Council of the European Union

Brussels, 19 December 2017
(OR. en)

15119/17
ADD 2

Interinstitutional File:
2017/0351 (COD)

COSI 336	VISA 458
FRONT 507	FAUXDOC 73
ASIM 142	COPEN 419
DAPIX 430	JAI 1212
ENFOPOL 622	CT 164
ENFOCUSTOM 285	CSCI 79
SIRIS 217	SAP 28
SCHENGEN 88	COMIX 840
DATAPROTECT 220	

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	13 December 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2017) 473 final
Subject:	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)

Delegations will find attached document SWD(2017) 473 final.

Encl.: SWD(2017) 473 final

EUROPEAN
COMMISSION

Strasbourg, 12.12.2017
SWD(2017) 473 final

PART 2/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL

on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226
and

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL

on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)

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

ANNEXES

1. ANNEX 1 - GLOSSARY

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

[1] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

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

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

2. ANNEX 2: PROCEDURAL INFORMATION

2.1. Lead DG, Decide Planning/CWP references

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

2.2. Organisation and timing

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

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

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

2.3. Consultation of the RSB

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

2.4. Evidence, sources and quality

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

[3] COM(2016)205, 6 April 2016.
[4] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

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

3. ANNEX 3: STAKEHOLDER CONSULTATION

Consultation strategy

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

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

Formal consultation activities

Open public consultation

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

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

Stakeholder events

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

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

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

Tripartite discussions with the European Parliament and the Council

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

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

Stakeholder participation

As set out above, stakeholders directly consulted included:

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

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

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

Methodology and tools

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

Results

Public consultation

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

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

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

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

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

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

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

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

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

Inception impact assessment

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

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

Taking account of feedback received

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

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

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

4. ANNEX 4: WHO IS AFFECTED AND HOW?

4.1. Practical implications of the initiative

The practical implications are given by stakeholder group.

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

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

- Border management

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

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

- Migration and asylum management

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

- Law enforcement officers

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

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

- eu-LISA

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

- IT organisation in Member States

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

4.2. Summary of costs and benefits

4.1.1. Costs for option 2

The overview of costs is indicated below.

II. Overview of costs – Preferred option						
	Third-Country Nationals		***Member State Administrations***		***Central Administration***	
	One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
Direct costs						
CRSS	0	0	€0m	€0m.p.a.	€6.9m	€0.7m.p.a.
ESP	0	0	€15.m	€3.0m.p.a.	€12.0m	€2.2mp.a.
Shared BMS	0	0	€0m	€0m.p.a.	€29.6m	€2.9mp.a.
CIR	0	0	€15	€3.1	€7.	€1.5

			.3m	mp.a.	3m	m.p.a.
Total	***0***	***0***	***€30.3m***	***€6.1m.p.a.***	***€555.8m***	***€7.3mp.a.***
Indirect costs						
None						

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

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

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

4.1.2. Benefits for Option 2

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

I. Overview of Benefits for Option 2		
Description	***Amount***	***Beneficiary***
Direct benefits		
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
Indirect benefits		
None identified	-	-
Total	***€27,5m p.a. and €8m one-off***	

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

1. Reduced training costs — the ESP removes to a large extent the need for recurrent re-training of staff when central systems are modified. The estimate is made assuming an average of 200,000 persons each year, out of the total end-user population, trained in sessions of 10 persons each. The cost for each training session is estimated at €1.000. Total annual recurrent cost is therefore at least €20m per year. Reduced training costs are mainly the result of ESP and CIR as they can be seen as two 'layers' that hide the complexity of central systems to end-users.

2. Reduced cost of changes to national applications when the central system is modified — if the proposed solution were not implemented, each national system would incur a change when the ICD (interface control document) of the corresponding central application is changed. The assumption made based on the history of changes to the current systems is that on average each system incurs an update at least once per year whether the reason for the change is due to technical or functional evolutions. Each change represents a workload of one man-year per

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

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

Calculation assumptions

The size of end-user population having to be trained is estimated taking the number of end-users of border management systems in Schengen countries (about 1,5 million) and considering one out of seven needs to be retrained annually given changes to central systems. The training cost per person takes only the additional cost of actually organising and delivering the training and does include the foregone personnel cost of the attendants.

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

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

4.1.3. Cost-benefit for option 2

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

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

4.1.4. Costs for option 3

The overview of costs is indicated below.

II. Overview of costs – Preferred option						
	Third-Country Nationals		***Member State Administrations***		***Central Administration***	
	One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
Direct costs						
CRRS			€0m	€0m	€6.9m	€0.7m.p.a.
ESP	0	0	€18m	€3.6mp.a.	€14.3m	€2.7mp.a.
Shared BMS	0	0	€0m	€0mp.a.	€29.6m	€2.9mp.a.

CIR	0	0	€22.5m	€4.5m.p.a.	€12.2m	€2.2mp.a.
MID	0	0	€45.0m	€9.0m.p.a.	€15.4m	€2.9mp.a.
MID link validation	0	0	€0m	€0mp.a.	€5.9m	€0mp.
Total	***0***	***0***	***€85.5m***	***€17.1m.p.a.***	***€84.3m***	***€11.4mp.a.***
Indirect costs						
None						

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

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

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

4.1.5. Benefits for Option 3

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

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

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

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

1. Reduced training costs — same as for option 2.
2. Reduced cost of changes to national applications when the central system is modified —. same as for option 2.
3. Cost saving of having one central shared - same as for option 2.
4. Saved cost of identification of multiple identities — the MID and CIR (based on a shared BMS) will enable a systematic identification of multiple identities. The estimate is that at least 500,000 third-country nationals use multiple identities for various reasons. To detect and handle each case of multiple identities with current means, an estimated 4 hours of work would be required valued at €25 per hour. The estimated value of the automated system therefore amounts to at least €50m per year for the EU. The benefit can only be achieved when MID, CIR and the shared BMS are implemented.

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

Calculation assumptions

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

4.1.6. Cost-benefit for option 3

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

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

5. ANNEX 5 – SUPPORTING STUDIES

5.1. European search portal

Executive summary of the technical study on the European search portal[6]

Introduction

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

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

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

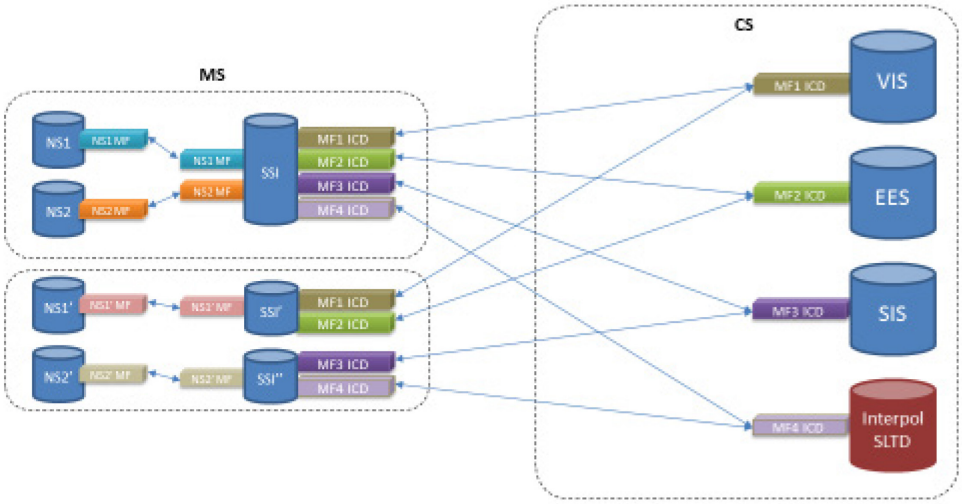


Fig. 1 - ESP problem representation

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

[6] Feasibility Study on the European Search Portal: ESP Feasibility Study Report – September 2017.
[7] Hereafter we use CS to refer to all centralised systems of eu-LISA, Europol and Interpol.

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

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

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

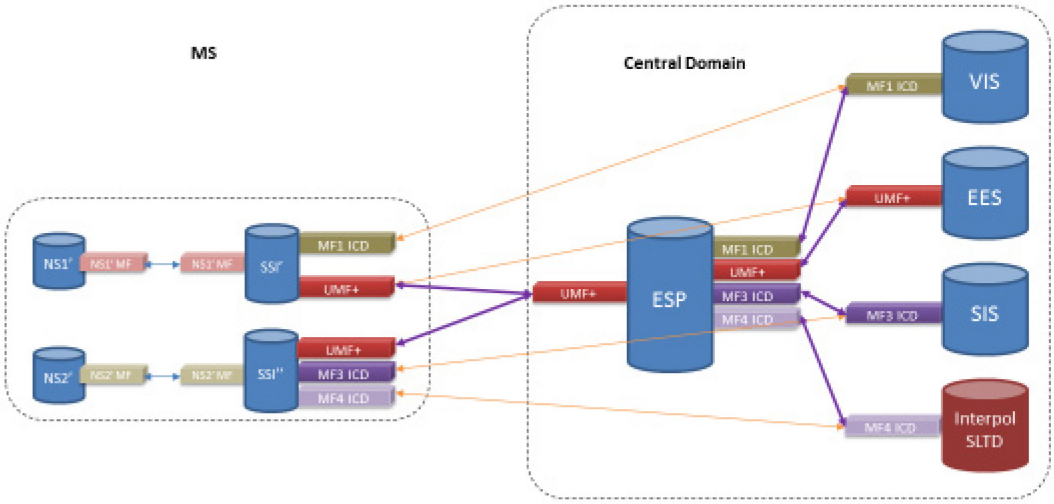


Fig. 2 - ESP implementation from MS Perspective

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

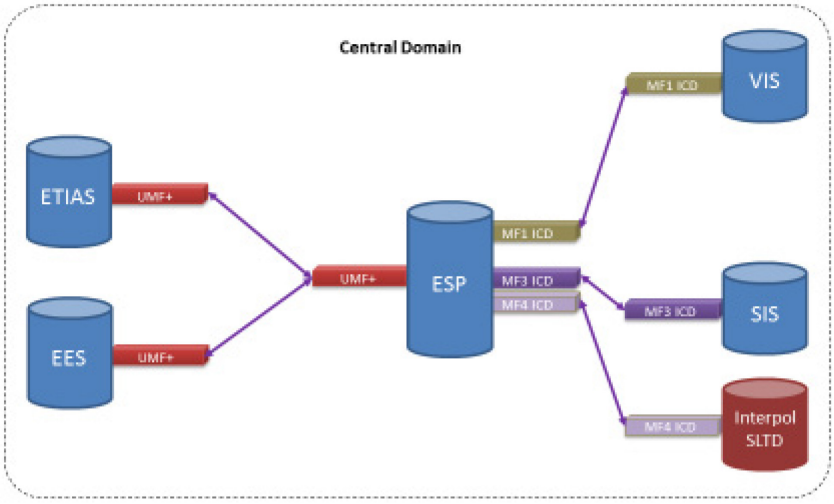


Fig. 3 - ESP implementation from a CS perspective

As-Is Analysis

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

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

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

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

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

Requirement/Use-cases

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

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

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

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

Architecture

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

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

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

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

[9] UMF is a specification for the exchange of information of interest to Law Enforcement organizations.

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

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

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

Practical Implementations

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

Implementation Considerations

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

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

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

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

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

Conclusion

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

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

5.2. Shared biometric matching service

Summary to be available mid-December.

5.3. Common identity repository

Executive summary to be available mid-December.

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

Schengen Information System (SIS)

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

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

Visa Information System (VIS)

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

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

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

[11] All, except Ireland, Cyprus, Croatia.
[12] Switzerland, Liechtenstein, Norway, Iceland.
[13] This rule is subject to change as envisaged by Commission proposal COM/2015/0670 on the amendment of the Schengen Borders Code.

Eurodac

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

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

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

Entry/Exit System

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

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

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

European Travel Information and Authorisation System

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

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

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

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

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

European Criminal Records Information System (ECRIS)

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

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

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

Europol data

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

Information exchange is channelled using the SIENA[15] platform, which is a secure electronic communication network between Europol, the liaison offices, the Europol

[15] Secure Information Exchange Network Application.

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

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

Stolen and Lost Travel Documents (SLTD)

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

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

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

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

Schengen Information System **both for EU and third-country nationals** **primary objective: both border management and law enforcement**		**Other systems** **only for third-country nationals** **primary objective: border / migration / asylum management** **secondary (ancillary) objective: law enforcement**				**Other systems** **only for third-country nationals** **primary objective: judicial cooperation**
	SIS (new*)	**VIS**	**EURODAC (new*)**	**EES**	**ETIAS (proposal)**	**ECRIS-TCN (proposal)**
Identity data recorded in system	- Biographic data - Passport/ID card details - Fingerprints - Palm prints* - Photographs - Facial images*	- Biographic data - Passport details - Fingerprints (10) - Facial images - Visa status	- Biographic data* - Passport/ID card details** (where available) - Fingerprints (10) - Facial images*	- Biographic data - Passport details - Fingerprints (4) - Facial images	- Biographic data - Passport details - Travel authorisation status - IP address	- Biographic data - Fingerprints (10) - Facial images
Additional categories of information held by system	- Refusal of Entry and stay - European Arrest warrant - Missing persons/ children at risk of parental abduction - Requested to assist in judicial criminal procedure - Persons and objects for discreet/inquiry*/ specific check - Objects which are lost/stolen/sought as evidence - Unknown wanted persons* - Return decisions*	- 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.	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	- 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 ETIAS watch list and Interpol system).	- Convicting Member State (including a reference number and the code of the convicting MS)

Schengen Information System **both for EU and third-country nationals** **primary objective: both border management and law enforcement**		**Other systems** **only for third-country nationals** **primary objective: border / migration / asylum management** **secondary (ancillary) objective: law enforcement**				**Other systems** **only for third-country nationals** **primary objective: judicial cooperation**
	SIS (new*)	**VIS**	**EURODAC (new*)**	**EES**	**ETIAS (proposal)**	**ECRIS-TCN (proposal)**
Possible actions by users of system	- Search alphanumeric data (biographic and/or passport/ID) - Search fingerprints - Search palm prints*[17] - Search facial images* - Create/Update/Delete	- Search alphanumeric data (biographic and/or passport) - Verify/Search fingerprints - Link records - Create/Update/Delete applications	- Search alphanumeric data (for law enforcement authorities) **[18] - Search fingerprints - Search facial image* - Take/Transmit/Update/ Delete	- Search alphanumeric data (biographic and/or passport) - Verify/ Search fingerprints - Verify / Search facial-images - Link records - Create/Update/Delete	- Search alphanumeric data (biographic and/or passport) - Process travel authorisation application - Create/Update/Delete	- Search alphanumeric data - Verify/ Search fingerprints - Create/update/delete
Purpose of access **Border control[19]**	*Access to categories of information*: **all** *Possible actions*: **all**	*Access to categories of information*: **all** *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints	*Access to categories of information*: **all** *Possible actions*: - Search fingerprints - Search facial image - Take/Transmit biometric data	*Access to categories of information*: **all** *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints - Verify facial images - Create/Update/Delete	*Access to categories of information*: - Travel authorisation status (ok/not ok) *Possible actions*: - Search alphanumeric data	**No access** (where appropriate, ECRIS-TCN can inform decisions on inclusion of alerts in the SIS).

* COM proposals.
** As proposed in Council Document 10079/17 (mandate for negotiations with the parliament).
[19] In the case of Eurodac the access for border control purposes refers to a situation of irregular crossing of the external border.

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

Schengen Information System **both for EU and third-country nationals** **primary objective: both border management and law enforcement**		**Other systems** **only for third-country nationals** **primary objective: border / migration / asylum management** **secondary (ancillary) objective: law enforcement**				**Other systems** **only for third-country nationals** **primary objective: judicial cooperation**
	SIS (new*)	**VIS**	**EURODAC (new*)**	**EES**	**ETIAS (proposal)**	**ECRIS-TCN (proposal)**
Purpose of access **Issuance of ETIAS authorisation**	*Access to categories of information*: - Refusals of entry and stay - Lost, stolen or invalidated travel documents - European Arrest Warrants *For information also*: - Missing persons/ children at risk of parental abduction - Requested to assist in judicial criminal procedure - Persons and objects for discreet/inquiry/ specific check - Objects which are lost/stolen/sought as evidence - Unknown wanted persons - Return decisions *Possible actions*: - Search alphanumeric data NB: access and actions are indirect, via ETIAS Central System	*Access to categories of information*: - Refusals, revocation and annulments of short stay visas *Possible actions*: - Search alphanumeric data NB: access and actions are indirect, via ETIAS Central System	*Access to categories of information*: - Return decisions or removal orders[20] *Possible actions*: - Search alphanumeric data NB: access and actions are indirect, via ETIAS Central System	*Access to categories of information*: - Refusal of entry data - Persons overstaying *Possible actions*: Search alphanumeric data NB: access and actions are indirect, via ETIAS Central System	*Access to categories of information*: **all** Possible actions**: all**	Not foreseen under ECRIS-TCN proposal

[20] According to the Eurodac proposal this information will not be recorded in that system.

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

[21] Teams of EBCG staff involved in return-related tasks, and members of the migration management support teams.

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

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

[22] Council Document 10079/17 (mandate for negotiations with the parliament) proposes to delete VIS.
[23] However, not applied in practice to date.

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

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

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

[24] Teams of Member State asylum experts deployed by EASO.

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

8. ANNEX 8 - SUPPLEMENTARY ANALYSIS & INFORMATION

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

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

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

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

ESP

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

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

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

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

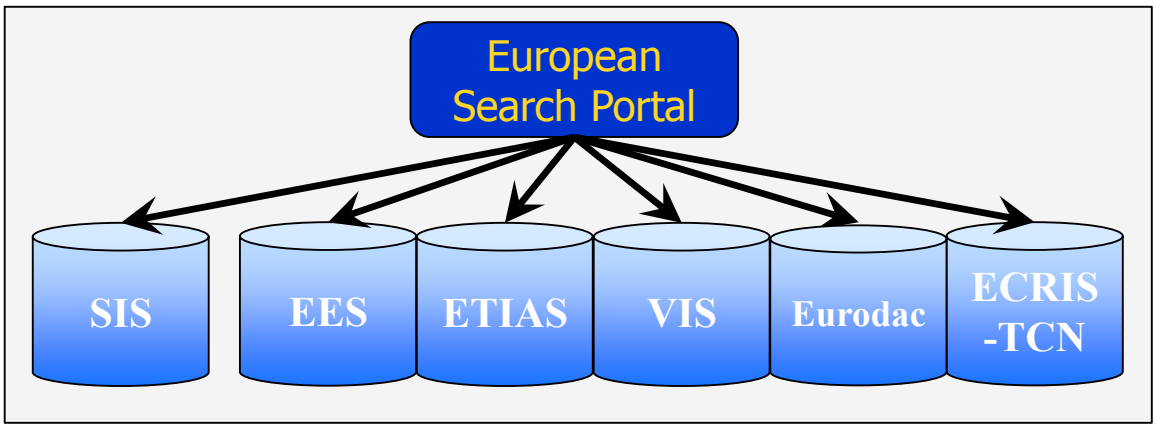
The ESP is not a 'system': it does not handle any new data, and it does not store any data; it only acts as a single window or 'message broker' to search various central systems and

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

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

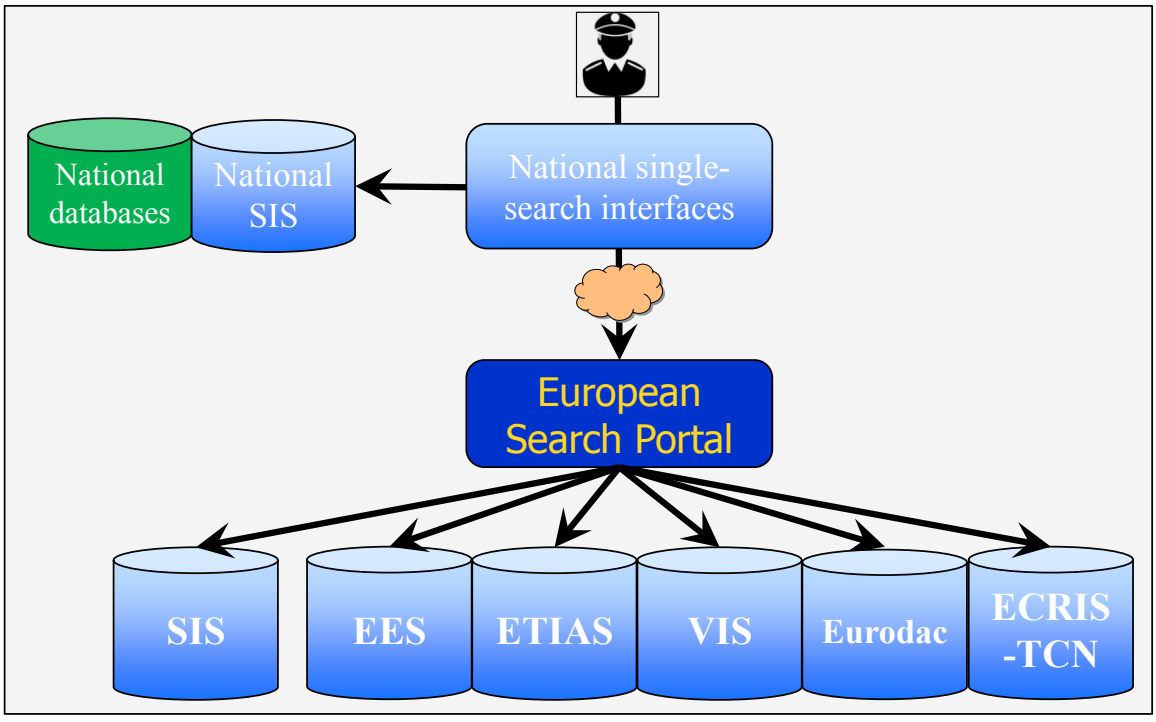
Establishing the ESP was one of the options identified in the April 2016 Communication to achieve interoperability (under the label 'single-search interface'), confirmed by the high-level expert group as regards its necessity and technical feasibility and that it should comply with data protection requirements,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

Figure 1 - European search portal



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

Figure 2 - ESP and national interfaces



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

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

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

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

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

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

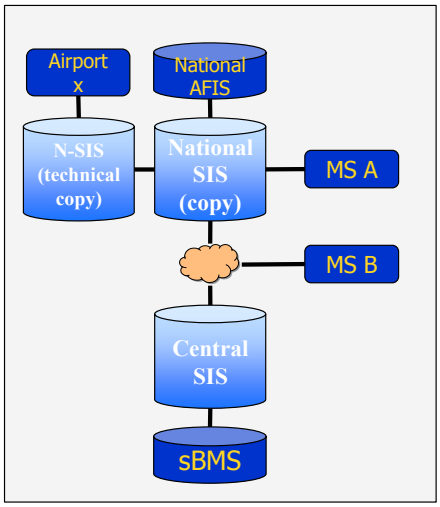
The ESP will, as a minimum, be capable of searching Eurodac, VIS, EES and the proposed ETIAS. In addition, the following other possibilities are being considered.

8.1.1. ESP with or without SIS data

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

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

Figure 3 - The SIS technical architecture



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

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

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

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

8.1.2. Access Interpol and Europol data: extend the ESP

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

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

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

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

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

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

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

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

Example

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

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

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

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

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

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

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

Extending ESP towards Europol data

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

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

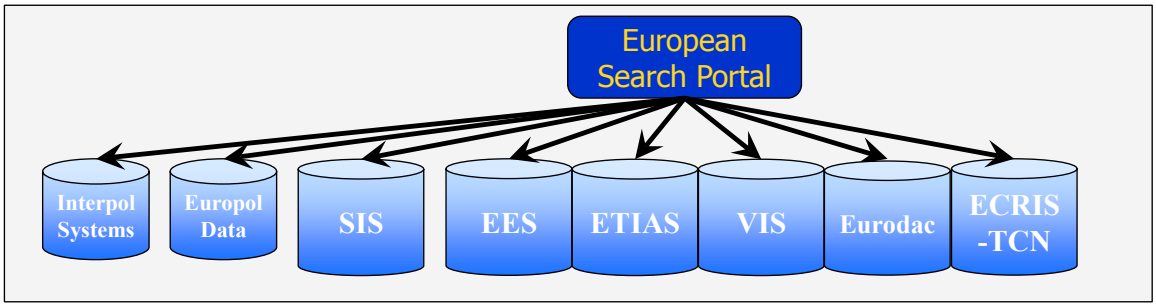
Europol indicated that the QUEST interface can indeed be made available towards Basic Protection Level data. This would enable a technical and legal usage of an ESP with the QUEST interface.

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

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

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

Figure 4 – Extending ESP to Europol and Interpol data



[26] QUerying Europol SysTems.

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

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

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

8.1.4. ESP with or without shared BMS

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

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

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

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

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

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

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

Technical facilitation and simplification through the ESP

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

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

Introduction of the ESP requires the use of a new interface (interface control document (ICD)) using the concepts of Universal Message Format projects[28].

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

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

Conclusion

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

The ESP will not extend or change existing access rights.

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

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

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

[28] Existing UMF description would need to be extended; the term UMF+ can be used to this end.

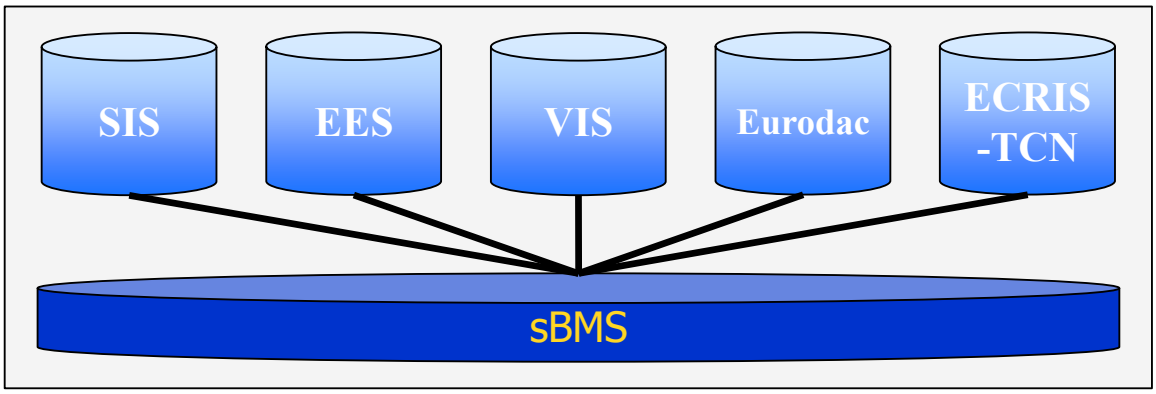
8.2. Detailed analysis of the shared biometric matching service

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

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

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

Figure 5 - Shared biometric matching service



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

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

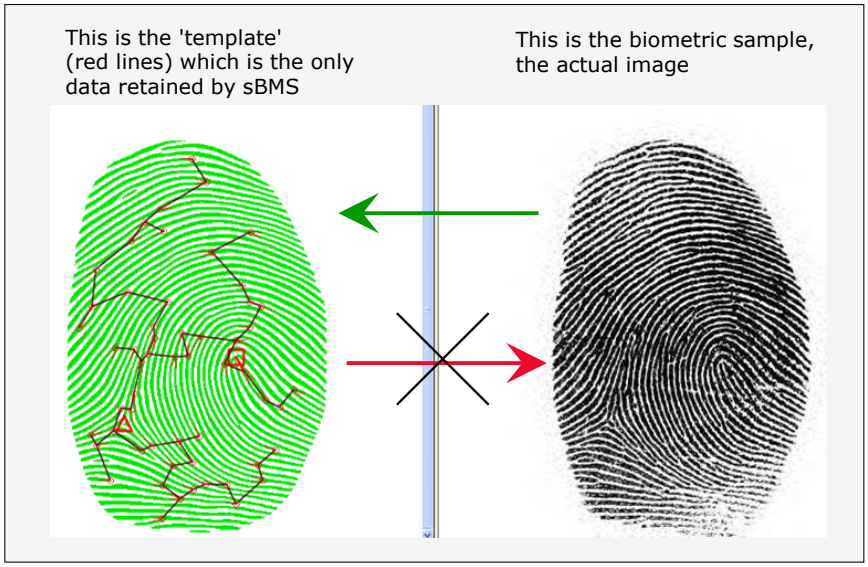
The biometric data (fingerprint and facial images) are fully retained by the central systems. The shared BMS creates a mathematical representation[30] of the samples (a

[29] These biometric search engines are technically referred to as automated fingerprint identification system (AFIS) or automated biometric identification system (ABIS).

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

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

Figure 6 - Template of fingerprint



Samples and templates

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

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

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

- The 4 flat fingerprints of EES would also search the rolled fingerprints in SIS and the 10 flat fingerprints in VIS.

- The 10 rolled fingerprints of an asylum seeker would also search the rolled fingerprints of SIS and the 10 flat fingerprints in VIS.

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

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

8.3. Detailed analysis of the common identity repository

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

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

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

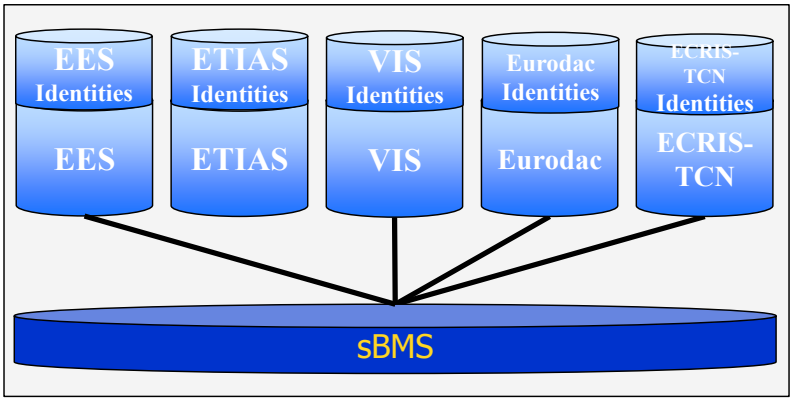
The CIR provides a unified view on a subset of biographical identity data[31] of third-country nationals that will be present (or are present) in Eurodac, VIS, EES, the proposed ETIAS and the proposed ECRIS-TCN system.

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

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

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

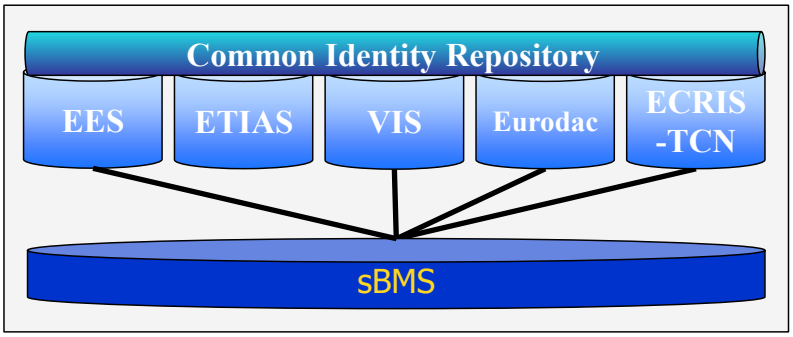
Figure 7 – Biographical identities in each system versus shared BMS



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

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

Figure 8 - Common identity repository



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

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

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

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

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

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

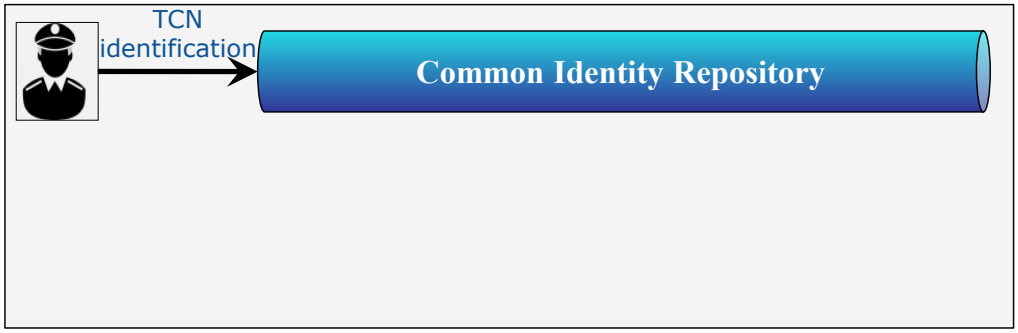
[32] EES and the proposed ETIAS would provide one single engine as they will have a common repository.
[33] Subset limited to the data that can be found in the travel document.

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

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

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

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



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

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

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

Table 1 - Identification of third-country nationals

	VIS	Eurodac (new)[34]	EES	ETIAS (proposal)	ECRIS-TCN (proposal)
	Identity data (accessible)				
Purpose of access **Police checks identification or verification of identity (in territory)** **direct access to identity data** **Through common identity repository**	- Biographical data - Passport details - Fingerprints (10) - Facial images	- Biographical data - Passport - Fingerprints (10) - Facial images	- Biographical data - Passport details - Fingerprints (4) - Facial images	- Biographical data - Passport details	- Biographical data - Fingerprints (10) - Facial images
	Additional information (not accessible)				
	- Visa status - Issued, refused, discontinued, extended, revoked or annulled single/double/multiple entry visa - Authority where visa application was lodged; - Background information: Member State(s) of destination, purpose of travel, intended date of arrival and intended stay, applicant's home address, occupation and employer etc. - (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 ETIAS watch list and Interpol system)	- Convicting Member State (including a reference number and the code of the convicting Member State)

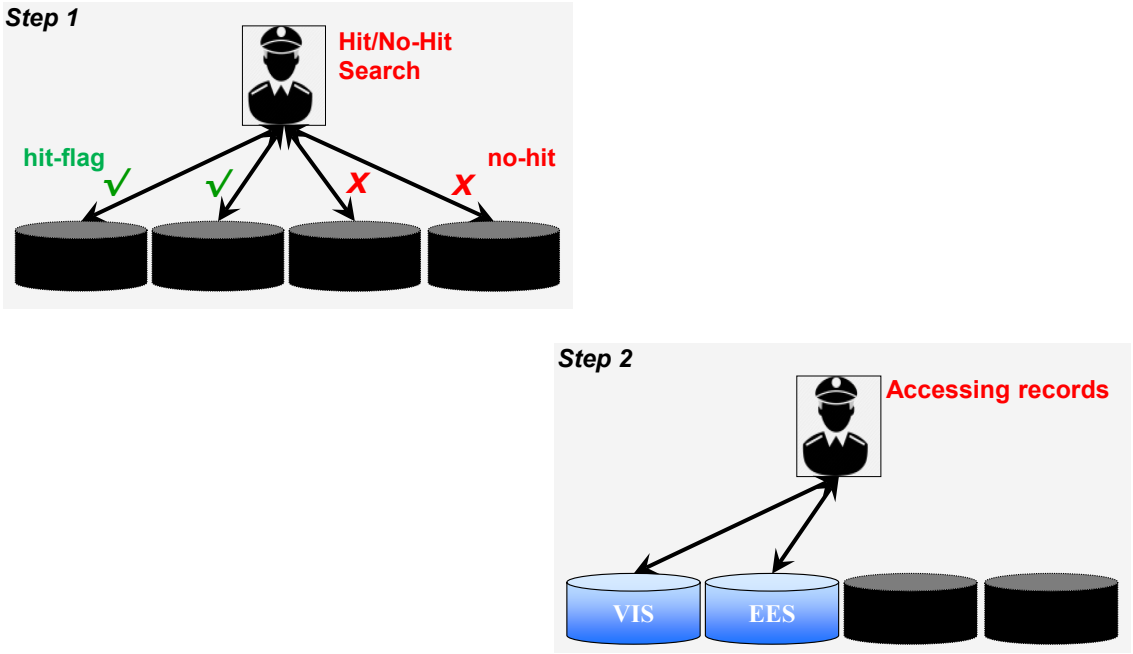
[34] Eurodac (new) refers to the proposed inclusion of biographical identity data in EURODAC, necessary to allow identification of persons.

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

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

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

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



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

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

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

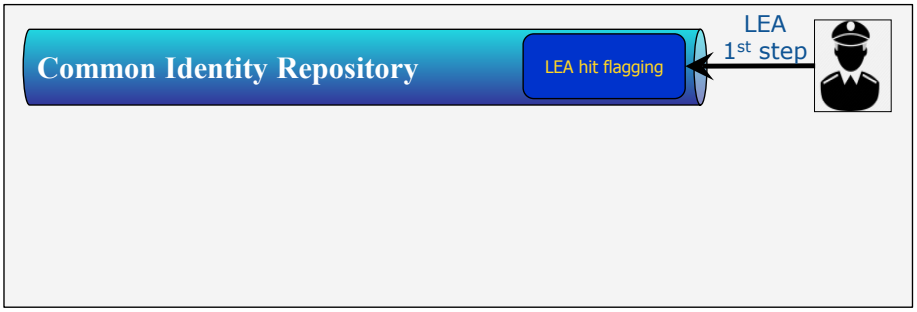
[35] The shared BMS will generate matching scores between 0 and 100 on each candidate in the candidate list, the highest score indicating the highest probability that the latent fingerprint belongs to that person.

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

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

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

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



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

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

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

Table 2 - Flagging for law enforcement purposes[36]

Purpose of access			
Prevention, detection and investigation of terrorist offences and other serious criminal offences			
Step 1: direct access to flags– through Common Identity Repository **Step 2: access to additional information (identity data + additional information) in flagged systems, in accordance with the legal bases of those systems**			
Flag indicating the system (accessible in step 1)			
VIS	**EURODAC (new*)**	**EES**	**ETIAS (proposal)**
Data on the third country national (accessible in step 2)			
- Biographic data - Passport details - Fingerprints (10) - Facial images - 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 case of families or groups): links between applications; - History of applications of person.	- Biographic data - Passport - Fingerprints (10) - Facial images* - 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	- Biographic data - Passport details - Fingerprints (4) - Facial images - Entry data - Exit data - Refusal of entry data - Remaining authorised stay - List if persons overstaying - Statistics on persons overstaying	- Biographic data - Passport details - 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 ETIAS watch list and Interpol system).

[36] Eurodac (new) refers to the proposed inclusion of biographical identity data in Eurodac, necessary to allow identification of persons.

8.4. Detailed analysis of the multiple-identity detector

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

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

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

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

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

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

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

Examples of links

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

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

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

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

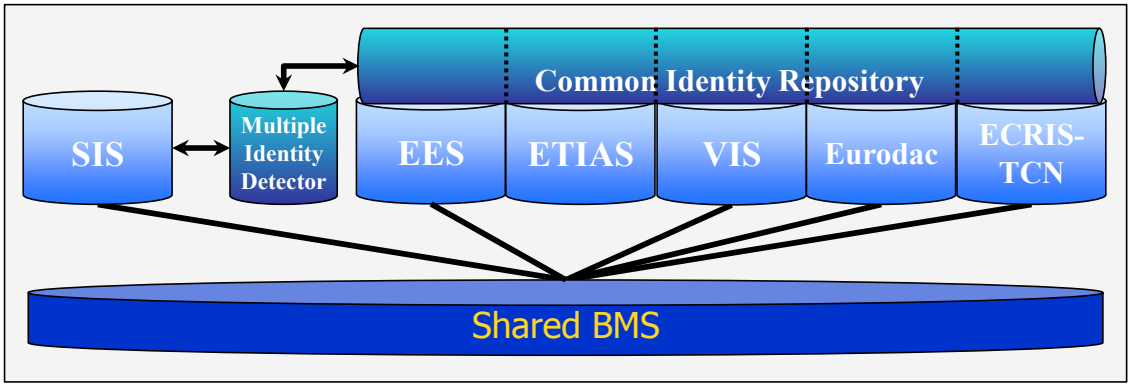
passport expired. Person D is registered in EES where the biometric data matches against the visa-record. The MID will show white links between the identity in VIS and the identity in EES.

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

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

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

Figure 12 - Multiple-identity detector



Examples

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

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

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

8.1.7. MID with SIS data

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

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

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

1) disambiguation of multiple biographical identities;

2) addressing identity fraud.

Examples

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

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

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

8.1.8. MID with the proposed ECRIS-TCN data

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

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

8.1.9. MID with cross-matching existing data

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

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

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

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

The fingerprint identification team

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

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

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

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

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

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

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

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