EUROPEAN
COMMISSION

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

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,***[1] the Commission presented its vision on how to address a number of structural shortcomings related to information systems.[2] 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,[3] 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,[4] 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.[5] The purpose of the roadmap was to support operational investigations and to swiftly

---

1 COM(2016) 205 of 6 April 2016.

2 (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.

3 European Council Conclusions, 17-18 December 2015.

4 State of the Union 2016 of 14 September 2016.

5 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.[6]

The **European Parliament** has also urged action in this area. In its July 2016 Resolution[7] 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).[8] In the meantime, following the Commission's proposal of May 2016,[9] 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),[10] 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),[11] 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)[12] 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:

---

6 European Council Conclusions, 15 December 2016.
7 European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 (2016/2773(RSP).
8 COM(2016) 883 final.
9 COM(2016) 272 final.
10 COM(2016) 194 final.
11 COM(2016) 731 final.
12 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**[13] 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.[14] 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[15] 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.[16] 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;[17]
- 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[18] or the Passenger

---

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

14 Scoping paper of the high-level expert group on information systems and interoperability.

15 COM(2016) 710 final.

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

17 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.

18 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.

Name Record directive[19], 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*,[20] 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[21]) 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.[22] The European Council conclusions of June 2017[23] reiterated the need to act. Building on the June 2017 conclusions[24] 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,[25] 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

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

20 COM(2017) 261 final.

21 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.

22 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.

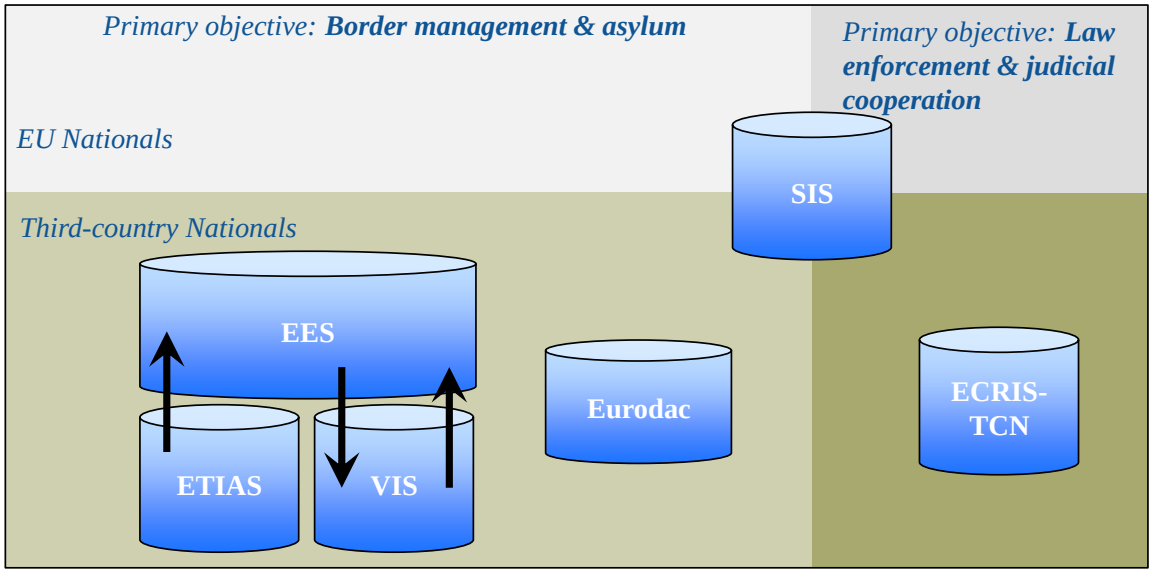
23 European Council conclusions, 22-23 June 2017.

24 Outcomes of the 3546th Council meeting on Justice and Home Affairs on 8 and 9 June 2017, 10136/17.

25 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.

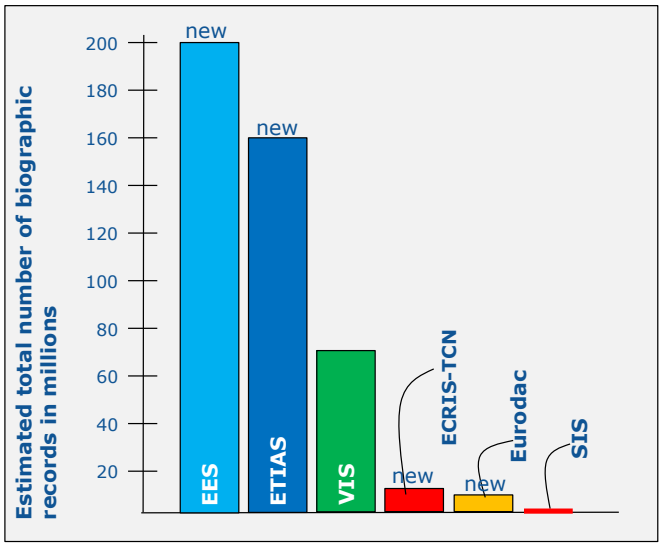
These three new systems are scheduled to be operational by 2020. It should be noted that the future EES and the proposed ETIAS have been conceived and proposed in such a way that they already present a degree of interoperability, i.e. between EES and ETIAS, and between EES and VIS.

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:[26]

- 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.

[26] 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[27] 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.

[27] 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.[28] 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

[28] 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',[29] 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

[29] '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 alphanumerical 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[30] 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

[30] 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,[31] the European Agenda on Security[32] and the Commission's work towards an effective and genuine Security Union;[33]

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.[34]
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.[35]
3. Facilitating identity checks of third-country nationals, on the territory of a Member State, by authorised officers.[36]
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.[37]

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

---

31 COM(2017)570 final.

32 COM(2015)185 final.

33 COM(2016)230 final.

34 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.

35 *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).

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

37 *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:

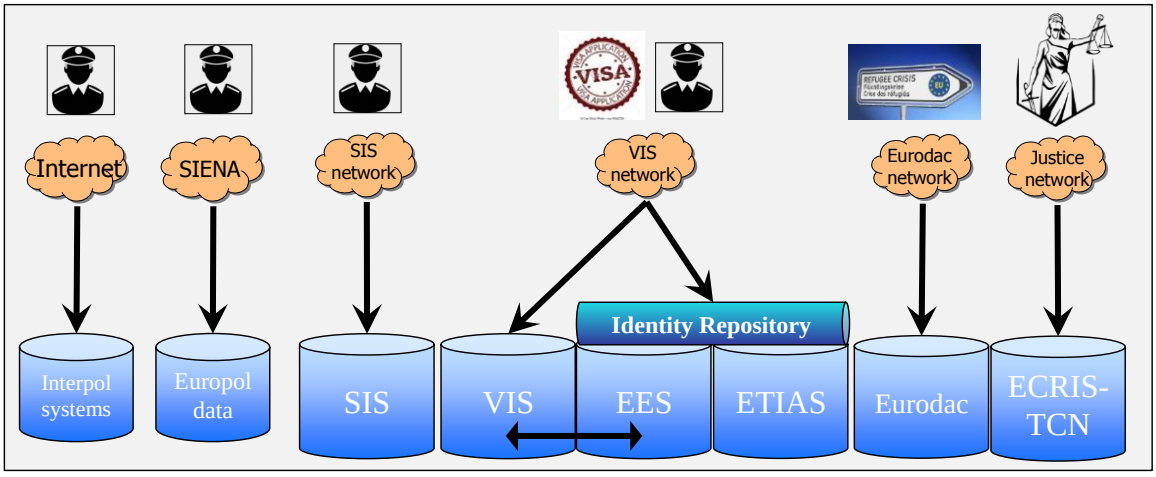
- Facilitating the technical and operational implementation by Member States of existing and future new information systems.
- Strengthening and streamlining the data security and data protection conditions that govern the respective systems.
- Improving and harmonising data quality requirements of the 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.[38]

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

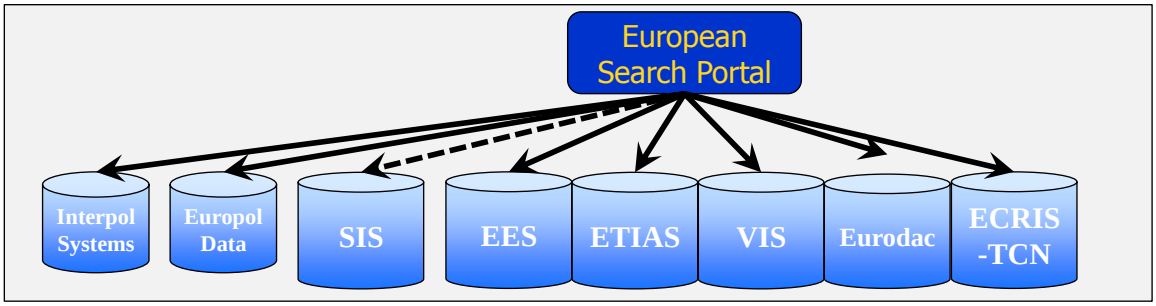
Under this option, these three components will handle data and be used according to the current legal instruments of each central system (SIS, VIS, Eurodac, EES, proposed ETIAS and proposed ECRIS-TCN system). The data protection risks and fundamental rights implications are those identified and mitigated 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 <u>not</u> 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.

[38] 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
Purpose of access **Border control**	X	X	X	X	X			X
Purpose of access **Issuance of short-stay visa**	X	X		X				
Purpose of access **Issuance of ETIAS authorisation**	X	X	X	X	X	X	X	X
Purpose of access **Police checks: Identification or verification of identity in territory of Member State**	X							
Purpose of access **Prevention, detection or investigation of terrorist offences and other serious criminal offences**	X	X	X	X	X		X	
Purpose of access **Migration management: verification of identity and verification of conditions for entry or stay (for TCNs, in territory)**	X	X	X	X				
Purpose of access **Return of irregular third-country nationals**	X	X	X	X				
Purpose of access **Assessment of request for asylum**	X	X	X					

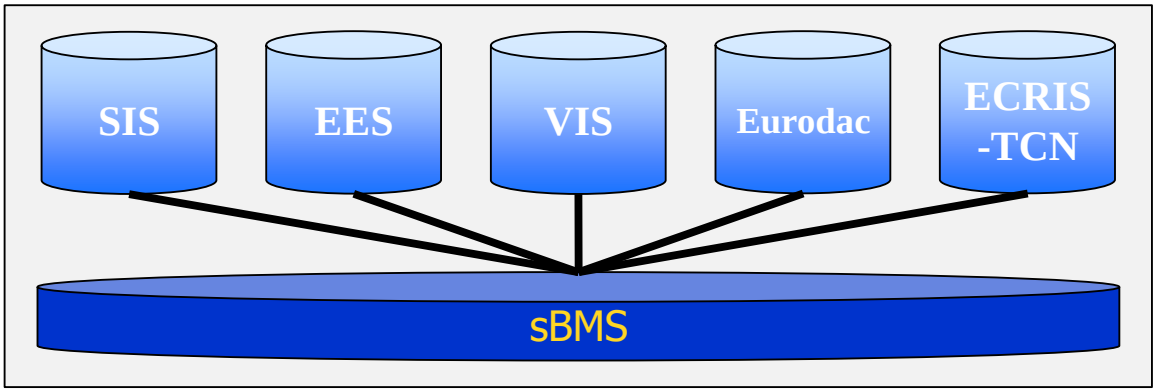
5.1.2. Shared biometric matching service

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,[39] 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

[39] 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[40] 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

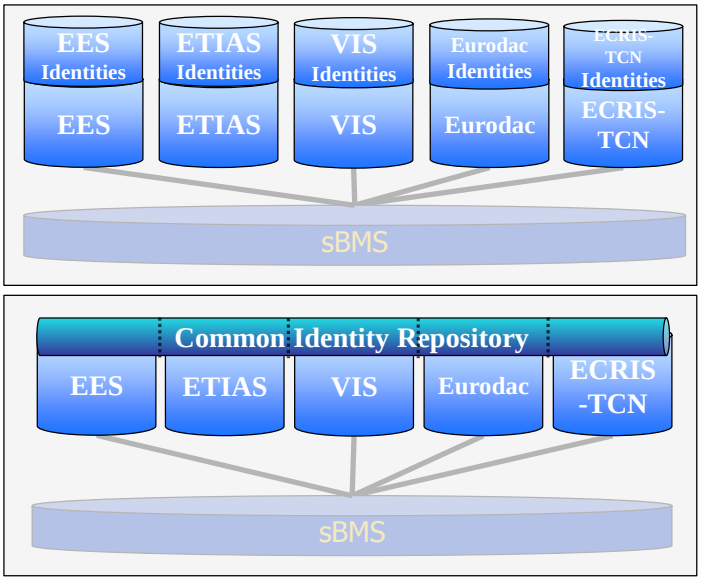
The common identity repository would provide for a unified view on biographical identity data[41] of third-country nationals that will be present (or are present) in Eurodac, VIS, EES, the proposed ETIAS and the proposed ECRIS-TCN system. Each of these five

[40] 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.

[41] 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

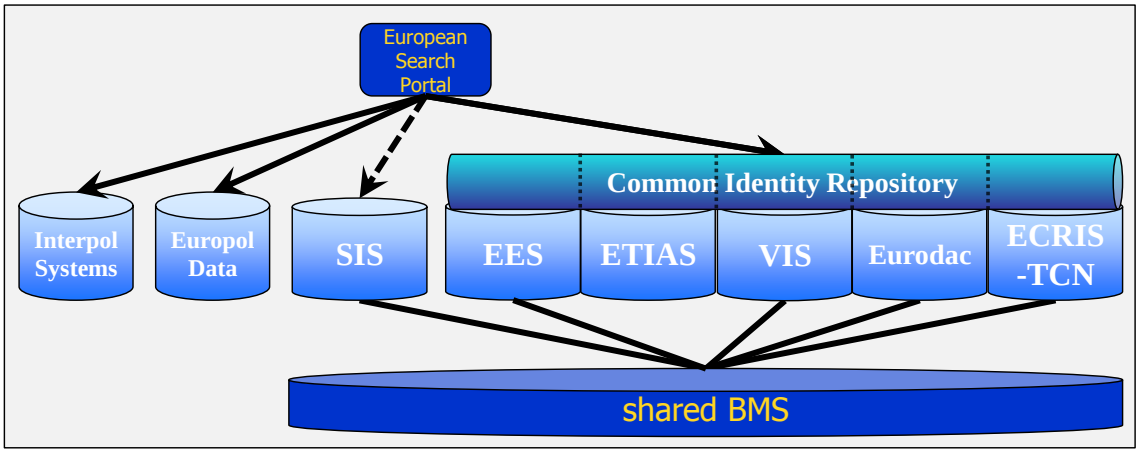
reporting and statistics, **CRRS**) capable of analysing anonymised data extracted from relevant information systems for statistical and reporting purposes. The Commission proposal to strengthen the mandate of eu-LISA[42] gives the Agency the task of establishing automated data quality control mechanisms 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**.

[42] 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 establishesend-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.

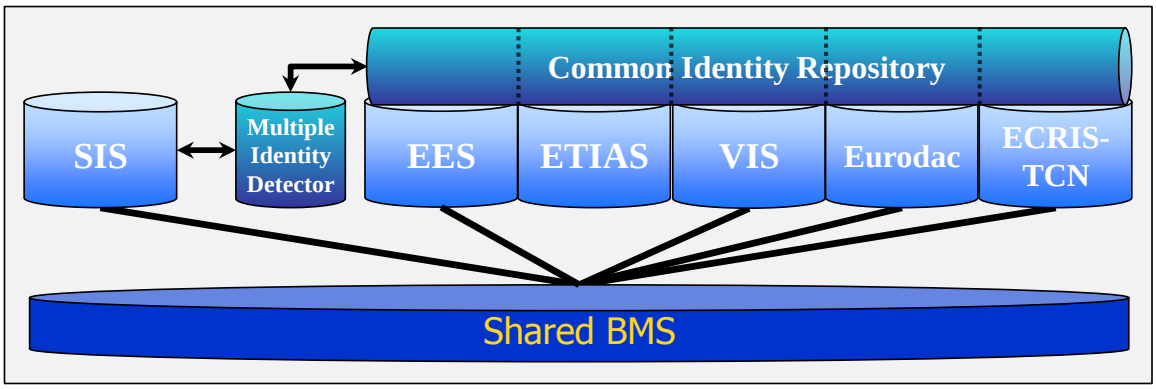
5.1.5. Adding a technical component to achieve interoperability: multiple-identity detector

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.[43]

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

[43] C(2017) 3349 final (12.5.2017).

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

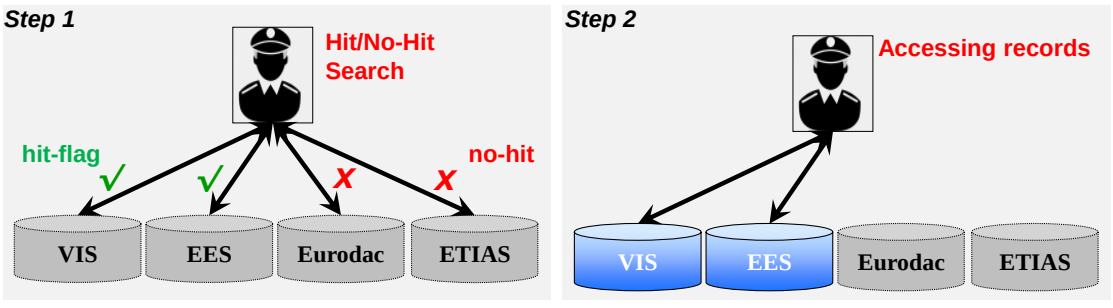
5.1.7. Streamlining the rules on access to EU information systems for law enforcement purposes: flagging

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*[44] 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.

[44] 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

	Purpose of access **Prevention, detection and investigation of terrorist offences and other serious criminal offences** **Step 1: direct access to <u>flags</u>– through <u>Common Identity Repository</u>** **Step 2: access to additional information (identity data + additional information) in flagged systems, in accordance with the legal bases of those systems**				
	VIS	**EURODAC (new)**	**EES**	**ETIAS (proposal)**	**ECRIS-TCN (proposal)**
	Identity data				
Purpose of access **<u>Police checks</u>** **identification or verification of identity (in territory)** **direct access to identity data** **through <u>common identity repository</u>**	- Biographic data - Passport details - Fingerprints (10) - Facial images	- Biographic data - Passport - Fingerprints (10) - Facial images	- Biographic data - Passport details - Fingerprints (4) - Facial images	- Biographic data - Passport details	- Biographic data - Fingerprints (10) - Facial images
	Additional information				
	- Visa status - Issued, refused, discontinued, extended, revoked or annulled single/double/multiple entry visa - Authority where visa application was lodged; - Background information: MS(s) of destination, purpose of travel, intended date of arrival and intended stay, applicant's home address, occupation and employer etc. - (In the case of families or groups): links between applications; - History of applications of person.	- ID card details (where available) - Information concerning third-country nationals or stateless persons above 6 years old: - applicants for international protection - persons apprehended in connection with the irregular crossing of an external border - persons found illegally staying in a Member State	- Entry data - Exit data - Refusal of entry data - Remaining authorised stay - List if persons overstaying - Statistics on persons overstaying	- Travel authorisation status - IP address - Issued, refused,, revoked and annulled travel authorisations - Declarative information provided in application - Additional information provided at request - Results of the processing of the travel authorisation request, notably hits against other EU systems, the proposed ETIAS watch list and Interpol system).	- Convicting Member State (including a reference number and the code of the convicting MS)

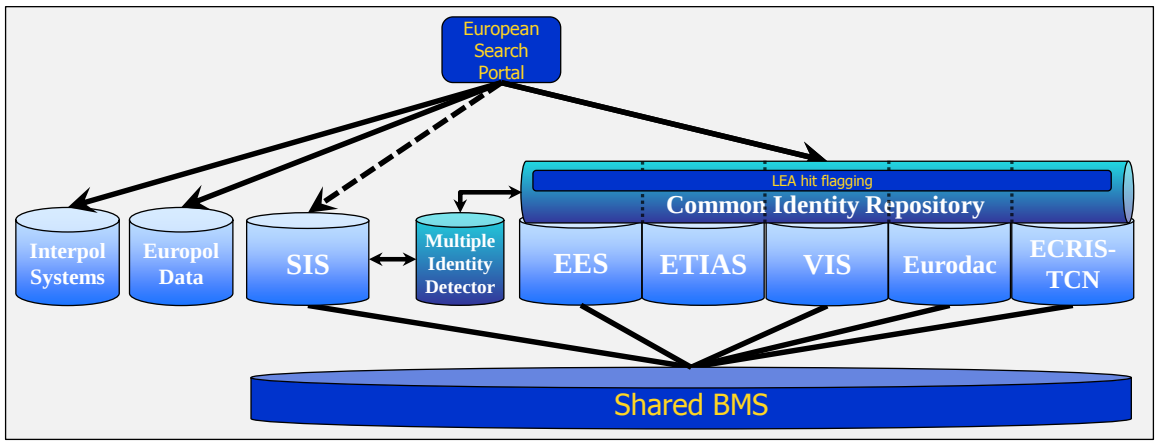
5.1.8. Complete picture of option 3

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 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,[45] 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.

[45] 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[46] 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

[46] 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:[47] *'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[48] 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

---

47 *Fundamental rights and the interoperability of EU information systems: borders and security*, Report by the EU Agency for Fundamental Rights.

48 *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.

protect an individual whose life is at risk, if they know or ought to have known of the existence of an immediate risk,[49] 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,[50] the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.[51]

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

---

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

50 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.

51 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,[52] 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,[53] and, where relevant, Directive (EU) 2016/680[54] 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,[55] 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.***[56] The importance of the concepts of data protection by design and by default[57] was repeatedly highlighted by the European Data Protection Supervisor regarding the e-Privacy reform.[58] 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).

---

52 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).

53 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.

54 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.

55 COM(2010) 385 final.

56 In the meaning of Article 25 of the General Data Protection Regulation.

57 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.

58 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 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 date 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 and 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 acceded 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 fundament 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 alphanumerical 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

	Member States and Europol		*eu-LISA*	
	One-off	**Recurrent**	**One-off**	**Recurrent**
Direct costs	(€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
Total	**30.3**	**6.1**	**55.8**	**7.3**

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. Overview of Benefits for Option 2		
Description	***Amount***	***Beneficiary***
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
Total	***€27.5m p.a. and €8m one-off***	

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

The cost/benefit analysis results in the following:

Option 2	***Member State Administrations***		***Central EU Agencies***		***Total***	
	One-off	***Recurrent***	***One-off***	***Recurrent***	***One-off***	***Recurrent***
	(€m)	(€m p.a.)	(€m)	(€m p.a.)	(€m)	(€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
Net Result	**-30.3**	**19.9**	**-47.8**	**-5.8**	**-78.1**	**14.1**

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.[59] 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.

[59] 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

	Member States & Europol		***eu-LISA***	
	One-off	**Recurrent**	**One-off**	**Recurrent**
Direct costs	(€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
Total	**85.5**	**17.1**	**84.3**	**11.4**

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

Overview of benefits (total for all provisions) — Option 3		
Description	***Amount***	***Beneficiary***
Direct benefits		
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
Total	***€77.5 m p.a. and €8m one-off***	

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

The cost/benefit analysis results in the following:

Option 3	***Member State Administrations***		***Central EU Agencies***		***Total***	
	One-off	***Recurrent***	***One-off***	***Recurrent***	***One-off***	***Recurrent***
	(€m)	(€m p.a.)	(€m)	(€m p.a.)	(€m)	(€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
Net Result	**-85.5**	**58.9**	**-76.2**	**-9.9**	**-161.7**	**49.0**

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[60] 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.

---

[60] 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 directly 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:

1. Fast, seamless and systematic access to authorised data sources	
• ESP is implemented in all Member States and for all relevant use cases.	• Number of Member States that implemented ESP multiplied by the number of use cases implemented.
• ESP is used for conducting searches on multiple systems.	• Number of searches handled by ESP v total number of searches (via ESP and systems directly).
2. Streamline access to authorised data sources for law enforcement purposes	
• Access streamlining possibility is used.	• Number of step 1 accesses for law enforcement purposes. • Number of step 2 accesses for law enforcement purposes.
3. Facilitate identifications of third-country nationals	
• Identification means are used.	• Number of identification checks performed v total number of transactions.
4. Detect multiple identities and fraud	
• Identification means are used. • Identity fraud is detected.	• Number of identities linked v number of identities with biographical information. • Number of detected cases of identity fraud v number of linked identities and total number of identities.

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