



Strasbourg, 12.12.2017  
SWD(2017) 473 final

PART 1/2

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**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)**

{COM(2017) 793 final} - {SWD(2017) 474 final}

# Table of contents

1.	INTRODUCTION: POLITICAL AND LEGAL CONTEXT .....	3
2.	PROBLEM DEFINITION .....	6
2.1.	What is the scope of the initiative?.....	6
2.2.	What is the problem?.....	9
2.3.	What are the problem drivers? .....	9
2.4.	How will the problem evolve? .....	12
3.	WHY SHOULD THE EU ACT? .....	12
3.1.	Legal basis .....	12
3.2.	Subsidiarity: necessity of EU action.....	13
3.3.	Added value of EU action from the point of view of EU citizens .....	13
3.4.	Public consultation .....	14
4.	OBJECTIVES: WHAT IS TO BE ACHIEVED? .....	15
4.1.	General objectives .....	15
4.2.	Specific objectives.....	15
5.	WHAT ARE THE AVAILABLE POLICY OPTIONS? .....	16
5.1.	Option 1: baseline representing current situation.....	16
5.2.	Option 2:High-level expert group approach to the management of data for borders and security .....	17
5.2.1.	European search portal .....	17
5.2.2.	Shared biometric matching service .....	19
5.2.3.	Common identity repository.....	20
5.2.4.	Complete picture of option 2.....	22
5.3.	Option 3: enhanced identity management and streamlined law enforcement access .....	22
5.3.1.	Adding a technical component to achieve interoperability: multiple-identity detector 23	
5.3.2.	Establishing the rules on the use of EU information systems for checks within the territory .....	24
5.3.3.	Streamlining the rules on access to EU information systems for law enforcement purposes: flagging .....	25
5.3.4.	Complete picture of option 3.....	28
6.	WHAT ARE THE IMPACTS OF ENHANCING INTEROPERABILITY?.....	29
6.1.	Social impacts.....	29
6.1.1.	Impact on EU citizens .....	29
6.1.2.	Impact on third-country nationals .....	30
6.2.	Economic impacts .....	30

6.2.1.	Impact on tourism.....	30
6.2.2.	Impact on airports, seaports and carriers.....	31
6.3.	Impact on public services .....	31
6.3.1.	Impact on border management .....	31
6.3.2.	Impact on migration and asylum management.....	31
6.3.3.	Impact on police cooperation and law enforcement.....	32
6.4.	Impact on fundamental rights .....	33
6.5.	Impact on the right to personal data protection .....	34
6.5.1.	General aspects .....	34
6.6.	Safeguards .....	44
7.	HOW DO THE OPTIONS COMPARE?.....	45
7.1.	Option 1: no interoperability .....	45
7.2.	Option 2:High-level expert group approach to the management of data for borders and security .....	46
7.2.1.	Costs .....	46
7.2.2.	Data protection impacts .....	47
7.2.3.	Feasibility and enforcement .....	48
7.3.	Option 3: new approach to identity management and law enforcement access.....	49
7.3.1.	Costs .....	49
7.3.2.	Data protection impacts .....	51
7.3.3.	Feasibility and enforcement .....	51
7.4.	Conclusion.....	51
8.	HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?.....	53
8.1.	Practical arrangements of the evaluation: when, by whom.....	53
8.2.	Operational objectives and monitoring indicators for the preferred option.....	53
9.	LIST OF ANNEXES .....	55

## 1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

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. EU citizens expect external border controls on persons to be effective, to enable effective management of migration and to contribute to internal security. These challenges have brought into sharper focus the urgent need to join up and strengthen in a comprehensive manner the EU's information tools for border management, migration and security.

Information management in the EU can and must be made more effective and efficient, in full respect of fundamental rights including, in particular, the right to the protection of personal data, in order to better protect the EU's external borders, improve the management of migration and enhance internal security for the benefit of all citizens. There are already a number of information systems at EU level, and more systems are being developed, to provide border guards, immigration and law enforcement officers with relevant information on persons, but the EU information management architecture is not perfect. In particular, **the various information systems at EU level are currently not interoperable** — that is, able to exchange data and share information so that authorities and competent officials have the information they need, when and where they need it. Interoperability of EU-level information systems can significantly contribute to eliminating the current blind spots where persons, including those possibly involved in terrorist activities, can be recorded in different, unconnected databases under different aliases.

In its April 2016 *Communication Stronger and smarter information systems for borders and security*,<sup>1</sup> the Commission presented its vision on how to address a number of structural shortcomings related to information systems.<sup>2</sup> The aim of the April 2016 Communication was to initiate a discussion on how information systems in the European Union can better enhance border management and internal security. The Communication responded to the **European Council** Conclusions of 18 December 2015,<sup>3</sup> which had stated that '*recent terrorist attacks demonstrate in particular the urgency of enhancing relevant information sharing, notably as regards [...] ensuring the interoperability of the relevant databases with regard to security checks*'. In his State of the Union address in September 2016,<sup>4</sup> President Juncker emphasised the importance of urgent progress in this area.

The **Council**, for its part, similarly recognised the urgent need for action in this area. In June 2016, it endorsed a **roadmap to enhance information exchange and information management**, including interoperability solutions in the Justice and Home Affairs area.<sup>5</sup> The purpose of the roadmap was to support operational investigations and to swiftly

---

<sup>1</sup> COM(2016) 205 of 6 April 2016.

<sup>2</sup> (1) Sub-optimal functionalities in some of the existing information systems; (2) information gaps in the EU's architecture of data management; (3) a complex landscape of differently governed information systems; and (4) a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots.

<sup>3</sup> [European Council Conclusions](#), 17-18 December 2015.

<sup>4</sup> [State of the Union 2016](#) of 14 September 2016.

<sup>5</sup> Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

provide front-line practitioners — such as police officers, border guards, public prosecutors, immigration officers and others — with comprehensive, topical and high-quality information to cooperate and act effectively. This was followed by further European Council Conclusions, in December 2016, which called for continued delivery on the interoperability of information systems and databases.<sup>6</sup>

The **European Parliament** has also urged action in this area. In its July 2016 Resolution<sup>7</sup> on the Commission's work programme for 2017, Parliament called for '*proposals to improve and develop existing information systems, address information gaps and move towards interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by necessary data protection safeguards*'.

In line with the April 2016 Communication, and the areas for action it identified, some progress has been made towards reinforcing the EU's information infrastructure in the area of borders and security.

First, the Commission took **action to strengthen and maximise the benefits of existing information systems**. In December 2016, the Commission adopted proposals for the further reinforcement of the existing Schengen Information System (SIS).<sup>8</sup> In the meantime, following the Commission's proposal of May 2016,<sup>9</sup> negotiations were accelerated on the revised legal basis for Eurodac — the EU asylum fingerprint database. A proposal for a new legal basis for the Visa Information System (VIS) is also under preparation, and will be submitted in the second quarter of 2018.

Second, the Commission proposed **additional information systems to address identified gaps** in the EU's data management architecture. Based on the Commission's April 2016 proposal to establish an Entry/Exit System (EES),<sup>10</sup> the co-legislators reached a political agreement, confirmed by the European Parliament in October 2017 and formally adopted by the Council in November 2017. In November 2016, the Commission also presented a proposal for the establishment of a European Travel Information and Authorisation System (ETIAS),<sup>11</sup> to strengthen security checks on visa-free travellers by enabling advance irregular migration and security vetting. The ETIAS proposal is currently under negotiation by the co-legislators. In June 2017, the European Criminal Record Information System for third-country nationals (ECRIS-TCN system)<sup>12</sup> was also proposed to address the gap identified with regards to exchange of information between Member States on convicted non-EU nationals.

Third, the Commission worked **towards the interoperability of information systems**, focusing on the four options presented in the April 2016 Communication to achieve interoperability:

---

<sup>6</sup> [European Council Conclusions](#), 15 December 2016.

<sup>7</sup> European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ([2016/2773\(RSP\)](#)).

<sup>8</sup> COM(2016) 883 final.

<sup>9</sup> COM(2016) 272 final.

<sup>10</sup> COM(2016) 194 final.

<sup>11</sup> COM(2016) 731 final.

<sup>12</sup> COM(2017) 344 final.

- a **single-search interface** to query several information systems simultaneously and to produce combined results from the systems queried on one single screen;
- the **interconnectivity of information systems** where data registered in one system will automatically be consulted by other systems;
- the establishment of a **shared biometric matching service** to enable searches across different information systems holding biometric data; and
- a **common identity repository** with alphanumeric data for different information systems (including common biographical attributes such as name and date of birth), *inter alia* to detect if a person is registered under multiple identities in different databases.

In June 2016, as a follow-up to the April 2016 Communication, the Commission set up a **high-level expert group on information systems and interoperability**<sup>13</sup> in order to address the legal, technical and operational challenges of the above options to achieve interoperability between central EU information systems for borders, migration and security. The high-level expert group was also asked to identify and address shortcomings and potential information gaps caused by the complexity and fragmentation of information systems.<sup>14</sup> The objective was to take a broad and comprehensive perspective on the information management landscape, taking into account also the relevant roles, responsibilities and systems for customs authorities. The Commission's 2017 work programme<sup>15</sup> signalled the intention to make border management and law enforcement systems more interoperable.

The **final report of the high-level expert group** was published in May 2017.<sup>16</sup> It set out a range of recommendations to strengthen and develop the EU's information systems and interoperability. The EU Agency for Fundamental Rights, the European Data Protection Supervisor and the EU Counter-Terrorism Coordinator had all participated actively in the work of the expert group. Each submitted supportive statements while acknowledging wider issues on fundamental rights and data protection had to be properly addressed. The high-level expert group concluded that it is **necessary and technically feasible to work towards the following three solutions for interoperability** and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements:

- a European search portal;<sup>17</sup>
- a shared biometric matching service; and
- a common identity repository.

The final report of the high-level expert group also addresses other issues such as the implementation of existing systems including the Prüm framework<sup>18</sup> or the Passenger

<sup>13</sup> Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability — 2016/C 257/03.

<sup>14</sup> [Scoping paper of the high-level expert group on information systems and interoperability.](#)

<sup>15</sup> [COM\(2016\) 710 final.](#)

<sup>16</sup> <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

<sup>17</sup> The term 'single-search interface' was changed to 'European search portal' to avoid any confusion with national single-search interfaces that exist in Member States for national information systems.

<sup>18</sup> [http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936184412&uri=CELEX:32008D06\\_15](http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936184412&uri=CELEX:32008D06_15).

Name Record directive<sup>19</sup>, and potential new systems such as a repository for long-stay visas. The Commission has undertaken to assess these and other recommendations that are not the subject of immediate follow-up through proposals, and for some of which studies have been commissioned.

Responding to the expert group's report and recommendations, the Commission set out, in the *Seventh progress report towards an effective and genuine Security Union*,<sup>20</sup> a **new approach to the management of data for borders and security** where all centralised EU information systems for security, border and migration management are interoperable in full respect of fundamental rights. The Commission announced its intention to pursue work towards creating a European search portal capable of searching in parallel all relevant EU systems in the areas of security, border and migration management, possibly with more streamlined rules for law enforcement access, and to develop for these systems a shared biometric matching service (possibly with a hit-flagging functionality<sup>21</sup>) and a common identity repository. It announced its intention to present, as soon as possible, a legislative proposal on interoperability.

This initiative responds to the Council's call for a comprehensive framework for law enforcement access to the various databases in the area of justice and home affairs, with a view to greater simplification, consistency, effectiveness and attention to operational needs.<sup>22</sup> The European Council conclusions of June 2017<sup>23</sup> reiterated the need to act. Building on the June 2017 conclusions<sup>24</sup> of the Justice and Home Affairs Council, the European Council invited the Commission to prepare, as soon as possible, draft legislation enacting the recommendations made by the high-level expert group. In order to reinforce the efforts to make the European Union a safer society, in full compliance with fundamental rights, the Commission announced, in its 2018 Work Programme,<sup>25</sup> a proposal on the interoperability of information systems to be presented by the end of 2017.

## 2. PROBLEM DEFINITION

### 2.1. What is the scope of the initiative?

This initiative addresses the lack of interoperability between EU-level information systems for security, border and migration management, and the way in which they provide data to national authorities for managing external borders, migration and combating crime and terrorism. It focuses on the six EU information systems that are operated at the central level, three of them existing, and three others still in preparation or

---

<sup>19</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936384641&uri=CELEX:32016L06 81>.

<sup>20</sup> COM(2017) 261 final.

<sup>21</sup> New privacy-by-design concept that restricts the access to all data by limiting it to a mere 'hit/no-hit' notification, indicating the presence (or non-presence) of data.

<sup>22</sup> The Council's Committee of Permanent Representatives (Coreper), upon giving the mandate to the Council Presidency to start interinstitutional negotiations on the EU Entry/Exit System on 2 March 2017, called on the Commission to propose a comprehensive framework for law enforcement access to the various databases in the area of justice and home affairs, with a view to greater simplification, consistency, effectiveness and attention to operational needs.

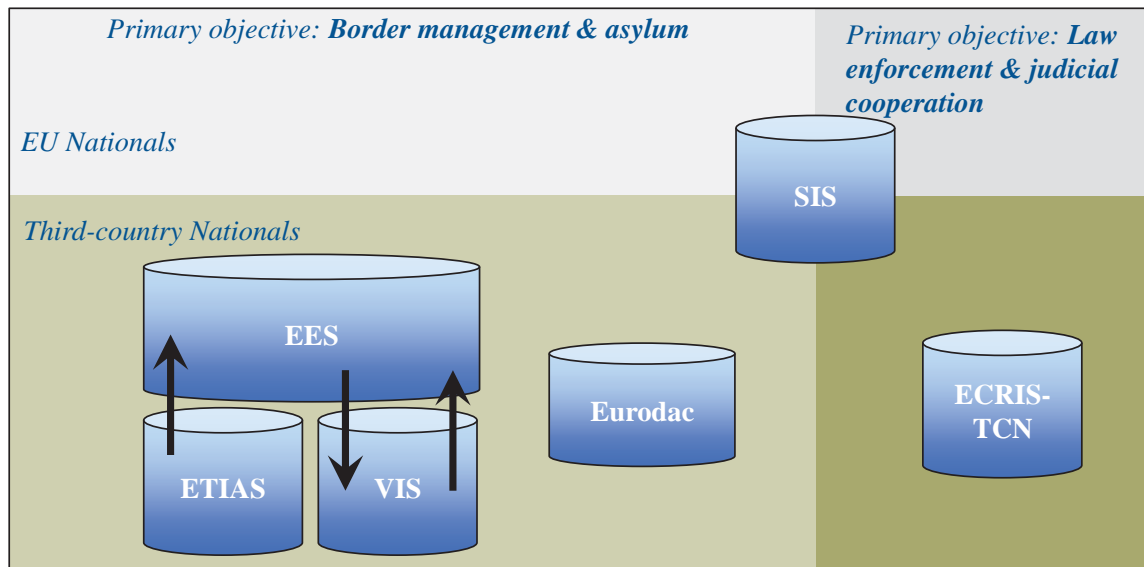
<sup>23</sup> [European Council conclusions](#), 22-23 June 2017.

<sup>24</sup> [Outcomes of the 3546th Council meeting on Justice and Home Affairs on 8 and 9 June 2017, 10136/17](#).

<sup>25</sup> COM(2017) 650 final.

development. Each system has its own objectives, purposes, legal bases, user groups and institutional context. But they also have similarities and overlaps. (See Annex 7 for a fuller description of each of the systems covered by the interoperability proposal.)

Figure 1 — Overview of the six central systems



The three centralised information systems developed by the EU so far are:

- the Schengen Information System (SIS) with a broad spectrum of alerts on persons (refusals of entry or stay; EU arrest warrant, missing persons, judicial procedure assistance, discreet checks) and objects (including lost, stolen and invalidated identity or travel documents);
- the Eurodac system with fingerprint data of asylum applicants and third-country nationals who have crossed the external borders irregularly or illegally staying in a Member State; and
- the Visa Information System (VIS) with data on short-stay visas.

These three systems are complementary and — with the exception of SIS — exclusively focused on third-country nationals. The systems support national authorities in managing borders, migration and asylum, and in fighting crime and terrorism. The latter applies in particular to the SIS, which is the most widely used law enforcement information-sharing instrument today.

In addition to these existing systems, the Commission proposed in 2016-2017 three new centralised EU information systems:

- the Entry/Exit System (EES), which was adopted in November 2017 and will replace the current system of manual stamping of passports. It will electronically register the name, type of travel document, biometrics and the date and place of entry and exit of third-country nationals visiting the Schengen area for a short stay;
- the European Travel Information and Authorisation System (ETIAS), which would, once adopted, be a largely automated system that would gather and verify information submitted by visa-free third-country nationals ahead of their travel to the Schengen area; and



- the proposed European Criminal Record Information System for third-country nationals (ECRIS-TCN system), which would be an electronic system for exchanging information on previous convictions handed down against third-country nationals by criminal courts in the EU.

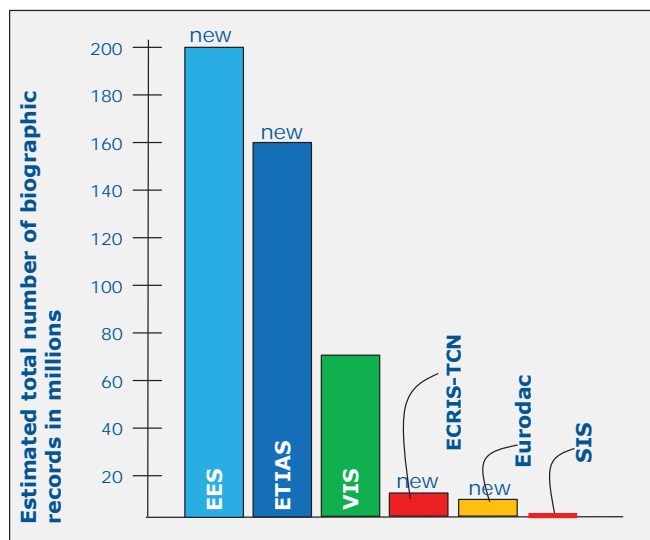
These three new systems are scheduled to be operational by 2020. It should be noted that the future EES and the proposed ETIAS have been conceived and proposed in such a way that they already present a degree of interoperability, i.e. between EES and ETIAS, and between EES and VIS.

The number and type of records varies greatly between central systems. As seen in Figure 2, the systems handling the most biographical identity records will be the future EES, the proposed ETIAS and VIS, followed by the proposed ECRIS-TCN system and Eurodac. These systems only hold data on third-country nationals.

The total number of people covered by this initiative is estimated to be close to 218 million:<sup>26</sup>

- Around 200 million third-country nationals visiting the Schengen area for a short-stay, either as a visa-exempt traveller or with a visa;
- Some 10 million third-country nationals for whom a conviction record in an EU Member State exists;
- Around 7 million asylum seekers and irregular migrants;
- Around 1 million persons for whom an alert is issued in SIS.

Figure 2 — Estimated biographical records by system by 2021



By focusing this initiative on enhancing the interoperability between SIS, Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system, the scope of the legislative proposal will primarily be on improving the management of data on **third-country nationals** stored in centralised EU information systems.

<sup>26</sup> Source: feasibility studies for EES and CIR, and current volumes for Eurodac and SIS.

## 2.2. What is the problem?

Information is one of the essential commodities the EU provides to support national authorities in managing the external border and countering crime and terrorism. To help national authorities addressing today's cross-border threats, the information provided by EU centralised information systems needs to be complete, accurate and reliable. Moreover, to make best use of existing information where necessary, end-users of competent national authorities need to have fast and systematic access to the information that they need to perform their tasks. However, there are currently **limits in the way EU systems provide information** to border guards, law enforcement officers, immigration officials and judicial authorities on the ground.

These limits manifest themselves in two ways. First, information provided by EU systems is **not always complete, accurate and reliable**. The information provided by EU systems is sometimes incomplete in as far as it does not recognise connections between different pieces of registered information, leading to blind spots and incomplete pictures for competent authorities. This makes it very difficult to detect multiple identities or to combat identity fraud.

Second, **end-users do not always have fast and systematic access to all the information they need** to perform their tasks. For most user purposes, the issue is not that the access rights of the end-users, as set out in EU legislation, are too limited. The problem is rather that the existing access rights, as laid down in the EU legal instruments that govern the systems, cannot be used to the full because of a lack of technical and practical means at national level. For example, determining the Member State responsible for examining an application for international protection under the Dublin Regulation<sup>27</sup> is inefficient and insecure because of the impossibility to perform a single parallel search in the VIS (i.e. country of issue of visas) and Eurodac (i.e. country of entry and/or stay). Additional difficulties exist as regards the access to information systems on migration management (VIS and Eurodac) for law enforcement purposes, i.e. for the prevention, detection or investigation of terrorist offences or other serious offences. Several Member States have reported that the complexity of the procedural requirements for accessing VIS and Eurodac for law enforcement purposes is in practice very difficult to handle for the relevant authorities and constitutes a deterrent for actual consultation of these systems. The final report of the high-level expert group confirms that the current rules for law enforcement access do not always meet operational needs.

## 2.3. What are the problem drivers?

As identified by the Communication *Stronger and smarter information systems for borders and security*, and confirmed by the findings of the high-level expert group, there are two main **underlying causes** for the limits in the way EU systems provide information:

- 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.

These problem drivers affect in several ways the functioning and added value of EU information systems.

---

<sup>27</sup> OJ L 180, 29.6.2013, p. 40.

(a) *Fragmented architecture of data management for borders and security*

The main driver for the problem related to incomplete information and the difficulties to detect multiple identities and combat identity fraud is that identity data (including biometric identifiers) are not treated in their own right across the different systems due to the **fragmentation of information systems where data is stored in separate silos**. As an example, a visa application contains application data valid at a given moment and data identifying the applicant that are mainly constant over time but which can undergo lawful changes under some circumstances. When not handling identification data distinctly, they are created again for each system.

The current situation where information is collected and stored in separate and unconnected information systems leads to blind spots or incomplete pictures for competent authorities, as it may be very difficult to identify connections between different pieces of registered information. This fragmentation makes it very difficult to detect multiple identities or to combat identity fraud, which presents significant risks in an area of free movement of persons. Repeated and separate storing of personal information in separate and unconnected systems makes it possible that people are recorded under different identities, without this being detected. Ultimately, as it has been reported, one person may end up having different identities recorded in SIS, Eurodac and VIS, while national authorities are unable to distinguish the cases where the difference points to identity fraud or to a regular situation (e.g. change of name, multiple nationalities etc.).

When this concerns *bona fide* persons, the issue can create major inconveniences for the persons concerned when these inconsistencies are discovered. If the mismatch is the result of the fraudulent use of travel or ID documents, it can become a serious breach of security.<sup>28</sup> Undetected cases of multiple (fictitious) identities, identity fraud and document fraud lead to inconsistency in the data that EU information systems provide to end-users. This in turn undermines the accuracy, reliability and added value of information as one of the key tools that the EU provides to national authorities in the fight against crime and terrorism.

Another driver of the problem related to difficulties to detect multiple identities and combat identity fraud concerns the **obstacles that exist for competent authorities to verify the identity of persons within the territory of a Member State**. In general, authorities know much less about fleetingly present third-country nationals than about stable residents (the vast majority of whom are EU nationals). For myriad tasks, authorities need to know who they are talking to. Today, it is very difficult for an authorised official to check, in the territory of a Member State, the identity of a third-country national who cannot or is not willing to present his/her passport, identity card or other identity document.

The possibilities for accessing EU systems for identification purposes are limited. SIS is normally the only information system an authorised officer may have access to for the search or verification of a (claimed) identity. No access to Eurodac, VIS or the future

---

<sup>28</sup> The Commission, in its *Action plan to strengthen the European response to tackle travel document fraud*, (COM(2016) 790) set out recommendations for Member States to tackle the phenomenon of travel document fraud and outlined a comprehensive set of actions for the Commission to take.

EES is, however, legally possible or envisaged, except if an officer is authorised to make a check in the context of migration management (as provided for by national law) or if the check takes place in the framework of law enforcement in relation to terrorist offences or other serious criminal offences. In other situations that are not related to migration management or to terrorism and other serious crimes, e.g. the prevention, detection or investigation of crimes that do not pass the threshold of ‘serious’,<sup>29</sup> or when helping victims of accidents or crime, the police officer is not authorised to access Eurodac, VIS or the future EES to identify a third-country national on the territory. This impedes authorities in detecting multiple identities and identity fraud.

*(b) Complex landscape of differently governed information systems*

End-users face a complex landscape of differently governed information systems at EU level, and this is the main driver for the problem of inadequate access to information. Access to information systems is governed by the ‘purpose of access’ as defined in individual legal instruments for each system. Multiple user groups or organisations may share the same purpose of access to (certain data in) information systems. However, where these various user groups belong to different organisational entities, the actual physical access to these information systems can, depending also on applicable national implementing rules and procedures, be complex. **Physically granting, providing and controlling access for an increasing number of end-users to the necessary information systems, as provided for in the various legal instruments, is proving more and more difficult for Member State authorities.** Differences in relevant national legislation among Member States, but also the organisation of their national police and border management structures and the human and financial resources available, lead to a great variety of approaches and performance levels regarding the actual use of the respective systems.

The challenges are particularly present in the context of access to border and migration systems for law enforcement purposes, i.e. for the prevention, detection or investigation of terrorist offences or other serious offences. Law enforcement is defined as a secondary or ancillary objective of Eurodac, VIS, the future EES and the proposed ETIAS. As a result, the possibility of accessing data from these systems for this purpose is limited. **The systems are governed by diverse access conditions and safeguards for law enforcement purposes that can hinder the efficiency of the legitimate use of the systems by these authorities.** The varying and complex access conditions for law enforcement authorities results from three sources: the specific functionalities and the legal bases of the information systems; the data protection *acquis* at the moment of concluding the legal basis of the respective system; and the former ‘three-pillar’ structure of the Treaty of the European Union. This latter structure, which had migration and security legal bases placed in different pillars, and contained more limited competences of the Union in the area of security and crime, was discontinued by the Treaty of Lisbon.

Purpose limitation is a key principle of data protection as enshrined in the Charter of Fundamental Rights. Due to the different institutional, legal and policy contexts in which information systems at EU level were developed, the principle of purpose limitation was

---

<sup>29</sup> ‘Serious criminal offences’ means the 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.

implemented through a compartmentalised structure of information management. This is one of the reasons for the current fragmentation in the EU's architecture of data management for borders and security. As set out in the April 2016 Communication, with the new comprehensive framework for the protection of personal data in the EU in place, and significant developments in technology and IT security, the principle of purpose limitation can be more efficiently implemented as regards access to and use of information stored, in full compliance with the Charter of Fundamental Rights and with recent jurisprudence of the European Court of Justice.

#### **2.4. How will the problem evolve?**

Limits in the way EU systems provide information already exist today, with only three central systems in place. With the planned development of EES, the proposed ETIAS and the proposed ECRIS-TCN system, the challenges will, if not adequately addressed, only increase. With each new system being implemented, Member States will need to provide and manage access to it for an extended number of end-users across an array of different entities, thereby increasing the risks related to data availability, quality and security.

It is to be expected that the threats of terrorism will not diminish in the near future. European citizens expect law enforcement services to be able to do their job adequately and as efficiently as possible. The number of third-country nationals visiting the EU for the purpose of tourism or business will increase, thereby putting a higher burden on border management authorities. The number of people seeking protection in the EU, or aiming to enter the EU irregularly, is also expected to remain high, thereby putting asylum and migration authorities to a test.

Issues with reliably identifying third-country nationals travelling to the EU will be further magnified when dealing with significant numbers of refugees, many of whom often do not carry any identity document at all. The revised and extended Eurodac, including alphanumeric data, and the new possibilities provided through Europol data access by the proposed ETIAS, further add to the need to address interoperability challenges.

### **3. WHY SHOULD THE EU ACT?**

#### **3.1. Legal basis**

The main legal basis will be the following articles of the Treaty on the Functioning of the European Union: Article 16(2), Article 74, Article 77(2)(a) and (b), Article 78(2), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2).

Under Article 16(2), the Union has the power to adopt measures relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Under Articles 74 and 77(2), the Union has the power to adopt measures relating to the crossing of the external borders of the Member States. Under Article 78, the Union has the power to adopt measures for a common European asylum system. Under Article 79(2), the Union has the power to adopt measures in the area of illegal immigration and unauthorised residence. Under Articles 82(1)(d) and 87(2)(a), the Union also has the power to adopt measures to strengthen police and judicial cooperation concerning the collection, storage, processing, analysis and exchange of relevant information. Under

Articles 85(1) and 88(2), the Union has the power to determine the tasks of Eurojust and Europol respectively.

### **3.2. Subsidiarity: necessity of EU action**

Key common databases at EU level are in place or in the process of being put in place. Enhanced interoperability among these databases necessarily entails EU-level action. At the heart of the proposal is the improved efficiency and use of centralised systems managed by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA). By reason of the scale, effects and impact of the envisaged actions, the fundamental objectives can only be achieved efficiently and systematically at EU level.

This initiative will require many consequential amendments in the legal instruments of current and proposed central systems. Where instruments are not in a stable state because they are still subject to negotiation among the co-legislators, amendments will only be proposed after a political agreement is reached. The scope and detail of these amendments are clear as they directly follow from this initiative.

### **3.3. Added value of EU action from the point of view of EU citizens**

While EU citizens generally seem confident in the level of cooperation between the police and other law enforcement agencies at national level, a Special Eurobarometer<sup>30</sup> survey shows that the EU's strategy of sharing information at EU level to combat crime and terrorism has widespread public support: almost all respondents (92 %) agree that national authorities should share information with the authorities of other Member States to better fight crime and terrorism.

The overall proportions of those who agree that information should be shared within the EU are similar across Member States. In almost all countries, more than nine in ten respondents agree with sharing information within the EU.

The report also shows a general trend, where the more respondents think terrorism and cybercrime are important challenges, the more likely they are to agree that the national police and other national law enforcement authorities should cooperate with other EU countries to fight crime and terrorism.

A clear majority (69 %) of respondents thinks that the police and other national law enforcement authorities should share information with other EU countries on a systematic basis. In all Member States, a majority of respondents think that information should be shared in every case.

The proposed set of actions to achieve the interoperability of EU information systems is not expected to have a direct impact on EU citizens. The measures are focused on third-country nationals whose data is recorded in an EU centralised information system. With the exception of SIS, the other information systems exclusively focus on third country nationals. The amended Schengen Borders Code (SBC), with mandatory checks for EU

---

<sup>30</sup> The 'Report on Europeans' attitudes towards security' analyses the results of the Special Eurobarometer public opinion survey (464b) regarding citizens' overall awareness, experiences and perceptions of security. This survey was carried out by TNS Political & Social network in the 28 Member States between 13 and 26 June 2017. Some 28 093 EU citizens from different social and demographic categories were interviewed.

citizens against the SIS, will not further affect EU citizens as their data will not be recorded in any of the other systems.

At the same time, on a general level, EU citizens will benefit from the actions in terms of enhanced security, and better border and migration management, resulting in higher confidence in public policy, as these actions will offer reassurance that any third-country national on the European territory has a known genuine identity and a valid reason to be there. Furthermore, the interoperability measures should strengthen the perception that measures are being taken to combat crime and terrorism and to ensure security.

### **3.4. Public consultation**

The open public consultation run while developing these proposals showed a similarly positive view of the need to share information effectively. The consultation received 18 responses from a variety of stakeholders, including Member State governments, private sector organisations, other organisations such as NGOs and think tanks as well as private citizens. Further details are contained in the synopsis report annexed to this impact assessment. Overall, the responses were broadly in favour of the underlying principles of this interoperability proposal. Respondents generally agreed that the issues the consultation identified were the correct ones, and that the objectives the interoperability package seeks to achieve are correct. In particular, respondents considered that the options outlined in the consultation paper would:

- help staff on the ground access the information they need;
- avoid duplication of data, reduce overlaps and highlight discrepancies in data;
- identify people more reliably — including people with multiple identities — and reduce identity fraud.

Respondents generally supported each of the proposed options and considered them to be necessary to achieve the objectives of this initiative, underlining in their responses: the need for strong and clear data protection measures, particularly in relation to access to the information stored in the systems and data retention; the need for up-to-date, high-quality data in the systems and measures to ensure this; and the potential for bias in decision-making or discriminatory profiling of individuals. Several respondents noted, in response to various consultation questions, the potential for issues arising from the inclusion of Interpol data (including biometric data), where some of this may have been included for politically motivated reasons. Other points raised include: the need for appropriate logging and audit arrangements for search requests; the need for future-proofing so that future systems can also be easily included; the need to maintain the rights of current data owners over their data; the need for greater harmonisation in terms of legislation and standards across the EU; and the need to avoid mass surveillance and the erosion of fundamental rights such as the right to a private life.

The points raised have been carefully considered and taken into account as the Commission has developed its policy in this area. In particular, the need for strong and clear data protection and security measures has been and continues to be an area of focus, to ensure that appropriate protections and safeguards for individuals and their data are in place.

## 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

### 4.1. General objectives

The general objectives of this initiative result from the Treaty-based goals:

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

They also stem from policy decisions by the Commission and relevant (European) Council Conclusions. These objectives are further elaborated in the European Agenda on Migration and subsequent communications, including the Communication on preserving and strengthening Schengen,<sup>31</sup> the European Agenda on Security<sup>32</sup> and the Commission's work towards an effective and genuine Security Union;<sup>33</sup>

### 4.2. Specific objectives

The specific policy objectives of this interoperability initiative respond directly to the problems identified in Chapter 2 above, and are intrinsically linked to the general objectives identified in Section 4.1:

1. Ensuring 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, whilst respecting the existing access rights laid down in the respective EU legal instruments.<sup>34</sup>
2. Providing a solution to detect multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud.<sup>35</sup>
3. Facilitating identity checks of third-country nationals, on the territory of a Member State, by authorised officers.<sup>36</sup>
4. 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 and terrorism.<sup>37</sup>

These four objectives were derived from the report of the high-level expert group and additional follow-up discussions with all stakeholders.

---

<sup>31</sup> COM(2017)570 final.

<sup>32</sup> COM(2015)185 final.

<sup>33</sup> COM(2016)230 final.

<sup>34</sup> Commission Communication on *Stronger and smarter information systems for borders and security* (COM(2016) 205 final, 6.4.2017). European Council conclusions of 23 June 2017.

<sup>35</sup> *Seventh progress report towards an effective and genuine Security Union* (COM(2017) 261 final, 16.5.2017). Council Conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems (8.6.2017).

<sup>36</sup> Commission Recommendation on proportionate police checks and police cooperation in the Schengen area (C(2017) 3349 final, 12.5.2017).

<sup>37</sup> *Seventh progress report towards an effective and genuine Security Union* (COM(2017) 261 final, 16.5.2017). Council Conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems (8.6.2017).



In addition to these primary operational objectives, some ancillary objectives can also be identified:

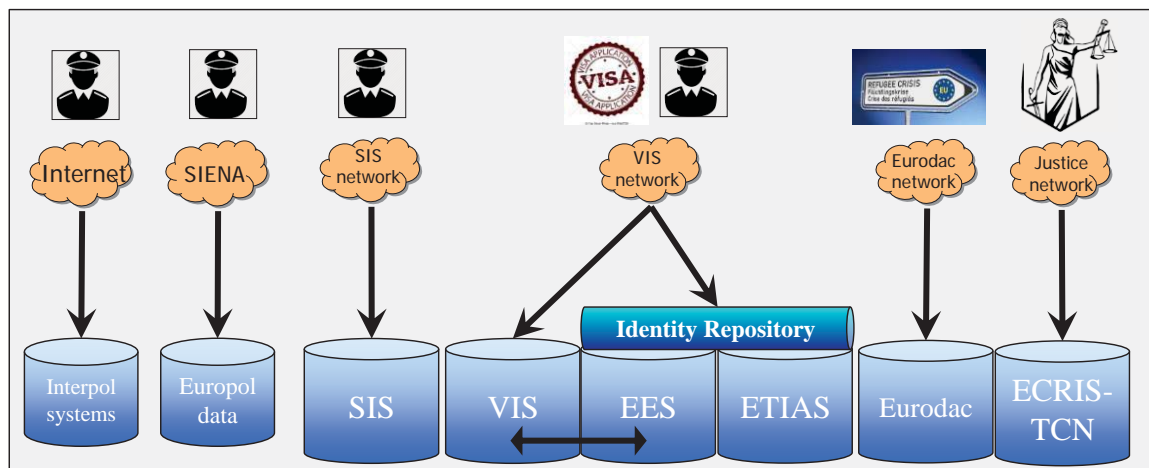
- Facilitating the technical and operational implementation by Member States of existing and future new information systems.
- Strengthening and streamlining the data security and data protection conditions that govern the respective systems.
- Improving and harmonising data quality requirements of the respective systems.

## 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

### 5.1. Option 1: baseline representing current situation

Option 1 represents the baseline of current existing (SIS, Eurodac, VIS) and planned or proposed (EES, ETIAS, ECRIS-TCN) systems as defined in the latest relevant legal acts (Commission proposals for ETIAS, SIS, Eurodac and ECRIS-TCN system, adopted legal instrument for EES). The existing Interpol systems (notably SLTD) and Europol data are also part of the baseline.

Figure 3 — Option 1: baseline



At the technical level, the baseline scenario assumes that no interoperability measure is implemented other than the integrated use of VIS and EES as described in the latter's legal act, and the common identity repository of EES and ETIAS as envisaged by the ETIAS proposal.

The current silo approach as reflected in above table, presents Member States and end-users with serious practical and technical difficulties to access data to which they legally have access, and to cross-check relevant data between systems. The silo approach as implemented so far creates obstacles to reliable identity management and makes it difficult for the EU to meet its policy objectives in the area of migration and security. If not properly addressed the silo approach will increase the likelihood of identity fraud and all problems and risks related to it.

The planned development of the future EES, the proposed ETIAS and the proposed ECRIS-TCN system, will magnify these challenges. With each new system being implemented, Member States will need to provide and manage access to it for an

extended number of end-users across an array of different entities, thereby increasing the risks related to data availability, quality and security.

For the above reasons option 1 ('doing nothing') has been rejected by the Commission, the Council and the European Parliament.

## **5.2. Option 2: High-level expert group approach to the management of data for borders and security**

The technical components considered in this option are those identified in the April 2016 Communication (ESP, shared BMS, CIR), confirmed by the findings of the high-level expert group on information systems and interoperability and endorsed by the Commission when setting out a new approach to the management of data for borders and security in the Seventh progress report towards an effective and genuine Security Union.<sup>38</sup>

- i. European search portal — **ESP**
- ii. Shared biometric matching service — **shared BMS**
- iii. Common identity repository — **CIR**

Under this option, these three components will handle data and be used according to the current legal instruments of each central system (SIS, VIS, Eurodac, EES, proposed ETIAS and proposed ECRIS-TCN system). The data protection risks and fundamental rights implications are those identified and mitigated by the current legal instruments. There are no additional risks for data protection or fundamental rights. In this configuration, these components do not modify any end-user access rights, and no additional safeguards to those currently identified and implemented will be necessary.

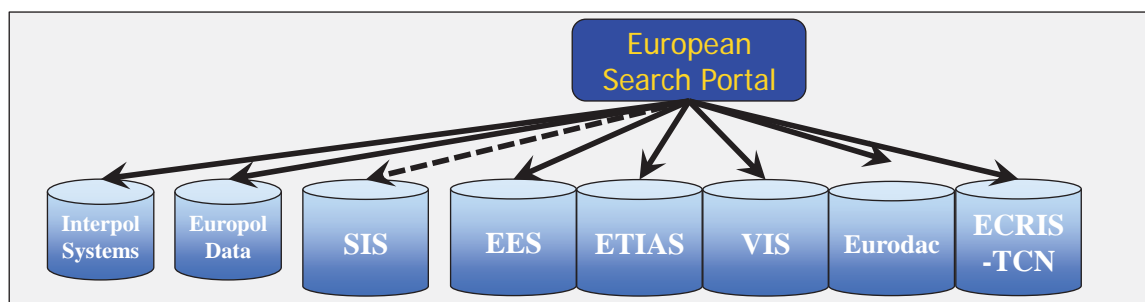
### *5.1.1. European search portal*

The centralised European search portal is the component that would enable the simultaneous search of multiple systems (SIS, Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system) using identity data (both biographical and biometric). It would ensure that users of the EU information systems have fast, seamless, efficient, systematic and controlled access to all information that they need to perform their tasks, in line with their existing access rights. A query via the European search portal would immediately, in a matter of seconds, return information from the various systems to which the user has legal access. Depending on the purpose of the search, and the corresponding existing access rights, the European search portal would be provided with specific configurations. **The European search portal does not handle any new data, it does not store any data and it would not modify any end-user access rights**; it would act as a single window or 'message broker' to search various central systems and retrieve the necessary information seamlessly, and would do so in full respect of the access control and data protection requirements of the underlying systems. The European search portal would facilitate the correct and authorised use of each of the existing and future EU information systems, and would make it easier and cheaper for Member States to consult and use the systems, in line with the legal instruments that govern these systems.

---

<sup>38</sup> COM(2017) 261 final (16.5.2017).

Figure 4 — European search portal



Given the specific technical architecture of the SIS, which includes national copies, it is to be expected that many queries to SIS will take place against these national SIS copies instead of the Central-SIS, hence the dotted line to indicate that the Central-SIS is not systematically queried.

Europol data would be queried by the ESP via a specific interface at Europol (so-called QUEST interface). When Member States query Europol data via the ESP, they will do so using their own designated login credentials. For the purposes of ETIAS, Europol will create a new 'read-only user' who cannot create/modify/delete any data. This is a feasible technical task for Europol. For Europol, only a few technical issues remain that will be resolved by Europol implementing the QUEST interface (QUering Europol SysTems) using basic protection level (BPL) data only.

Interpol systems (Stolen and Lost Travel Documents and Travel Documents Associated with Notices) would be queried by the ESP following the obligations stipulated in existing legal instruments (notably the Schengen Borders Code) while removing any possibilities of sharing data with third-countries. The technical interfaces at Interpol allow two different levels of detail to be retrieved when a hit is detected. The low-level detail never leads to a notification towards the owner of the records. By contrast, the deeper-level detail does. The ESP will be configured and used in such a way that only the low-level detail can be retrieved, thereby effectively safeguarding data protection and fundamental rights via a privacy-by-design implementation.

When Member States query Interpol data via the ESP, they will do this using their own designated login credentials. For the purposes of ETIAS, and as for Europol, Interpol will create a new 'read-only user' that cannot create/modify/delete any data. This change was discussed with Interpol at the technical level, and appears to be feasible.

When it comes to access rights, the ESP would be configured in such a way that end-users would only be able to consult data to which they have legal access, as summarised in Table 1 (a more detailed overview can be found in Annex 8 of this impact assessment).

**Table 1 — Overview of existing access to relevant information systems**

	SIS	VIS	Eurodac	EES	ETIAS (proposal)	ECRIS TCN (proposal)	Europol data	Interpol SLTD
<i>Purpose of access</i>	X	X	X	X	X			X
<b>Border control</b>								
<i>Purpose of access</i>	X	X		X				
<b>Issuance of <u>short-stay visa</u></b>								
<i>Purpose of access</i>	X	X	X	X	X	X	X	X
<b>Issuance of <u>ETIAS</u> authorisation</b>								
<i>Purpose of access</i>	X							
<b>Police checks: Identification or verification of identity in territory of Member State</b>								
<i>Purpose of access</i>	X	X	X	X	X		X	
<b>Prevention, detection or investigation of <u>terrorist offences</u> and other <u>serious criminal offences</u></b>								
<i>Purpose of access</i>	X	X	X	X				
<b>Migration management: verification of identity and verification of conditions for entry or stay (for TCNs, in territory)</b>								
<i>Purpose of access</i>	X	X	X	X				
<b>Return of irregular third-country nationals</b>								
<i>Purpose of access</i>	X	X	X					
<b>Assessment of request for <u>asylum</u></b>								

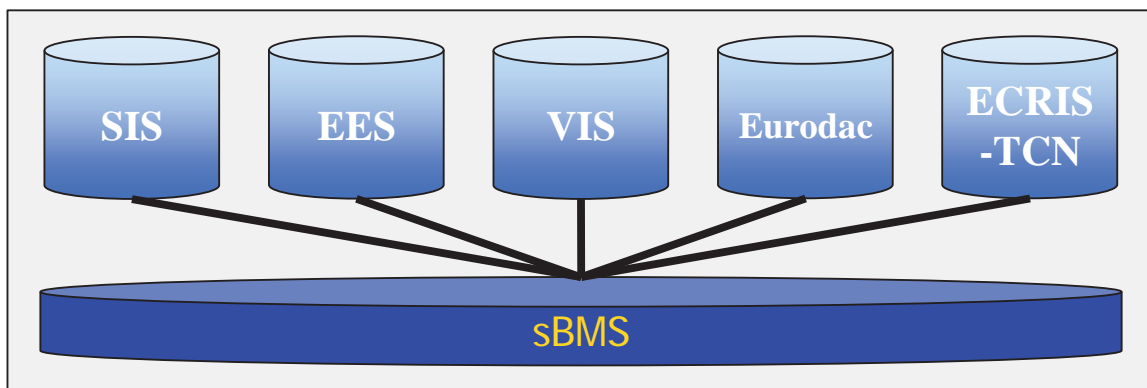
### 5.1.2. Shared biometric matching service

The shared biometric matching service would enable the searching of biometric data (fingerprints and facial images) from several central systems (SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN system). The proposed ETIAS will not contain biometric data and would therefore not be served by the shared biometric matching service. Where each existing central system (SIS, Eurodac, VIS) currently has a dedicated, proprietary search engine for biometric data,<sup>39</sup> a shared biometric matching service would provide a common platform where the data is searched simultaneously. The shared biometric matching service would generate substantial benefits in terms of security, cost, maintenance and operation by relying on one unique technological

<sup>39</sup> These biometric search engines are technically referred to as automated fingerprint identification system (AFIS) or automated biometric identification system (ABIS).

component instead of five different ones. The biometric data (fingerprint and facial images) are exclusively retained by the underlying systems. The shared biometric matching service would create a mathematical representation<sup>40</sup> of the samples (a search vector or template) but would discard the actual data, which remains thus stored in one location, only once. Like the European search portal, the shared biometric matching service would not be a ‘system’, **it does not handle any new data and it would not modify any end-user access rights**. It would however be a key enabler to help detect connections between data sets and different identities assumed by the same person in different central systems. Without a shared biometric matching service, the European search portal and the common identity repository would not be able to function as regards biometric data.

Figure 5 — Shared biometric matching service



Matching biometric templates in one shared system enables better and harmonised quality control of biometric samples, which can lead to better quality and higher accuracy. Provided that appropriate data quality standards are in place the shared BMS will not lead to higher rates of false-positive errors.

The integration of potential additional EU systems using biometric data is greatly facilitated as the shared BMS provides a ready-to-use platform for matching biometric data avoiding that this would need to be redeveloped for every new system.

The shared BMS can only be accessed via a central system; it contains non-sensitive biometric templates without any biographical data.

### 5.1.3. Common identity repository

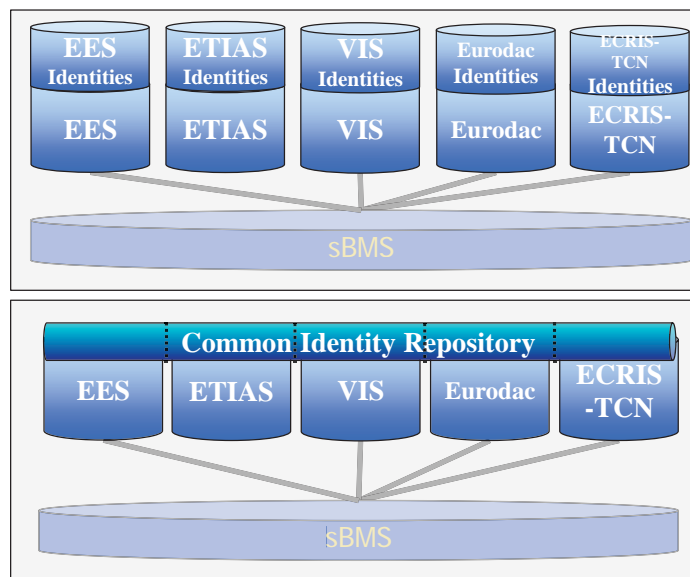
The common identity repository would provide for a unified view on biographical identity data<sup>41</sup> of third-country nationals that will be present (or are present) in Eurodac, VIS, EES, the proposed ETIAS and the proposed ECRIS-TCN system. Each of these five

<sup>40</sup> Contrary to common misconception, an automated biometric identification system (ABIS) does not actually search with fingerprint images or facial images, or store them. A feature extraction creates a mathematical representation (template) from the images. Only the templates are retained by the ABIS.

<sup>41</sup> Biographical data that can be found on the travel document includes; last name, first name, gender, date of birth, travel document number. They do not include addresses, former names, biometric data, etc.

central systems records or will record biographical data on specific persons for specific reasons. A common repository was proposed as part of the EES/ETIAS proposals to hold common data. This initiative extends it to a common identity repository that would be the shared component between all these systems to store and search, and potentially enable linking, the identity data. **The CIR does not handle any new data and it would not modify any end-user access rights.** 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. It also offers increased speed of operations, improved efficiency and economies of scale in particular for the development of new systems like ETIAS, ECRIS-TCN or the new Eurodac.

**Figure 6 — From silos of identities to a common identity repository**



The SIS data is not included in the example in Figure 6. Including biographical data from SIS would be necessary in order to be able to link persons under alert to potentially different biographical identities (i.e. identity fraud) in other systems. The complex technical architecture of SIS containing national copies, partial national copies and possible national biometric matching systems would make the CIR very complex, and changes to the 30 (non-standardised) national copies would be excessively expensive to a degree where it may no longer be feasible. However, the absence of SIS data from the CIR would leave an identity-fraud gap. This could either be accepted as a residual risk that continues to exist (option 2), or be effectively addressed by introducing an additional component that can bridge the gap between SIS and CIR. Under the more ambitious option 3, this new component is the multiple-identity detector.

The integration of potential additional EU systems using biographical identity data is greatly facilitated as the CIR provides a ready-to-use platform for storing and searching biographical data, avoiding that this would need to be redeveloped for every new system.

In addition to the three technical components to achieve interoperability, the Commission also announced in the Seventh progress report towards an effective and genuine Security Union that it will take forward the recommendation of the high-level expert group on **automated data quality control** and a **'data warehouse'** (or central repository for

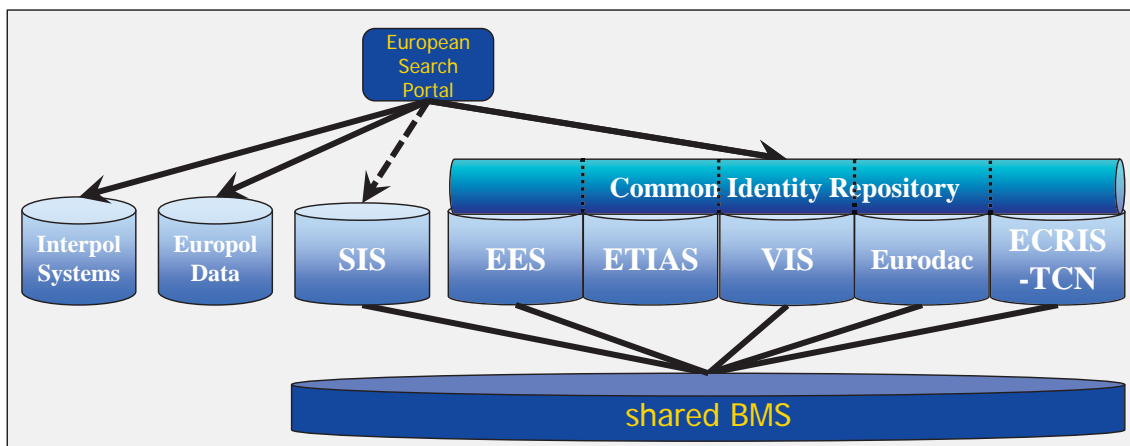
reporting and statistics, **CRRS**) capable of analysing anonymised data extracted from relevant information systems for statistical and reporting purposes. The Commission proposal to strengthen the mandate of eu-LISA<sup>42</sup> gives the Agency the task of establishing automated data quality control mechanisms and common data quality indicators and developing a central repository for reporting and statistics. These concepts for enhanced data quality are therefore part of this option.

#### 5.1.4. Complete picture of option 2

The European search portal would permit searching alerts on persons in SIS and the identity data of the future EES, the proposed ETIAS, VIS, Eurodac and the proposed ECRIS-TCN system via the Common identity repository. The ESP would also permit searching Europol data and Interpol systems.

All systems using biometric data would benefit from a shared biometric matching service. This complete configuration would not modify existing end-user access rights, as these are defined in the legal instruments of the central systems. Therefore, this option does not generate any additional data protection or fundamental rights concerns as it is fully aligned with those legal instruments.

Figure 7 — Complete overview of option 2



### 5.3. Option 3: enhanced identity management and streamlined law enforcement access

Following the Communication on *Stronger and smarter information systems for borders and security*, the findings of the high-level expert group, the *Seventh progress report towards an effective and genuine Security Union*, and subsequent further technical analysis with stakeholders and supported by technical studies, the following elements are considered in addition to option 2. Together they constitute option 3:

- (a) adding a technical component to achieve interoperability: **multiple-identity detector (MID)**;
- (b) extending the rules on the use of EU information systems for **checks within the territory**;
- (c) streamlining the rules on access to EU information systems for law enforcement purposes: **flagging**.

<sup>42</sup> COM(2017) 352 final (29.6.2017).

These complementary elements are closely linked to the drivers of the problem identified in Section 2.3. The high-level expert group discussed these problems but without naming or designing actual solutions.

The **multiple-identity detector** is the only possible additional component to achieve interoperability that has been identified as a policy option to consider beyond the technical components of option 2. This new component establishes end-user access rights for those very specific cases where identity fraud or the need for identity disambiguation is detected.

Under this option, the three components of option 2 will be used to support the two additional functionalities (b) and (c) above, which will establish end-user access rights on the CIR for these specific purposes only.

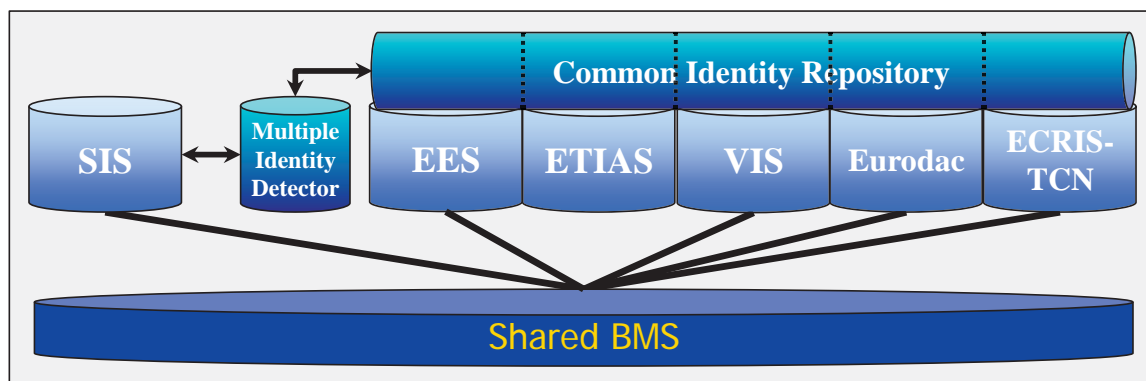
#### 5.1.5. Adding a technical component to achieve interoperability: multiple-identity detector

The common identity repository in option 2 would become extremely complex and expensive when extracting the biographic data from SIS and migrating this to the CIR. To provide an alternative to not including SIS data in the CIR and not being able to link SIS data with biographical data of third-country nationals, a new component would be necessary.

The multiple-identity detector would be this new technical component to check whether the biographical identity data contained in the search exists in any of the systems covered by the common identity repository (Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system) and in the SIS. This would enable the detection of multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The linking functionality would thus no longer be part of the CIR but completely be covered by the MID. SIS data would no longer be part of the CIR.

The multiple-identity detector would enable the correction of conflicting data to the benefit of the traveller. It would directly address the fraudulent use of identities as a serious breach of security. The multiple-identity detector would only show those biographical identity records that have a link in different central systems. These links would be detected by the shared biometric matching service on the basis of biometric data and would ultimately need to be confirmed or rejected by the users of the system.

Figure 8 — Multiple-identity detector





The MID would greatly facilitate the work of the end-user who is tasked with the responsibility of establishing the correct identity of the person in front of him or her. These checks will become more robust and systematic, and will be based on neutral indicators, thus lowering the risk of discriminatory profiling. It would be a new front-end system that needs to be included in every search on persons or documents. When a potential link between identities is detected by using biometric data, a human fingerprint expert should confirm the correctness of this link, especially when treating large volumes of historical data from systems like Eurodac, VIS and SIS.

#### *5.1.6. Establishing the rules on the use of EU information systems for checks within the territory*

National authorities have reported difficulties in using EU information systems to identify third-country nationals within the territory that are unable or unwilling to present their documents. This is due to the purposes of the respective systems. Conceived and designed as border management systems primarily used at the external Schengen borders, it was considered that identity and security checks on the territory of a Member State beyond the purpose of migration management were not necessarily required. As a consequence, in situations related to the prevention, detection or investigation of crimes below the threshold of serious crimes, or in other situations that are unrelated to migration management, national authorities cannot access the information systems to identify a third-country national on the territory. This impedes Member States' ability to detect and combat identity fraud within their territory. Moreover, in light of the recent development of the Schengen *acquis*, it runs contrary to the Commission's objective of encouraging proportionate police checks within the territory including around internal borders, as reflected in the Commission Recommendation of May 2017 on proportionate police checks and police cooperation in the Schengen area.<sup>43</sup>

The identification of undocumented or insufficiently documented persons by a police officer does not necessarily have to be an act of migration management or law enforcement in the strict definition of the VIS, Eurodac, EES and proposed ETIAS legal instruments (the two cases provided for in the existing legal bases of these systems). It should also be possible to undertake them within the scope of the police competences determined by national law. For this identification, the person is physically present and is presumed innocent. The aim is simply for the competent authorities to be able to address the person by their name.

Access to EU information systems for checks within the territory could in principle be provided in two ways: First, access could be granted only to biographical identity data (i.e. the data stored in the common identity repository). Second, access could be granted to all data recorded on a person in the individual EU information systems. As the latter approach would go beyond what is necessary and proportionate to identify a person within the territory, this impact assessment will only address the possibility of granting access to biographical identity data stored in the common identity repository for checks within the territory.

This new purpose of the CIR thus establishes end-user access rights to the data in the CIR in the case where competent authorities need to identify a third-country national

---

<sup>43</sup> C(2017) 3349 final (12.5.2017).

within the territory (border control is a different purpose and already allows such identifications).

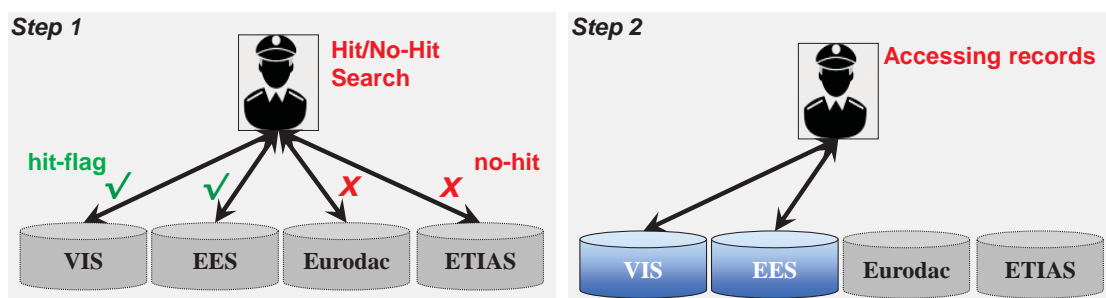
### 5.1.7. Streamlining the rules on access to EU information systems for law enforcement purposes: flagging

In its April 2016 Communication, the Commission acknowledged the need to optimise the existing tools for law enforcement purposes, without compromising on data protection requirements. This necessity was confirmed and reiterated by Member States and relevant agencies in the framework of the high-level expert group.

The main restriction for law enforcement access to the migration databases is set by the ‘cascade’ mechanism for accessing Eurodac and the future EES that requires first a so-called Prüm check through the crime databases of other Member States. While a Prüm check in itself certainly has an added value for the possible identification, it is not necessarily sufficient for the identification. There is no *a priori* certainty why the identity revealed through Prüm would be the same as an identity possibly revealed in other systems. Given the challenges faced by the use of multiple identities, all systems should be used to determine the (possibly multiple and possibly differing) identity/identities of a person. For each individual system in the ‘cascade’, authorities must first submit a reasoned request to a different authority justifying the necessity of access. This creates a considerable amount of administrative burden, results in delays, and increases the data flow potentially leading to data security risks.

The ‘hit-flag’ functionality is a new concept that restricts access to data by limiting it to a mere ‘hit/no-hit’ notification, indicating the presence (or non-presence) of data. It was developed during the work of the high-level expert group. The end-user performing a search with biographical data (last name, first name, date of birth, travel document number) or biometric data (set of good fingerprints and/or good-quality facial image) could search various central systems at the same time (in parallel, no ‘cascade’) while the only returned results would be a ‘hit-flag’ in the case where this data existed in a particular system. This first step would not require an *ex ante* authorisation and would enable *ex post* verification on the basis of a written justification.

Figure 9 — Two-step approach, based on the ‘hit-flag’ functionality



Only in a second step and where considered necessary would the end-user request actual access to those systems that provided a ‘hit-flag’, on the basis of existing access rights and conditions. Where a system does not return a ‘hit-flag’, no access will need to be requested.

The ‘hit-flag’ functionality would **not lead to new access** to personal data, as it would not allow the competent law enforcement authorities in the Member States to access any data that they would not be allowed to access under the existing legislation. The ‘hit-flag’ functionality would instead constitute a change in the *conditions applicable to data processing*<sup>44</sup> as the competent authorities are already allowed to access the data subject to certain conditions. Under the ‘hit-flag’ functionality, an authority would have direct access to the information (flag) that would allow it to verify whether or not the database contains information about a specific individual. In case of a positive answer, the authority would have to fulfil specific conditions to access further information.

Table 2 below gives a consolidated view of the two new functionalities of the CIR:

- a) police checks to identify or verify identity of third-country nationals in the territory;
- b) law enforcement access for the prevention, detection and investigation of terrorist offences and other **serious** criminal offences.

For the first of these functionalities, police authorities will obtain, when necessary, the biographical data and passport details (in the grey horizontal block) of a third-country national regardless of the system owning this data. While this requires establishing end-user access-rights, these data will normally be found in a passport and no other data (i.e. the additional information) will be provided; police authorities will not know if this identity data came from VIS, Eurodac, EES, ETIAS or the ECRIS-TCN system.

For the second case, law enforcement authorities will need to perform two steps:

1. Perform a query in the CIR using a combination of data from 'the grey block' (i.e. biographic, biometric, passport data)

This query will only produce a flag indicating which system (or no system) that may contain further information related to the person searched for.

2. In a second step, the authorities then need to request access to the 'identity data' and the 'additional information' linked to this identity data, of the system that was indicated by the flag, in line with the rules and procedures as laid down in the legal bases of the relevant systems.

While this two-step approach leads to changes in access procedures, it does **not** lead to an end-user having access to **more** data.

---

<sup>44</sup> On the difference between *new access* and *conditions applicable to data processing*, see the European Data Protection Supervisor’s ‘[Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice](#)’ (17 November 2017).

Table 2 — Consolidated view of identification of third-country nationals and flagging for law enforcement purposes

<p style="text-align: center;"><i>Purpose of access</i></p> <p style="text-align: center;"><b>Prevention, detection and investigation of terrorist offences and other serious criminal offences</b></p> <p style="text-align: center;"><b>Step 1: direct access to <u>flags</u>– through <u>Common Identity Repository</u></b></p> <p style="text-align: center;"><b>Step 2: access to additional information (identity data + additional information) in flagged systems, in accordance with the legal bases of those systems</b></p>				
VIS	EURODAC (new)	EES	ETIAS (proposal)	ECRIS-TCN (proposal)
Identity data				
<p><i>Purpose of access</i></p> <p><b>Police checks</b></p> <p><b>identification or verification of identity (in territory)</b></p> <p><b>direct access to identity data through <u>common identity repository</u></b></p>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Fingerprints (4)</li> <li>- Facial images</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>
Additional information				
<ul style="list-style-type: none"> <li>- Visa status</li> <li>- Issued, refused, discontinued, extended, revoked or annulled single/double/multiple entry visa</li> <li>- Authority where visa application was lodged;</li> <li>- Background information: MS(s) of destination, purpose of travel, intended date of arrival and intended stay, applicant's home address, occupation and employer etc.</li> <li>- (In the case of families or groups): links between applications;</li> <li>- History of applications of person.</li> </ul>	<ul style="list-style-type: none"> <li>- ID card details (where available)</li> <li>- Information concerning third-country nationals or stateless persons above 6 years old:</li> <li>- applicants for international protection</li> <li>- persons apprehended in connection with the irregular crossing of an external border</li> <li>- persons found illegally staying in a Member State</li> </ul>	<ul style="list-style-type: none"> <li>- Entry data</li> <li>- Exit data</li> <li>- Refusal of entry data</li> <li>- Remaining authorised stay</li> <li>- List if persons overstaying                             <ul style="list-style-type: none"> <li>- Statistics on persons overstaying</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- Travel authorisation status</li> <li>- IP address</li> <li>- Issued, refused,, revoked and annulled travel authorisations</li> <li>- Declarative information provided in application</li> <li>- Additional information provided at request                             <ul style="list-style-type: none"> <li>- Results of the processing of the travel authorisation request, notably hits against other EU systems, the proposed ETIAS watch list and Interpol system).</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- Convicting Member State (including a reference number and the code of the convicting MS)</li> </ul>

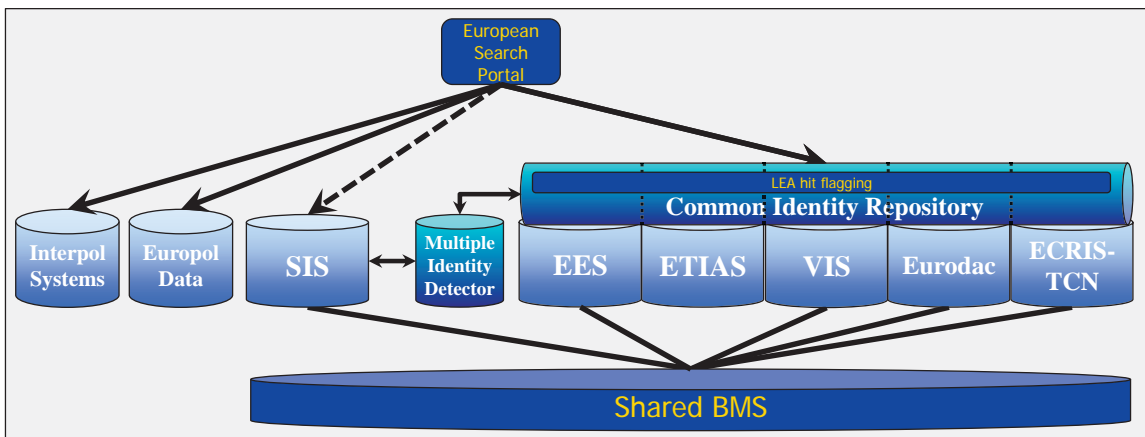
### 5.1.8. Complete picture of option 3

The multiple-identity detector would enable showing persons that have different identities in different systems. The MID would also permit disambiguation of different persons having the same biographical identity. This new component is the cost-effective, proportionate alternative to modifying the SIS architecture to allow SIS data in the CIR.

The common identity repository, containing biographical data of third-country nationals (and linked to their biometric data in the shared BMS) would have an additional purpose of allowing police to perform identifications of a person physically present but not having a (reliable) identity document. This new purpose establishes CIR end-user access rights for competent police authorities needing to identify a third-country national in the territory who can otherwise not reliably be identified.

Since the CIR only contains basic biographical data (linked to the biometric data in the shared BMS), it would implement a new streamlined law enforcement access method based on a two-step approach. The first step is a data presence search that only flags the possible existence of further data in an EU information system. Only in a second step and where considered necessary would the end-user request actual access to those systems.

Figure 10 — Complete overview of option 3



## 6. WHAT ARE THE IMPACTS OF ENHANCING INTEROPERABILITY?

This chapter looks into the various impacts of enhancing interoperability between the centralised EU systems for borders and security. Where positive impacts are described they will in most cases only reach their full potential under option 3, although some benefits will also be achieved under option 2.

The most detailed part of this chapter is Section 6.5, which assesses the **specific data protection impacts** of each of the proposed components, and the proposed streamlining of law enforcement access.

### 6.1. Social impacts

The major social impact will be the improvement of border management and increased internal security within the European Union. The new facilities will streamline and expedite access by national authorities to the required information and identification of third-country nationals. They will enable authorities to make cross-links to already existing, relevant information on individuals during border checks, for visa or asylum applications, and for police work. This will enable, notably under option 3, access to information that can support reliable decisions being made, whether relating to investigations of crime and terrorism or decisions in the field of migration and asylum. The new facilities are also expected to generate increased public trust by ensuring that their design and use increases the security of European citizens.

#### 6.1.1. Impact on EU citizens

The proposed set of interoperability measures is not expected to have a direct impact on a significant number of EU citizens. The measures are focused on third-country nationals whose data is recorded in an EU centralised information system.

No information on EU citizens will be recorded or can be found in the CIR or MID. If or when an alert regarding an EU citizen is entered in the SIS, a potential link in the MID towards identity data in the CIR on 'another person' will be analysed directly by the owner of the SIS alert, in particular by using biometric data. No other data on EU citizens (other than SIS) are created or queried at any time or place.

The impact on the right to data protection addressed in Section 6.5 concerns the rights of third-country nationals whose data is stored in EU centralised information systems. However, on a general level, the measures will have an impact on many EU citizens, as they will help reassure citizens that any third-country national on the European territory has a known genuine identity and a valid reason to be there. Furthermore, the interoperability measures should strengthen the perception that measures are being taken to combat crime and terrorism and to ensure security.

The worst-case scenario could occur in the event of a police identification involving an EU citizen carrying no identification documents (whether official or not) and being unwilling or incapable to cooperate to clarify that (s)he is in fact an EU citizen. The resulting follow-up will not be very different to today's situation where police authorities can launch an investigation by taking facial images from the person. Following this initiative, biometric data including fingerprints can be used to perform an identification via the CIR but this will lead to no results in the case of EU citizens.

EU citizens holding multiple nationalities, including third-country identity documents, will not use this third-country nationality to enter or exit the EU.

### 6.1.2. *Impact on third-country nationals*

In the same way as for EU citizens, the proposed interoperability measures — whether taken separately or combined — do not affect third-country nationals directly. No additional biographical or biometric data will be requested from them compared with the baseline situation except for a search of the CIR with biometric data for the purpose of identification of an undocumented or insufficiently documented person.

The indirect effect of the shared BMS, CIR and notably (under option 3) the MID is to be a possible deterrent for attempts to make fraudulent use of another identity. As checks become stricter, third-country nationals who might otherwise be inclined to commit identity fraud may consider desisting as the likelihood of detection will be higher compared now. These checks will also become more robust and systematic, based on neutral indicators such as the links in the MID, reducing the risk of discriminatory profiling.

## 6.2. **Economic impacts**

Immediate economic impacts of any of the above options will be limited to the design, development and operation of the new facilities. The costs will fall to the EU budget and to Member State authorities operating the systems. Generally, the proposed measures are not expected to have an impact on small and medium-sized enterprises.

### 6.1.3. *Impact on tourism*

The impact on tourism can be expected to be positive as the proposed measures will both improve the security of the EU and should also be beneficial for a speedier border control. In its report released in 2017,<sup>45</sup> the World Travel and Tourism Conference noted that global tourism grew by 3.3 % in 2016 despite ongoing terror threats around the world and that destinations must continue to focus on security to ensure that their markets remain resilient. As an example of the effect of security threats, the report noted that, following attacks in 2016, there were reductions in inbound tourism spending in Belgium (-4.4 %), France (-7.3 %) and Turkey (-22 %). In North Africa, the impact on tourism (visitor exports) was again negative in 2016 (-16 %).

The expected positive impact on the (speed of) border control is based on the fact that CIR and (under option 3) MID would keep a record of legitimate cases of multiple identities, differentiating a legitimate traveller's identity from one belonging to a *male fide* traveller. Without the proposed options, such (second-line) investigations would be repeated at each border check, whereas the MID would record resolved cases from their first occurrence, thereby minimising disruption for legitimate travellers.

---

<sup>45</sup> See press release on <https://www.wttc.org/media-centre/press-releases/press-releases/2017/resilience-is-key-as-impact-of-terrorism-on-tourism-becomes-clearer-wttc-report/>.

#### *6.1.4. Impact on airports, seaports and carriers*

The impact on airports, seaports and carriers is also expected to be positive. The interoperability of systems does not require any additional data elements to be captured or checked. The use of MID (under option 3) would help in resolving the legitimate cases of multiple identities from the first occurrence. This measure would therefore contribute to expediting border control checks.

### **6.3. Impact on public services**

#### *6.1.5. Impact on border management*

The organisation of border management by Member States is expected to benefit from interoperability. By applying the ESP, significantly simpler changes would need to be made by Member State to enable their national systems to also consult the future EES and the proposed ETIAS. The search message issued by a national system will essentially stay as it is now, as the ESP would consult EES and the proposed ETIAS in addition to SIS and VIS. National systems would need to be able to handle the EES and ETIAS responses contained in combined answers returned via the ESP, but the standardisation of these return messages<sup>46</sup> would substantially reduce the required changes to Member State systems.

A second improvement would stem from the ability to check identity more effectively. In the baseline situation, the biometric sample (facial image or fingerprint) is only sent to VIS/EES, but the shared BMS (under option 2) will ensure that this sample also queries SIS. If (under option 3) the MID is implemented, links with identities found in other systems would also be reported. As such, the shared BMS — preferably in combination with MID — would highlight multiple identities, leading to a more correct decision than if it were not in place, e.g. a third-country national travelling under an identity different to his/her identity in SIS would not be introduced in the future EES with that second identity.

#### *6.1.6. Impact on migration and asylum management*

Migration and asylum management are also expected to benefit from interoperability measures. In the case of checks on the territory of Member States, in particular to identify undocumented persons, the current Eurodac, VIS and EES legislation provides for conducting a biometric identification check in these different systems. The ESP would simplify access arrangements to these systems but, more importantly, with the MID (under option 3), links between identities contained in different systems would be revealed.

For asylum purposes, migration officers essentially run biometric searches against Eurodac, although current legislation also allows them to consult VIS. Simultaneous consultation of VIS would have the benefit of identifying asylum applicants faster. Member States doing this find that about 30-35 % of asylum seekers can be identified using VIS. However, not all Member States use VIS for this purpose. This is because

---

<sup>46</sup> Messages are expected to be standardised to a further version of the Universal Message Format (UMF).



dedicated access to VIS must be added to the IT infrastructure of the administration in charge of asylum, and the national application must be modified to handle the answer returned by VIS. The shared BMS used in combination with CIR would have the same positive effect for identifying undocumented persons, explained above.

Finally, by including biometrics in SIS, creating links with identities known in the proposed ECRIS-TCN system and using information from Europol, relevant authorities would be able to filter out asylum claims from known criminals who mix in with the flow of asylum seekers in the hope of passing undetected. The actual number of such cases is low, but the impact of non-detected cases is potentially high, and undermines European public support to EU approach towards migration and asylum.

#### *6.1.7. Impact on police cooperation and law enforcement*

Police cooperation and law enforcement are expected to experience a very positive effect from the interoperability measures (notably under option 3), mainly for three reasons.

First, consistent identity management *across* current systems (as opposed to only within a single system as at present, leading to the identified problem of undetected multiple identities) would be possible with the shared BMS in conjunction with the MID. This would make the data that EU information systems provide to national law enforcement authorities more complete, accurate and reliable. It would therefore considerably enhance the support that the EU provides to Member States in the fight against crime and terrorism. It would also close the blind spots that currently exist due to the fragmentation of EU information systems for security, border and migration management, and it would enable law enforcement authorities to recognise connections between data fragments stored in different systems.

Second, by granting competent authorities access to the CIR for the purpose of identification (option 3), this initiative would address an important information gap in relation to fleetingly present third-country nationals, who may not be able or willing to show their identity documents during a police check. This will enable police authorities to carry out more effective police checks and identify undocumented third-country nationals.

Third, option 3 would streamline the so-called cascading mechanism for accessing border control, asylum and immigration systems (Eurodac, VIS, the future EES, the proposed ETIAS) for law enforcement purposes. Currently, access must be requested for each system in sequence. The essence of the proposed new conditions (under option 3) is that they remain related to a specific case but that, as a first step, the 'hit-flagging' functionality would provide 'hit-flags' on any system that contains data related to the search. As a second step law enforcement authorities would then be able to obtain parallel access to all systems that actually contain data and to which they have access, whilst fully respecting all other access conditions and safeguards as provided for in the existing legal instruments of the underlying systems.

The expected positive results can only be achieved to the extent that the technical implementation of the systems is accompanied by an adequate training of the different services dealing with law enforcement. This is however not a new task as the current use of large-scale IT systems by law enforcement services is already supported by such trainings in particular as organised by CEPOL (the European Union Agency for Law

Enforcement Training). The importance and magnitude of the task is increased with the proposed interoperability measures.

#### **6.4. Impact on fundamental rights**

In accordance with the Charter of Fundamental Rights of the EU, to which EU institutions and Member States, when they implement EU law, are bound (Article 51(1) of the Charter), the opportunities offered by interoperability need to be balanced with the obligation to ensure that interferences with fundamental rights that may derive from the new system are limited to what is strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality (Article 52(1) of the Charter).

As mentioned by the EU Agency for Fundamental Rights in its report:<sup>47</sup> *‘Interoperability involves both risks and opportunities for fundamental rights. Receiving the full picture about a person contributes to better decision-making. To this end, safeguards need to be in place to ensure the quality of the information stored about the person and the purpose of the data processing. Such safeguards should prevent unauthorised access and unlawful sharing of information with third parties. To ensure the right to an effective remedy, practical possibilities to rebut a false assumption by the authorities and to have inaccurate data corrected need to be in place.’*

The proposed interoperability solutions are complementary components to existing systems. As such, they would not alter the balance already ensured by each of the existing central systems as regards their impact on fundamental rights.

Nevertheless, interoperability does have the potential of having an additional, indirect impact on a number of fundamental rights. Indeed, the correct identification of a person has a positive impact on the right to respect for private life, and in particular the right to one’s identity (Article 7 of the Charter), as it can contribute to avoid identity confusions (i.e. the right to good administration). On the other hand, the collection of biometric data can interfere with the person’s right to dignity (in particular, where it is perceived as humiliating) (Article 1). Yet in a survey<sup>48</sup> by the EU Agency for Fundamental Rights, respondents were specifically asked whether they believed that giving their biometrics in the context of border control might be humiliating. The majority of respondents did not feel that it would.

This initiative only proposes to acquire (not store) biometric data if a third-country national cannot reliably be identified. The collection of stored biometric data was previously obtained on the basis of the legal instrument of each central system.

The proposed interoperability components (and notably those under option 3) offer the opportunity to adopt targeted preventive measures to enhance security. As such, they can contribute to the protection of people’s right to life (Article 2 of the Charter), which also implies a positive obligation on authorities to take preventive operational measures to

---

<sup>47</sup> [Fundamental rights and the interoperability of EU information systems: borders and security](#), Report by the EU Agency for Fundamental Rights.

<sup>48</sup> *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers’ views on and experiences of smart borders*, Report by the EU Agency for Fundamental Rights: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart\\_borders\\_pilot\\_-\\_technical\\_report\\_annexes\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf).

protect an individual whose life is at risk, if they know or ought to have known of the existence of an immediate risk,<sup>49</sup> as well as to uphold the prohibition of slavery and forced labour (Article 5).

The two-step law-enforcement access method of option 3 would lower the impact on the presumption of innocence compared to today's situation of fully accessing a central system after authorisation. In the first step, no personal data or additional data will be retrieved. Only in a targeted second step would actual data be retrieved.

A reliable, more accessible and easier identification could also contribute to ensuring that the right to asylum (Article 18 of the Charter) and the prohibition of refoulement (Article 19 of the Charter) are effectively ensured. Furthermore, notably through option 3, identity fraud will be more easily identified. Interoperability could in fact prevent situations where asylum applicants are unlawfully apprehended, detained and made subject to undue expulsion. It would also prevent that data and information about asylum applicants are shared with third countries (particularly the country of origin) for the purpose of establishing the person's identity and obtaining travel documents, as this may endanger the person concerned.

It could, for example, contribute to enhance the effectiveness of the authorities' interventions on missing children. If a child who has been previously recorded in SIS as missing is encountered by the authorities and checked against one of the other databases, the SIS entry would be visible because of interoperability, enabling the authorities to take appropriate action. This is particularly relevant in the context of synergies with Eurodac, with regards to the particularly vulnerable category of asylum-seeking children. Also, through a reliable, more accessible and easier identification, interoperability can support the detection of missing children or children subject to people trafficking, and facilitate swift and targeted responses.

## **6.5. Impact on the right to personal data protection**

### *6.1.8. General aspects*

Interoperability has an impact on the right to the protection of personal data. This right is established by Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union, and in Article 8 of the European Convention on Human Rights. As underlined by the Court of Justice of the EU,<sup>50</sup> the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.<sup>51</sup>

Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(2) of the General Data Protection

---

<sup>49</sup> European Court of Human Rights, *Osman v United Kingdom*, No. 87/1997/871/1083, 28 October 1998, para. 116.

<sup>50</sup> Court of Justice of the EU, judgment of 9.11.2010, *Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert* [2010] ECR I-0000.

<sup>51</sup> In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

Regulation,<sup>52</sup> which indicates that the EU protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The General Data Protection Regulation, with Regulation (EC) 45/2001,<sup>53</sup> and, where relevant, Directive (EU) 2016/680<sup>54</sup> 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.

According to the Commission Communication of July 2010 on information management in the area of freedom, security and justice,<sup>55</sup> data protection rules should be embedded in any new instruments relying on the use of information technology. This implies the inclusion of appropriate provisions limiting data processing to what is necessary for the specific purpose of that instrument and granting data access only to those entities that 'need to know'. It also implies the choice of appropriate and limited data retention periods depending solely on the objectives of the instrument and the adoption of mechanisms ensuring an accurate risk management and effective protection of the rights of data subjects.

In this respects, the interoperability concept is based on ***data protection by design and by default***.<sup>56</sup> The importance of the concepts of data protection by design and by default<sup>57</sup> was repeatedly highlighted by the European Data Protection Supervisor regarding the e-Privacy reform.<sup>58</sup> Concerning the interoperability concept:

- Data protection is embedded into the design and architecture of the existing and proposed IT systems for borders and security, of the new interoperability components and of the business practices related to them.
- Specified purposes are clear, limited and relevant to the circumstances (purpose specification); the collection of personal information is limited to that which is necessary for the specified purposes (collection limitation); the collection of personally identifiable information is kept to a strict minimum (data minimisation); the use, retention, and disclosure of personal information is limited to the relevant purposes (use, retention and disclosure limitation).

---

<sup>52</sup> 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).

<sup>53</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

<sup>54</sup> 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.

<sup>55</sup> COM(2010) 385 final.

<sup>56</sup> In the meaning of Article 25 of the General Data Protection Regulation.

<sup>57</sup> A recent Eurobarometer survey showed that almost 90 % of EU citizens indeed agree on the importance of data protection by default settings. *TNS Political & Social at the request of the European Commission, 'Flash Eurobarometer 443 — July 2016, 'e-Privacy' Report, EN'* (December 2016), at p. 43.

<sup>58</sup> European Data Protection Supervisor, Opinion 6/2017, *EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*.

- The security of personal information is ensured; the applied security standards assure the confidentiality, integrity and availability of personal data throughout its life cycle including, *inter alia*, strong access control and logging methods.

According to the General Data Protection Regulation, the free movement of data within the EU is not to be restricted for reasons of data protection. However, a series of principles must be met. Indeed, to be lawful, any limitation on the exercise of the fundamental rights protected by the Charter must comply with the following criteria, laid down in its Article 52(1):

- it must be provided for by law;
- it must respect the essence of the rights;
- it must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;
- it must be necessary; and
- it must be proportional.

Indeed, if the essence of the right is affected, the measure is unlawful and there is no need to proceed further with the assessment of its compatibility with the rules set out in Article 52(1) of the Charter. In the case of the interoperability components the essence of the right is respected, similar to what happens today with existing EU information systems, the right to personal data is affected only to a limited extent. However, despite being limited, the impact on the right to personal data must be assessed to determine whether it is necessary and proportional.

Each of the components and legal elements constituting option 2 and 3 should be assessed against the following three criteria:

- (a) Do they meet an **objective of general interest**? This objective provides the background against which the necessity of a measure shall be assessed. The objective of general interest must be defined in sufficient detail so as to enable the assessment whether the measure is necessary.
- (b) Are they **necessary**?
- (c) If so, are they **proportional**?

When assessing these criteria, a series of principles should be taken into account under the terms of the General Data Protection Regulation, including respect of the **data minimisation principle** (Article 5(1)(c)), according to which access to personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, data accuracy (Article 5(1)(d)) and **purpose limitation** (Article 5(1)(b)), according to which data is to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

### *6.1.8.1. European search portal*

#### Objective of general interest

The ESP as described under Section 5.2.1 is a message broker with the specific purpose of ensuring 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 and in line with their access rights. It would also facilitate the implementation by Member States of existing and future new information systems. The ESP would support information systems in achieving their goals in an effective and efficient way.

#### Necessity

The ESP provides end-users a new tool to systematically and easily search all the EU information systems and the Europol and Interpol databases to which they already have legal access today but sometimes not the operational or technical capability to do so.

The ESP will also be used to enable central systems to search other central systems, such as the future EES searching VIS, and the proposed ETIAS searching various other systems. Indeed, the proposal for an ETIAS Regulation envisages that the ETIAS central system will query the central systems for the purpose of automated checks. Should an ESP not be developed, a connection simulating the tasks of the ESP would nevertheless have to be established to enable the proposed ETIAS to carry out its operations. Creating an ESP and centralising all types of searches through it delivers economies of scale and efficiency gains.

The ESP should be able to consult the proposed ECRIS-TCN system, the Europol data, and the Interpol SLTD and TDAWN databases. Indeed, some of the ESP end-users need to query those systems or databases under existing Union law, therefore enabling the ESP to perform these searches would contribute to meeting its main objective. It is worth recalling that searches against these systems would only be performed when the end-user already today has access rights to those systems.

#### Proportionality

The actual impact of the ESP in terms of data processing is very limited. The ESP only envisages an additional single operation of forwarding a search transaction to various central systems. The ESP would be configured in such a way that an authority using the ESP would only trigger a search in the information systems to which it already has legal access. For example, even though the ESP is connected to the proposed ECRIS-TCN system, when a border guard uses the ESP to carry out a search on a third-country national at an external border, the search would not be conducted against the proposed ECRIS-TCN system, as today border guards do not have access to such data.

The ESP would not store any data, except information regarding the various user profiles of the ESP, the data and information systems to which they have access, and the logs, to keep track of the use of the ESP.

This approach also applies when querying the Interpol databases. This would only take place where already provided for by the current existing legal framework (e.g. query of Interpol SLTD by border guards while assessing entry conditions at the external borders). Moreover, the initial search performed by the ESP against the Interpol databases will be carried out on a hit/no-hit basis and the ESP will not share in an automated manner any data with the third country which is at the origin of the data.

### ***Conclusion on ESP***

The role of the ESP, limited to being a message broker, an enabler and a facilitator, is proportionate, necessary and limited in terms of searches and access rights to support the objectives of the existing information systems and obligations provided for by Union law.

#### *6.1.8.2. Shared biometric matching service*

##### Objective of general interest

The shared BMS is a technical tool to reinforce and facilitate the work of the relevant EU information systems and the other interoperability components. Its functionality enables the performing of searches on biometric data from various sources in an efficient, easy and systematic way. Indeed, currently the SIS, Eurodac and VIS central systems each have a dedicated biometric engine performing these biometric searches within each system. In the future, the EES and the proposed ECRIS-TCN system would need to develop a new one. By creating a central shared BMS, there is a clear gain in terms of economies of scale and efficiency.

Moreover, the shared BMS also acts as an enabler and a supporting tool for the CIR and the multiple-identity detector (MID) and therefore is a key element allowing achieving the objectives of facilitating identity checks in the territory of Member States and of detecting multiple identities and addressing identity fraud.

##### Necessity

Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for identifying a person. Indeed, the main purpose of the shared BMS is to facilitate the identification of an individual who may be registered in different databases. By doing so, it provides a solution to detect and combat identity fraud but also to prevent situations in which — due to similar profiles — persons are confused with others, for instance resulting in repeated inconveniences for *bona fide* third-country national travellers. The shared BMS will generate substantial security, financial, maintenance and operational benefits by relying on one unique technological component instead of five different ones in each of the underlying systems.

To achieve the above objectives it is necessary that all EU central systems using biometrics (i.e. SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN system) use the shared BMS.

##### Proportionality

The shared BMS will transform the biometric data (i.e. fingerprints, facial images) stored in the underlying systems into templates. The shared BMS would then use all these templates to search the biometric data in each EU central system. These transactions ensure full reliability for searching with biometrics while keeping at a minimum the personal data used: it is not the biometric data as taken from the individual as such but only a mathematical representation of this data that is used in order to carry the searches. These templates alone, without the biometric data that originated them, do not allow for the identification of a person.

Concerning the storage of data, it is worth recalling that biometric data are fully retained by the underlying systems. The shared BMS creates a mathematical representation of the samples (the template) but will discard the actual images. The data is stored in one location, only once: there is no duplication of data. The existing information systems using biometric data (e.g. VIS) already use biometric templates to perform the biometric searches within that same system. The shared BMS would just group those templates in one single piece of infrastructure.

### ***Conclusion on shared BMS***

The shared BMS is necessary in order to achieve the objectives of this initiative, notably the purpose of correct identification of a person and detecting cases of multiple identities. The data processes are strictly limited to what is needed to achieve this goal and the data stored in the shared BMS is the minimum necessary.

#### *6.1.8.3. Common identity repository*

##### Objective of general interest

The CIR has the main objective of facilitating identity checks on the territory of a Member State of third-country nationals by authorised officers. Due to its design it would also contribute to ensuring that end-users have fast, seamless, systematic and controlled access to all the information that they need to perform their tasks and, working together with the MID, to the detection of multiple identities.

The fulfilment of these objectives relies on achieving an accurate and reliable identification of third-country nationals. Indeed, the accurate and reliable identification of third-country nationals is fundamental to the correct functioning of the information systems covered by the scope of this initiative.

##### Necessity

Carrying out identity checks on the territory of a Member State is a key part of police work. Indeed, the first step for a police officer encountering a person is the identification of this person. Without a proper identification, 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.

Today, Member State' authorities have different means to identify EU nationals or third-country nationals resident in the territory of a Member State. For example, all Member States keep a register of their nationals and residents. However, Member States cannot keep complete registers on third-country nationals present for a short stay, as those third-country nationals can enter, travel and exit through different Member States. This places those third-country nationals in a different situation as compared to EU nationals and EU residents. The CIR can address this gap by allowing access for Member State authorities to Eurodac, VIS, EES, the proposed ETIAS and the proposed ECRIS-TCN system for the purpose of identification of persons in the territory of the EU and enable them to carry out correctly and efficiently their different tasks and obligations.

The CIR should include data contained in the proposed ECRIS-TCN system as the identities of third-country nationals stored in this system are verified by a judicial authority. Therefore, although relatively limited in numbers, the quality of the ECRIS-TCN data will be very high when it comes to identification purposes.

##### Proportionality



In order to fulfil its objective, the CIR should contain the biographical data of the third-country nationals stored in Eurodac, VIS, the future EES, in the proposed ETIAS and in the proposed ECRIS-TCN system. The CIR will store the biographical data contained in each of these systems, and will thereby — to avoid duplication of data — replace the current identity storage within the systems. The addition, deletion and modification of these identity data will, as appropriate, be done in accordance with the respective legal bases of the underlying systems. Although kept together in the CIR, the data of each of these systems will be kept separate in accordance with their legal basis. Therefore, the data contained in the CIR can either be accessed for the purposes provided for in each of the existing legal bases of the underlying systems or for the purposes of the CIR, namely the facilitation of identity checks and the detection of multiple identities.

The alternative scenario in which there is no CIR but access is granted to all individual systems for the purpose of identity checks would entail launching as many searches as there are systems to be consulted, thereby substantially multiplying the number of data processing operations.

The purpose of correct identification of a person by competent officers should be added as a new ancillary purpose to Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system. Indeed, their main purpose is not affected by the CIR. Only a limited subset of data would be used in order to enable identification by competent officers. No additional data is being collected or further processed for this purpose.

The CIR would contain biometric data, biographical data limited to what it is necessary to establish the identity of a person (e.g. last name, first name, gender, age) and data related to the travel document. These data are strictly needed in order to perform the correct identification of a person. Indeed, today all of these data is contained in a travel document, possession of which is an obligation for third-country nationals present for a short stay and, where relevant, such document must be shown to Member State authorities. No data related, for instance, to a visa application, a travel authorisation application or the entry or exit of a third-country national would be included in the CIR.

Concerning access to the CIR, safeguards would be put in place to avoid unlawful use. Such safeguards would include logging and the fact that searches should only be performed in the presence of the third-country national by using biometrics or all the data contained in the machine-readable zone of the travel document. Safeguards also include the appropriate training of the users of the system. In line with good practices in information security risk management, strict data security measures would apply to ensure the security of personal data processed.

Data retention periods are fully aligned with the data retention provisions of the underlying information system providing the identity data. Where the data retention for data in a central system expires and is deleted from the system, it would be automatically deleted from the CIR.

### ***Conclusion on CIR***

The CIR is necessary for the purpose of conducting identity checks in the territory of Member States. This purpose becomes a new ancillary purpose of Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system. The data processes are strictly limited to what is needed to achieve this goal, and adequate safeguards will be established to ensure access rights are respected.

#### 6.1.8.4. Multiple-identity detector

##### Objective of general interest

The MID has the objective of providing a solution to detect multiple identities, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. By doing so, the MID will also support the objectives of the underlying EU systems (i.e. border management, asylum, law enforcement, judicial cooperation) and contribute to a high level of security.

##### Necessity

Detecting multiple identities is a key prerequisite in order for the EU central systems to achieve their respective purposes. Today, as a result of the silo approach applied to the design and functioning of the systems covered by the scope of this initiative, it is generally not possible to conduct cross-system identity checks. With the exception of VIS, the future EES and the proposed ETIAS (which to a certain extent will be interconnected), the central systems do not ‘know’ whether a person is also recorded in another system. While this approach respects the differentiated purposes of the various systems it creates an unjustifiable information gap when it comes to the identification of a third-country national. As a result it indirectly protects those persons committing identity fraud.

Using the MID as a tool for detecting multiple identities requires additional data processing. Indeed, each time new data is added or modified in one of the underlying information systems, the MID will verify — through the shared BMS and the ESP respectively for searches with biometric and alphanumeric data — whether data on that same person is also present in other systems. This additional data processing is the key to being able to establish links and hence detect cases of multiple identities, identity fraud but also cases *bona fide* persons are confused with different persons. Without these queries, the MID is not able to deliver on this purpose.

The MID would also contribute to improving and harmonising data quality requirements of the respective systems by linking the different files regarding the same person and therefore enabling the comparison between the data stored in each system.

##### Proportionality

The MID has the purpose of detecting multiple identities and identity fraud. Contrary to the CIR, this purpose does not need to become a new ancillary purpose of the existing EU central systems as, for achieving their own respective purposes, a correct identification of the third-country national is already required.

The MID will contain the links between identity data stored in at least two of the systems that are part of the CIR (Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system) as well as the SIS.

The data processing through the ESP and the shared BMS in order to link individual files across individual systems is kept to a minimum. The searches using biometric (through the shared BMS) or alphanumeric (through the ESP) data would be carried out every time data is added or modified in one of the information systems. This is needed in order to keep up-to-date and reliable links between files. The links should remain in the system as long as data is present in more than one system. Indeed, failing to do so would result in having to perform a biometric search against all data, every time an identity search is performed, resulting in unnecessary repetition of biometric searches. Maintaining these links is also in the interest of the *bona fide* third-country national, as they prevent

repetitive false-positives or minor disambiguation operations each time the person travels to the EU.

Access to the MID for the purpose of detecting multiple identities will be granted to all categories of users that today have access to one or several of the central information systems under the scope of the MID.

The data contained in the MID for the purposes of detecting multiple identities will be kept to the minimum necessary to achieve this objective. The data that needs to be contained in the MID will be limited to the actual link, and a reference to the information systems containing the data. No identity data will be stored in the MID. To verify the identity, subsequent access to the related identity data necessary to establish the link (the minimum set of identity data) will be provided in line with access rights to the CIR and the SIS.

The reference to the information systems containing the data is needed in order to be able to indicate which information system contains the data. Concerning the links, these are the data the end-user needs to fulfil the task of dealing with multiple identities. The links should cover the different scenarios: same identity, lawful multiple identities, identity fraud, uncertain multiple identities and different identity (false-positive).

Concerning the reply given by the MID for the purposes of detecting multiple identities, it should be limited to cases of identity fraud or uncertain multiple identities (the latter only when data is added, updated in an information system and for the purposes of verifying the potential multiple identities). In those cases, access rights to the CIR and the SIS will be used to get access to the biographical data in order to proceed to verifying the identity and to enable the third-country national to justify why he or she has multiple identities.

Each link should be associated with follow-up actions in accordance with the nature of the link and in accordance with relevant EU or national law.

Links indicating lawful multiple identities or false-positives will be stored in the MID for the purpose of the convenience of the third-country national but should not be revealed to the end-user querying the MID. Indeed those links will prevent future and recurring inconveniences for the persons concerned.

The MID will include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities. The MID should also include safeguards against any misuse of data or any unlawful access to the data contained within it. Such safeguards should include the appropriate training of the users of the system. In line with good practices in Information Security Risk Management, strict data security measures will apply to ensure the security of personal data processed.

Data retention periods are fully aligned with the data retention provisions of the underlying information system containing the linked data. Where the data retention for data in a central system expires and is deleted from the system, the corresponding link will be automatically deleted from the CIR.

### ***Conclusion on MID***

The MID is necessary in order to achieve the purpose of detecting multiple identities and identity fraud. The data processes are strictly limited to what is needed to achieve this goal, and adequate safeguards are to be established to ensure access rights are respected and the data stored in the MID is the minimum necessary.

#### 6.1.8.5. Streamlining of law enforcement access

##### Objective of general interest

The streamlining of law enforcement access to Eurodac, VIS, the future EES and the proposed ETIAS, as described under Section 5.3.2, builds on the current ancillary purpose of these systems. It therefore aims at an objective of general interest: the prevention, investigation, detection or prosecution of terrorism and other serious criminal offences.

##### Necessity

Current restrictions on law enforcement authorities to consult Eurodac, VIS, EES and the proposed ETIAS were envisaged to ensure strong data protection safeguards. However, one of the safeguards turned out to be such that it is detrimental to the main purpose of ensuring the prevention, investigation, detection or prosecution of terrorism and other serious criminal offences in a genuinely effective way. This issue concerns the ‘cascade’ requirement to first check national databases and Prüm, envisaged for example in the EES. Indeed, the principle of cascading, although intended as a mere data protection safeguard, effectively limits the possibility of Member State’ authorities to consult systems for justified law enforcement purposes. The cascade requires the law enforcement service to end its query once information is found in one system. However, this does not mean that the next or even a later system in the cascade could not also contain valuable information for the prevention, investigation, detection or prosecution of terrorism and other serious criminal offences. The cascade could thereby result in missed opportunities to uncover necessary information. It is impossible to anticipate *a priori* which system would contain necessary information for a specific case of terrorism or serious crime, so using the cascade could result in searching one by one all systems before finding the one that contains the information that is needed. As a result, the cascade mechanism does not only fail to meet the need of investigators, but is also falls short of meeting the data protection criterion of data minimisation.

The two-step ‘hit-flag’ approach envisages the possibility to search directly Eurodac, VIS, EES and the proposed ETIAS via the proposed CIR without an *ex ante* authorisation. The results of this search would however only show the existence of one or several hits, which would inform the officer about the existence of additional data in one or several of the EU central systems but nothing else. In order to access the actual data contained in one of these systems, the officer would need to fully comply with the conditions laid down in the various legal instruments of Eurodac, VIS, EES and the proposed ETIAS and therefore be subject to an *ex ante* evaluation (except in cases of urgent need as mentioned above).

##### Proportionality

Replacing the cascading safeguard by a ‘two-step’ approach involves new data processing (hit/no-hit) and a change in the *conditions of access* to personal data envisaged to fulfil the law enforcement ancillary purpose of the Eurodac, VIS, EES and the proposed ETIAS. Indeed, informing of the existence of a hit involves searching the systems and providing the reply indicating a hit, which actually grants direct access to law enforcement authorities to these systems (hit/no-hit). However, both operations are kept to the minimum required as the authority would only get a yes (hit) or no (no-hit) answer.

Concerning searches of central systems, it would be limited to a one-to-many search in cases of a justified law enforcement investigation into serious crime or terrorism. Indeed, while conducting such searches, a law enforcement authority should provide a written justification of the purpose and necessity of the search and a reference to the case relevant for the search. Such information would enable an independent *ex post* verification of the first-step access under this approach. Search logs will be kept in the respective information systems subject to supervision by the relevant authorities for the purpose of supervising the security and lawfulness of the law enforcement access.

Providing a hit/no hit response to a law enforcement search, before prior review by an independent authority, streamlining today's access rights for law enforcement authorities to Eurodac, VIS, the future EES and the proposed ETIAS. However, by providing this minimum set of data (hit/no-hit) before obliging law enforcement authorities to justify to an independent authority their access needs — individually for each of the information systems they can consult — the number of law enforcement access requests will be limited to those cases where access is necessary for the prevention, investigation, detection or prosecution of terrorism and other serious criminal offences.

The presence of a flag in a system reveals information about an individual (for example the fact that the person is a third-country national, applied for a visa, or for asylum). However this information is without practical use if not complemented by further information contained in the underlying systems, which can only be accessed in accordance with the legal bases of these instruments and their respective safeguards. The ex-ante verification, before granting access to the information system in accordance with the second step of this approach, and the fulfilment of the conditions for the second step would remain as they are today.

The two-step hit-flagging approach guarantees that data is shared with law enforcement authorities only in those cases where there is information linked to the prevention, investigation, detection or prosecution of terrorism and other serious criminal offences. It would also envisage the necessary safeguards to ensure that the mechanism is not abused such as *ex post* verification as to whether the access conditions actually existed and the keeping of logs.

#### ***Conclusion on law enforcement access***

Replacing the cascading safeguard by a two-step hit-flagging approach creates new data processing streamlines current access rights. However, this new data processing and this streamlining of current access rights for law enforcement authorities is necessary in order to achieve the purpose of the prevention, investigation, detection or prosecution of terrorism and other serious criminal offences in an efficient manner and enabling EU law enforcement authorities to focus efforts in fulfilling their tasks. It also includes the sufficient safeguards to avoid abuse of the mechanism by its users.

### **6.6. Safeguards**

As explained above, data protection and fundamental rights risks in relation to option 2 do not increase and do not get modified with respect to those identified in the legal instruments of the central systems. The new elements of option 3 streamline or establish access rights for certain specific end-user groups. These changes may in certain ways affect fundamental rights (including the right to respect for private life, the right to one's

identity, the right to good administration and the presumption of innocence) and require commonly used safeguards to be applied, such as:

- appropriate end-user management by Member States and agencies;
- logging of access and usage by users of each component;
- appropriate monitoring and evaluation of components and functionalities;
- appropriate monitoring of accuracies, false-positives and false-negatives of the shared BMS and the CIR;
- appropriate development, configuration and maintenance methodologies for each component in accordance with the legal instruments;
- appropriate security measures to protect data;
- appropriate fallback procedures and means;
- apply common quality indicators and reporting with minimum quality standards to maximise data quality;
- stipulate that the existence of links in itself will not constitute a ground for refusal of entry;
- make sure that links are analysed and resolved without delay;
- extension of eu-LISA's security plan, business continuity and disaster recovery plan.

All these safeguards have been identified and are addressed in the legislative proposal.

## **7. HOW DO THE OPTIONS COMPARE?**

This chapter compares the three options, and notably option 2 (ESP, shared BMS and CIR combined) against option 3 (option 2, supplemented with MID, extension of access rights for the purpose of identification, establishing law enforcement access).

### **7.1. Option 1: no interoperability**

Interoperability issues already exist today, with only three central systems in place. With the planned development of EES, the proposed ETIAS and the proposed ECRIS-TCN system, the challenges will, if not adequately addressed, only increase. With each new system being implemented, Member States will need to provide and manage access to it for an extended number of end-users across an array of different entities, thereby increasing the risks related to data availability, quality and security.

It is to be expected that the threats of terrorism will not diminish in the near future. The number of third-country nationals visiting the EU for the purpose of tourism or business will further increase. The amount of people seeking protection in the EU, or aiming to enter the EU irregularly is also expected to remain high. After implementation of the additional systems (EES, the proposed ETIAS, the proposed ECRIS-TCN system) the actual law enforcement cascade would become longer and the number of data records and complexity greatly increases. Multiple identities linked to a single set of biometric data would occur more often and there would be no means to detect or address them.

Issues with reliably identifying third-country nationals travelling to the EU will be further magnified, including when dealing with asylum seekers and irregular migrants. The proposed revised and extended Eurodac, including alphanumeric data, and the new

possibilities provided through Europol data access by the proposed ETIAS, further add to the need to address interoperability challenges.

For these reasons option 1 has been rejected.

## 7.2. Option 2: High-level expert group approach to the management of data for borders and security

### 7.1.1. Costs

The cost estimations are detailed in the annex 4. The overview of all costs (both one-off and recurrent) for all components, both for eu-LISA and the Member States, are the following:

Table 3 — Costs of option 2

	<i>Member States and Europol</i>		<i>eu-LISA</i>	
	<b>One-off</b>	<b>Recurrent</b>	<b>One-off</b>	<b>Recurrent</b>
<i>Direct costs</i>	(€m)	(€m p.a.)	(€m)	(€m p.a.)
CRRS	0	0	6.9	0.7
ESP	15.0	3.0	12.0	2.2
Shared BMS	0.0	0.0	29.6	2.9
CIR	15.3	3.1	7.3	1.5
<b>Total</b>	<b>30.3</b>	<b>6.1</b>	<b>55.8</b>	<b>7.3</b>

The cost of the central repository for reporting and statistics (CRRS) is added although it is not as such an interoperability component and, since it is the same in option 3, is not a differentiator.

Shared BMS also includes the data migration cost (from legacy systems to shared BMS) estimated at €10m.

One-off and recurrent costs were computed as additional costs on top of the implementation of the EES that will implement the basis for the shared BMS and the CIR. All one-off and recurrent costs are implementation costs. No regulatory charges, hassle costs, administrative costs, or indirect costs were identified.

The one-off total cost for the development and putting into operation of ESP shared BMS and CIR amounts to €86.1m. Total recurrent costs for this option are estimated to amount to €13.4 m per year.

Annex 4 contains the details of the computation of direct benefits that can be monetised for option 2. There are no indirect benefits.

Table 4 — Benefits of option 2

<i>I. Overview of Benefits for Option 2</i>		
<i>Description</i>	<i>Amount</i>	<i>Beneficiary</i>
1. Reduced training costs.	€20m p.a.	Member State administrations for border management, migration and law enforcement authorities.
2. Reduced cost of changes to national applications when the central system is operational.	€6m p.a.	Member State IT departments
3. Cost saving of having one central shared BMS rather than one BMS per central system containing biometrics.	€1.5m p.a. and reduction of €8m in one-off investment	EU central administration
<b>Total</b>	<b>€27.5m p.a. and €8m one-off</b>	

All benefits are reduced implementation costs and are based on very cautious estimates.

The cost/benefit analysis results in the following:

<i>Option 2</i>	<i>Member State Administrations</i>		<i>Central EU Agencies</i>		<i>Total</i>	
	<i>One-off</i> (€m)	<i>Recurrent</i> (€m p.a.)	<i>One-off</i> (€m)	<i>Recurrent</i> (€m p.a.)	<i>One-off</i> (€m)	<i>Recurrent</i> (€m p.a.)
Costs	30.3	6.1	55.8	7.3	86.1	13.6
Benefits	0	26.0	8.0	1.5	8.0	27.5
<b>Net Result</b>	<b>-30.3</b>	<b>19.9</b>	<b>-47.8</b>	<b>-5.8</b>	<b>-78.1</b>	<b>14.1</b>

The net additional marginal investment of €78,1 million is thus expected to be recovered after around 5,6 years after the full implementation, which is about nine years after the project start. Even if there is still a lot of approximation about these figures (both on benefits and on costs) it can be concluded that the proposed measures provide a positive cost/benefit ratio. The cost recovery time for Member States will be less than two years.

#### 7.1.2. Data protection impacts

The three technical components of option 2 (ESP, shared BMS, CIR) respect the essence of the right to personal data, meet clearly defined objectives of general interest that justify an interference with fundamental rights, and provide for the processing of personal data that is necessary and proportionate to achieve these objectives (see sections 6.4 and 6.5).



### 7.1.3. Feasibility and enforcement

The components (ESP, shared BMS, CIR) covered by this option are new but the underlying technical solutions already exist and are well proven. The three feasibility studies for these components all state that they can technically be implemented. The technical architecture of SIS however presents a major difficulty for the CIR. To mitigate this risk, SIS data is not included in the CIR.

When developing and implementing this option, three main challenges will need to be addressed:

- 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 shared BMS only)

The **ESP** holds no data and relies on existing functionalities of current and future systems. It will technically be built using proven technology.<sup>59</sup> Several Member States have implemented similar single-search interface concepts at the national level. The ESP will complement such existing interfaces only where searches for persons and travel documents in centralised EU information systems are concerned.

The expected difficulties lie specifically in integrating new search transactions in the existing national systems, national workflows and national processes. The introduction of the future EES and the proposed ETIAS will benefit from the ESP and vice versa. Substantial training and sharing of best practices will be required.

The technical solution of a **shared BMS** is widely implemented and used in countries outside the EU. Similar tools are also developed for third countries to combine voting registers with national population registers and criminal registers.

The shared BMS is a back-end system not visible to Member States and will not generate any integration efforts.

The historical biometric data in Eurodac, VIS and SIS will need to be migrated. This constitutes a separate project for eu-LISA with limited impact on Member States. Previous migrations of Eurodac and VIS biometric data have already been successfully implemented.

The **CIR** will be put in place as a specific set of database tables during the development of the EES, holding the biographical data of third-country nationals entering and exiting Schengen. It will thus be empty at go-live and gradually filled thereafter. It will need to be protected for data security issues in the same way as the current identity data in the underlying systems.

Member States will need to interface with the CIR as part of the EES/VIS development. The expected difficulties lie in integrating the new search transactions in the existing national systems, national workflows and national processes. Substantial training and sharing of best practices will be required.

---

<sup>59</sup> See ESP feasibility study: the use of an Enterprise Service Bus.

Developments of the proposed ETIAS, the new Eurodac and the proposed ECRIS-TCN will be quicker and easier since an important ‘part’ of these new systems, the storage of biographical data, can be fully aligned with the EES/VIS development.

### 7.3. Option 3: new approach to identity management and law enforcement access

#### 7.1.4. Costs

Cost estimations are based on various references such as the technical feasibility studies, experience from previous projects and consultation of and dialogue with eu-LISA. The overview of all costs (both one-off and recurrent) for all components, both for eu-LISA and the Member States, are the following:

Table 5— Costs of option 3

	<i>Member States &amp; Europol</i>		<i>eu-LISA</i>	
	<b>One-off</b>	<b>Recurrent</b>	<b>One-off</b>	<b>Recurrent</b>
<i>Direct costs</i>	(€m)	(€m p.a.)	(€m)	(€m p.a.)
CRRS (like option 2)	0	0	6.9	0.7
ESP	18	3.6	14.3	2.7
Shared BMS	0	0	29.6	2.9
MID	45.0	9.0	15.4	2.9
Link validation MID	0	0	5.9	0
CIR (like option 2)	15.3	3.1	7.3	1.5
CIR — identification functionality	3.6	0.7	2.4	0.3
CIR — law enforcement access flagging	3.6	0.7	2.5	0.4
<b>Total</b>	<b>85.5</b>	<b>17.1</b>	<b>84.3</b>	<b>11.4</b>

The cost of CRRS is added although it is not as such an interoperability component and since it is the same in option 3, is not a differentiator.

Shared BMS also includes the data migration cost (from legacy systems to shared BMS) estimated at €10m.

The ESP solution is amended for option 3. The link validation when creating MID is a one-off cost of €5,9m. It is put under eu-LISA although it might turn out to be implemented in another agency.

One-off and recurrent costs were computed for this option 3. All one-off and recurrent costs are compliance costs. No regulatory charges, hassle costs, administrative costs, or indirect costs were identified and therefore quantified.

The main costs are directly related to establishing the multiple-identity detector and validating the links on historical data during the transitional period. As can be concluded from the table above, the total one-off costs for option 3 amounts to €169.7 m. Total recurrent costs for option 3 are estimated to amount to €11.4 m per year.

The estimated costs of this option are to be set against the expected benefits that can be monetised as follows (see also Annex 4.2):

Table 6 — Expected savings

<i>Overview of benefits (total for all provisions) — Option 3</i>		
<i>Description</i>	<i>Amount</i>	<i>Beneficiary</i>
<i>Direct benefits</i>		
Reduced cost of changes to national applications when the central system is operational	€6m p.a.	Member State IT departments
Cost saving of having one central shared BMS rather than one BMS per central system containing biometrics	€1.5m p.a. €8m one-off	eu-LISA
Saved cost of identification of multiple identities.	€50m p.a.	Member State administrations for border management, migration and law enforcement.
Reduced training costs	€20m p.a.	Member State administrations for border management, migration and law enforcement
<b>Total</b>	<b>€77.5 m p.a. and €8m one-off</b>	

All benefits are reduced implementation costs and are based on very cautious estimates.

The cost/benefit analysis results in the following:

<i>Option 3</i>	<i>Member State Administrations</i>		<i>Central EU Agencies</i>		<i>Total</i>	
	<i>One-off</i> (€m)	<i>Recurrent</i> (€m p.a.)	<i>One-off</i> (€m)	<i>Recurrent</i> (€m p.a.)	<i>One-off</i> (€m)	<i>Recurrent</i> (€m p.a.)
Costs	85.5	17.1	84.3	11.4	169.8	28.5
Benefits	0	76.0	8.0	1.5	8.0	77.5
<b>Net Result</b>	<b>-85.5</b>	<b>58.9</b>	<b>-76.2</b>	<b>-9.9</b>	<b>-161.7</b>	<b>49.0</b>

The net additional marginal investment of €161.8 million is thus expected to be recovered after around 3.3 years after the full implementation, which is about six years after the project start. Even if there is still a lot of approximation about these figures (both on benefits and on costs) it can be concluded that the proposed measures provide a

positive cost/benefit ratio. The cost recovery time for Member States will be less than two years.

#### 7.1.5. *Data protection impacts*

The four technical components (ESP, shared BMS, CIR and MID) and two procedural changes (identity checks in the territory, law enforcement access via two-step approach with flagging) respect the essence of the right to personal data, meet clearly defined objectives of general interest that justify an interference with fundamental rights, and provide for the processing of personal data that is necessary and proportionate to achieve these objectives (see Sections 6.4 and 6.5).

The interference with the right to personal data by data processing in the CIR and the MID under options 3 is **not more intrusive** than the data processing in the CIR under option 2, given that under option 2, the CIR performs the same data processing that is performed by the CIR and the MID under option 3. While the TCN identifications and the law enforcement with flagging under option 3 have an impact on the right to privacy, they are limited to what is absolutely necessary and ensure that option 3 can address the problems identified and meet the objectives of general interest **more effectively**.

#### 7.1.6. *Feasibility and enforcement*

The proposed elements of option 3 are new but with the exception of the MID, fully rely on and reuse components of option 2.

When developing and implementing this option, two further challenges will need to be addressed, in addition to the ones mentioned under option 2:

- Development complexities of the multiple-identity detector;
- Integration of the multiple-identity detector in existing systems, processes, and workflows, both at the central level and at the level of Member States.

The **MID** needs to interface with the SIS and the new CIR and will be consulted by the ESP making this a challenging infrastructure development. The MID relies on the access control mechanisms put in place by the underlying systems. It will need to be protected for data security issues in the same way as the other central systems.

The capability of conducting **identity checks** fully relies on an existing CIR coupled with the shared BMS. Since the CIR is already used for identifications at border control, this is essentially a legal change, without system design consequences on other systems. Identity checks will not add or modify data in the CIR. The expected complexity lies with the Member States needing to purchase and customise handheld biometric terminals<sup>60</sup> and connect them to their national police systems.

## 7.4. **Conclusion**

The (essentially technical) components of the less ambitious option 2 will enable a number of changes to the way end-users access data, to which they already today have legal access. These components will facilitate the way new systems (like the EES, ETIAS, new Eurodac, ECRIS-TCN) will be developed and used.

---

<sup>60</sup> The European Network of Law Enforcement Technology Services (ENLETS) mobile project has studied best practices for this purpose ([Council document 14750/17](#)).

Option 2 supports specific objective 1 (ensuring fast, seamless, systematic and controlled access to needed information) but does little for the other three objectives. Under this objective, no end-user access rights are modified.

The absence of SIS data in the CIR under option 2, leads to a reduced functionality on detecting identity fraud. The new multiple-identity detector of option 3 is a direct result of further reflections when trying to find an alternative to modifying the SIS architecture to allow including SIS data in the CIR.

By introducing the MID option 3 offers a privacy-by-design approach to objective 2 on detecting and managing multiple identities across all central systems, including the SIS. This objective could not be reached by option 2.

Option 3 furthermore adds two new important functionalities to the CIR: the possibility to perform identity checks in the territory; and the possibility for a two-step law enforcement access approach. These functionalities directly relate to the objectives 3 and 4 of this initiative. These objectives cannot be reached by option 2.

Only option 3 is capable of meeting all four objectives.

When comparing option 2 and option 3 against the criteria of costs, data protection and feasibility and enforcement, it can be concluded as follows:

**Costs:** option 3 is more expensive than option 2 (€169.8 m versus €86.1 m one-off costs and €28.5 m per year versus €14.1 m per year recurrent costs). The benefits are however about €50 m per year higher for option 3 than for option 2. The cost recovery period of option 3 is of 3.3 years and that of option 2 of 5.5 years. Option 3 is therefore more favourable than option 2 from a cost/benefit point of view.

**Data protection:** data protection by the respective technical components under option 3 is not more intrusive than data processing under option 2. While the additional functionalities of option 3 have an impact on the right to privacy, they are limited to what is absolutely necessary.

**Feasibility and enforcement:** both option 2 and 3 are technically and operationally feasible. Both put certain technical and operational challenges to eu-LISA and the Member States, but none of these are unsurmountable.

Option 3 will be more effective in meeting the objectives of this initiative, and will allow authorised end-users a simpler and more efficient access to necessary information. For these reasons option 3 is the preferred option.

## 8. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

### 8.1. Practical arrangements of the evaluation: when, by whom

The Commission will ensure that systems are in place to monitor the functioning of the four components (ESP, shared BMS, CIR and MID) and evaluate them against the main policy objectives. Four years after the functionalities are put in place and operating, and every four years thereafter, eu-LISA should submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components. In addition, one year after each report from eu-LISA, the Commission should produce an overall evaluation of the components, including on the either direct or indirect impact of the components and of its practical implementation on fundamental rights. It should examine results achieved against objectives and assess the continuing validity of the underlying rationale and any implications for future options. The Commission should submit the evaluation reports to the European Parliament and the Council.

### 8.2. Operational objectives and monitoring indicators for the preferred option

The monitoring indicators in the next sections are essentially expected to be collected on an ongoing basis by the systems or technical components themselves. For evaluation purposes, annual statistics will be computed and compared between successive years. Where possible, a comparison with the baseline situation taken as the trend or average of the three years that precede the entry into operations can be used.

Operational objectives and indicators for each specific objective:

<i>1. Fast, seamless and systematic access to authorised data sources</i>	
<ul style="list-style-type: none"> <li>• ESP is implemented in all Member States and for all relevant use cases.</li> </ul>	<ul style="list-style-type: none"> <li>• Number of Member States that implemented ESP multiplied by the number of use cases implemented.</li> </ul>
<ul style="list-style-type: none"> <li>• ESP is used for conducting searches on multiple systems.</li> </ul>	<ul style="list-style-type: none"> <li>• Number of searches handled by ESP v total number of searches (via ESP and systems directly).</li> </ul>
<i>2. Streamline access to authorised data sources for law enforcement purposes</i>	
<ul style="list-style-type: none"> <li>• Access streamlining possibility is used.</li> </ul>	<ul style="list-style-type: none"> <li>• Number of step 1 accesses for law enforcement purposes.</li> <li>• Number of step 2 accesses for law enforcement purposes.</li> </ul>
<i>3. Facilitate identifications of third-country nationals</i>	
<ul style="list-style-type: none"> <li>• Identification means are used.</li> </ul>	<ul style="list-style-type: none"> <li>• Number of identification checks performed v total number of transactions.</li> </ul>
<i>4. Detect multiple identities and fraud</i>	
<ul style="list-style-type: none"> <li>• Identification means are used.</li> <li>• Identity fraud is detected.</li> </ul>	<ul style="list-style-type: none"> <li>• Number of identities linked v number of identities with biographical information.</li> <li>• Number of detected cases of identity fraud v number of linked identities and total number of identities.</li> </ul>

Monitoring indicators for the development of each component (ESP, shared BMS, CIR, MID) result from project reporting and include the following:

- Each component is put into operation within the time span and budget of the development project set after the adoption of the Regulation;

- All Member States use the shared BMS and CIR functionalities at the date agreed for ‘entry into operations’;
- All components are delivered, including the periodic delivery of reliable and precise statistics on the use of the components and the results produced.

Monitoring once the system is live essentially stems from systems operations reporting, supplemented in a small number of cases by specific data:

- The number of errors is minimal (errors refer to the number of incorrectly reported cases of linked identities);
- Statistics on the number of identities recorded in CIR and linked identities are available on demand and standard reports are produced regularly, on the basis of system operations reports;
- All expired data are deleted and there is no unwanted loss or erasure of data, based on system operations reviews;
- All access to data was authorised and there are no cases of unauthorised access to data, as observed from system operations reviews;
- Incidents on data access are reported, the origin of the problem analysed and a remedy provided, as reported by system operations reviews;
- Identification and assessment of reported and potential issues concerning the either direct or indirect impact of the components and of its practical implementation on fundamental rights.

## **9. LIST OF ANNEXES**

1. ANNEX 1 - GLOSSARY
2. ANNEX 2: PROCEDURAL INFORMATION
  - 2.1. Lead DG, Decide Planning/CWP references
  - 2.2. Organisation and timing
  - 2.3. Consultation of the RSB
  - 2.4. Evidence, sources and quality
3. ANNEX 3: STAKEHOLDER CONSULTATION
4. ANNEX 4: WHO IS AFFECTED AND HOW?
  - 4.1. Practical implications of the initiative
  - 4.2. Summary of costs and benefits
5. ANNEX 5 – SUPPORTING STUDIES
  - 5.1. European search portal
  - 5.2. Shared biometric matching service
  - 5.3. Common identity repository
6. ANNEX 6 - INVENTORY OF EXISTING INFORMATION SYSTEMS FOR BORDER MANAGEMENT AND LAW ENFORCEMENT
7. ANNEX 7 - MATRIX ON ACCESS TO CENTRAL EU SYSTEMS FOR BORDERS AND SECURITY
8. ANNEX 8 - SUPPLEMENTARY ANALYSIS & INFORMATION
  - 8.1. Detailed analysis of the ESP's sub-options
    - 8.1.1. ESP with or without SIS data
    - 8.1.2. Access Interpol and Europol data: extend the ESP
    - 8.1.3. ESP with or without the proposed ECRIS-TCN data
    - 8.1.4. ESP with or without shared BMS
  - 8.2. Detailed analysis of the shared biometric matching service
  - 8.3. Detailed analysis of the common identity repository
    - 8.3.1. Allow police to perform identification of TCNs: additional purpose for the CIR
    - 8.3.2. Facilitate law enforcement access: two-step flagging on the CIR
  - 8.4. Detailed analysis of the multiple-identity detector
    - 8.4.1. MID with SIS data
    - 8.4.2. MID with the proposed ECRIS-TCN data
    - 8.4.3. MID with cross-matching existing data





Strasbourg, 12.12.2017  
SWD(2017) 473 final

PART 2/2

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**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)**

{COM(2017) 793 final} - {SWD(2017) 474 final}

## ANNEXES

1.	ANNEX 1 - GLOSSARY .....	1
2.	ANNEX 2: PROCEDURAL INFORMATION .....	3
2.1.	Lead DG, Decide Planning/CWP references .....	3
2.2.	Organisation and timing.....	3
2.3.	Consultation of the RSB .....	3
2.4.	Evidence, sources and quality.....	3
3.	ANNEX 3: STAKEHOLDER CONSULTATION .....	4
4.	ANNEX 4: WHO IS AFFECTED AND HOW?.....	8
4.1.	Practical implications of the initiative .....	8
4.2.	Summary of costs and benefits .....	12
4.2.1.	Costs for option 2.....	12
4.2.2.	Benefits for Option 2.....	13
4.2.3.	Cost-benefit for option 2 .....	14
4.2.4.	Costs for option 3.....	15
4.2.5.	Benefits for Option 3.....	16
4.2.6.	Cost-benefit for option 3 .....	17
5.	ANNEX 5 – SUPPORTING STUDIES.....	18
5.1.	European search portal.....	18
5.2.	Shared biometric matching service.....	23
5.3.	Common identity repository .....	23
6.	ANNEX 6 - INVENTORY OF EXISTING INFORMATION SYSTEMS FOR BORDER MANAGEMENT AND LAW ENFORCEMENT .....	24
7.	ANNEX 7 - MATRIX ON ACCESS TO CENTRAL EU SYSTEMS FOR BORDERS AND SECURITY .....	28
8.	ANNEX 8 - SUPPLEMENTARY ANALYSIS & INFORMATION .....	39
8.1.	Detailed analysis of the ESP's sub-options .....	39
8.1.1.	ESP with or without SIS data .....	41
8.1.2.	Access Interpol and Europol data: extend the ESP .....	42
8.1.3.	ESP with or without the proposed ECRIS-TCN data .....	45
8.1.4.	ESP with or without shared BMS.....	45
8.2.	Detailed analysis of the shared biometric matching service .....	47
8.3.	Detailed analysis of the common identity repository .....	49
8.3.1.	Allow police to perform identification of TCNs: additional purpose for the CIR.....	50
8.3.2.	Facilitate law enforcement access: two-step flagging on the CIR .....	53
8.4.	Detailed analysis of the multiple-identity detector .....	56
8.4.1.	MID with SIS data .....	57
8.4.2.	MID with the proposed ECRIS-TCN data .....	58
8.4.3.	MID with cross-matching existing data.....	58

## 1. ANNEX 1 - GLOSSARY

<i>Term or acronym</i>	<i>Meaning or definition</i>
ABIS	Automated biometric identification system
AFIS	Automated fingerprint identification system
API Directive	Advance Passenger Information Directive <sup>1</sup>
Charter	Charter of Fundamental Rights of the EU
CIR	Common identity repository
CS	Central system
EASO	European Asylum Support Office
EBCG	European Border and Coast Guard Agency <sup>2</sup>
ECRIS-TCN system	European criminal record information system for third-country nationals (proposal)
EES	Entry/Exit System
ESP	European search portal
ETIAS	European Travel Information and Authorisation System (proposal)
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
Eurodac	European asylum fingerprint database
Europol	European Union Agency for Law Enforcement Cooperation
FIND	Fixed Interpol Network Database
FRA	EU Agency for Fundamental Rights
Frontex	See EBCG
Hit/no-hit	Result of a data-presence search in a system containing a certain category of data (i.e. SIS, VIS, EES)
ICD	Interface control document
Interpol	International Criminal Police Organization

<sup>1</sup> Council Directive [2004/82/EC](#) of 29 April 2004 on the obligation of carriers to communicate passenger data.

<sup>2</sup> Regulation (EU) [2016/1624](#) of the European Parliament and of the Council of 14 September 2016.

<i>Term or acronym</i>	<i>Meaning or definition</i>
MID	Multiple-identity detector
PNR	Passenger name record system
Prüm	Police cooperation mechanism for exchanging information on DNA, fingerprints and vehicle registration data
Shared BMS	Shared biometric matching service
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entries
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents database (Interpol)
TCN	Third-country nationals and stateless persons
TDAWN	Travel Documents Associated with Notices (Interpol)
UMF	Universal Message Format: format of messages to allow compatibility between information systems
UMF+	Extension of the existing UMF description
VIS	Visa Information System

## **2. ANNEX 2: PROCEDURAL INFORMATION**

### **2.1. Lead DG, Decide Planning/CWP references**

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME). The agenda planning reference is PLAN/2017/1570.

### **2.2. Organisation and timing**

Work to prepare the draft proposal and the impact assessment began in early June. This followed the final report of the high-level expert group on information systems and interoperability, and the Commission's *Seventh progress report towards an effective and genuine Security Union* (16 May).

The European Council Conclusions of 22/23 June 2017 invited the Commission to prepare, as soon as possible, draft legislation enacting the recommendations made by the high-level expert group.

The interservice task force for the impact assessment was composed of: Secretariat-General (E1), DG HOME (B3, A2, B2, C2, C3, D1 and D2), DG JUST (B1, C3 and C4), Legal Service (SJ); TAXUD (B2), and CNECT. Three meetings were held (4.7.2017, 15.9.2017, 6.11.2017).

### **2.3. Consultation of the RSB**

The draft impact assessment was submitted to the Regulatory Scrutiny Board on 24 November and examined by the Board on 6 December 2017. The Board delivered its opinion (positive with reservations) on 8 December indicating that the impact assessment be adjusted in order to integrate the Board's recommendations on specific aspects. These related firstly to additional measures under the preferred option streamlining end-users' existing data access rights in EU information systems, and to illustrate associated safeguards for data protection and fundamental rights. The second main consideration was to clarify the integration of the Schengen Information System under option 2, including effectiveness and costs to facilitate its comparison with the preferred option 3. The Commission updated its impact assessment to respond to these main considerations and to address a number of other comments made by the Board.

### **2.4. Evidence, sources and quality**

The first major reference document is the Commission's Communication *Stronger and Smarter Information Systems for Borders and Security*<sup>3</sup>. This was followed by the setting-up of the high-level expert group on information systems and interoperability, which delivered its final report on 11 May 2017<sup>4</sup>. The work and report of the high-level expert group constituted an in-depth analysis of the issues concerned relating to borders, security and migration management and an assessment of the technical and operational possibilities offered by innovative functionalities with a view to addressing identified shortcomings in EU information systems.

---

<sup>3</sup> COM(2016)205, 6 April 2016.

<sup>4</sup> <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

To advance the assessment of the functionalities, the Commission commissioned feasibility studies on a European search portal, on a shared biometric matching service, and on a common identity repository. The report on the feasibility study for the European search portal has been completed, for which an executive summary is included in this impact assessment as Annex 5.1. The results of the other studies will be made available as soon as they are finalised.

### **3. ANNEX 3: STAKEHOLDER CONSULTATION**

#### **Consultation strategy**

In order to ensure that the general public interest of the EU is properly considered in the Commission's approach to interoperability and, in particular, any legislative proposals that may be required to implement this, the Commission regards it as a duty to conduct stakeholder consultations, and wishes to consult as widely as possible.

To do this, the Commission has identified relevant stakeholders and has consulted them as appropriate throughout the development of these proposals. The Commission has sought views from subject matter experts, national authorities, civil society organisations, and views from members of the public on their expectations and concerns relating to interoperability. A key method of consultation for this initiative was an online open public consultation, seeking views from all interested parties. More targeted stakeholder events focusing on subject matter experts, including practitioners at national level, were also held. An inception impact assessment was also published. This diversity of perspectives has been valuable in helping the Commission to ensure that its proposals address the needs, and take account of the concerns, of a wide range of stakeholders.

#### **Formal consultation activities**

##### *Open public consultation*

An open public consultation was held, seeking views from any interested stakeholders. This was available to complete online in all the EU's official languages (with the exception of Irish, due to resource constraints). The consultation was open for response from 27 July to 19 October 2017.

The consultation contained 38 questions, including a mix of closed and open questions, to seek detailed views on this complex subject. It was supported by a background paper providing more information about the issues and challenges, and the options that were being considered to tackle these. Respondents were also able to submit short position papers of their own, if they wished, to provide more background on their views expressed in the survey.

##### *Stakeholder events*

Stakeholder workshops were held on 27 July and 6 October 2017, to which were invited representatives of Member States and Schengen associated countries, the EU Counter-Terrorism Coordinator and the European Data Protection Supervisor, relevant agencies (eu-LISA, Europol, EU Agency for Fundamental Rights, European Asylum Support Office and Frontex), the General Secretariat of the Council and the secretariat and advisors to Parliament's Committee on Civil Liberties, Justice and Home Affairs. Commission participants included representatives of the following services: Secretariat-

General, Legal Service, DG JUST, DG CNECT and DG TAXUD. During these workshops, participants were provided with updates on the work being done on the options being considered as part of this interoperability package, leading to more detailed discussion.

A further workshop was held on 10 October with the European Data Protection Supervisor, with the participation of the EU Agency for Fundamental Rights. Commission participants included staff working on data protection issues, information systems for borders and security, and in the Commission's Legal Service.

#### *Tripartite discussions with the European Parliament and the Council*

As indicated above, the secretariat and advisors to Parliament's Committee on Civil Liberties, Justice and Home Affairs were invited to the two workshops hosted by the Commission. In addition, a tripartite technical meeting was held on 7 November as a further opportunity directly to inform the secretariat and advisors — and through them members of the committee — about the intended objectives and the feasibility of technical components to address them, and of course to receive their views.

This tripartite discussion was followed up in a meeting of the committee where an exchange of views took place with Estonia's Permanent Representative, representing the current Presidency, and the Commissioner for the Security Union.

#### **Stakeholder participation**

As set out above, stakeholders directly consulted included:

- representatives of Member States and Schengen associated countries
- the EU Counter-Terrorism Coordinator
- the European Data Protection Supervisor
- relevant agencies (eu-LISA, Europol, EU Agency for Fundamental Rights, European Asylum Support Office and Frontex)
- the General Secretariat of the Council
- the secretariat and advisors to Parliament's Committee on Civil Liberties, Justice and Home Affairs
- representatives of the following Commission services: Secretariat-General, Legal Service, DG JUST, DG CNECT and DG TAXUD.

The open public consultation also received responses from members of the public, Member States, political parties, NGOs, think tanks and charities with an interest in this field.

This diversity of responses and perspectives has been valuable in assisting us in drawing up our proposals and we are grateful to all who have participated in this consultation process.

#### **Methodology and tools**

Given the small number of results and the high number of open questions in the survey, designed to seek detailed views from respondents, the feedback from the consultation — as with the feedback received from stakeholder events — has been processed manually. This involved reading the consultation responses in full, noting support and any issues and concerns that were raised, and feeding back on these internally as appropriate.

## Results

### *Public consultation*

The public consultation received 18 responses from a variety of stakeholders, including private citizens, Member State governments, private sector organisations and other organisations such as NGOs and think tanks. These responses have been published in full online; some have been anonymised at the request of respondents.

Overall, the responses were broadly in favour of the underlying principles of this interoperability proposal. The vast majority of respondents agreed that the issues the consultation identified were the correct ones, and that the objectives the interoperability initiative seeks to achieve are correct.

With regard to the more detailed options proposed in the consultation, responses were more mixed. Although a majority of respondents supported each of the proposed options, considering them to be necessary to achieve the objectives of this initiative, concerns were repeatedly raised. These included: the need for strong and clear data protection measures, particularly in relation to access to the information stored in the systems and data retention; the need for up-to-date, high-quality data in the systems and measures to ensure this; and the potential for bias in decision-making or discriminatory profiling of individuals. Several respondents noted, in response to different consultation questions, the potential for problems arising from the inclusion of Interpol data (including biometric data), where some of this may have been included for politically motivated reasons.

Other issues noted include: the need for appropriate logging and audit arrangements for search requests; the need for future-proofing so that future systems can also be easily included; the need to maintain the rights of current data owners over their data; the need for greater harmonisation in terms of legislation and standards across the EU; and the need to avoid mass surveillance and the erosion of fundamental rights such as the right to a private life.

With regard to a European search portal in particular, the majority of respondents agreed that the search portal would help staff on the ground access the information they need, particularly in agencies and Member States that do not have their own national single-search interfaces. Several respondents considered that the portal should not search particularly sensitive personal data (such as sexual orientation or religion). Multiple respondents were also concerned that the possibility of hit/no-hit flags in relation to the European search portal may mean that officers on the ground make decisions based on the existence of a hit in a given system, even without further details.

The majority of respondents agreed that a common identity repository would help to avoid duplication of data, reduce overlaps and highlight discrepancies in data. It was considered by the majority of respondents to be able to help identify people more reliably – including people with multiple identities – and reduce identity fraud. Several respondents noted that sensitive personal data (especially medical data) should not be contained in a common identity repository. One respondent further noted that particular care should be taken with regard to information stored about children, which may otherwise inform decisions taken about them in adult life.

Respondents were similarly generally positive about the option of a shared biometric matching service, with comments noting that it would improve data quality, improve reliability and provide a powerful tool to identify people and false identity documents. However, respondents also raised data protection concerns with regard to biometric



information, including: the need for strict access controls and clear definition of retention periods; purposes for which searches could be carried out and types of data stored; and potential difficulties that individuals might face in correcting errors and the risk of false matches due to quality issues. Several respondents again recommended that sensitive personal data – including ethnicity and health issues, potentially revealed by DNA profiles – should not be included in this system. Views on hit/no-hit flagging were similar to those expressed with regard to the European search portal, in that they were generally considered operationally useful, but respondents were concerned that the existence of a flag risks influencing decisions being made, even without full knowledge of the details.

With regard to the possibility of more streamlined rules for law enforcement access to information, a majority of respondents considered that this would be an effective way of achieving the desired objectives. However, respondents also noted the need for good access management and control systems and the need for proper audit and logging of all search requests, if these rules for access were adopted, to ensure that data is accessed appropriately and by those with the proper authorisation.

### *Inception impact assessment*

The inception impact assessment was published on 26 July 2017 and was available for comment until 23 August 2017. The full published results of the consultation are available online<sup>5</sup>. By the deadline, comments were received from two public authorities, one non-governmental organisation and one citizen. One submission was withdrawn at the request of the submitting authority. Three public authorities submitted feedback offline after the deadline.

Most respondents offered global support for the interoperability initiative. One respondent stated that the initiative would be ambitious and complex and that the proposal should clearly identify legal, technical and governance requirements, and operational aspects, a view shared by others. Costs and benefits should also be identified, especially for end-users. Some respondents expressed support for facilitating access for law enforcement authorities to information held in the central EU systems. Data protection aspects had to be fully addressed in preparing the initiative.

### **Taking account of feedback received**

Feedback, including from the public consultation, on the first option proposed – a single database, bringing about the complete interconnectivity of information systems, where data registered in one system will automatically be shared across all other systems – raised a number of serious concerns about the risks posed by such a comprehensive interconnectivity of systems, in particular for data protection and data security. As a result, the Commission agrees that this option would not be the best way to achieve our objectives, and will not be taking work on this option forward any further.

The concerns raised regarding the other elements being considered as part of the interoperability initiative have been carefully considered and taken into account when developing policy in this area. In particular, the need for strong and clear data protection and security measures has been and continues to be an area of focus, to ensure that appropriate protections and safeguards for individuals and their data are in place.

---

<sup>5</sup> [https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3765711\\_en](https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3765711_en).

#### 4. ANNEX 4: WHO IS AFFECTED AND HOW?

##### 4.1. Practical implications of the initiative

The practical implications are given by stakeholder group.

- EU citizens: there are no direct practical implications.
- Third-country nationals

European search portal	None
Shared biometric matching service	When biometric data have been provided once, they can be used multiple times. This idea has already been applied for EES and VIS where fingerprints provided for a visa application are also used for border crossing. The purpose of the additional use of personal data needs to remain compatible with the reason for collecting the data originally. The shared BMS can at least provide a technical support for an authorised reuse of data.
Common identity repository	None. The CIR acts as a tool for the MID.
Multiple-identity detector	The MID can store the information that a <i>bona fide</i> traveller who is often confused with a similarly named <i>mala fide</i> traveller is a different person.  Identity theft and abuse of identity can be systematically detected.

- Border management

European search portal	In Member States where there is already a single-search interface, there is no impact.  In Member States where there is no or an unsatisfactory single-search interface implemented, border guards will have the benefit of directing searches to a single component that will return the complete information the end-user is entitled to. This is not more information than currently, but the same information obtained more easily.
Shared biometric matching service	A claimed identity can be authenticated with high accuracy against a previously recorded identity.  At data entry, the biometric identification process avoids recording two claimed identities for the same physical person.

Common identity repository	None. The CIR acts as a tool required for the MID.
Multiple-identity detector	The MID can store the information that a <i>bona fide</i> traveller who is often confused with a similarly named <i>mala fide</i> traveller is a different person.  Identity theft and abuse of identity can be systematically detected.

- Migration and asylum management

European search portal	Migration officers will have the benefit of directing searches to a single component that will return the complete information the end-user is entitled to. This is not more information than currently but the same information obtained more easily.  Migrants can be more easily and more quickly identified (e.g. using the VIS data systematically) using the available information, speeding up the recognition of claims for protection/asylum.
Shared biometric matching service	A non-documented third-country national can be identified with the help of all available information improving the accuracy and fair treatment of migrants and asylum claims.
Common identity repository	None. The CIR acts as a tool required for the MID.
Multiple-identity detector	Identity theft and abuse of identity can be systematically detected, avoiding cases of granting protection to persons who represent a threat to the security of the EU.

- Law enforcement officers

European search portal	In Member States where there is already a single-search interface for law enforcement searches, there is no impact.  In Member States where implementation of a single-search interface for law enforcement is absent or unsatisfactory, law enforcement officers will have the benefit of directing searches to a single component that will return the complete information the end-user is entitled to.
------------------------	--

Shared biometric matching service	A non-documented third-country national can be identified with the help of all available information enabling the right legal follow-up.
Common identity repository	<p><b>Identity verifications</b> - The CIR gives access to identity data only. As an example, the data scanned from a passport are sent to the CIR, which returns the data recorded for that person and enables the verification of whether these correspond with the used passport and bearer.</p> <p><b>Law enforcement access</b> - The 'hit-flagging' functionality will enable law enforcement searches using the CIR without any cascading and without <i>ex ante</i> authorisation, which will still be necessary if full access to the information is needed. The only result of such a search would be 'hit-flags' by those systems that contain data related to the search.</p>
Multiple-identity detector	<p>In the case of <b>identity verification</b>, the MID informs on the availability of multiple identities and on the cases where a <i>bona fide</i> traveller should not be confused with a <i>male fide</i> traveller having a similar name.</p> <p>In the case of law enforcement access, the MID returns in the second step (so after the law enforcement officer received the proper authorisation) the origin of the systems where different identities corresponding with the same person are found, and the specific data contained in these systems.</p>

- eu-LISA

European search portal	ESP is an additional component to be developed, maintained and serviced.
Shared biometric matching service	Shared BMS is a simplification compared with a situation where an ABIS (automated biometric identification system) is implemented for each central system.
Common identity repository	CIR avoids a database of identities to be built for each new system. It requires a system migration for Eurodac only but which will be required when the new system is being developed.
Multiple-identity detector	MID is an additional component to be developed, maintained and serviced.

- IT organisation in Member States

European search portal	An initial investment needs to be done to implement search messages addressing the ESP rather than each individual system as well as for treating the response message. Once done, further changes to each system become less dependent on changes to the central systems as the national systems continue to access the ESP and it is the ESP (single component as opposed to 30 Member State systems) that then adapts to the modifications of the central system.
Shared biometric matching service	None. Use of shared BMS or of different biometric engines centrally has no technical impact on Member States. It has a huge impact however on what the central system delivers as functionality.
Common identity repository	CIR and MID only by the ESP. Therefore the impact on national systems is expected to be limited to handling the contents of the response to searches.
Multiple-identity detector	

## 4.2. Summary of costs and benefits

### 4.1.1. Costs for option 2

The overview of costs is indicated below.

<b>II. Overview of costs – Preferred option</b>						
	<i>Third-Country Nationals</i>		<i>Member State Administrations</i>		<i>Central Administration</i>	
	<b>One-off</b>	<b>Recurrent</b>	<b>One-off</b>	<b>Recurrent</b>	<b>One-off</b>	<b>Recurrent</b>
<b>Direct costs</b>						
CRSS	0	0	€0 m	€0m.p.a.	€ 6.9 m	€0.7m.p.a.
ESP	0	0	€15.m	€3.0m.p.a.	€12.0m	€2.2m p.a.
Shared BMS	0	0	€0m	€0m.p.a.	€29.6m	€2.9m p.a.
CIR	0	0	€15.3m	€3.1m p.a.	€7.3m	€1.5m.p.a.
<b>Total</b>	<b>0</b>	<b>0</b>	<b>€30.3m</b>	<b>€6.1m.p.a.</b>	<b>€55.8m</b>	<b>€7.3m p.a.</b>
<b>Indirect costs</b>						
None						

One-off and recurrent costs were computed as additional costs on top of the implementation of the Entry/Exit System. All one-off and recurrent costs are implementation costs. No regulatory charges, hassle costs, administrative costs, or indirect costs were identified and therefore are not quantified. These are all provisional estimates that will need to be confirmed. What is stable is how the costs of the various measures compare with each other.

Cost estimates are based on the results of the feasibility studies performed for each system. The costs are based on identifying for each project the end result, discerning its main components and costing each of them. The cost for some components can later on appear to be different due to changes in pricing policy, volume discounts or precise technical requirements. As an example of the latter, availability requirements on a same technical platform can modify prices by 30%. As a result, the confidence margin of cost estimates cannot be better than 20-25% at this early stage in a project.

As can be concluded from the table above, the one-off total cost amounts to € 86,1 and an annual cost increase of €13.4m.

#### 4.1.2. Benefits for Option 2

The table below contains the summary of benefits that can be monetized for the option 2

<b><i>I. Overview of Benefits for Option 2</i></b>		
<b><i>Description</i></b>	<b><i>Amount</i></b>	<b><i>Beneficiary</i></b>
<b><i>Direct benefits</i></b>		
1. Reduced training costs	€20m p.a.	Member State administrations for border management, migration and law enforcement authorities.
2. Reduced cost of changes to national applications when the central system is operational.	€6m p.a.	Member State IT departments
3. Cost saving of having one central shared BMS rather than one BMS per central system containing biometrics	€1,5m p.a. and reduction of €8m in one-off investment	EU central administration
<b><i>Indirect benefits</i></b>		
None identified	-	-
<b><i>Total</i></b>	<b><i>€27,5m p.a. and €8m one-off</i></b>	

All benefits are reduced implementation costs and are based on very cautious estimates.

1. Reduced training costs — the ESP removes to a large extent the need for recurrent re-training of staff when central systems are modified. The estimate is made assuming an average of 200,000 persons each year, out of the total end-user population, trained in sessions of 10 persons each. The cost for each training session is estimated at €1.000. Total annual recurrent cost is therefore at least €20m per year. Reduced training costs are mainly the result of ESP and CIR as they can be seen as two 'layers' that hide the complexity of central systems to end-users.
2. Reduced cost of changes to national applications when the central system is modified — if the proposed solution were not implemented, each national system would incur a change when the ICD (interface control document) of the corresponding central application is changed. The assumption made based on the history of changes to the current systems is that on average each system incurs an update at least once per year whether the reason for the change is due to technical or functional evolutions. Each change represents a workload of one man-year per

Member State counting from specification to actual testing. Without the proposed interoperability measure each Member State would spend on average 6 man-years of work on an annual basis for making changes to the national systems connected with the central systems. Over all Member States, this represents roughly 180 man-years of work per annum valued at €18m. The real cost could in reality be a multiple of this. The proposed measures can be expected to reduce this effort by at least a third which results in a saving of € 6 million per year. This is again a benefit from ESP and CIR that, by virtue of being positioned between national systems and central systems, they absorb the majority of changes occurring in the central systems.

3. Cost saving of having one central shared BMS rather than one BMS per central system containing biometrics — the development costs of the BMS are not proportional to the database size as such while hardware and software are proportional to volume. Having one shared BMS is estimated to cost €8m less than developing three biometric systems. This lower investment cost then leads also to a lower recurrent maintenance cost of €1,5m per year. This benefit is obviously completely dependent on the implementation of a shared BMS.

#### *Calculation assumptions*

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 given changes to central systems. The training cost per person takes only the additional cost of actually organising and delivering the training and does include the foregone personnel cost of the attendants.

The cost of changing national applications is based on the frequency of releases of current systems. The cost figures are rule-of-thumbs estimates (like one man-year of IT work being valued at 100 k€ is used as a rough calculation basis as there is an enormous spread within the European Union on personnel costs which reflects itself in the cost of services).

The cost of BMS systems is using historical cost figures from currently operated systems. As an average only the software license cost for the individual ABIS systems represents a cost of one euro per biometric identifier. If Eurodac, SIS and ECRIS-TCN have each an individual ABIS, the software license cost represents a one-off cost of at least €20 million, plus a yearly maintenance fee of €4.5 million. When the biometric identifiers are added to an existing ABIS of a large size, then the marginal cost of extending the software licenses reduces to about €0.35 per biometric identifier with an according impact on maintenance fee. Only a share of €8 million of the license fee reduction of €0.65 per biometric identifier (this would represent €13 million) is included in the benefit calculation as the individual biometric systems will not be replaced simultaneously. On an annual basis the maintenance fee is reduced to a third of the estimate (€ 1,5 million).

#### *4.1.3. Cost-benefit for option 2*

The proposed solution entails an annual cost increase of €13.4m and a benefit of €27.5m. The annual net benefit amounts to €14.1m. The net additional marginal investment of €78.1 million (€86.1m minus €8 m one-off benefit) is thus recovered about six years (5.5 years) after the full implementation, which is about nine years after the project start. As



there is still a lot of approximation (20-25%) about the figures mentioned (both on benefits and on costs), the main conclusion is that even by only taking the monetised benefits, the measures provide a positive cost-benefit ratio and costs are recovered after around nine years.

#### 4.1.4. Costs for option 3

The overview of costs is indicated below.

<b>II. Overview of costs – Preferred option</b>						
	<b>Third-Country Nationals</b>		<b>Member State Administrations</b>		<b>Central Administration</b>	
	<b>One-off</b>	<b>Recurrent</b>	<b>One-off</b>	<b>Recurrent</b>	<b>One-off</b>	<b>Recurrent</b>
<b>Direct costs</b>						
CRRS			€0m	€0m	€6.9m	€0.7m.p.a.
ESP	0	0	€18m	€3.6m p.a.	€14.3m	€2.7m p.a.
Shared BMS	0	0	€0m	€0m p.a.	€29.6m	€2.9m p.a.
CIR	0	0	€22.5m	€4.5m.p.a.	€12.2m	€2.2m p.a.
MID	0	0	€45.0m	€9.0m.p.a.	€15.4m	€2.9m p.a.
MID link validation	0	0	€0m	€0m p.a.	€5.9m	€0m p.
<b>Total</b>	<b>0</b>	<b>0</b>	<b>€85.5m</b>	<b>€17.1m .p.a.</b>	<b>€84.3m</b>	<b>€11.4m p.a.</b>
<b>Indirect costs</b>						
None						

One-off and recurrent costs were computed as additional costs on top of the implementation of the Entry/Exit System. All one-off and recurrent costs are implementation costs. No regulatory charges, hassle costs, administrative costs, or indirect costs were identified and therefore are not quantified. These are all provisional estimates that will need to be confirmed. What is stable is how the costs of the various measures compare with each other.

The same comment as in Section 4.2.1 applies here and as a result the confidence margin of cost estimates cannot be better than 20-25% at this early stage in a project.

As can be concluded from the table above, for option 3, the one-off total cost amounts to €169.8 million and the recurrent cost to €28.5million.

#### 4.1.5. Benefits for Option 3

The table below contains the summary of the benefits that can be monetized for the preferred option, selected at the end of Chapter 7.

<b><i>I. Overview of Benefits (total for all provisions) – Option 3</i></b>		
<b><i>Description</i></b>	<b><i>Amount</i></b>	<b><i>Beneficiary</i></b>
<b><i>Direct benefits</i></b>		
1. Reduced training costs	€20m p.a.	Member State administrations for border management, migration and law enforcement authorities.
2. Reduced cost of changes to national applications when the central system is operational	€6m p.a.	Member State IT departments
3. Cost saving of having one central shared BMS rather than one BMS per central system containing biometrics	€1,5m p.a. and reduction of €8m in one-off investment	EU central administration
4. Saved cost of identification of multiple identities.	€50m p.a.	Member State administrations for border management, migration and law enforcement authorities.
<b><i>Indirect benefits</i></b>		
None identified	-	-
<b><i>Total</i></b>	<b><i>€77,5m p.a. and €8m one-off</i></b>	

The benefits numbered 1 to 3 are the same in option 3 as in option 2 (see section 4.2.1).

All benefits are reduced implementation costs and are based on very cautious estimates.

1. Reduced training costs — same as for option 2.
2. Reduced cost of changes to national applications when the central system is modified — same as for option 2.
3. Cost saving of having one central shared - same as for option 2.
4. Saved cost of identification of multiple identities — the MID and CIR (based on a shared BMS) will enable a systematic identification of multiple identities. The

estimate is that at least 500,000 third-country nationals use multiple identities for various reasons. To detect and handle each case of multiple identities with current means, an estimated 4 hours of work would be required valued at €25 per hour. The estimated value of the automated system therefore amounts to at least €50m per year for the EU. The benefit can only be achieved when MID, CIR and the shared BMS are implemented.

The most important benefit — the avoidance of consequences of identity fraud — is not monetized in the calculation above.

#### *Calculation assumptions*

The calculation assumptions for benefits numbered 1 to 3 are the same as for option 2. The assumption on the number of third-country nationals using multiple identities is the same as used for sizing the fingerprint verification unit. The number of hours per case is an assumption based on feedback from operational services. The average cost per hour is a value used for the same purpose in the impact assessment for the Entry/Exit System.

#### *4.1.6. Cost-benefit for option 3*

The proposed solution entails an annual cost increase of €28.5m and a benefit of €77.5m. The annual net benefit amounts to over €49m.

The net additional marginal investment of €161.8 million (€169.8 minus €8 million one-off benefit) is thus recovered after little more than three years after the full implementation, which is about six years after the project start. As there is still a lot of approximation about the figures mentioned (both on benefits and on costs), the main conclusion is that even by only taking the monetised benefits, the measures provide a positive cost-benefit ratio, and costs are recovered after a few years.

## 5. ANNEX 5 – SUPPORTING STUDIES

### 5.1. European search portal

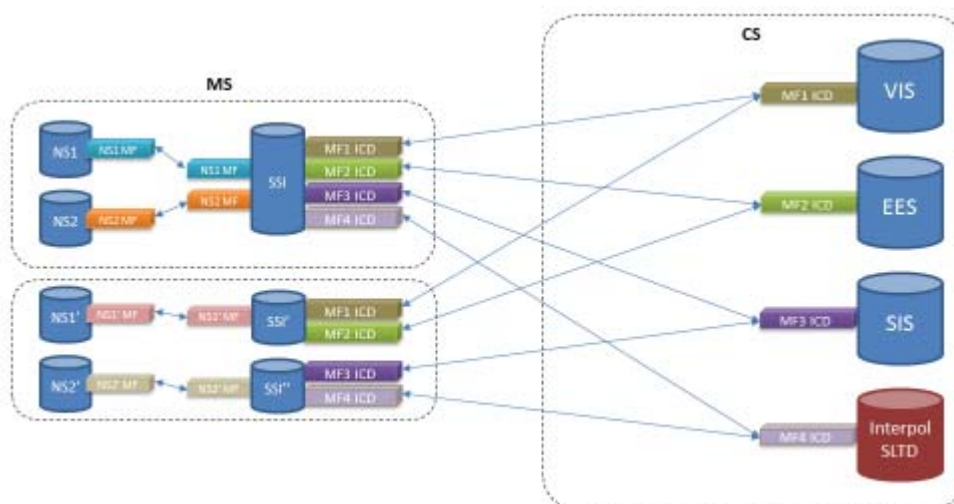
#### Executive summary of the technical study on the European search portal<sup>6</sup>

##### Introduction

The successful introduction of the Schengen Information System (SIS) and Visa Information System (VIS) as Central Systems (CS) has allowed collaboration between Member States (MS) at scale in the domain of Justice and Home Affairs. This success has driven demand for ever-further collaboration with the foreseen implementation of the European Travel Information and Authorisation System (ETIAS) and the Entry/Exit System (EES).

However, the growing number of CS with individual protocols, message formats and interfaces has given rise to a requirement for better interoperability at the central level and a reduction of the burden on the MS from the requirement to interoperate with these systems. The current scenario is depicted in Fig. 1 which shows that, although many National Systems (NS) have aggregated connections to the CS via national Single Search Interfaces (SSI), each new CS still requires implementation of corresponding interfaces (depicted as “MF<sub>x</sub>” ICD in Fig. 1 at the national (SSI) level.

This issue has been the subject of investigation by the High-level Expert Group on Information Systems and Interoperability, established by the European Commission (EC) in May 2016. The group recommended that the EC and the European Agency for the Operational Management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) should work towards the creation of a European Search Portal (ESP) in the areas of borders, security and asylum.



**Fig. 1 - ESP problem representation**

The purpose of the ESP would be to provide the capability to have a single entry point for searches against Central Systems<sup>7</sup> (CS) by MS National Systems (NS). A schematic representation of the ESP is presented in Fig. 2. The ESP would translate messages between the various messaging formats and combine the answers from

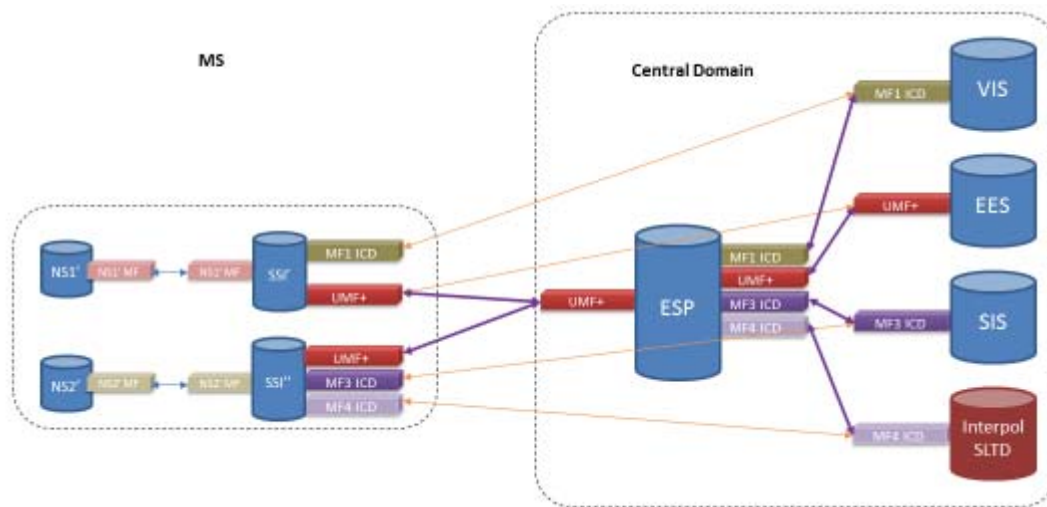
<sup>6</sup> Feasibility Study on the European Search Portal: ESP Feasibility Study Report – September 2017.

<sup>7</sup> Hereafter we use CS to refer to all centralised systems of eu-LISA, Europol and Interpol.

multiple systems into a single response to the NS. It would not provide its own search engine capability.

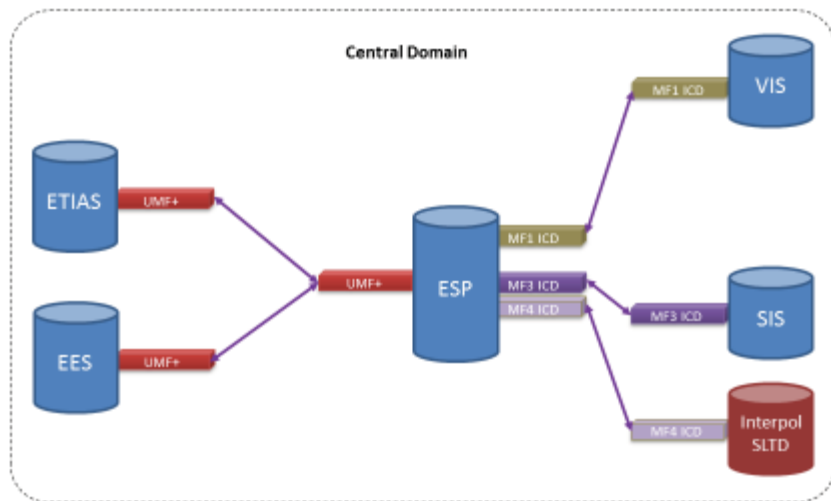
The Create, Update and Delete transactions (depicted by the orange lines) would continue to be direct between the NS and the CS as there is no intention to have the ESP handle these system specific transactions. Similarly, existing single purpose queries from NS to either the CS or, in the case of SIS, National Copies would continue to function as today (without going through the ESP).

For new use-cases requiring combined queries against the CS, the ESP would provide a service allowing multiple CS to be searched with a single query (depicted by the purple lines in Fig. 2 and would combine the answers into an aggregated response to the original request. The NS would only be able to query, via the ESP, those CS for which the End-User in question has an approved access.



**Fig. 2 - ESP implementation from MS Perspective**

The ESP is envisaged as an additive capability, meeting the needs for new capabilities or improving the efficiency of existing uses of the CS. For the introduction of new systems such as ETIAS, the ESP could provide a mechanism for these CS to query existing CS (represented in Fig. 3) without the need to implement multiple interfaces on the new systems or multiple CS-CS interconnections with all the security constraints that that entails. This not only gives fewer combinations of interconnections but also allows for a single point of control from a security perspective. This report presents the findings of the examination into how the ESP might be implemented.



**Fig. 3 - ESP implementation from a CS perspective**

### *As-Is Analysis*

The starting point of the study was desk research into the relevant specifications for the existing systems (referred to as the As-Is Analysis) that would influence the implementation of the ESP. This analysis was mainly focused on SIS and VIS. The key points that emerged from the desk research carried out into the As-Is situation for the CS were:

- Access Control mechanisms used for SIS and VIS:  
SIS and VIS have complex Access Control mechanisms that, while they differ, are based on the same elements (User & End-User Role 'declared' in the transaction). The Access Control mechanisms in both provide a fine grained control over access to the data in line with the legal basis for such access. The ESP can build on this to ensure that searches are compliant with the declared End-User Roles.
- Network constraints due to legal basis rather than technical issues:  
From a technical perspective, there is little to distinguish between the SIS and VIS networks. Both networks are capable of carrying the same traffic with similar security elements (encryption, etc.). However, the legal basis for SIS and VIS prohibit data from being carried over any network other than that specific for each. The legal basis for the implementation of the ESP would need to clarify over which networks it would be acceptable to carry aggregated content (queries and responses) from SIS, VIS, and other CS.
- Biometric Fingerprint (NIST) Files:  
While the NIST file formats used in the CS all vary, there is enough commonality to be able to transform files in one system's format to that of another with certain constraints. Manipulation of the image itself (e.g. down-scaling or sub-sampling) is out of scope of this study but it is possible to map the fields use in one format to those of another such that the file can be used to search multiple systems. This would allow a NIST file compatible with the VIS format to also be used to search SIS<sup>8</sup> and Interpol, for example.

<sup>8</sup> It is also possible to search Eurodac but a fuller examination of Eurodac connectivity to the ESP was not undertaken due to the late inclusion of biometric searches in the study. The Shared Biometric Matching

- Search mechanisms are different in SIS and VIS (and invariably in Europol Information System (EIS) and Interpol Databases):

The search algorithms used in the CS are different and can produce different results for the same input in the case of partial or fuzzy searches. The purpose of the ESP is not to change in any way the search functions of the CS but we present herein an analysis of the search differences between VIS and SIS so as to better understand the effect of different common inputs on the results obtained. As the ESP usage will be use-case driven, defining the valid search modes will need to be part of the ESP governance.

### *Requirement/Use-cases*

The ESP will provide a System-to-System (S2S) interface for NS and other CS (e.g. ETIAS) to connect to in order to query the CS. A User-to-System (U2S) interface that would enable End-Users to query the CS via a Graphical User Interface (GUI) is also considered in the form of a Web Portal.

For the current study, we restrict the queries to standard searches (as opposed to extended searches) that are sent simultaneously (synchronously) to those systems it is required to search. Four specific Use-cases are examined as a means for analysing the various aspects of the ESP:

1. Visa Application Examination;
2. Immigration Hotspot;
3. Europol Access for Basic Protection Level (BPL) queries;
4. ETIAS querying other CS.

These Use-cases are indicative only and do not constitute an exhaustive list of possible uses of the ESP.

### *Architecture*

Having identified typical Use-cases, the key requirements the ESP would need to meet are identified. Given the sensitivities relating to the data being accessed, we specify separately the Data Protection requirements that are the key guiding principles of the Privacy by Design approach used.

Based on these requirements, a number of options at various levels are analysed. These include the overall system architecture, the XML schema, the interface specifications, the NIST file formats and Access Control elements. The key conclusions of this analysis are a proposed architecture based on:

- A central Enterprise Service Bus architecture for the ESP;
- A distributed Web Portal implementation where each MS or organisation (e.g. European Border and Coast Guard Agency (EBCG), European Asylum Support Office (EASO)) can manage their own portal and End-Users;
- A centralised Web Portal is also retained as a potential solution but the End-User management in this case becomes more complex;
- Using an XML schema that builds on UMF9 to form a new standard which includes the border control data elements, tentatively referred to in this document as UMF+, for messaging between the NS and the ESP;

---

System is expected to investigate this subject in greater detail. It is to be noted that biometric searches of SIS are not yet operational.

<sup>9</sup> UMF is a specification for the exchange of information of interest to Law Enforcement organizations.

- Introducing a new interface towards NS to interoperate with the ESP based on UMF+;
- Re-using the existing Users in SIS and VIS but introducing new End-User Roles for each Use-case of the ESP for Access Control to ensure strict compliance with the allowed uses of the data (data minimisation principle).

With this proposed architecture, the impact on the existing CS is minimised while the potential for adding value is maximised (i.e. implementation of new business logic based on existing message patterns/content). Specifically, nothing is lost of the fine-grained Access Control offered by the CS. On the contrary, the proposed introduction of new End-User Roles will ensure that only the specific data required and authorised can be accessed via the ESP. In addition, the ESP would have the capability of completely filtering out the data sent in reply by the CS and replacing it with a simple Hit/No-Hit response. A Silent Alarm capability, where a search does not get an answer but in case of a hit sends an Alarm to the data owner or responsible agent is also included.

The ability to exclude certain CS from queries in specific Use-cases is foreseen. For instance, while it may be desirable to query the Interpol Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated with Notices (TDAWN) in some instances, such as Immigration Hot-spots, in others, such as Visa Application, it may not as Interpol have a legal obligation to notify data owners when returning detailed responses to a hit in their systems<sup>10</sup>.

#### *Practical Implementations*

In light of this analysis, the Use-cases presented are revisited to show how, in detail, the proposed solution could be used. Again we do not focus on the network aspects but look specifically at the Access Control, Message Format and Orchestration, NIST Transformations and Search Parameters. In each case we identify how the Access Control could be implemented to restrict access to the data for which there is a legal basis by implementing new End-User Roles (SIS and VIS). Examples are given of how the message header would be constructed for the messages from NS → ESP and from ESP → CS. The possibility for transformation of the NIST files and the search parameters for the searches are also examined.

#### *Implementation Considerations*

In terms of implementation, the impact on the CS is mainly in the creation of new End-User Roles and the data centre changes associated with implementing and interconnecting the ESP with the CS. The ESP can re-use the existing functionality of the CS without adaptation, including existing ICDs.

Where new Users (e.g. EASO or the European Border and Coast Guard Agency (Frontex)) would be added to the CS in order to use the ESP, this would of course necessitate the addition of new CS components (e.g. Central National Interfaces (CNI)).

For the implementation of new CS, such as ETIAS, which need to query other CS, the ESP can facilitate this by providing the single interface towards those other CS. This would avoid the need to create multiple CS-CS interconnections and implementation

---

<sup>10</sup> It is possible to search Interpol without such notifications being generated but in this case only a hit/no-hit response is received.



of new interfaces in existing CS and imposing un-necessarily complex Interface Control Documents (ICDs) on new systems.

### *Conclusion*

In conclusion, the study confirms that, from a technical perspective, the implementation of an ESP in the proposed manner is feasible. Evolving UMF (Universal Message Format) to a new UMF+ standard and using this as a basis for the ESP would serve to reduce the effort to implement new CS such as ETIAS and EES as they could then adopt the UMF+ standard from the beginning to query other CS (e.g. SIS and VIS). Application of Privacy by Design principle allows the elaboration of an ESP that avoids exposing data where there is no legal basis or no provision of access rights.

In selecting an Enterprise Service Bus architecture, the impacts on the CS are minimised. Such an architecture provides a very powerful new capability to implement new business logic without imposing new requirements on single purpose end systems where performance or scalability could otherwise be impacted.

## **5.2. Shared biometric matching service**

Summary to be available mid-December.

## **5.3. Common identity repository**

Executive summary to be available mid-December.

## **6. ANNEX 6 - INVENTORY OF EXISTING INFORMATION SYSTEMS FOR BORDER MANAGEMENT AND LAW ENFORCEMENT**

### Schengen Information System (SIS)

SIS is the largest and most widely used information exchange platform on immigration and law enforcement. It is a centralised system used by 25 EU Member States<sup>11</sup> and four Schengen associated countries<sup>12</sup>, currently containing 63 million alerts. These are entered and consulted by competent authorities, such as police, border control and immigration. It contains records on third-country nationals prohibited to enter or stay in the Schengen area as well as on EU and third-country nationals who are wanted or missing (including children) and on wanted objects (firearms, vehicles, identity documents, industrial equipment, etc.). The distinctive feature of SIS in comparison with other information sharing instruments is that its information is complemented by an instruction for concrete action to be taken by officers on the ground, such as arrest or seizure.

SIS checks are mandatory for the processing of short-stay visas, for border checks for third-country nationals and, on a non-systematic basis<sup>13</sup>, for EU citizens and other persons enjoying the right of free movement. Moreover, each police check on the territory should include an automatic check in SIS.

### Visa Information System (VIS)

The VIS is a centralised system for the exchange of data on short-stay visas between Member States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen area. All the consulates of the Schengen states (around 2,000) and all their external border crossing points (in total some 1,800) have been connected to the system.

The VIS contains data on visa applications and decisions, as well as whether issued visas are revoked, annulled, or extended. It currently contains data on 50 million visa applications and, at peak times, it handles over 135,000 transactions per hour. Each visa applicant provides detailed biographical information, a digital photograph and ten fingerprints. As such, it is a reliable means to verify the identity of visa applicants, to assess possible cases of irregular migration and security risks, and to prevent 'visa shopping'.

At border crossing points or within the territory of the Member States, the VIS is used to verify the identity of visa holders by comparing his/her fingerprints with the fingerprints stored in the VIS. This process guarantees that the person that applied for the visa is the same person as the one crossing the border. A fingerprint search in the VIS also enables the identification of a person who applied for a visa in the last five years and who may not carry identity documents.

---

<sup>11</sup> All, except Ireland, Cyprus, Croatia.

<sup>12</sup> Switzerland, Liechtenstein, Norway, Iceland.

<sup>13</sup> This rule is subject to change as envisaged by Commission proposal COM/2015/0670 on the amendment of the Schengen Borders Code.

## Eurodac

Eurodac (European Dactyloscopy) was established to facilitate the application of the Dublin Regulation. It is a fingerprint database enabling Member States to compare the fingerprints of asylum applicants in order to see whether they have previously applied for asylum or entered the EU irregularly via another Member State. It is available at border crossing points, but unlike SIS and VIS it is not a border management system.

Fingerprints of irregular migrants entering the EU unlawfully are taken at border crossing points. These are stored in Eurodac to verify the identity of the person in case of a future asylum application. Immigration and police authorities can also compare fingerprint data from illegally staying migrants found in Member States to check if they have applied for asylum in another Member State. Law enforcement authorities and Europol are also entitled to search Eurodac to prevent, detect or investigate a serious crime or terrorist offence.

Fingerprint registration of asylum seekers or irregular migrants in a centralised system enables the identification and monitoring of their secondary movements<sup>14</sup> within the EU. The extension of the scope of Eurodac to include the possibility for Member States to search and store data belonging to third-country nationals or stateless persons who are not applicants for international protection will assist the competent authorities in their task of identifying those persons for return purposes.

## Entry/Exit System

The Commission proposed in April 2016 to create a new IT system to modernise and strengthen the EU's external borders. This new Entry/Exit system (EES) will replace the current system of manual stamping of passports and will electronically register the name, type of travel document, biometrics and the date and place of entry and exit. It will also record refusals of entry.

EES will apply to all non-EU citizens who are admitted for a short stay in the Schengen area (maximum 90 days in any 180-day period). EES will enable the effective management of authorised short-stays, increased automation at border controls, and improved detection of document and identity fraud. This will facilitate the border crossing of *bona fide* travellers, detect overstayers and identify undocumented persons in the Schengen area.

The Commission expects the development of the Entry/Exit System to start in 2018, in view of having the system operational as of early 2020.

## European Travel Information and Authorisation System

The Commission proposed in November 2016 to establish an additional centralised information system, the European Travel Information and Authorisation System (ETIAS).

---

<sup>14</sup> For example, refugees arriving in Greece with no intention of making an asylum application in Greece but travelling further by land to other Member States.

The proposed ETIAS will be a largely automated system that will gather information on all visa-free travellers that intend to travel to the Schengen area. The proposed ETIAS will verify the information submitted via an online application ahead of their travel to the EU's external borders, to assess if they pose a risk for irregular migration, security or public health.

Applications will be automatically processed against other EU information systems (such as SIS, VIS, Europol's data, Interpol's databases, the future EES, Eurodac, ECRIS), a dedicated ETIAS watch list (established by Europol) and targeted, proportionate and clearly defined screening rules to determine if there are factual indications or reasonable grounds to issue or refuse a travel authorisation. In cases where no hits or elements requiring further analysis are identified, travel authorisations will be issued automatically within minutes after the application has been submitted.

The Commission expects the development of ETIAS to start not long after the Entry/Exit System, in view of also having this new system in place in 2020.

#### European Criminal Records Information System (ECRIS)

ECRIS is an electronic system for exchanging information on previous convictions handed down against a specific person by criminal courts in the EU for the purposes of criminal proceedings against a person and, if so permitted by national law, for other purposes. Convicting Member States must notify convictions handed down against a national of another Member State to the Member State of nationality. The Member State of nationality must store this information and can thus provide up-to-date information on the criminal records of its nationals upon request, regardless of where in the EU convictions were handed down.

ECRIS allows, too, the exchange of information on convictions of third-country nationals and stateless persons. Designated central authorities in every Member State are the contact points in the ECRIS network, dealing with all tasks such as notifying, storing, requesting and providing criminal record information.

Since this system only supports bilateral exchanges between the Member States, and has no centralised data storage, it is not further considered for interoperability in this impact assessment, which only focuses on the new (centralised) ECRIS-TCN system, as proposed by the Commission on 29 June 2017.

#### Europol data

Europol data are held on centralised criminal information databases for investigative and analytical purposes. It can be used by Member States and Europol to store, query and analyse data on serious crime and terrorism. The information stored concerns data on persons, identity documents, cars, firearms, telephone numbers, emails, fingerprints, DNA and cybercrime-related information, which can be linked to each other in different ways to create a more detailed and structured picture of a crime case. The Europol data supports law enforcement cooperation and is not available for border control authorities.

Information exchange is channelled using the SIENA<sup>15</sup> platform, which is a secure electronic communication network between Europol, the liaison offices, the Europol

---

<sup>15</sup> Secure Information Exchange Network Application.

national units, designated competent authorities (such as customs, asset recovery offices, etc.) and connected third parties.

In May 2017, a new legal framework for Europol entered into application. This framework will enable an enhanced operational ability for Europol to conduct analysis, and to better identify links between available information.

### Stolen and Lost Travel Documents (SLTD)

Interpol's Stolen and Lost Travel Documents (SLTD) database is a central database on passports and other travel documents that have been reported stolen or lost by the issuing authorities to Interpol. It includes information about stolen blank passports. Travel documents reported lost or stolen to the authorities of countries participating in SIS are entered both in SLTD and SIS. The SLTD also holds data on travel documents entered by countries not participating in SIS (Ireland, Croatia, Cyprus and third countries).

As stated in the Council Conclusions of 9 and 20 November 2015, and the Commission's proposal of 15 December 2015 for a regulation on a targeted modification of the Schengen Borders Code,<sup>16</sup> the travel documents of all third-country nationals and persons enjoying the right of free movement should be verified against SLTD. All border control posts have to be connected to SLTD. On top of this, in-country law enforcement searches in SLTD would generate additional security benefits.

---

<sup>16</sup> COM(2015) 670 final Proposal for a Regulation of the European Parliament and of the Council amending Regulation No 562/2006 (EC) as regards the reinforcement of checks against relevant databases at external borders.

## 7. ANNEX 7 - MATRIX ON ACCESS TO CENTRAL EU SYSTEMS FOR BORDERS AND SECURITY

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
<b>Identity data recorded in system</b>	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>
	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport/ID card details</li> <li>- Fingerprints</li> <li>- Palm prints*</li> <li>- Photographs</li> <li>- Facial images*</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> <li>- Visa status</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data*</li> <li>- Passport/ID card details** (where available)</li> <li>- Fingerprints (10)</li> <li>- Facial images*</li> </ul>	<ul style="list-style-type: none"> <li>- Entry data</li> <li>- Exit data</li> <li>- Refusal of entry data</li> <li>- Remaining authorised stay</li> <li>- List if persons overstaying</li> <li>- Statistics on persons overstaying</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Travel authorisation status</li> <li>- IP address</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>
<b>Additional categories of information held by system</b>						
	<ul style="list-style-type: none"> <li>- Refusal of Entry and stay</li> <li>- European Arrest warrant</li> <li>- Missing persons/ children at risk of parental abduction</li> <li>- Requested to assist in judicial criminal procedure</li> <li>- Persons and objects for discreet/inquiry*/ specific check lost/stolen/sought as evidence</li> <li>- Unknown wanted persons*</li> <li>- Return decisions*</li> </ul>	<ul style="list-style-type: none"> <li>- Issued, refused, discontinued, extended, revoked or annulled single/double/multiple entry visa</li> <li>- Authority where visa application was lodged;</li> <li>- Background information: MS(s) of destination, purpose of travel, intended date of arrival and intended stay, applicant's home address, occupation and employer etc.</li> <li>- (In the case of families or groups): links between applications;</li> <li>- History of applications of person.</li> </ul>	<ul style="list-style-type: none"> <li>- Information concerning third-country nationals or stateless persons above 6 years old:</li> <li>- applicants for international protection</li> <li>- persons apprehended in connection with the irregular crossing of an external border</li> <li>- persons found illegally staying in a Member State</li> </ul>	<ul style="list-style-type: none"> <li>- Issued, refused, revoked and annulled travel authorisations</li> <li>- Declarative information provided in application</li> <li>- Additional information provided at request</li> <li>- Results of the processing of the travel authorisation request, notably hits against other EU systems, the ETIAS watch list and Interpol system).</li> </ul>	<ul style="list-style-type: none"> <li>- Issued, refused, revoked and annulled travel authorisations</li> <li>- Declarative information provided in application</li> <li>- Additional information provided at request</li> <li>- Results of the processing of the travel authorisation request, notably hits against other EU systems, the ETIAS watch list and Interpol system).</li> </ul>	<ul style="list-style-type: none"> <li>- Convicting Member State (including a reference number and the code of the convicting MS)</li> </ul>

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
<b>Possible actions by users of system</b>	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>
	<ul style="list-style-type: none"> <li>- Search alphanumeric data (biographic and/or passport/ID)</li> <li>- Search fingerprints</li> <li>- Search palm prints<sup>*17</sup></li> <li>- Search facial images*</li> <li>- Create/Update/Delete</li> </ul>	<ul style="list-style-type: none"> <li>- Search alphanumeric data (biographic and/or passport)</li> <li>- Verify/Search fingerprints</li> <li>- Link records</li> <li>- Create/Update/Delete applications</li> </ul>	<ul style="list-style-type: none"> <li>- Search alphanumeric data (for law enforcement authorities)<sup>**18</sup></li> <li>- Search fingerprints</li> <li>- Search facial image*</li> <li>- Take/Transmit/Update/Delete</li> </ul>	<ul style="list-style-type: none"> <li>- Search alphanumeric data (biographic and/or passport)</li> <li>- Verify/ Search fingerprints</li> <li>- Verify/ Search facial-images</li> <li>- Link records</li> <li>- Create/Update/Delete</li> </ul>	<ul style="list-style-type: none"> <li>- Search alphanumeric data (biographic and/or passport)</li> <li>- Process travel authorisation application</li> <li>- Create/Update/Delete</li> </ul>	<ul style="list-style-type: none"> <li>- Search alphanumeric data</li> <li>- Verify/ Search fingerprints</li> <li>- Create/update/delete</li> </ul>
<i>Purpose of access</i>	<i>Access to categories of information: all</i>	<i>Access to categories of information: all</i>	<i>Access to categories of information: all</i>	<i>Access to categories of information: all</i>	<i>Access to categories of information: - Travel authorisation status (ok/not ok)</i>	<b>No access</b>
<b>Border control</b> <sup>19</sup>	<i>Possible actions: all</i>	<i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints	<i>Possible actions:</i> - Search fingerprints - Search facial image - Take/Transmit biometric data	<i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints - Verify facial images - Create/Update/Delete	<i>Possible actions:</i> - Search alphanumeric data	(where appropriate, ECRIS-TCN can inform decisions on inclusion of alerts in the SIS).

\* COM proposals.

\*\* As proposed in Council Document 10079/17 (mandate for negotiations with the parliament).

<sup>19</sup> In the case of Eurodac the access for border control purposes refers to a situation of irregular crossing of the external border.

<p><b><u>Schengen Information System</u></b> both for EU and third-country nationals primary objective: both border management and law enforcement</p>	<p><b><u>Other systems</u></b> only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement</p>				<p><b><u>Other systems</u></b> only for third-country nationals primary objective: judicial cooperation</p>	
<p><i>Purpose of access</i> <b>Issuance of short-stay visa</b></p>	<p><b>SIS (new*)</b> <i>Access to categories of information:</i> - Refusal of entry and stay - Certain categories of lost/stolen objects (blank official, and issued identity documents), as provided for by national law  <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images</p>	<p><b>VIS</b> <i>Access to categories of information: all</i>  <i>Possible actions: all</i></p>	<p><b>EURODAC (new*)</b>  No access</p>	<p><b>EES</b> <i>Access to categories of information: all</i>  <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints and facial image (using EES/VIS interconnection)</p>	<p><b>ETIAS (proposal)</b>  No access</p>	<p><b>ECRIS-TCN (proposal)</b>  No direct access, but information may be requested through criminal records authorities where possible under national law</p>



<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>	
<p>both for EU and third-country nationals  primary objective: both border management and law enforcement</p>		<p>only for third-country nationals  primary objective: border / migration / asylum management  secondary (ancillary) objective: law enforcement</p>				<p>only for third-country nationals  primary objective: judicial cooperation</p>	
		<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	
<p><i>Purpose of access</i></p> <p><b>Issuance of ETIAS authorisation</b></p>		<p><i>Access to categories of information:</i></p> <ul style="list-style-type: none"> <li>- Refusals of entry and stay</li> <li>- Lost, stolen or invalidated travel documents</li> <li>- European Arrest Warrants</li> </ul> <p><i>For information also:</i></p> <ul style="list-style-type: none"> <li>- Missing persons/ children at risk of parental abduction</li> <li>- Requested to assist in judicial criminal procedure</li> <li>- Persons and objects for discreet/inquiry/ specific check</li> <li>- Objects which are lost/stolen/sought as evidence</li> <li>- Unknown wanted persons</li> <li>- Return decisions</li> </ul> <p><i>Possible actions:</i></p> <ul style="list-style-type: none"> <li>- Search alphanumeric data</li> </ul> <p>NB: access and actions are indirect, via ETIAS Central System</p>	<p><i>Access to categories of information:</i></p> <ul style="list-style-type: none"> <li>- Refusals, revocation and annulments of short stay visas</li> </ul> <p><i>Possible actions:</i></p> <ul style="list-style-type: none"> <li>- Search alphanumeric data</li> </ul> <p>NB: access and actions are indirect, via ETIAS Central System</p>	<p><i>Access to categories of information:</i></p> <ul style="list-style-type: none"> <li>- Return decisions or removal orders<sup>20</sup></li> </ul> <p><i>Possible actions:</i></p> <ul style="list-style-type: none"> <li>- Search alphanumeric data</li> </ul> <p>NB: access and actions are indirect, via ETIAS Central System</p>	<p><i>Access to categories of information:</i></p> <ul style="list-style-type: none"> <li>- Refusal of entry data</li> <li>- Persons overstay</li> </ul> <p><i>Possible actions:</i></p> <ul style="list-style-type: none"> <li>- Search alphanumeric data</li> </ul> <p>NB: access and actions are indirect, via ETIAS Central System</p>	<p><i>Access to categories of information:</i></p> <p><b>all</b></p> <p><i>Possible actions: all</i></p>	<p>Not foreseen under ECRIS-TCN proposal</p>

<sup>20</sup> According to the Eurodac proposal this information will not be recorded in that system.

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>
<i>Specific user</i> <b>EBCG Agency</b>	<i>Access to categories of information:</i> - Alerts for refusal of entry or stay  <i>Possible actions:</i> - Search some biographic data (for analytical purposes)	No access	No access	<i>Access to categories of information:</i> - Entry and exit data - Number of persons overstay <i>Possible actions:</i> - Search some biographic data (for the purpose of risk analyses and vulnerability assessments)	<i>EBCG hosts the ETIAS central unit (see box on "issuance of travel authorisation");</i>	No access
<i>Specific user</i> <b>EBCG teams<sup>21</sup></b>	<i>Access to categories of information:</i> <b>all</b>  <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	No access	<i>Access to categories of information: all</i>  <i>Possible actions:</i> - Search fingerprints - Search facial image - Take/Transmit biometric data (on behalf of requesting state)	No access	No access	No access
<i>Specific user</i> <b>Carriers</b>	No access	<i>Access to categories of information:</i> - Existence of valid visa (ok/not ok)  <i>Possible actions:</i> - Search alphanumeric data	No access	<i>Access to categories of information:</i> - Usage of single/double entry Schengen short stay visa (ok/not ok) (through website) <i>Possible actions:</i> - Search alphanumeric data	<i>Access to categories of information:</i> - Existence of valid travel authorisation (ok/not ok)  <i>Possible actions:</i> - Search alphanumeric data	No access

<sup>21</sup> Teams of EBCG staff involved in return-related tasks, and members of the migration management support teams.

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>
<i>Specific user</i>	No access	No access	No access	<i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search facial-images	No access	No access
National authorities examining applications for national travel facilitation programmes	No access	No access	No access	No access	No access	No access
<i>Purpose of access</i> <b>Police checks: Identification or verification of identity (in territory)</b>	<i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	No access	No access	No access	No access	No access

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
Purpose of access <b>Prevention, or detection or investigation of terrorist offences and other serious criminal offences</b>	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>
	Access to categories of information: <b>all</b> (but in context of counter-terrorism implementation is subject to national law (direct-indirect access))  Possible actions: <b>all</b>	Access to categories of information: <b>all</b>  Possible actions: - Search alphanumeric data - Search fingerprints (after ex-ante authorisation)	Access to categories of information: <b>all</b>  Possible actions: - Search alphanumeric data - Search fingerprints (after ex-ante authorisation and cascade via national databases, Prüm and VIS) <sup>22</sup>	Access to categories of information: <b>all</b>  Possible actions: For <b>identification</b> : Search alphanumeric data, fingerprints, facial image (after ex-ante authorisation & cascade via national databases and Prüm; specific procedure for emergencies and terrorist offences).  For <b>investigation</b> : Search alphanumeric data (no cascading)	Access to categories of information: <b>all</b> (but restrictions applicable for specific fields)  Possible actions: Search alphanumeric data (after ex-ante authorisation & cascade via national databases and Europol data)	No direct access, but information may be requested through criminal records authorities
Specific user <b>Europol</b>	Access to categories of information: <b>all</b>  Possible actions: <b>all</b> , except Create/Update/delete	As above <sup>23</sup>	As above (cascading via databases that are accessible to Europol)	As above (cascading (for identification) via databases that are accessible to Europol)	As above ((cascading via Europol data)	Access to categories of information: <b>all</b>  Possible actions: - Search alphanumeric data - Search fingerprints

<sup>22</sup> Council Document 10079/17 (mandate for negotiations with the parliament) proposes to delete VIS.

<sup>23</sup> However, not applied in practice to date.

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
<i>Purpose of access</i> <b>Judicial cooperation between Member States</b>	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>
	<i>Access to categories of information:</i> <b>all</b> , but implementation is subject to national law (direct-indirect access) <i>Possible actions:</i> <b>all</b> , but the implementation subject to national law (direct-indirect access)	No access	No access	<i>Access to categories of information:</i> <b>all</b> , but subject to national law <i>Possible actions:</i> <b>all</b> , but subject to national law	No access	<i>Access to categories of information:</i> <b>all</b> <i>Possible actions:</i> <b>all</b>
<i>Specific user</i> <b>Eurojust</b>	<i>Access to categories of information:</i> - European arrest warrant - Missing persons/ children at risk of parental abduction - Requested to assist in judicial criminal procedure - Lost/stolen objects - Unknown wanted persons <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints - Search facial images	No access	No access	No access	No access	<i>Access to categories of information:</i> <b>all</b> <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
Purpose of access <b>Migration management: verification of identity and verification of conditions for entry or stay (for TCNs, in territory)</b>	<b>SIS (new*)</b> <i>Access to categories of information: all</i> but implementation is subject to national law (direct-indirect access) <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	<b>VIS</b> <i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints	<b>EURODAC (new*)</b> <i>Access to categories of information: all</i> <i>Possible actions:</i> - Search fingerprints - Search facial images	<b>EES</b> <i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	<b>ETIAS (proposal)</b>  No access	<b>ECRIS-TCN (proposal)</b>  No direct access, but information may be requested through criminal records authorities where possible under national law
	<i>Access to categories of information: all</i> , but implementation is subject to national law (direct-indirect access) <i>Possible actions: all</i> as defined in national law	<i>Access to categories of information: all</i> <i>Possible actions: all</i>	<i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints - Update the file with the date of removal or date when person has left the country	<i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	<b>No access</b>	No direct access, but information may be requested through criminal records authorities where possible under national law
Purpose of access <b>Return of irregular third-country nationals</b>	<i>Access to categories of information: all</i> , but implementation is subject to national law (direct-indirect access) <i>Possible actions: all</i> as defined in national law	<i>Access to categories of information: all</i> <i>Possible actions: all</i>	<i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Search facial images - Update the file with the date of removal or date when person has left the country	<i>Access to categories of information: all</i> <i>Possible actions:</i> - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	<b>No access</b>	No direct access, but information may be requested through criminal records authorities where possible under national law

<u>Schengen Information System</u>		<u>Other systems</u>				<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				only for third-country nationals primary objective: judicial cooperation
Purpose of access <b>Assessment of request for asylum</b>	<b>SIS (new*)</b> <i>Access to categories of information:</i> all but implementation is subject to national law (direct-indirect access) <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	<b>VIS</b> <i>Access to categories of information:</i> all <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints	<b>EURODAC (new*)</b> <i>Access to categories of information:</i> all <i>Possible actions:</i> - Search fingerprints - Search facial images - Take/Transmit/Update/Delete	<b>EES</b> No access	<b>ETIAS (proposal)</b> No access	<b>ECRIS-TCN (proposal)</b> No direct access, but information may be requested through criminal records authorities where possible under national law
	<i>Specific user</i> <b>Member State asylum expert teams</b> <sup>24</sup>	No access	No access	<i>Access to categories of information:</i> all <i>Possible actions:</i> - Search fingerprints - Search facial image - Take/Transmit biometric data (on behalf of requesting state)	No access	No access

<sup>24</sup> Teams of Member State asylum experts deployed by EASO.

<u>Schengen Information System</u>		<u>Other systems</u>					<u>Other systems</u>
both for EU and third-country nationals primary objective: both border management and law enforcement		only for third-country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement					only for third-country nationals primary objective: judicial cooperation
	<b>SIS (new*)</b>	<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS-TCN (proposal)</b>	
<i>Purpose of access</i> <b>Issuance of residence permits / long-stay visas</b>	<i>Access to categories of information:</i> <b>all</b> but implementation is subject to national law (direct-indirect access) <i>Possible actions:</i> - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	No access	No access	No access	No access	No access	
<i>Purpose of access</i> <b>Customs checks</b>	<i>Access to categories of information:</i> <b>all</b> <i>Possible actions:</i> <b>all</b>	No access	No access	No access	No access	No access	



## 8. ANNEX 8 - SUPPLEMENTARY ANALYSIS & INFORMATION

This annex contains a more detailed analysis and additional information on the various components and the sub-options.

### 8.1. Detailed analysis of the ESP's sub-options

By providing a centralised state-of-the-art search portal or message broker<sup>25</sup>, the EU could support Member States and facilitate a systematic and efficient use of all relevant systems, and the information they contain, by all authorised users.

As regards the objective of ensuring fast, seamless, systematic and controlled access to relevant information systems, the retained policy option is to consider the establishment of a European search portal (ESP) and look at various sub-options for this ESP.

#### ESP

- With/without SIS data
- With/without Interpol & Europol data
- With/without the proposed ECRIS-TCN data
- With/without biometric search

The centralised European search portal (ESP) is a new information technology component enabling the simultaneous search of multiple systems (in particular, SIS, the new Eurodac, VIS, the future EES and the proposed ETIAS, and possibly the Europol data and Interpol systems, and also the proposed ECRIS-TCN system), using identity data (both biographical and biometric).

The ESP would forward a search transaction with identity data to various central systems, using existing user credentials, logins and roles that Member States currently use for those systems. The individual results from those systems searched would be combined by the ESP into one single answer.

The search portal facility would enable a faster, seamless and more systematic use of existing EU-level information systems. A query via the European search portal would immediately return information from the various systems to which the end-user has access. Depending on the purpose of the search, and the corresponding existing access rights, the ESP will be provided with specific configurations.

The ESP is not a 'system': it does not handle any new data, and it does not store any data; it only acts as a single window or 'message broker' to search various central systems and

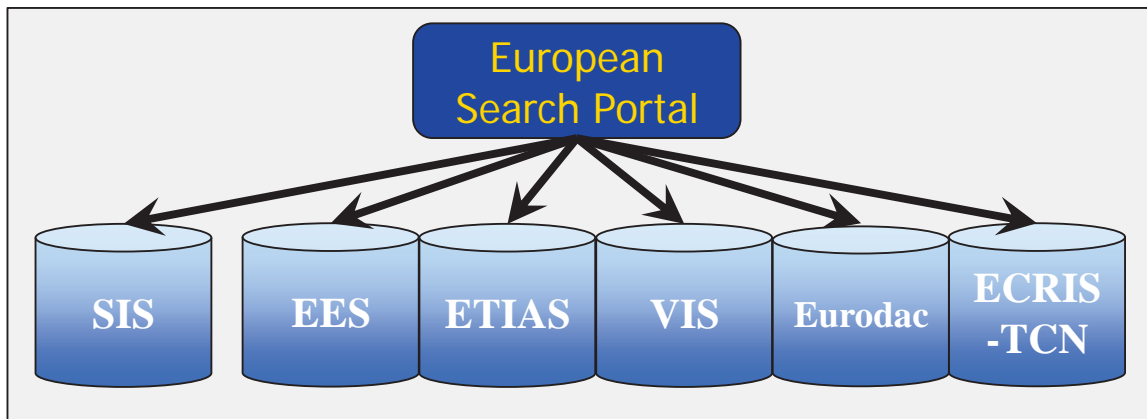
---

<sup>25</sup> In computer programming, a message broker is an intermediary programme module that translates a message from the formal messaging protocol of the sender to the formal messaging protocol of the receiver.

retrieve the necessary information seamlessly, and does so in full respect of the access-control and data protection requirements.

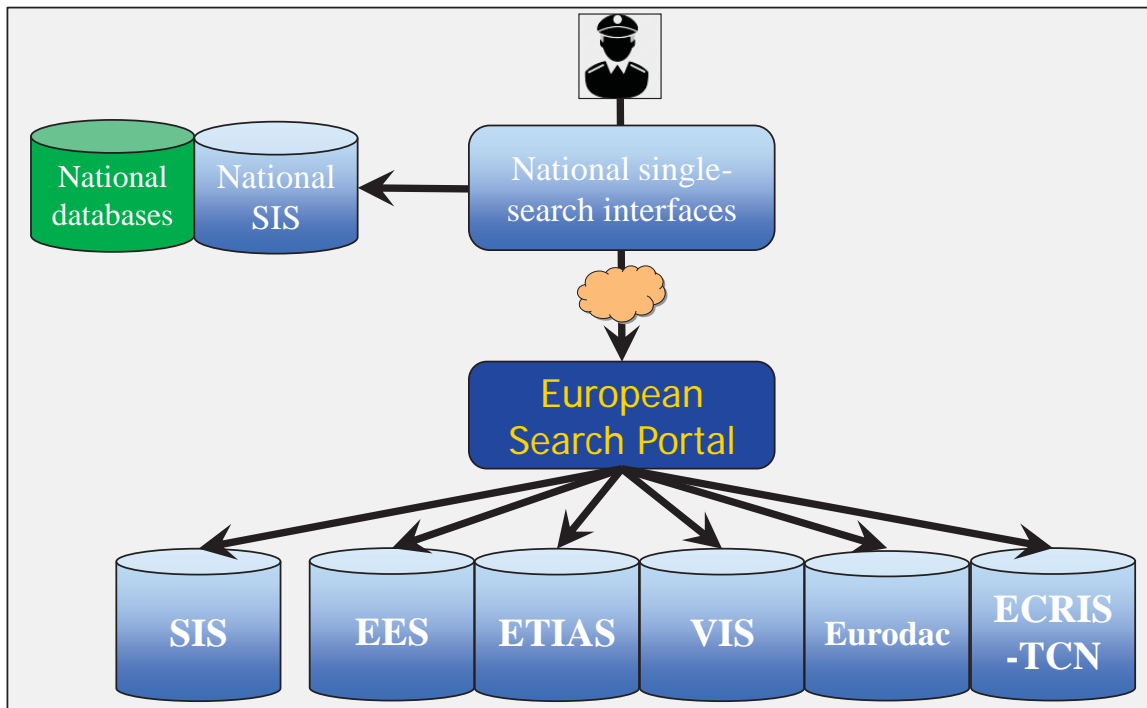
Establishing the ESP was one of the options identified in the April 2016 Communication to achieve interoperability (under the label 'single-search interface'), confirmed by the high-level expert group as regards its necessity and technical feasibility and that it should comply with data protection requirements, and endorsed by the Commission in the *Seventh progress report towards an effective and genuine Security Union*.

**Figure 1 - European search portal**



The ESP is inspired by and comparable with the various national single-search interfaces that Member States have developed for their national systems but it will be located and operated on a central level by eu-LISA. It is envisaged that, where available, these national single-search interfaces will continue to be used as the first-line device for end-users for the consultation of both national databases and to connect to the ESP.

**Figure 2 - ESP and national interfaces**



As the ESP simply forwards the search transaction (following Universal Message Format (UMF) concepts) to the various central systems, it fully relies on the search engines, on the logging functionality and on the access control limitations of those systems.

The ESP not only facilitates end-user queries to data but also creates a standardised, interoperable and controllable component to allow central systems to search other central systems, such as EES searching VIS, and the proposed ETIAS searching various other systems, which is essential for these systems to fulfil their very purpose.

The ESP would be hosted within the secure central sites of eu-LISA behind the connectivity and firewall protection infrastructure, as an additional component right in front of the central systems. This component thus benefits from the same data security safeguards, controls and monitoring as all central systems do.

As explained in the ESP technical feasibility study (see Annex 5), a specific data security and access control mechanism will be implemented to manage the various access rights of different types of end-user from different services and countries. The central systems to be searched by the ESP will be determined by the purpose of access and will be systematic. The ESP will implement and enforce the access control described in Table 2 below.

The residual risks related to a data breach or data leakage are much lower with a single ESP connected to the secure Trans-European Services for Telematics between Administrations (TESTA) networks than when currently employing 28 different national single-search interfaces.

The ESP is a technical component providing fast, seamless and systematic access to data. The access rights to this data are governed in the respective legal instruments (see Table 1 below). They will not be changed through this interoperability initiative. The ESP will be configured in such a way that the user will receive information from systems to which legal access already exists. The configuration of the ESP will therefore be different for different groups of end-users, in line with the purpose of the access.

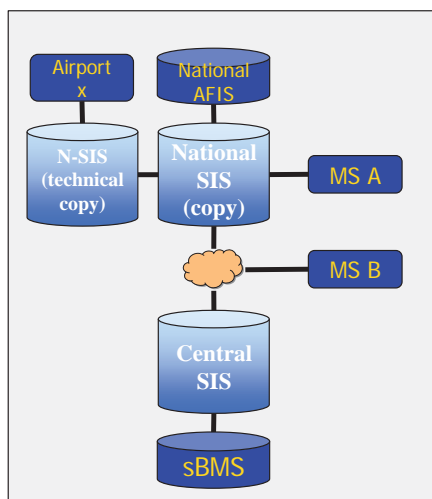
The ESP will, as a minimum, be capable of searching Eurodac, VIS, EES and the proposed ETIAS. In addition, the following other possibilities are being considered.

#### *8.1.1. ESP with or without SIS data*

SIS is a very important system for detecting persons under alert, to be used by police officers but also by many other users for other purposes, as can be seen in Table 1.

The SIS architecture is based on a flexible approach with a centralised system at eu-LISA and **national copies** in the Member States. These national copies can be complete (including all data) or partial/technical (for instance not including biometric data). The centralised system will use the shared BMS while certain Member States will opt for a national AFIS (automated fingerprint identification system) that will not have the EES, VIS or Eurodac biometric data.

**Figure 3 - The SIS technical architecture**



Depending on the operational situation and which data is used, end-users may want (or need) to use the national SIS copy or the central system. This will lead to situations where the end-user does not use the ESP to search the central SIS system but uses a national single-search interface to search the national SIS copy.

However, specifically for non-police users primarily using central systems like EES, VIS and Eurodac, the ESP could facilitate consulting the **central SIS** and make those searches systematic.

Since the proposed ETIAS will also need to consult SIS data, it would also benefit from an ESP as the ETIAS central team at the European Border and Coast Guard Agency will need to cross-check ETIAS data against the central SIS.

For these reasons, it is considered that the ESP should include the possibility of searching SIS data as contained in the central SIS.

#### *8.1.2. Access Interpol and Europol data: extend the ESP*

The law enforcement databases at Interpol, notably for Stolen and Lost Travel Documents (SLTD), provide valuable information primarily concerning third-country nationals. This complements information held in the SIS.

The European search portal could a central functionality for searching not only European systems (SIS, Eurodac, VIS, EES, the proposed ETIAS, Europol data, the proposed ECRIS-TCN system) but also the Interpol systems (Stolen and Lost Travel Documents, Travel Documents Associated with Notices, and Alert Notices).

Searching Interpol's SLTD is a Schengen Borders Code requirement and Member States have implemented this search in national single-search interfaces for border control purposes. The proposed ETIAS will also need to search the SLTD (and TDawn) and by analogy the visa application process should in due course include a search to the SLTD.

The Interpol systems are configured with 'hit notifications' to data owners when accessing certain data. This could constitute certain risks in terms of fundamental rights, notably where data owners create alerts in order to limit the movement of certain persons or want to be informed about the whereabouts of certain persons.

Detailed technical discussions with Interpol have led to an alternative workaround that the ESP would implement to be able to search the Interpol databases.

The FIND interface (Fixed Interpol Network Database) provides a system-to-system interface to allow an ESP to search the Interpol systems. The FIND interface provides two different levels of detail to the data. For the first hit/no-hit level, the interface provides the end-user with basic information on the hit (for instance, for the SLTD, the travel document number and the country of issuance). When using this first level, silent hits are not generated to the data owner.

For the second level, additional details on the hit can be obtained (for instance, for the SLTD, detailed reference on country of issue, place and date where the document was lost or stolen, type of fraud, date of recording in the SLTD and the expiry date of the document).

When retrieving these additional details, silent hits will indeed be generated to the data owner.

### **Example**

Third-country XYZ created an alert on a stolen document: XYZ 123456 expiry date 01/06/2022 stolen in SomeCity on 15/09/2016.

The ESP implements the first-level search towards the SLTD. At border control, the passport "XYZ 123456" is used to search various systems. The SLTD will generate the following hit response: passport; XYZ; 123456. No notification will be generated to the authorities of country XYZ.

If the ESP implements the first and second-level search towards the SLTD and the same passport is used, the same hit will be generated but additional information will be downloaded from the SLTD: electronic passport from XYZ; issued on 01/06/2012; expires on 01/06/2022; stolen in SomeCity on 15/09/2016. The authorities of country XYZ will be notified that this search and hit took place, including which authority performed the search and where.

The ESP could implement the exact same behaviour to support searches towards the SLTD for visa issuance and asylum applications. This would require a legal change in the respective legal instruments.

While the European Union is currently not a member of Interpol, the EU Member States are all members of Interpol. Any search towards the Interpol systems would be performed by an end-user in a Member State and the transaction would be logged in the Interpol systems as a national transaction. Preliminary discussions with Interpol indicated that a memorandum of understanding between eu-LISA and Interpol would be created to arrange the technical cooperation.

Where a search towards the Interpol systems would originate from ETIAS, a new user (likely to be 'EU-ETIAS') would need to be created on the Interpol systems. Since the EU would never create any new data in the Interpol systems, there would not be a need to establish an EU Interpol local bureau as is the case for each Member State. The EU would be limited to a consulting entity and would never be an owner of any data. Further discussions with Interpol are necessary to establish the exact legal framework while Interpol already indicated that this would certainly be feasible.

The ESP should thus include the optional search towards Interpol data (SLTD, TDAWN). In cases where Interpol databases are included in the search (to be defined in each respective legal instrument), the ESP will only implement by default the first-level hit/no-hit; this would never generate notifications to data owners. If an end-user needs to retrieve the additional details (thus generating a notification to the data owner), a specific transaction via the ESP will be initiated in a second step.

#### Extending ESP towards Europol data

The Europol data contained in the systems at Europol can now be searched by the QUEST<sup>26</sup> interface. This new system-to-system interface permits the use of an ESP where either an end-user in a Member State or a system such as ETIAS would search Europol data.

Since the central systems at eu-LISA have no security accreditation, they cannot be connected to accredited systems. The QUEST interface at Europol would therefore also need to be available at this 'non-accredited level' which Europol identifies as 'basic protection level' (BPL) data.

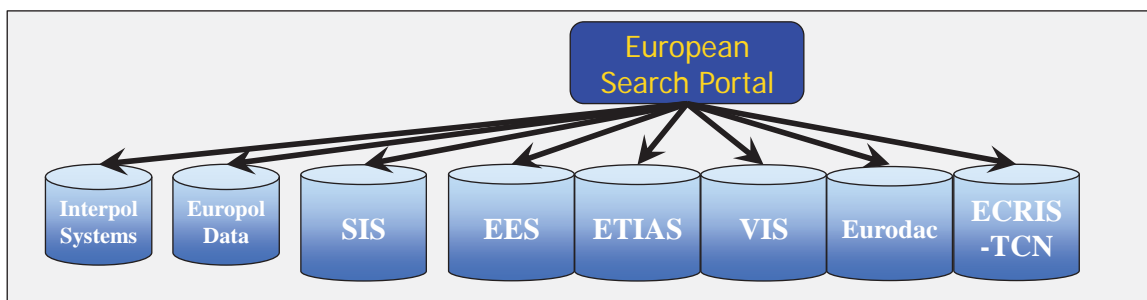
Europol indicated that the QUEST interface can indeed be made available towards Basic Protection Level data. This would enable a technical and legal usage of an ESP with the QUEST interface.

As indicated in Table 2, for the purpose of prevention, detection or investigation of terrorist offences and other serious criminal offences, Europol provides a wealth of data not present in any other central system. The ESP would provide faster, seamless and systematic access to those persons that have a legal access to Europol data for these purposes.

In the process described in ETIAS for granting the travel authorisation, the first step consists in an automated check of the applicant's identity data and information on the travel document vs. different information sources. One of these information sources should be Europol data.

The ETIAS system would be a 'user' of the ESP in order to consult Europol data.

**Figure 4 – Extending ESP to Europol and Interpol data**



<sup>26</sup> QUerying Europol SysTems.

### *8.1.3. ESP with or without the proposed ECRIS-TCN data*

As can be seen from Table 2, the proposed ECRIS-TCN system data is envisaged to be used by ETIAS. As explained, ETIAS will need to consult many different systems and it would greatly benefit from the use of an ESP.

The ETIAS system would be a 'user' of the ESP in order to consult ECRIS-TCN system data. The ESP should thus include the proposed ECRIS-TCN system data.

### *8.1.4. ESP with or without shared BMS*

The ESP can and should contain biometric data in the search transaction when the transaction in question utilises such data. Depending on which biometric search engine is used, it might need to be converted into the respective formats of each individual system. This converted data would then be sent to each individual system, which in turn would ask the relevant biometric engines to search with this data. Where biographical searches are generally quick and less resource intensive, biometric searches take longer and require considerable computing resources. Although technically possible, such parallel biometric searches would be slow and difficult as they would require a complete harmonisation of response times of biometric searches<sup>27</sup>. The ESP without shared BMS is therefore not an efficient option when it comes to biometric searches.

The combined use of the ESP with the shared biometric matching service would enable simultaneous biometric searches not only in the central systems at eu-LISA but also in the Interpol data, which cannot be integrated in the shared BMS.

This combined option of ESP and shared BMS requires no additional changes compared with those of the ESP alone on the central systems or at the level of Member States.

There is no overlap of functionalities between the ESP distributing the searches and the shared BMS performing the biometric searches.

Where the shared BMS detects biometric records in all systems (depending on the access rights of the end-user), the (possibly different) biographical data linked to this biometric record would be retrieved by the ESP from the individual systems and facilitate the analyses.

However, with this option, the links between the same, similar or different identities used by the same person across multiple systems do not become persistent data in the system. Each addition of new data or each search would potentially deliver hits on identities in different systems, which an end-user would need to analyse and manage in order to detect identity fraud. For example, the person requesting asylum and having submitted a previous visa application will be detected by an end-user when creating the asylum request. This end-user, however, will have no means of indicating this link as persistent data for it to be available for later use.

---

<sup>27</sup> The service level agreement (SLA) for VIS response time is 10 minutes, for Eurodac 1 hour, and for SIS 15 seconds. In many cases, the response time reached is even far below these SLA values.

## **Technical facilitation and simplification through the ESP**

This new ESP component needs to be developed, implemented, operated and maintained centrally by eu-LISA. The required changes to the existing central systems will generally be very small, limited to assuring similar service-level agreements for the response times of searches (i.e. having a response in 2 seconds from one system while having to wait another 15 seconds to have the response from a second system needs to be avoided). If an existing search engine were to turn out to be insufficient or unreliable for use with an ESP, this individual search engine (or multiple engines) would need to be adapted.

The ESP would only enable the searching of centralised systems (national systems are out of its scope). It offers no functionality for creating, updating or deleting any data, which will remain to be done through the individual systems so the current interfaces to these centralised systems remain in place.

Introduction of the ESP requires the use of a new interface (interface control document (ICD)) using the concepts of Universal Message Format projects<sup>28</sup>.

The national systems (and central systems like the proposed ETIAS) wanting to use the ESP need to implement this new ICD interface, which can be implemented gradually and does not need any EU rollout synchronisation.

Once a national system has implemented this new ESP ICD, it is very easy to add a new central system to the search via the ESP. The ICD of the new system is added to the ESP, the Member State does not need therefore to implement this new ICD for searching this new system. Instead, only the interface between the Member State and the ESP is changed marginally.

### ***Conclusion***

Based on an analysis of technical and operational aspects,, in order to ensure fast, seamless, systematic and controlled access to relevant information systems, the establishment of an ESP will be a feasible and viable solution.

The ESP will not extend or change existing access rights.

The ESP can be developed in a way that enables searching Interpol systems (in the Stolen and Lost Travel Documents (SLTD) database and Travel Documents Associated with Notices (TDAWN) database, searching Europol data, searching SIS data and searching the proposed ECRIS-TCN system data.

The ESP should make use of a shared BMS for biometric searches.

A more detailed and final comparison of this option, including on legal, financial, data quality and data protection aspects, is presented in Chapter 5 of the impact assessment.

---

<sup>28</sup> Existing UMF description would need to be extended; the term UMF+ can be used to this end.



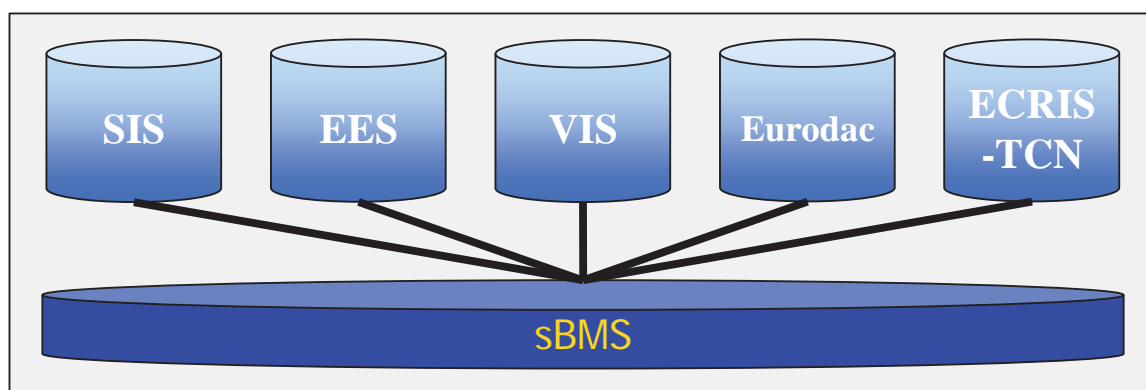
## 8.2. Detailed analysis of the shared biometric matching service

A shared biometric matching service (shared BMS) is also a new information technology component that enables the searching of biometric data (fingerprints and facial images) from several central systems (in particular, SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN system). The proposed ETIAS will not contain biometric data and will therefore not be served by the shared BMS.

Where each central system (SIS, Eurodac, VIS) currently has a dedicated, proprietary search engine for biometric data<sup>29</sup>, a shared biometric matching service provides a common platform where the data is searched simultaneously.

Establishing a shared biometric matching service was one of the options identified in the April 2016 Communication to achieve interoperability, confirmed by the high-level expert group as regards its necessity and technical feasibility and that it should comply with data protection requirements, and endorsed by the Commission in the *Seventh progress report towards an effective and genuine Security Union*.

**Figure 5 - Shared biometric matching service**



The shared BMS will generate substantial benefits in terms of security, cost, maintenance and operation by relying on one unique technological component instead of five different ones.

Its key objective is to facilitate the identification of an individual who may be registered in different databases (under the same or different identities). An appropriate set of biometric data is unique and therefore much more reliable than alphanumeric data to identify a person. A query of this service would thus indicate, if the end-user has access to these records, whether a record exists in any of the central systems linked to the shared biometric matching service. This makes the shared BMS a key enabler to help detect connections between data sets and different identities assumed by the same person in different central systems.

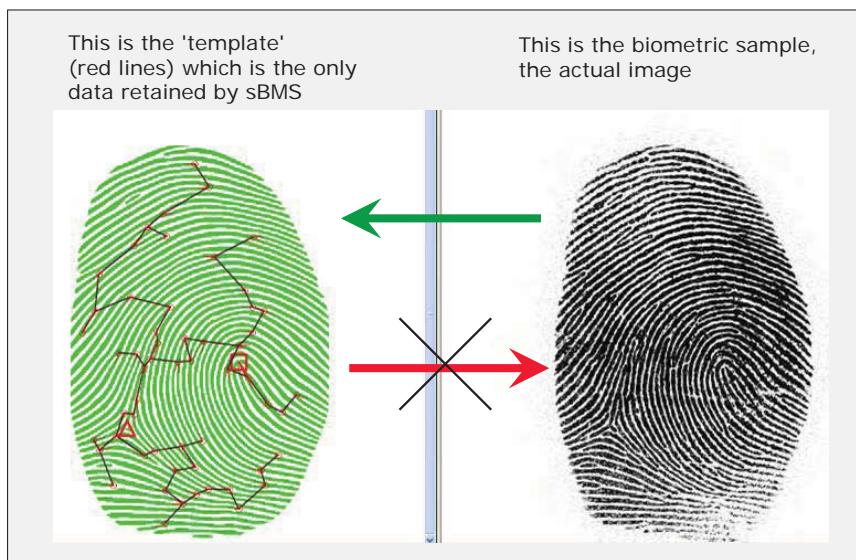
The biometric data (fingerprint and facial images) are fully retained by the central systems. The shared BMS creates a mathematical representation<sup>30</sup> of the samples (a

<sup>29</sup> These biometric search engines are technically referred to as automated fingerprint identification system (AFIS) or automated biometric identification system (ABIS).

<sup>30</sup> Contrary to common misconception, an automated biometric identification system (ABIS) does not actually search with fingerprint images or facial images, or store them. A feature extraction creates a mathematical representation (template) from the images. Only the templates are retained by the ABIS.

search vector or template) but will discard the actual data, which is thus stored in one location, only once.

**Figure 6 - Template of fingerprint**



### *Samples and templates*

The exact biometric samples used to identify or verify a person depend on various current and historical factors. While 10 rolled fingerprints will give the highest accuracy, it is also more time-consuming to capture them. The EES will capture 4 flat fingerprints (the fastest to capture) and combine it with a facial image, while the VIS continues capturing 10 flat fingerprints.

The shared BMS would transform these biometric samples into templates, regardless of the type of fingerprint, the number of fingerprints, or the presence or absence of a facial image, and would use all these templates regardless of the biometric samples used to search.

- The 10 flat fingerprints of a visa applicant would thus be used to also search the collection of the 10 rolled fingerprints in SIS and the 4 flat fingerprints of EES.
- The 4 flat fingerprints of EES would also search the rolled fingerprints in SIS and the 10 flat fingerprints in VIS.
- The 10 rolled fingerprints of an asylum seeker would also search the rolled fingerprints of SIS and the 10 flat fingerprints in VIS.

The inclusion of all biometric 'templates' in one location permits the detection of a match, not only when searching but also when adding new data. If biometric data were distributed over the various systems, every new addition of data would need to be searched against all other systems to detect the existence of data on the same person.

The access to the templates in the shared BMS will be determined by the purpose of access and will be systematic. The shared BMS will thus also implement and enforce the access control described in Table 2.

### 8.3. Detailed analysis of the common identity repository

The common identity repository (CIR) is not an additional database but a new IT architecture bringing together existing biographical identity data of third-country nationals (TCNs), such as name, date of birth, travel documents, that would otherwise have been stored in the various central systems. It is comparable to a shared biometric matching service but handling a subset of biographical data instead of biometric data.

The numbers of biographical data sets that are or will be stored in the respective central EU systems vary substantially, but are overall in the order of hundreds of millions.

Establishing a common identity repository was one of the options identified in the April 2016 Communication to achieve interoperability, confirmed by the high-level expert group as regards its necessity and technical feasibility and that it should comply with data protection requirements, and endorsed by the Commission in the *Seventh progress report towards an effective and genuine Security Union*.

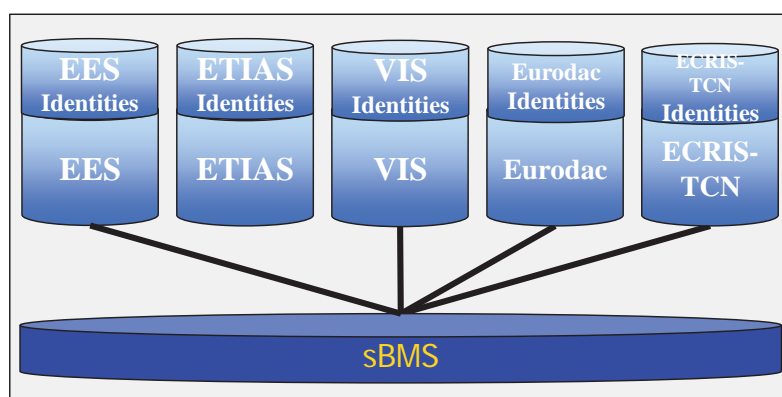
The CIR provides a unified view on a subset of biographical identity data<sup>31</sup> of third-country nationals that will be present (or are present) in Eurodac, VIS, EES, the proposed ETIAS and the proposed ECRIS-TCN system.

Each of the central systems dealing with third-country nationals (in particular the new EES, the proposed ETIAS, the new Eurodac, VIS, and the proposed ECRIS-TCN system) stores or will store biographical data on specific persons for specific reasons.

The EES, the proposed ETIAS and the proposed ECRIS-TCN are new systems to be developed by eu-LISA; the current Eurodac does not have biographical data, so including this data will also be a new development. The creation of the CIR, therefore, does not in any way involve copying existing data to a new component. Instead, the CIR would be a shared component between these systems to store and search biographical data.

The VIS presents an exception as it already contains biographical data. The necessary interactions between VIS and EES will require new developments on the existing VIS. As part of these developments, the biographical data of visa applicants can be ‘moved’ to the CIR thereby facilitating the interoperability between these two systems.

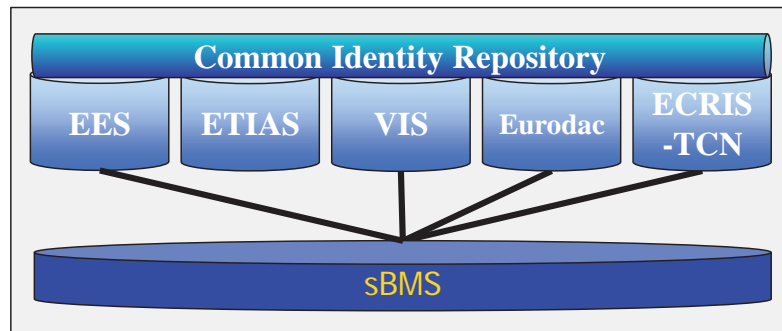
**Figure 7 – Biographical identities in each system versus shared BMS**



<sup>31</sup> Biographical data that can be found on the travel document. Indicative list: last name, first name, gender, date of birth, travel document number. The subset would not include addresses, former names, biometric data, etc.

Each system provides<sup>32</sup> (or will have to provide) a specific search engine for these data while being completely unaware of a potential existence of the same data in another system. The CIR would create a common search engine for a subset of biographical data in the central systems, thus delivering consistent reproducible results with identical transaction times, regardless of the source of this data.

**Figure 8 - Common identity repository**



Its key objective is to facilitate the biographical identification of a third-country national regardless of the identity and the central system used. It does this by providing easier, faster, seamless and more systematic access to the biographical data contained in the central systems to which the end-user has legal access. The CIR cannot function without the shared BMS, as identities can only safely be confirmed (or repudiated) by using biometric data.

The central systems mentioned in Figure 8 would create their own biographical records in the CIR thereby fully managing the access control rights and the data retention rules on these records. For example, where the VIS created a record on person X and Eurodac created a record on the same person X, the CIR would contain two distinct records, only containing the basic biographical data, with distinct access control and data retention rules.

Similar to the functioning of the shared BMS, the inclusion of biographical identity data in one location permits the detection of a match not only when searching but also when adding new data. When biographical data are distributed over the various systems, every new addition of data would need to be searched against all other systems to detect the existence of the same data of a person.

Inclusion of data from systems at Europol would be very complex from a technical point of view. Including such data from Interpol systems would probably be impossible from a legal point of view. The Europol and Interpol data are thus excluded from usage in a CIR and shared BMS.

*8.1.5. Allow police to perform identification of TCNs: additional purpose for the CIR*

By developing an identity data repository for the specific purpose of identification of third-country nationals using only a small subset<sup>33</sup> of already existing data in EU information systems, the EU would fill an important gap in the existing information system architecture.

<sup>32</sup> EES and the proposed ETIAS would provide one single engine as they will have a common repository.

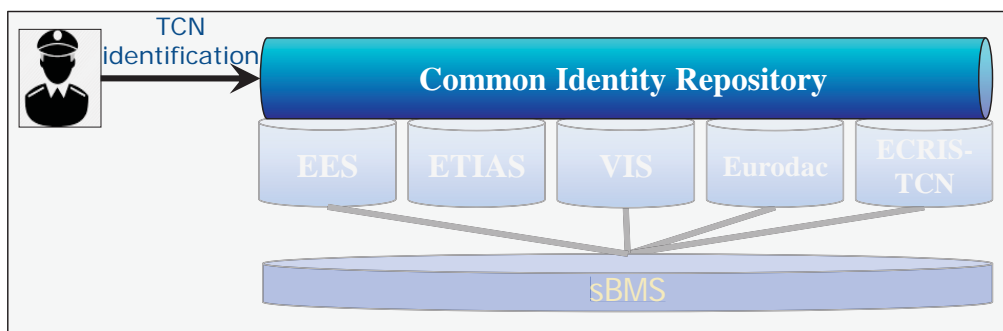
<sup>33</sup> Subset limited to the data that can be found in the travel document.

This option also requires amending the legal instruments of Eurodac, VIS and EES to enable police officers or other authorised officers to perform identifications of undocumented or ill-documented third-country nationals in the Schengen territory.

From a technical perspective, the CIR would be used to streamline, facilitate and restrict the access to biographical identity data. Since the CIR contains the necessary biographical data (and the shared BMS the necessary biometric data) to identify a third-country national, this is the only architectural component to which the police officer needs access. The business-specific case data (visa details, person inviting visa holder, asylum background, etc.) remain in the central systems and do not need to be visible. The authorised officer has no access to these data.

For this specific purpose, the CIR would not indicate the origin of the data. It would not be possible for the officer to see if the person is a visa holder, visa-exempt or an asylum seeker (except by possible deduction from the issuing state of a possible travel document) Only the biographical identity or identities is or are revealed.

**Figure 9 – Identification of third-country nationals using the CIR**



The biographical identity data in the proposed ECRIS-TCN system will be very trustworthy as it will be established during thorough judicial procedures and data exchanges. Including the proposed ECRIS-TCN data in the CIR facilitates correct identification by police officers for those persons present in the proposed ECRIS-TCN system.

The authorised officer would not see the origin of the data. He would not detect that this identity comes from the proposed ECRIS-TCN system nor would he have any details whatsoever concerning the past conviction of the person.

The way the CIR identifications would be implemented is shown in the following table.

**Table 1 - Identification of third-country nationals**

	<b>VIS</b>	<b>Eurodac (new)<sup>34</sup></b>	<b>EES</b>	<b>ETIAS (proposal)</b>	<b>ECRIS- TCN (proposal)</b>
<b>Identity data (accessible)</b>					
<i>Purpose of access</i>  <b>Police checks identification or verification of identity (in territory)</b>  direct access to identity data  Through <u>common identity repository</u>	<ul style="list-style-type: none"> <li>- Biographical data</li> <li>- Passport details</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>	<ul style="list-style-type: none"> <li>- Biographical data</li> <li>- Passport</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>	<ul style="list-style-type: none"> <li>- Biographical data</li> <li>- Passport details</li> <li>- Fingerprints (4)</li> <li>- Facial images</li> </ul>	<ul style="list-style-type: none"> <li>- Biographical data</li> <li>- Passport details</li> </ul>	<ul style="list-style-type: none"> <li>- Biographical data</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> </ul>
<b>Additional information (not accessible)</b>					
	<ul style="list-style-type: none"> <li>- Visa status</li> <li>- Issued, refused, discontinued, extended, revoked or annulled single/double/multiple entry visa</li> <li>- Authority where visa application was lodged;</li> <li>- Background information: Member State(s) of destination, purpose of travel, intended date of arrival and intended stay, applicant's home address, occupation and employer etc.</li> <li>- (In the case of families or groups): links between applications;</li> <li>- History of applications of person</li> </ul>	<ul style="list-style-type: none"> <li>- ID card details (where available)</li> <li>- Information concerning third-country nationals or stateless persons above 6 years old:</li> <li>- applicants for international protection</li> <li>- persons apprehended in connection with the irregular crossing of an external border</li> <li>- persons found illegally staying in a Member State</li> </ul>	<ul style="list-style-type: none"> <li>- Entry data</li> <li>- Exit data</li> <li>- Refusal of entry data</li> <li>- Remaining authorised stay</li> <li>- List if persons overstaying</li> <li>- Statistics on persons overstaying</li> </ul>	<ul style="list-style-type: none"> <li>- Travel authorisation status</li> <li>- IP address</li> <li>- Issued, refused, revoked and annulled travel authorisations</li> <li>- Declarative information provided in application</li> <li>- Additional information provided at request</li> <li>- Results of the processing of the travel authorisation request, notably hits against other EU systems, the ETIAS watch list and Interpol system)</li> </ul>	<ul style="list-style-type: none"> <li>- Convicting Member State (including a reference number and the code of the convicting Member State)</li> </ul>

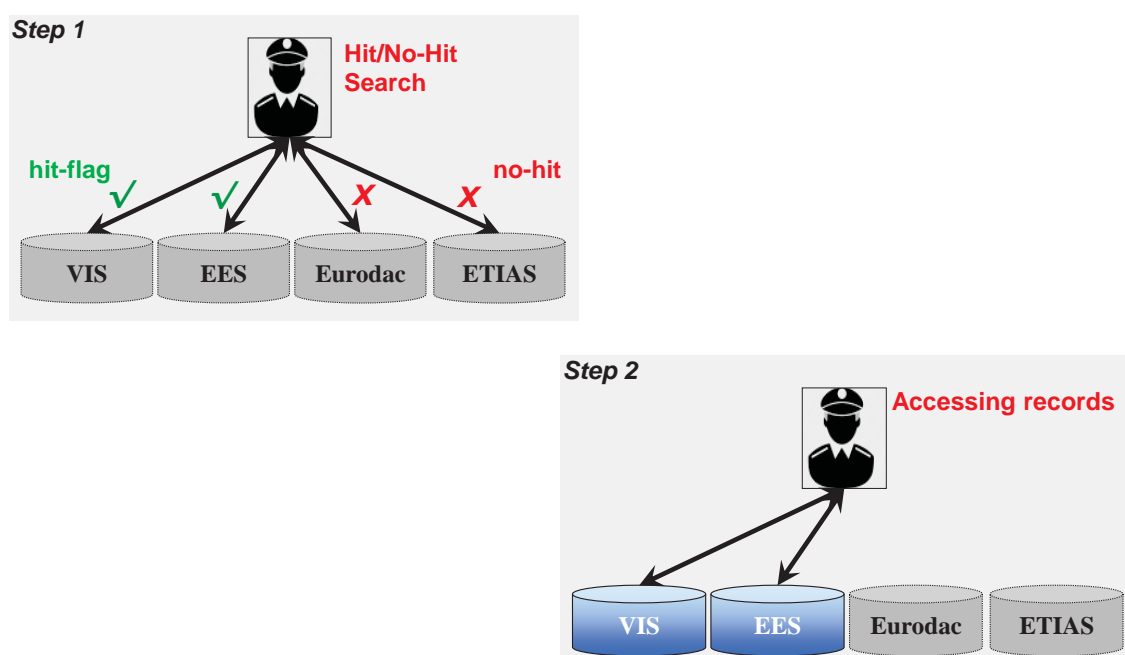
<sup>34</sup> Eurodac (new) refers to the proposed inclusion of biographical identity data in EURODAC, necessary to allow identification of persons.

### 8.1.6. Facilitate law enforcement access: two-step flagging on the CIR

The 'hit-flag' functionality is a new concept that restricts access to data by limiting it to a mere 'hit/no-hit' notification, indicating the presence (or non-presence) of data. It was developed during the work of the high-level expert group and further refined when analysing the CIR.

The end-user performing a search with biographical data (last name, first name, date of birth, travel document number) or biometric data (set of good fingerprints and/or good-quality facial image) could search various central systems at the same time (in parallel, no cascade) while the only returned results would be a 'hit-flag' in the case where this data existed in a particular system. This first step would not require an *ex ante* authorisation and would enable *ex post* verification.

**Figure 10 - Two-step approach, based on the 'hit-flag' functionality**



Only in a second step and where considered necessary would the end-user request actual access to those systems that provided a 'hit-flag'. Where a system does not return a 'hit-flag', no access will need to be requested.

For the second step, the access rights and procedures that are laid down in the respective legal instruments will remain applicable.

In cases where investigative access (using partial or latent fingerprints from crime scenes) is required, the 'hit-flag' approach would also work but in a less deterministic way as the results of such an inexact search would produce ranked lists of potential candidates<sup>35</sup>. The investigator would then first request access to the fingerprints of the system that generated the highest matching score in a candidate list. After manual verification of the fingerprint records in the 'best' candidate list, it is still possible that

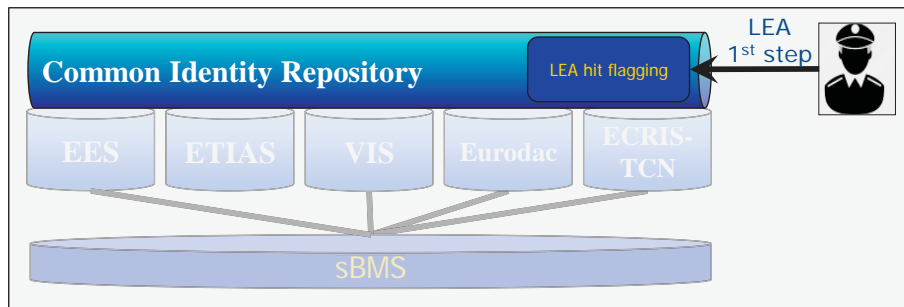
<sup>35</sup> The shared BMS will generate matching scores between 0 and 100 on each candidate in the candidate list, the highest score indicating the highest probability that the latent fingerprint belongs to that person.

only false matches were present in this candidate list. The investigator would then need to access the fingerprints of the system that generated the 'second-best' candidate list.

The 'hit-flag' approach can replace the current 'cascading' as an alternative data protection safeguard.

The two-step approach described can be built in the CIR platform. CIR already contains the subset of biographical data, linked to biometric data in the shared BMS, which will be necessary to enable data presence checks for law enforcement searches.

**Figure 11 – Hit/no-hit flagging for law enforcement access**



The single, harmonised and high-performing biographical search engine of the CIR could from the onset be developed to enable data presence checks without retrieving any data from the CIR and log the search transactions using harmonised user-roles.

The physical separation of the biographical identity data in the CIR, the biometric data in the shared BMS and the business specific case data (the actual sensitive data) in the central systems creates an additional data security safeguard. Having access to any of the components (lawfully or via a security breach) does not automatically give access to data in other components. In order to access the case specific (sensitive) data, one needs access to the CIR or the shared BMS.

The way the CIR hit-flagging functionality would be implemented is shown in the following table:



**Table 2 - Flagging for law enforcement purposes<sup>36</sup>**

<i>Purpose of access</i>			
<b>Prevention, detection and investigation of terrorist offences and other serious criminal offences</b>			
Step 1: direct access to <b>flags</b> – through <b>Common Identity Repository</b>			
Step 2: access to additional information (identity data + additional information) in flagged systems, in accordance with the legal bases of those systems			
<b>Flag indicating the system (accessible in step 1)</b>			
<b>VIS</b>	<b>EURODAC (new*)</b>	<b>EES</b>	<b>ETIAS (proposal)</b>
<b>Data on the third country national (accessible in step 2)</b>			
<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Fingerprints (10)</li> <li>- Facial images</li> <li>- Visa status</li> <li>- Issued, refused, discontinued, extended, revoked or annulled single/double/multiple entry visa</li> <li>- Authority where visa application was lodged;</li> <li>- Background information: MS(s) of destination, purpose of travel, intended date of arrival and intended stay, applicant's home address, occupation and employer etc.</li> <li>- (In case of families or groups): links between applications;</li> <li>- History of applications of person.</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport</li> <li>- Fingerprints (10)</li> <li>- Facial images*</li> <li>- ID card details** (where available)</li> <li>- Information concerning third country nationals or stateless persons above 6 years old:</li> <li>- applicants for international protection</li> <li>- persons apprehended in connection with the irregular crossing of an external border</li> <li>- persons found illegally staying in a Member State</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Fingerprints (4)</li> <li>- Facial images</li> <li>- Entry data</li> <li>- Exit data</li> <li>- Refusal of entry data</li> <li>- Remaining authorised stay</li> <li>- List if persons overstaying</li> <li>- Statistics on persons overstaying</li> </ul>	<ul style="list-style-type: none"> <li>- Biographic data</li> <li>- Passport details</li> <li>- Travel authorisation status</li> <li>- IP address</li> <li>- Issued, refused,, revoked and annulled travel authorisations</li> <li>- Declarative information provided in application</li> <li>- Additional information provided at request</li> <li>- Results of the processing of the travel authorisation request, notably hits against other EU systems, the ETIAS watch list and Interpol system).</li> </ul>

<sup>36</sup> Eurodac (new) refers to the proposed inclusion of biographical identity data in Eurodac, necessary to allow identification of persons.

#### 8.4. Detailed analysis of the multiple-identity detector

The shared BMS can be used to detect persons whose biographical identity data are present in any of the central systems.

Two different persons can share the same (or very similar) biographical identity. The disambiguation of similar identities takes time and effort and presents a considerable burden to the person(s) carrying these identities. In the absence of a place where the results of such disambiguation are retained, the person(s) will continue to be bothered. Such a person would for example not be able to make use of automated border control facilities.

Similarly, one person could present different biographical identities. We then speak about identity fraud<sup>37</sup>. Identity fraud can thus be detected by comparing the biographical identity data (across all central systems) of a person based on a biometric match.

Identified cases of identity fraud, multiple identities or identity disambiguation could be made visible in a multiple-identity detector (MID).

A MID would be a small new component that would enable verification of multiple identities. It would only show those biographical identity records (i.e. part of the data that is in the CIR) that have a link in different central systems. These links would be detected by the shared BMS on the basis of biometric data and would ultimately need to be confirmed by the data owners (of each record) to declare if it is a case of identity fraud (red link) or identity disambiguation (green link). Awaiting this final analysis, the MID could indicate a new link as a 'potential link' (yellow link).

Towards an end-user the links that are shown could be colour-coded as follows:

- Green link: Different persons sharing the same biographical identity
- Yellow link: Potentially differing biographical identities on the same person
- White link: Person present in multiple systems with the same biographical identity
- Red link: Differing confirmed biographical identities on the same person.

##### *Examples of links*

Visa applicant A is stopped at border-control as a SIS alert exists on identity A. After biometric verification, visa applicant A is not the person under SIS alert. This case of identity disambiguation is shown as a green link by the MID. Visa applicant A will not be bothered next time and could now use automated border control because of the green link.

When crossing the external Schengen border for the first time, the biographical details of visa applicant G are entered into EES. These biographical data in EES are slightly different from the details in VIS. The MID will show a yellow-link indicating a potential problem. Yellow links are temporary and after verification become either red or white.

Person D has a past visa application in VIS but his country of origin became visa-exempt. Person D applies for an ETIAS authorisation with a new passport as the old

---

<sup>37</sup> Persons legally changing biographical identity (married persons changing last name for example) is not a case of identity fraud but in these cases, only part of the biographical identity changes.

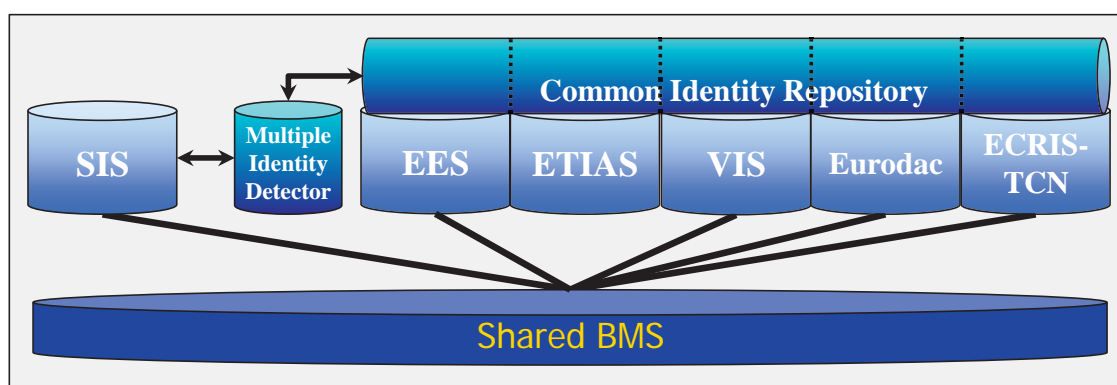
passport expired. Person D is registered in EES where the biometric data matches against the visa-record. The MID will show white links between the identity in VIS and the identity in EES.

Asylum seeker X (claimed identity not based on any travel document) is identified in VIS (based on fingerprints) as Y. The biographical identities are analysed and very different. This case of multiple identities is shown as a red link by the MID.

The MID would complement the CIR in enabling the linking of biographical identities across systems, including data from SIS.

While it builds on the CIR and the shared BMS, the solution of establishing a MID is a new option that was not included in previous policy documents. It is a result of the further technical analysis and consultations with stakeholders (including eu-LISA, the European Data Protection Supervisor and the EU Agency for Fundamental Rights) that the Commission announced in the *Seventh progress report towards an effective and genuine Security Union* and has conducted since.

**Figure 12 - Multiple-identity detector**



### **Examples**

Asylum seeker X is identified in VIS (based on fingerprints) as Y. An end-user creates a link in the MID between the record in Eurodac, the record in VIS and the records in the shared BMS indicating multiple identities and potentially identity fraud. When searching the MID with X or Y, both the Eurodac and VIS records are returned.

Asylum seeker X is identified in the proposed ECRIS-TCN system (based on fingerprints) as Z. A link is created in the MID between the record in Eurodac, the record in the ECRIS-TCN system and the records in the shared BMS. Searching the MID with either X or Z will return both the ECRIS-TCN record and the Eurodac record.

Person A is under an Article 36 discreet check alert in SIS, including biometrics. This person uses identity B to request a visa. Although a fingerprint match against the SIS data exists, the consular officer cannot be made aware. The MID creates a 'potential link' between the biographical data B of VIS and the biographical data A of SIS. When the MID is searched with either A or B, the SIS alert is found.

#### *8.1.7. MID with SIS data*

When detecting a link, based on a biometric match, between data in SIS and data in the other central systems (or the CIR), such links cannot currently be made persistent as SIS data cannot be included in the CIR.

Each end-user needs to perform a biometric search and manually compare the biographical data returned from the various central systems (or CIR).

Including SIS identity data in the MID, in those cases where a link to multiple biographical identities was detected, enables management of two different cases:

- 1) disambiguation of multiple biographical identities;
- 2) addressing identity fraud.

### **Examples**

Mr X has an alert in SIS. Mr Y is registered in EES. Both identities are identical but concern two different persons, determined via a biometric match. To prevent Mr Y repeatedly being stopped — to perform the disambiguation with the identity data in SIS — the MID would store the link between the identity data in SIS and the identity data in EES (or any other system) indicating that these are two different persons. The differentiating biographical data will be the travel document details.

Ms A has an Article 36 alert in SIS, she purchases a genuine travel document under the name B, and applies for a visa. The biometric match from shared BMS leads to the creation of a link in the MID, linking the biographical identities A and B indicating that this concerns the same person, so highlighting identity fraud. At border control, the biographical identity B will reveal the SIS alert on A via a search towards the MID. (Fingerprints from visa-holders are not used to search any system at border control.)

For this purpose, the MID should include links to SIS data.

#### *8.1.8. MID with the proposed ECRIS-TCN data*

Similar to the option of including the ECRIS-TCN data in the CIR, links to identity data of the proposed ECRIS-TCN system should be stored in the MID.

The biographical identity data in the proposed ECRIS-TCN system will be much more trustworthy as it will be established during thorough judicial procedures and data exchanges. Including links to the proposed ECRIS-TCN data in the MID enables the detection of identity fraud and improves data quality on certain records.

#### *8.1.9. MID with cross-matching existing data*

The Eurodac, VIS and SIS central systems already have considerable amounts of biometric data that have been 'matched' against the data within one single system but not cross-matched against data in other systems.

When the shared BMS is implemented, one could either cross-match all the existing data against each other or leave the data as they currently are with a high probability that a match will never be detected.

When performing a cross-match of 70 million VIS records against 10 million Eurodac records and against 1 million SIS records, the results from the shared BMS may need to be verified before creating a link in the MID. In the absence of the shared BMS, the biometric data quality may indeed differ substantially between systems.

To help Member States in rejecting false hits, a fingerprint verification team could be established during the time of the initial cross-matching of existing data.

***The fingerprint identification team***

Based on experiences of a number of Member states, the cross-matching of fingerprints of Eurodac, VIS and SIS in a shared BMS could lead to an estimated 5% hit-rate.

On the 10 million Eurodac records, this gives 500,000 hits. On the 1m SIS records this gives 50,000 hits. A total of 550,000 hits estimated to be reviewed.

The great majority of records are good-quality 10 prints, the estimated verification time to discard a false-hit is estimated at 5 minutes per record.

This leads to a total verification time of 45,830 hours or 6,550 days or 30 man-years.

An estimated team of 30 persons would work 1 year to discard false hits.

This team could potentially work in a centralised team at Frontex (potentially part of the proposed ETIAS central unit).

This team would analyse every single cross-system biometric hit to remove the false hits. The actual true hits would lead to the creation of a link between records in the MID.

By creating a component that shows the links between multiple identities corresponding to the same biometric identifiers, and by showing these links to all public authorities involved in border management, security and migration the EU, one provides a powerful tool to detect and combat identity fraud and bolster its internal security.