCN:** The centralised system to be developed under the Commission's 2017 proposal, ECRIS-TCN should contain only the identity information of TCNs convicted by a criminal court within the European Union, including: • alphanumeric data • fingerprint data in accordance with Framework Decision 2009/315/JHA, as amended by the 2016 proposed Directive; and • facial images to the extent they are recorded in the national criminal records databases.
Size of system	300,000 messages had been exchanged between Member States by the end of 2012. This increased significantly to 2016, which saw the exchange of 1,978,104 messages within the year covering notifications, updates, requests, replies, denials, other replies, exchanges of additional information. In 2016, 331,878 notifications of new convictions were sent; 364,751 requests were sent and 350,681 replies were sent.
Data retention specifications	Data retention of data held in national criminal records databases is governed by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on 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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
Data input process	Data input governed by the national authorities responsible for the storage of criminal records data at the national-level. **ECRIS-TCN:** Data input by central authorities designated under Framework Decision 2009/315/JHA, to be amended by the Commission's 2016 proposal.
Access rights	Member State central authorities do not have direct access to data held by other Member States. **ECRIS-TCN:** Member States have hit/no-hit access to the centralised system proposed under the Commission's 2017 proposed Regulation.

Relevant data protection regulatory framework	Data held in national criminal records databases are governed by Directive (EU) 2016/680. The conditions for the use of personal data transmitted via ECRIS are established in Article 9 of Council Framework Decision 2009/315/JHA.
Participating states	All 28 EU Member States are connected to ECRIS, with Slovenia and Portugal joining in January 2017; however, no Member State is exchanging information through ECRIS with all other 27 Member States. 76% of the total number of interconnections between Member States had been used by the end of 2016.[267]
Cost of the system	Member States are required to bear their own costs in relation to implementation, administration, use and maintenance of their criminal records database and the interconnection software used to enable the exchange of information through S-TESTA. **ECRIS-TCN:** Anticipated costs for the implementation of the Commission's 2017 proposed Regulation: • EU budget: one-off costs of approximately EUR 13,002,000; and ongoing costs of EUR 2,133,000. • Member State budgets: one-of costs of approximately EUR 13,344,000; and ongoing costs of EUR 6,087,000 (anticipated to increase over the years up to a maximum of EUR 15,387,000.
Roles and responsibilities of EU bodies	S-TESTA, the common communication infrastructure used for the exchange of information under ECRIS, is operated under the responsibility of the Commission. As such, the Commission shall provide general support and technical assistance to ensure the efficient operation of ECRIS. **ECRIS-TCN:** Under the Commission's proposed Regulation, eu-LISA would take responsibility for the centralised system.
Data storage and security specifications, where available	As per article 6 of Council Framework Decision 2009/315/JHA, the relevant departments of the Member States and the Commission shall coordinate their action, in particular regarding the adoption of technical specifications of the exchange, including security requirements Article (6)(2)(b)(ii).
Challenges	The original ECRIS configuration requires that, in order to request information on third-country nationals (TCNs), Member States need to send 'blanket requests' to all Member States. This is because ECIRS is based on the principle that criminal records information can be retrieved from the Member State of nationality of the individual. TCNs do not have such nationality and thus cannot be the subject of a targeted search. Hence the 2016 and 2017 Commission proposals have been developed.

[267] European Commission (2017), Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States.

APPENDIX 2: BIBLIOGRAPHY

- Baldaccini, A (2008) 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases' (2008) 10(1) *European Journal of Migration and Law*.
- CJEU Huber v. Germany, C-524/06, 16 December 2008, paras 78–79.
- Commission Decision of 17 June 2016 setting up the High-Level Expert Group on Information Systems and Interoperability (2016/C 257/03).
- Commission Implementing Decision (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the Sirene Manual and other implementing measures for the second-generation Schengen Information System (SIS II) (notified under document C(2015) 326).
- Commission Recommendation of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area.
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).
- Council Decision establishing the Visa Information System (VIS), 2004/512/EC, 8.6.2004; Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).
- Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States.
- Council Framework Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA.
- Council of the European Union (2016) European Council meeting (15 December 2016) – Conclusions, Document EUCO 34/16 (15.12.2016).
- Council of the European Union (2016) Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, Document 9368/1/16 (06.06.2016).
- Council of the European Union, Combating terrorism, Document 13176/01 (24.10.2001).
- Council of the European Union, Council Conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal immigration, Document 6975/10 (01.03.2010), point 20, p. 7.
- Council of the European Union, Declaration condemning the terrorist attacks on London, Document 11116/05 (Presse 187).
- Council of the European Union, Declaration on combating terrorism, Document 7906/04 (29.03.2004).
- Council of the European Union, European Council meeting (17 and 18 December 2015) – Conclusions, Document EUCO 28/15 (18.12.2015).
- Council of the European Union, Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016, Statements and remarks 158/16 (24.03.2016).

- Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.
- Council Regulation (EC) No. 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national.
- Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA.
- Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States.
- De Hert, P. and Gurtwirth, S. (2006) Interoperability of Police Databases within the EU: An Accountable Political Choice? *International Review of Law Computers and Technology*, Vol. 20, Nos 1&2, pp. 21–35, March–July 2006.
- Estonian Department of State Information Systems, Ministry of Economic Affairs and Communications. Estonian IT Interoperability Framework.
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography
- ECtHR, S. and Marper v. United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 124–125.
- EDPS (2006) Comments on the Communication of the Commission on interoperability of European databases. Brussels, 10 March 2006, p.6.
- EDPS (2017) Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice.
- EDPS (2017) Summary of the Opinion of the European Data Protection Supervisor on the Proposal for a European Travel Information and Authorisation System (ETIAS), 2017.
- ENISA (2016) Security guidelines on the appropriate use of qualified electronic time stamps.
- EPRS (2017) Addressing migration in the European Union, Selected publications by the European Parliamentary Research Service.
- EPRS (2017) European information systems in the area of justice and home affairs: An overview.
- EPRS (2018) Interoperability between EU information systems for security, border and migration management. Briefing: Initial Appraisal of a European Commission Impact Assessment.
- eu-LISA (2014) Report on the technical functioning of VIS, eu-LISA.
- eu-LISA (2017) Annual report on the 2016 activities of the Eurodac central system, including its technical functioning and security pursuant to Article 40(1) of Regulation (EU) No 603/2013.
- eu-LISA, (2016) 'Eurodac – 2015 Statistics'.
- European Commission (2001) Development of the Schengen Information System II, COM(2001)720 final, 18.12.2001.

- European Commission (2005) Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. COM(2005) 597 final (24.11.2005).
- European Commission (2008) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions: Preparing the next steps in border management in the European Union. COM(2008) 69 final.
- European Commission (2014) Technical Study on Smart Borders, DG HOME.
- European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe {SWD(2015) 100 final}.
- European Commission (2016) Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security. COM(2016) 205 final (06.04.2016).
- European Commission (2017) Fourth progress report towards an effective and genuine Security Union. COM(2017) 41 final (25.01.2017).
- European Commission (2017) New European Interoperability Framework: Promoting seamless services and data flows for European public administrations. p.5.
- European Commission (2017) Seventh progress report towards an effective and genuine Security Union. COM(2017) 261 final (16.5.2017).
- European Commission (2017) Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States.
- European Commission Staff Working Document. Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation.
- European Council (2017) European Council meeting (22 and 23 June 2017) – Conclusions, Document EUCO 8/17 (23.06.2017).
- European Interoperability Framework for Pan-European eGovernment Services, Office of Official Publications of the European Communities, 2004, point 1.1.2.
- European Parliament (2017) European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection. Study for the LIBE Committee.
- Fundamental Rights Agency (FRA) (2017) Fundamental rights and the interoperability of EU information systems: borders and security.
- High-Level Expert Group on Information Systems and Interoperability: Final report. May 2017. Ref.Ares(2017)2412067 – 11/05/2017.
- High-Level Expert Group on Information Systems and Interoperability: Scoping Paper, June 2016.
- Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and The Council on establishing a framework for interoperability between EU

information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

- Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in Member States of the European Union in the course of new criminal proceedings.
- Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Ireland* (08.04.2014) para 62.
- Jones, C (2014). 11 Years of Eurodac, *Statewatch.*
- Kubicek, H. and Cimander, R. (2005) Interoperability in Government. A survey on information needs of different EU stakeholders. *European Review of Political Technologies*, No 3, pp. 1–17, December 2005.
- Meijers Committee. CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM (2017) 794.
- Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS) and replacing Council Decision 2009/316/JHA.
- Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011, 29 June 2017.
- Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, Brussels 28.2.2013.
- Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, Brussels, 12.12.2017.
- Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 793 final, Strasbourg, 12.12.2017.
- Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.
- Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624.
- PwC (2016) European Travel Information and Authorisation System (ETIAS).

- Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second-Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates.
- Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).
- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
- Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Regulation of The European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.
- Report from the Commission to the European Parliament and the Council (201) concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States.
- Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, 2016.

- Report from the Commission to the European Parliament and the Council on the evaluation of the second-generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA, 2016.
- Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, 2016.
- State of the Union 2016 by Jean-Claude Juncker, President of the European Commission, 14 September 2016.
- The Hague Programme: strengthening freedom, security and justice in the European Union, 10 May 2005.
- Vavoula, N. (2015) The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals? in Céline Bauloz and others (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Brill 2015).
- Vavoula, N (2018) *Immigration and Privacy in the Law of the EU – The Case of Databases* (Brill Nijhoff, forthcoming 2018).
- Wallwork, A. and Baptista, J. Future of Identity in the Information Society (FIDIS) Deliverables, Understanding interoperability.

APPENDIX 3: LIST OF CONTACTS

Table 11: List of stakeholder authorities / organisations interviewed

Country	Authority / organisation
EU level	
EU	EDPS
EU	eu-LISA
EU	FRA
EU	Frontex
EU	Unit B3, DG Migration and Home Affairs, European Commission
EU	Unit B3, DG Migration and Home Affairs, European Commission
Member State level	
Germany	Federal Ministry of the Interior
Germany	University of Freiburg
Estonia	Head of IT policy of the Ministry of the Interior, National SIS II project manager
Estonia	IT and Development Centre, Ministry of the Interior
France	Ministère de l'intérieur
France	French Permanent representation in Brussels
Sweden	Swedish Migration Agency
Sweden	Swedish Migration Agency, VIS Expert

NOTES

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, at the request of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), primarily assesses the Commission's December 2017 proposals for a Regulation on establishing a framework for interoperability between EU Justice and Home Affairs information systems. The study first analyses the relationships between the information systems in the current and proposed implementation before assessing the key elements of the Commission's proposals, including the concept of interoperability used, the problem definition and objectives and the proposed solutions, as well as the implementation, fundamental rights and data security implications.

Print ISBN 978-92-846-2678-6| doi: 10.2861/933364| QA-01-18-219-EN-C
PDF ISBN 978-92-846-2679-3| doi: 10.2861/603266| QA-01-18-219-EN-N