Council of the European Union

Brussels, 7 April 2016
(OR. en)

7644/16

JAI 257
COSI 51
FRONT 159
ASIM 49
DAPIX 49
ENFOPOL 86
SIRIS 61
DATAPROTECT 23
VISA 90
FAUXDOC 9
COPEN 96

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	6 April 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2016) 205 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Stronger and Smarter Information Systems for Borders and Security

Delegations will find attached document COM(2016) 205 final.

Encl.: COM(2016) 205 final

EUROPEAN
COMMISSION

Brussels, 6.4.2016
COM(2016) 205 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Stronger and Smarter Information Systems for Borders and Security

1. INTRODUCTION

Europe is a mobile society. Millions of EU citizens and third-country nationals cross internal and external borders every day. In 2015, more than 50 million non-EU nationals visited the EU, accounting for more than 200 million border crossings at the external borders of the Schengen area.

Beyond these regular travel flows, in 2015 alone, conflict in Syria and crises elsewhere triggered 1.8 million irregular border crossings at Europe's external borders. EU citizens expect external border controls on persons to be effective, to allow effective management of migration and to contribute to internal security. The terrorist attacks in Paris in 2015 and in Brussels in March 2016 bitterly demonstrated the ongoing threat to Europe's internal security.

Both elements brought into sharper focus the need to join up and strengthen the EU's border management, migration and security cooperation frameworks and information tools in a comprehensive manner. Border management, law enforcement, and migration control are dynamically interconnected. EU citizens are known to have crossed the external border to travel to conflict zones for terrorist purposes and pose a risk upon their return. There is evidence that terrorists have used routes of irregular migration to enter the EU and then moved within the Schengen area undetected.

The European Agendas on Security and on Migration have set the direction for the development and implementation of EU policy to address the parallel challenges of migration management and the fight against terrorism and organised crime. This Communication builds on the synergies between these two Agendas and is intended as a starting point for a discussion on how existing and future information systems could enhance both external border management and internal security in the EU. It is complementary to the December 2015 proposal on the creation of a European Border and Coast Guard and the improvement of crisis prevention and intervention at the external borders.

There are a number of information systems at EU level that provide border guards and police officers with relevant information on persons, but the EU data management architecture is not perfect. This Communication sets out some possible options for maximising the benefits of existing information systems and, if necessary, developing new and complementary actions to address gaps. It also highlights the need to improve the interoperability of information systems as a long-term objective, as also identified by the European Council and the Council,[1] and presents ideas on how information systems can be developed in the future to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.

Any future initiative would be prepared on the basis of better regulation principles with public consultation and assessment of the impacts, including as concerns fundamental rights and in particular the right to the protection of personal data.

[1] Conclusions of the European Council meeting of 17 and 18 December 2015; Joint Statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016 (24 March 2016); Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism (20 November 2015).

2. CHALLENGES TO BE ADDRESSED

The absence of internal borders in the Schengen area requires strong and reliable management of the movement of persons across the external borders. This is a prerequisite to ensure a high level of internal security and the free movement of persons within that area. At the same time, the absence of internal borders means that law enforcement authorities in the Member States also have access to relevant data on persons. There are a number of information systems and databases at EU level that provide border guards, police officers and other authorities with relevant information on persons, in accordance with their respective purposes.[2]

However, there are also shortcomings related to information systems that impede the work of these national authorities. Better information exchange was therefore highlighted as a key priority in the European Agenda on Security. The main shortcomings are: (a) sub-optimal functionalities of existing information systems, (b) gaps in the EU's architecture of data management, (c) a complex landscape of differently governed information systems, and (d) a fragmented architecture of data management for border control and security.

The existing information systems in the EU for border management and internal security cover a wide range of functionalities. Nevertheless, there are still **shortcomings in the functionalities of existing systems**. When looking at border control processes applicable to different categories of travellers, it becomes clear that there are shortcomings in some of these processes and between the respective information systems used for border controls. Likewise, the performance of existing tools for law enforcement needs to be optimised. This calls for consideration of action to improve existing information systems (section 5).

Moreover, there are **gaps in the EU's architecture of data management**. Issues remain for border controls of specific categories of travellers, such as third country nationals holding a long-term visa. Also, there is an information gap prior to arrival at the borders as concerns third-country nationals who are exempt from holding a visa. Consideration should be given to whether there is a need to address these gaps by developing additional information system where necessary (section 6).

Border guards and notably police officers face a **complex landscape of differently governed information systems** at EU level. This complexity creates practical difficulties specifically as to which databases should be checked in a given situation. Moreover, not all Member States are connected to all existing systems.[3] The current complexity of acceding information systems at EU level could be reduced by establishing a single search interface at national level which respects the different purposes for access (section 7.1).

---

[2] See section 4 for an overview of information systems for border and security, and annex 2 for a more detailed inventory.

[3] Subject to the specific terms of Protocol 22 as concerns Denmark and Protocol 21 and 36 as concerns the United Kingdom and Ireland and the respective Acts of Accession.

The current EU's architecture of data management for border control and security is marked by **fragmentation**. This is caused by the various institutional, legal and policy contexts in which the systems have been developed. Information is stored separately in various systems that are rarely inter-connected. There is inconsistency between databases and diverging access to data for relevant authorities. This can lead to blind spots notably for law enforcement authorities, as it may be very difficult to recognise connections between data fragments. It is therefore necessary and urgent to work towards integrated solutions for improved accessibility to data for border management and security, in full compliance with fundamental rights. For that, there is a need to initiate a process towards the interoperability of existing information systems (section 7).

3. FUNDAMENTAL RIGHTS

Full respect of fundamental rights and data protection rules is an essential precondition to addressing any of the above challenges.

Compliance with fundamental rights requires well-designed and correctly-used technology and information systems. Technology and information systems can help public authorities to protect the fundamental rights of citizens. Biometric technology can reduce the risk of mistaken identities, and of discrimination and of racial profiling. It can also contribute to addressing protection risks for children such as children going missing or falling victims of trafficking, provided it goes hand in hand with Fundamental Rights safeguards and protection measures. It can reduce the risk of people being wrongfully apprehended and arrested. It can also contribute to increasing the security of citizens residing in the Schengen area as it will help in the fight against terrorism and serious crime.

The existence of large-scale information systems also implies potential privacy risks, which need to be anticipated and addressed appropriately. The collection and use of personal data in these systems has an impact on the right to the privacy and the protection of personal data, enshrined in the Charter of Fundamental Rights of the European Union. All systems need to comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data. Safeguards must be in place to ensure the rights of the data subjects in relation to the protection of their private life and personal data. Data should only be retained for as long as necessary for the purpose for which they were collected. Mechanisms ensuring an accurate risk management and effective protection of data subjects' rights need to be foreseen.

In December 2015 the co-legislators reached a political agreement on the Data Protection reform. Once adopted, the new General Data Protection Regulation and the Data Protection Directive for police and criminal justice authorities[4] will become applicable in 2018 and will provide a harmonised framework for the processing of personal data.

[4] See http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

Purpose limitation is a key principle of data protection as enshrined in the Charter of Fundamental Rights. Due to the different institutional, legal and policy contexts in which information systems at EU level were developed, the principle of purpose limitation was implemented through a compartmentalised structure of information management.[5] This is one of the reasons for the current fragmentation in the EU's architecture of data management for border control and internal security. With the new comprehensive framework for the protection of personal data in the EU in place and significant developments in technology and IT security, the principle of purpose limitation can be more easily implemented at the level of access and use to data stored, in full compliance with the Charter of Fundamental Rights and with recent European Court of Justice's jurisprudence. Safeguards such as compartmentalising data within one system and specific access and use rules for each category of data and user should ensure the necessary purpose limitation in integrated solutions for data management. This opens a way towards the interoperability of information systems accompanied by the necessary strict rules on access and use without affecting the existing purpose limitation.

'Data protection by design' and 'Data protection by default' are now principles of EU data protection rules. When developing new instruments that rely on the use of information technology, the Commission will seek to follow this approach. This implies embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a specified purpose and granting data access only to those entities that 'need to know.'[6]

The requirements of the Charter of Fundamental Rights and in particular the new Data Protection reform instruments will guide the Commission in addressing the current gaps and shortcomings in the EU's architecture of data management for border control and security. This will ensure that further development of information systems in these areas will be in line with the highest standards of data protection, and that they will respect and contribute to fundamental rights as guaranteed by the Charter of Fundamental Rights.

---

5 COM(2010) 385 final.

6 For a comprehensive description of 'privacy by design,' see the Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, European Data Protection Supervisor, 18.3.2010.

4. OVERVIEW OF INFORMATION SYSTEMS FOR BORDERS AND SECURITY[7]

The existing information systems in the EU for border management and internal security each have their own objectives, purposes, legal bases[8], user groups and institutional context. Together they provide a complex pattern of relevant databases.

The three main **centralised information systems** developed by the EU are (i) the Schengen Information System (SIS) with a broad spectrum of alerts on persons and objects, (ii) the Visa Information System (VIS) with data on short-stay visas, and (iii) the EURODAC system with fingerprint data of asylum applicants and third-country nationals who have crossed the external borders irregularly. These three systems are complementary, and – with the exception of SIS – primarily targeted at third-country nationals. The systems also support national authorities in fighting crime and terrorism[9]. This applies in particular to the SIS as the most widely-used information-sharing instrument today. Information exchange for these systems is carried out in a secured dedicated communication infrastructure called sTESTA[10].

In addition to these existing systems, the Commission proposes to establish a fourth centralised border management system, the **Entry-Exit System** (EES)[11], which is expected to be implemented by 2020, again addressing third-country nationals.

---

7 See Annex 2 for an inventory of existing information systems for border management and law enforcement.

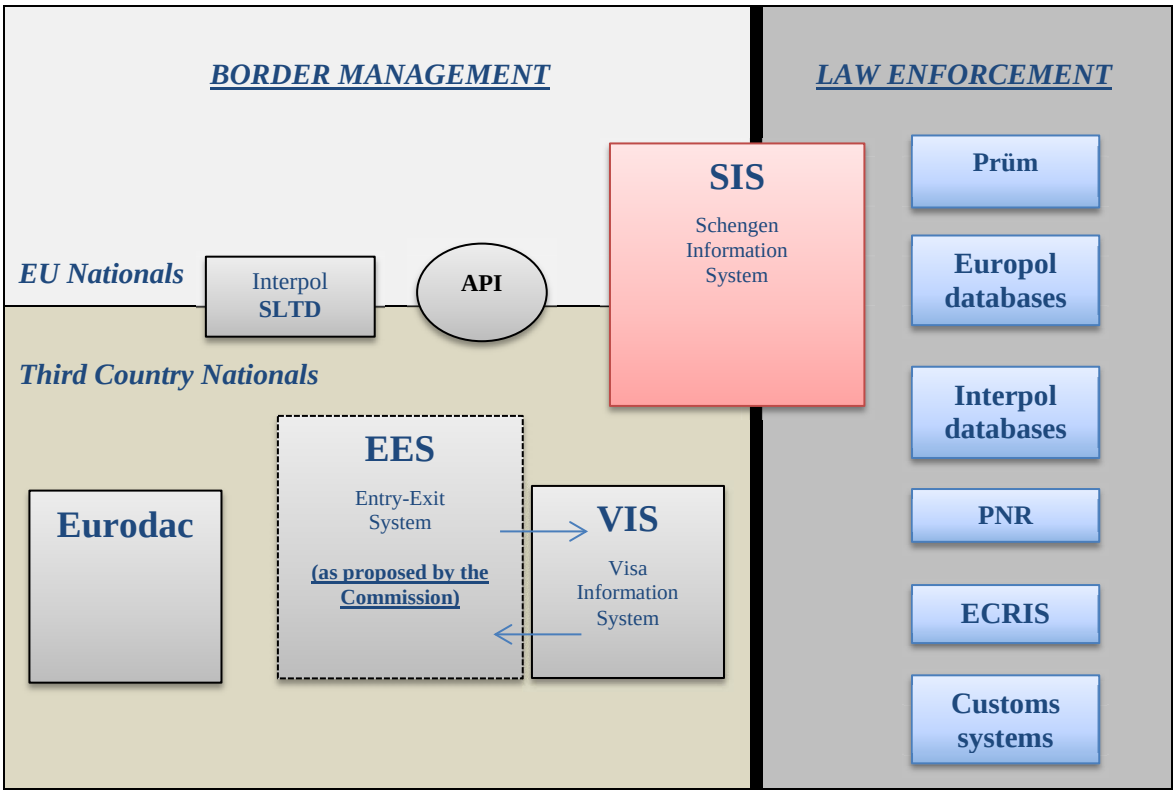
8 Subject to the specific terms of Protocol 22 as concerns Denmark and Protocol 21 and 36 as concerns the United Kingdom and Ireland.

9 Law enforcement access to VIS and EURODAC can be exercised under limited conditions due to the fact that law enforcement is an ancillary objective of those systems. Concerning VIS, Member States have to designate an authority responsible for controlling law enforcement access and the police must provide evidence that their access is necessary for criminal investigations. Concerning EURODAC, the investigative authority needs to search the national AFIS, Prüm and the VIS before being given access to EURODAC.

10 Soon to be replaced by TESTA-NG.

11 COM(2016)194 final.

Figure 1 *Schematic overview of the main information systems for border management and law enforcement:*



Additional existing instruments for border management are Interpol's Stolen and Lost Travel Documents (SLTD) database and the Advance Passenger Information (API) that collects information on passengers ahead of inbound flights to the EU. These instruments are relevant to both EU citizens and third country nationals.

Specifically for law enforcement, criminal investigation and judicial cooperation purposes, the EU developed **decentralised tools for information exchange**, namely (i) the Prüm framework to exchange DNA, fingerprints and vehicle registration data, and (ii) the European Criminal Records Information System (ECRIS) to exchange national criminal record information. ECRIS enables the exchange of information, through a secured network, on previous convictions handed down against a specific person by criminal courts in the European Union. Requests are mainly based on alphanumeric identity information though the exchange of biometric data is possible.

Europol supports the exchange of information between national police authorities as the EU criminal information hub. The Europol Information System (EIS) provides a centralised criminal information database for Member States to store and query data on serious crime and terrorism. Focal Points at Europol provide subject-focused analysis work files with information on ongoing operations in Member States. Europol's Secure Information Exchange Network Application (SIENA) allows Member States to exchange information in a swift, secure and user-friendly way with each other, with Europol, or with third parties that have a cooperation agreement with Europol. At the same time, SIENA has a strong focus on interoperability with other systems at Europol, for instance to directly exchange data with Focal Points. It provides the possibility to feed Europol's databases with information that is being exchanged between Member States. SIENA should therefore be Member States' channel of first choice for law enforcement information sharing across the EU.

An additional set of personal data processing systems that will be developed across Member States is the **Passenger Name Records** (PNR).[12] PNR data consists of booking information provided at the time of booking and check-in.

Finally, **customs authorities** are also a crucial actor in the multi-agency cooperation at the external borders. They have various systems[13] and databases which contain data on movements of goods, identification of economic operators and risk-related information that can be used to reinforce internal security. These systems also have their own controlled, restricted and secure infrastructure (Common Communication Network), which has proven its viability. Synergies and convergence between information systems and their corresponding infrastructures for EU border management and for customs operations should be further explored.

5. IMPROVING EXISTING INFORMATION SYSTEMS

The existing information systems in the EU for border management and internal security cover a wide range of functionalities. However, there are still **shortcomings** in the systems that need to be addressed in order to optimise their performance.

Schengen Information System (SIS)

Border checks against the **Schengen Information System** (SIS) currently take place on the basis of alphanumeric searches (i.e. name and date of birth). Fingerprints can only be used to verify and confirm the identity of a person who has already been identified on the basis of his/her name. This security gap allows persons subject to an alert to use fraudulent documents to escape from an exact match in SIS.

This critical weakness will be addressed by adding a fingerprint search functionality to the SIS through an **Automated Fingerprint Identification System (AFIS)**, as foreseen by the existing legal framework[14]. The AFIS should be operational by mid-2017[15]. Once developed, the AFIS will be accessible by Europol and will thereby complement Europol's systems for criminal investigation and counter-terrorism, as well as fingerprint exchanges performed under the Prüm framework. The Commission and eu-LISA will examine the potential for such wider use of the future AFIS.

---

12 See section 6.2.

13 The customs information systems include all systems created under the Community Customs Code (Regulation 2913/92) and future Union Customs Code (Regulation 952/2013), the Decision on a paperless environment for customs and trade (Decision 70/2008/EC) and the Customs Information system was established under the CIS Convention of 1995. Its aim is to assist in combating customs related crime by facilitating co-operation between European customs authorities.

14 Articles 22 (c) of Regulation (EC) No 1987/2006 of the European Parliament and the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision 533/2007/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4 and OJ L 2015, 7.8.2007 p.63).

15 In March 2016 the Commission has presented a report to the European Parliament and the Council on the availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II).

On the basis of the on-going evaluation and a technical study, the Commission is currently examining **possible additional functionalities of the SIS** with a view to presenting proposals to revise the legal basis of the SIS. Aspects under consideration include:

- the creation of SIS alerts on irregular migrants subject of return decisions;
- the use of facial images for biometric identification, in addition to fingerprints;
- the automatized transmission of information on a hit following a check;
- the storing of hit information on discreet and specific check alerts in the SIS Central System.
- the creation of a new alert category on 'Wanted Unknown Person' for which forensic data may exist in national databases (e.g. a latent print left behind at a crime scene)[16].

The Commission will continue to support with EU funding the implementation of projects that enable simultaneous searches in SIS and Interpol's databases on Stolen and Lost Travel Documents (SLTD) and wanted criminals, vehicles or firearms (iARMS) that are complementary with EU information systems.[17]

Interpol's database on Stolen and Lost Travel Documents (STLD)

It is of key importance for effective border management that the travel documents of all third-country nationals and EU citizens are verified against the **SLTD database**. Law enforcement authorities should also use the SLTD database for queries within the Schengen area. Following the terrorist attacks in Paris on 13 November 2015, the Council called for electronic connections to the relevant Interpol databases at all external border crossing points and automatic screening of travel documents by March 2016.[18] All Member States should establish the relevant electronic connections and put in place systems allowing the automatic update of data on stolen or lost travel documents in the SLTD database.

Advance Passenger Information (API)

In line with existing best practice, Member States should also increase the added-value of **Advance Passenger Information** (API) data by establishing automated cross-checking of this data against SIS and Interpol's SLTD database. The Commission will assess the need to revise the legal basis for the processing of API data to ensure wider implementation, and to include an obligation for Member States to require and use API data for all inbound and outbound flights. This is particularly relevant in the context of the implementation of the future Passenger Name Records Directive, as a combined use of PNR and API data further enhances the effectiveness of PNR data in the combating of terrorism and serious crime.[19]

---

16 The creation of this new alert will be assessed with a view to seek complementarity and avoid overlap with the existing Prüm framework for searching fingerprints in the different national databases of EU Member States.

17 Information search tools developed by Interpol, such as the Fixed Interpol Networked Database (FIND) and the Mobile Interpol Networked Database (MIND), aim to facilitate simultaneous searches in the Interpol systems and in SIS.

18 Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, 20 November 2015.

19 See section 6.2 on the proposed Passenger Name Record Directive.

Visa Information System (VIS)

The Commission is also in the process of conducting an overall evaluation of the **Visa Information System** (VIS), due to be concluded in 2016. The evaluation looks at, among others, how the VIS is used for checks at the external borders and within the territory of Member States, and at how it contributes to the fight against identity and visa fraud. On this basis, the Commission will then examine the possibilities of enhancing the functionalities of the VIS, including by:

- improving the quality of facial images to enable biometric matching;
- using the biometric data of visa applicants to search in the future Automated Fingerprint Identification System to be developed for the SIS;
- reducing the age limit for collecting fingerprints of children between the age of 6 and 12 years old, whilst providing for robust Fundamental Rights safeguards and protection measures;[20]
- facilitating the checking of Interpol's SLTD database during a visa application.

As regards the possibilities under the existing legal framework to access VIS data for **law enforcement purposes**, Member States apply these possibilities in an uneven way. In this context, Member States have reported practical problems in the procedures to access the VIS by law enforcement authorities. Likewise, the implementation of access to EURODAC for law enforcement purposes is still very limited. The Commission will examine if there is a need to reconsider the legal framework for law enforcement access to VIS and EURODAC.

EURODAC

As set out in the Communication towards a reform of the Common European Asylum System and Enhancing Legal Avenues to Europe[21], the Commission will present a proposal to reform **EURODAC** to further enhance its functionalities as regards irregular migration and return. This will address a current gap concerning the ability to track secondary movements of irregular migrants between Member States. Moreover, the proposal will seek to enhance the effectiveness of return and readmission procedures by providing means to identify and re-document irregular migrants for return purposes. In this context, the proposal will also cover exchange with third countries of information contained in EURODAC, bearing in mind the necessary data protection safeguards.

Europol

The EU has granted **Europol** access to the main central databases, but the Agency has not yet made full use of this opportunity. Europol has the right to access and search directly data entered into SIS for arrests, for discreet and specific check and for objects for seizure. So far Europol has carried out only a relatively limited number of searches in SIS. Access to the VIS for consultation has been legally possible for Europol since September 2013. Since July 2015 the legal basis of EURODAC allows access by Europol. The Agency should accelerate the on-going work to establish the connection to VIS and EURODAC. More generally, the Commission will assess if it is necessary to provide further access for other EU Agencies in the field of home affairs to information systems, notably for the future European Border and Coast Guard.

[20] As indicated as technically feasible in the JRC study 'Fingerprint Recognition for children"; EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013.

[21] COM(2016)197 final.

Prüm Framework

The **Prüm framework** is currently falling short of its potential. This is because not all Member States have implemented their legal obligations in terms of integrating the network with their own systems. Member States have received significant financial and technical support for its implementation, and should now fully implement the Prüm framework. The Commission is using the powers conferred upon it to ensure the full implementation of Member States' legal obligations and began a structured dialogue (EU Pilot) with Member States concerned in January 2016. Should the responses of Member States prove unsatisfactory, the Commission will not hesitate to launch infringement proceedings.

European Criminal Records Information System (ECRIS)

The European Criminal Records Information System **ECRIS** allows exchanging information on convictions concerning third country nationals and stateless persons, but there is no procedure in place to do so efficiently. In January 2016, the Commission adopted a legal proposal to address this lacuna.[22] In this context, the Commission proposed to enable national authorities to search for third-country nationals on the basis of fingerprints for more secure identification. The European Parliament and the Council should adopt the legislative text in 2016.

Horizontal issues

A general concern in relation to information systems is the **level of implementation** by Members States. The uneven implementation of the Prüm framework and the missing electronic connections to the SLTD database are striking examples for this. To enhance the level of implementation in relation to information systems, the Commission will closely monitor the performance of each Member State.[23] The monitoring will not only examine if Member States meet their legal obligations in the area of information systems, but also how they make use of existing instruments and if they follow best practices. The Commission will draw on various sources when monitoring and promoting the level of implementation, including notifications by Member States and the visits conducted under the Schengen Evaluation and Monitoring Mechanism.

Another general concern in relation to information systems is the **quality of inserted data**. If Member States do not respect minimum quality requirements, the reliability and value of the stored data becomes very limited, and the risk of mismatches and non-hits undermines the value of the very systems. In order to improve the quality of inserted data, eu-LISA will develop a **central monitoring capacity for data quality** for all systems under its competence.

[22] COM(2016) 7 final, 19.1.2016.

[23] Subject to the specific terms of Protocol 22 as concerns Denmark and Protocol 21 and 36 as concerns the United Kingdom and Ireland.

Most information systems in the area of border controls and security handle identification data coming from travel and ID documents. To enhance borders and security, beyond well-performing systems, travel and identity documents must be authenticated easily and securely. To that end, the Commission will present measures to enhance electronic **document security** and ID management and to strengthen the fight against document fraud. The interoperable levels of secure identification achievable through the eIDAS Regulation[24] could provide a possible means for this.

Actions to improve existing information systems

Schengen Information System (SIS)

- Commission and eu-LISA to develop and implement an Automated Fingerprint Identification System (AFIS) functionality in the SIS by mid-2017.
- Commission to present proposals by the end of 2016 to revise the legal basis of the SIS to further enhance its functionality.
- Member States to maximise their use of the SIS, both by inserting all relevant information and by consulting the system whenever required.

Interpol's database on Stolen and Lost Travel Documents (SLTD)

- Member States to establish electronic connections to Interpol tools at all their external border crossings.
- Member States to respect their obligation to enter and consult data on stolen or lost travel documents in SIS and the SLTD database at the same time.

Advance Passenger Information (API)

- Member States to automate the use of API data for checks against SIS and Interpol's Stolen and Lost Travel Documents (SLTD) database, in line with existing best practice.
- Commission to assess the need to revise the legal basis for the processing of API data.

Visa Information System (VIS)

- Commission to examine further improvements of the VIS before the end of 2016.

EURODAC

- Commission to present a proposal to revise the legal basis of EURODAC to further enhance its functionalities as regards irregular migration and return.

Europol

- Europol to make full use of its existing access rights for consultation purposes to SIS, VIS and EURODAC.
- Commission and Europol to explore and promote synergies between the Europol Information System (EIS) and other systems, notably the SIS.
- Commission and eu-LISA to examine whether the Automated Fingerprint Identification System (AFIS) to be developed for the SIS can complement Europol's systems for criminal investigation and counter-terrorism purposes.

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

Prüm framework

- Member States to fully implement and use the Prüm framework.
- If necessary, Commission to launch infringement proceedings against Member States that have not connected to the Prüm framework.
- Commission and eu-LISA to examine whether the Automated Fingerprint Identification System (AFIS) to be developed for the SIS can complement fingerprint data exchanges performed under the Prüm framework.

European Criminal Records Information System (ECRIS)

- European Parliament and Council should adopt in 2016 the legislative proposal to enable national authorities to search for third-country nationals in ECRIS on the basis of fingerprints.

Horizontal issues

- Commission to **monitor and promote the level of implementation** in relation to information systems.
- eu-LISA to develop a **central monitoring capacity for data quality** for all systems under its competence.
- Commission to present measures to enhance electronic **document security and ID management** and to strengthen the fight against document fraud.
- Commission to explore synergies and convergence between information systems and their corresponding infrastructures for EU border management and for **customs operations.**

6. DEVELOPING ADDITIONAL INFORMATION SYSTEMS AND ADDRESSING GAPS

While existing information systems cover a very broad spectrum of data that is required in the framework of border management and law enforcement, there are also important gaps. Some of these gaps have been addressed by the Commission with legislative proposals, namely the proposals for an Entry-Exit System and for an EU Passenger Name Record (PNR) scheme. For other gaps that have been identified, a careful assessment is needed as to whether additional EU tools are necessary.

1. Entry-Exit System

The Commission has presented the revised legislative proposals for the establishment of an Entry-Exit System (EES) in parallel to this Communication. After adoption by the co-legislators, it will be for eu-LISA to develop and implement the system, in cooperation with the Schengen Member States.

The EES will register border crossings (entry and exit) for all third-country nationals visiting the Schengen area for a short stay (maximum 90-day period in any period of 180 days), both visa-required and visa-exempt travellers, or stays on the basis of the new touring visa (up to one year). The objectives of the EES are (a) to improve the management of external borders, (b) to reduce irregular migration, by addressing the phenomenon of overstaying and (c) to contribute to the fight against terrorism and serious crime, thereby contributing to ensuring a high level of internal security.

The EES will register the identities of third-country nationals (alphanumeric data, four fingerprints and facial image) together with details of their travel documents, and will link these to electronic entry and exit records. The current practice of stamping travel documents will be discontinued. The EES will allow for the effective management of authorised short-stays, increased automation at border-controls, and improved detection of document and identity fraud. The central registration will enable the detection of over-stayers and the identification of undocumented persons in the Schengen area. The proposed EES therefore addresses an important gap in the landscape of existing information systems.

2. Passenger Name Records

Passenger Name Record (PNR) data consists of booking information with contact details, complete trip and reservation details, special remarks, seat and baggage information, means of payment. PNR data are helpful and necessary to identify high risk travellers in the context of combatting terrorism, drugs trafficking, trafficking in human beings, child sexual exploitation and other serious crimes. The proposed PNR Directive will ensure better cooperation between national systems and reduce security gaps between Member States. The proposed PNR Directive therefore addresses an important gap in the availability of data that is necessary for combatting serious crime and terrorism. **The PNR Directive should be adopted and implemented as a matter of urgency**.

The future Directive will provide that Member States have to set up Passenger Information Units (PIU) that will receive PNR data from carriers. It will not involve the creation of a central system or database, but will benefit from a certain degree of standardisation of national technical solutions and procedures. This will facilitate the exchange of PNR data between PIUs as foreseen in the proposed Directive. To that end, the Commission will support Member States analysing different scenarios for interconnectivity between PIUs, with a view to offering standardised solutions and procedures. Once the Directive is adopted, the Commission will accelerate the work on common protocols and supported data formats for the transfer of PNR data by air carriers to the PIUs. The Commission will prepare a draft implementing act within three months after adoption of the Directive.

3. Information gap prior to arrival of visa-exempt third-country nationals

While the identity, contacts and background information of visa-holders are registered in the VIS, the only information on visa-exempt persons comes from their travel document. For travellers arriving by air or sea this may be supplemented prior to arrival by API data. Under the proposed PNR Directive, their PNR data will also be collected if they arrive in the EU by air. For persons entering the EU through land borders, no information is available prior to their arrival at the EU's external border.

While law enforcement authorities can obtain information on visa-holders from the VIS if necessary for the combating of serious crime and terrorism, no comparable data is available on visa-exempt persons. This lack of information is particularly relevant for the management of the land borders of the EU, in a situation where substantial numbers of visa-exempt travellers arrive by car, bus or train. Several neighbouring countries of the EU are already visa-free, and visa liberalisation dialogues between the EU and other neighbouring countries are proceeding. This is likely to lead to a considerable increase of visa-exempt travellers in the near future.

The Commission will assess whether a new EU tool to address this issue is necessary, feasible and proportional. An option that could be considered is an **EU Travel Information and Authorisation System** (ETIAS), where visa-exempt travellers would register relevant information regarding their intended journey. The automatic processing of this information could help border guards in their assessment of third-country visitors arriving for a short stay. Countries such as the USA, Canada and Australia have already put similar systems into place, including for EU citizens.

Travel authorisation systems are based on online applications where the applicant provides details on his/her identity, contact details, purpose of the journey, itinerary, etc. before departure. Once the authorisation is obtained, border procedures at arrival become faster and smoother. Beyond the security and border management benefits, and its potential relevance in the context of visa-reciprocity, a system like ETIAS would therefore also serve as a travel facilitation tool.

4. European Police Records Information System (EPRIS)

As indicated in the European Agenda on Security, the real-time availability of existing police data across Member States is an area for future work on information exchange. The Commission will assess the necessity, technical feasibility and proportionality of a European Police Record Index System (EPRIS) to facilitate cross-border access to information held in national law enforcement databases. In this context, the Commission supports with EU funding the implementation of a pilot project by a group of five Member States to establish a mechanisms for automated cross-border searches in national indexes on a 'hit'/'no hit' basis.[25].The Commission will take the project's results into account in its assessment.

Actions to develop additional information systems and to address information gaps

Entry-Exit System (EES)

- European Parliament and Council should treat the legislative proposals on the EES as a matter of utmost priority, with the aim of adopting the proposals by the end of 2016.

Passenger Name Records (PNR)

- European Parliament and Council should adopt the PNR Directive by April 2016.
- Member States to implement the PNR Directive, once adopted, as a matter of urgency.
- Commission to support the exchange of data between Passenger Information Units through standardised solutions and procedures.
- Commission to prepare a draft Implementing Decision on common protocols and supported data formats for the transfer of PNR data by air carriers to the PIUs within three months after adoption of the PNR Directive.

[25] The Automated Data Exchange Process (ADEP) pilot project aims to create a technical system which allows, through an index, to see if police records on an individual or criminal police investigation exist in one or several other Member States. The automated reply to a search in the index would only indicate whether or not data is available; a so-called "hit" or "no hit" reply. Additional personal data would have to be requested in a second step in case of a "hit" via usual police cooperation channels.

Information gap prior to arrivals of visa-exempt third-country nationals

- Commission to assess in 2016 the necessity, technical feasibility and proportionality of establishing a new EU tool such as an EU Travel Information and Authorisation System.

European Police Records Information System (EPRIS)

- Commission to assess in 2016 the necessity, technical feasibility and proportionality of establishing an EPRIS.

7. TOWARDS THE INTEROPERABILITY OF INFORMATION SYSTEMS

Interoperability is the ability of information systems to exchange data and to enable the sharing of information. One can distinguish **four dimensions of interoperability**, each raising legal[26], technical and operational issues including on data protection:

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

In order to initiate a process towards the interoperability of information systems at EU level, the Commission will set up an **Expert Group on Information Systems and Interoperability** at senior level with EU agencies, national experts and relevant institutional stakeholders. The Expert Group will be tasked to address the legal, technical and operational aspects of the different options to achieve interoperability of information systems, including the necessity, technical feasibility and proportionality of available options and their data protection implications. It should address the current shortcomings and knowledge gaps caused by the complexity and fragmentation of information systems at the European level. The Expert Group will take a broad and comprehensive perspective on border management and law enforcement, taking account also of the customs authorities' roles, responsibilities and systems in this respect. The group's working method will aim at synergizing all relevant experiences, which in the past were too often developed in silos.

The objective of this process is to provide an overall strategic vision of the EU's architecture of data management for border control and security, as well as to provide solutions to implement it.

This consultation process shall be **guided by the following objectives**:

- Information systems should be complementary. Overlaps should be avoided, and existing overlaps should be eliminated. Gaps shall be appropriately addressed.
- A modular approach should be pursued, making full use of technological developments and building on the principles of privacy by design.
- Full respect of all fundamental rights of both EU citizens and third country nationals should be ensured from the outset in line with the Charter of Fundamental Rights.

[26] Subject to the specific terms of Protocol 22 as concerns Denmark and Protocol 21 and 36 as concerns the United Kingdom and Ireland.

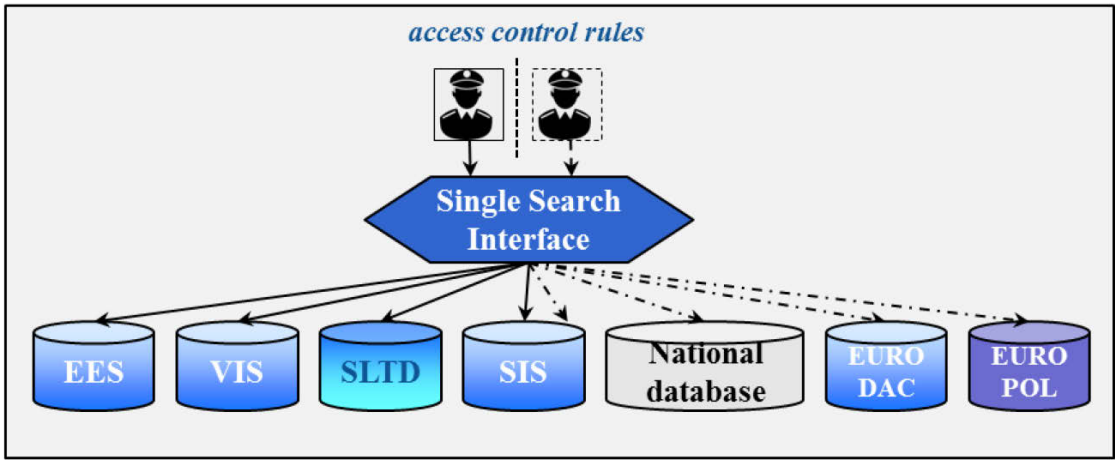
- Where necessary and feasible, information systems should be interconnected and interoperable. Simultaneous searches of systems should be facilitated, to ensure that all relevant information is available to border guards or police officers when and where this is necessary for their respective tasks, without modifying existing access rights.

1. Single search interface

The first dimension of interoperability is the **ability to query several information systems simultaneously, and to produce combined results on one single screen** for border guards or police officers, with full respect of their access rights, in line with the respective purposes. This requires platforms with a single search interface that are capable of consulting information systems simultaneously with one single query. For instance, by reading the chip of a travel document or by using biometric data, this platform could query several different databases at the same time. The single search approach applies to all authorities with a need to access and use the data (i.e. border guards, law enforcement authorities, asylum services) in line with the purpose limitation and strict access control rules. It can also be used with mobile equipment. Establishing a single search interface reduces the complexity of information systems at the European level, as it enables border guards and police officers to query several information systems simultaneously through one procedure, and in accordance with their access rights.

Several Member States have already installed such platforms with a single search interface. Based on this existing best practice, the Commission together with eu-LISA will work towards establishing a standardised solution for a single search interface. Member States should use EU funding under their national programme of the Internal Security Fund to finance the installation of such functionality. The Commission will closely monitor how Member States make use of the functionality of a single search interface at national level.

Figure 2 *Single Search Interface*



Searching multiple centralised or national systems (as depicted) is easier to achieve than searching decentralised systems. The Commission and eu-LISA will explore if a Single Search Interface can also be used to perform one-stop-shop simultaneous searches on decentralised systems such as Prüm and ECRIS. The Commission and eu-LISA will conduct this analysis together with the Expert Group on Information Systems and Interoperability, without modifying existing access rights.

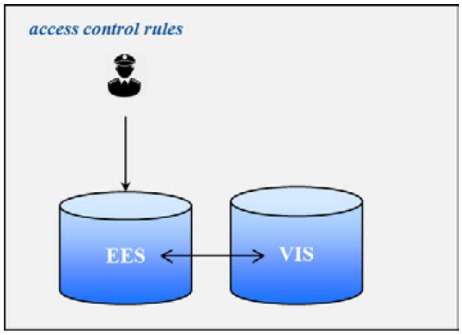
2. Interconnectivity of information systems

A second dimension of interoperability is the interconnectivity of information systems. This means that different systems or databases are able 'to talk to each other' technically. **Data registered in one system could be consulted by another system automatically at a central level**. This requires technical compatibility between the systems, and the data elements stored in those systems (e.g. fingerprints) need to be interoperable. Interconnectivity can reduce the amount of data circulating on communication networks and transiting through national systems.

Interconnectivity requires appropriate data protection safeguards and strict access control rules. The political agreement reached by the co-legislators in December 2015 on the Data Protection reform will put in place a modern data protection framework across the EU that will provide for these safeguards. It is important that the co-legislators adopt the General Data Protection Regulation and the Data Protection Directive without delay.

The concept of interconnectivity is inbuilt in the future EES system. The future EES will be able to communicate directly with the VIS at the central level and vice versa. This is an important step in addressing the current fragmentation in the EU's architecture of data management for border control and security, as well as the related problems. The automated cross-checking will relieve Member States of the need to query the VIS at border checks, reduce maintenance requirements and improve system performance.

Figure 3 *Interconnectivity of systems: the example of EES/VIS*



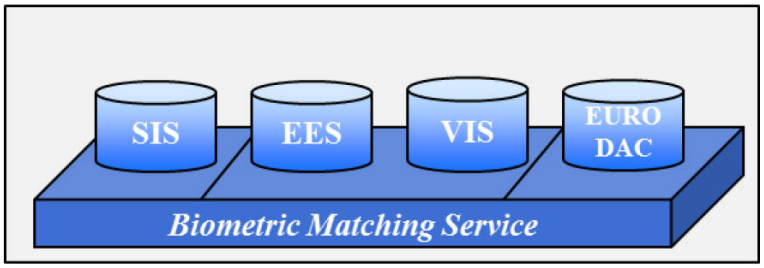
As a next step, the Commission and eu-LISA will analyse if the central-level interconnectivity between the future EES and the VIS can be extended to the SIS, and whether interconnectivity can be established between EURODAC and SIS. The Commission and eu-LISA will conduct this analysis together with the Expert Group on Information Systems Interoperability.

3. Shared biometric matching service

A third dimension of interoperability is in the area of biometric identifiers. For example, when fingerprints are collected at a consulate of one Member State with specific equipment, it is of crucial importance that these prints can be matched through VIS at a border post of another Member State, using equipment of another type. The same requirement applies to fingerprint queries in other systems: biometric samples need to meet minimum quality and format requirements, in order to achieve this type of interoperability without difficulty.

At the system's level the interoperability of biometric identifiers enables the use of a shared biometric matching service for several information systems, respecting personal data protection rules by compartmentalising the data, with separate access control rules for each category of data[27]. Such shared services generate serious financial, maintenance and operational benefits.

Figure 4 *Shared biometric matching service*



The Commission and eu-LISA will analyse whether establishing a shared biometric matching service for all relevant information systems is necessary and technically feasible. The Commission and eu-LISA will conduct this analysis together with the Expert Group on Information Systems and Interoperability.

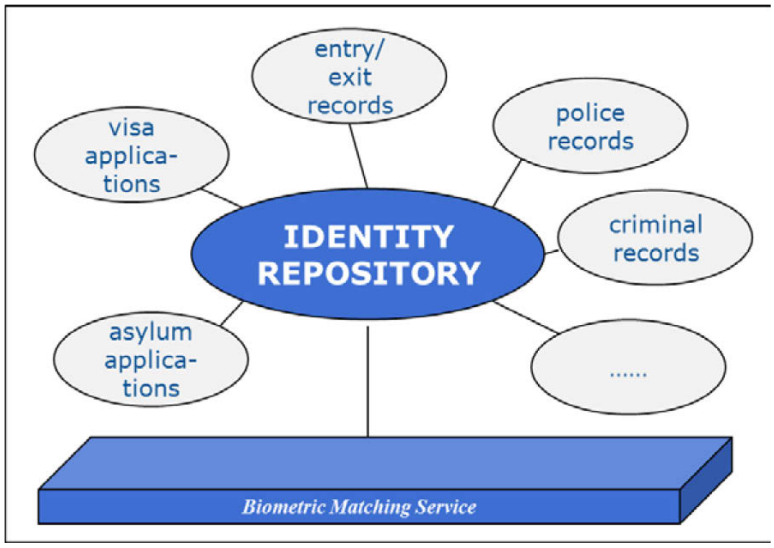
4. Common repository of data

The most ambitious long-term approach to interoperability would be a **common repository of data at EU level for different information systems**. The common repository would constitute a core module that contains the basic data (alphanumeric and biometric data), while other data elements and specific features of the different information systems (e.g. visa data) would be stored in specific modules. The core module and the specific modules would be connected with each other to link the respective data sets. This would create a **modular and integrated identity management for borders and security**. Compliance with data protection rules would need to be ensured, for instance by compartmentalising the data, with separate access controls rules for each category of data.

Establishing a common repository of data would overcome the current fragmentation in the EU's architecture of data management for border control and security. This fragmentation is contrary to the data minimisation principle, as it results in the same data being stored several times. Where necessary, the common repository would allow for the recognition of connections and provide an overall picture by combining individual data elements stored in different information systems. It would thus address the current knowledge gaps and shed light on blind spots for border guards and police officers.

[27] Comparable to sharing one physical file-server with a multitude of users, each having specific access rights to certain folders only.

***Figure 5** Common data repository*



The option of establishing a common repository of data at EU level raises important questions of definition of purpose, necessity, technical feasibility and proportionality of the data processing involved. It would require a complete revision of the legal framework establishing the various information systems and could only be an objective to be achieved in the long-term. The Expert Group on Information Systems and Interoperability will address the legal, technical and operational questions linked to a common repository of data, including questions of data protection.

For all four dimensions of interoperability mentioned above (single search interface, interconnectivity of systems, single biometric matching service and common repository of data), it is necessary that the data stored in different information systems or modules is compatible. To achieve this, it is important that the work on a **Uniform Message Format** (UMF) is taken forward in order to create a common standard for all relevant information systems.[28]

Actions towards the interoperability of information systems

- Commission to set up an **Expert Group on Information Systems and Interoperability** with EU Agencies, Member States and relevant stakeholders to explore the legal, technical and operational aspects of enhancing interoperability of information systems, including the necessity, technical feasibility and proportionality of available options and their data protection implications.

Single search interface

- Commission and eu-LISA to support Member States in installing a single search interface to query central systems.

[28] The Commission has supported the continued development of UMF in the 2012 Communication on the European Information Exchange Model (EIXM) and is currently financing the third UMF pilot project, with the aim of creating a common standard for all relevant databases, to be used at national (Member States') level, at EU level (for the central systems, and by Agencies) and at the international level (Interpol).

- Commission and eu-LISA to explore, together with the Expert Group, if single search interfaces could be used to perform one-stop-shop simultaneous searches for all relevant systems without modifying existing access rights.

Interconnectivity of information systems

- Commission and eu-LISA to analyse, together with the Expert Group, whether interconnectivity between centralised information systems could be further promoted, beyond the already proposed interconnectivity between the Entry-Exit System and the Visa Information System.

Biometric matching service

- Commission and eu-LISA to analyse, together with the Expert Group, the necessity and technical feasibility of establishing a shared biometric matching service for all relevant information systems.

Common repository of data (core module)

- Commission and eu-LISA to explore, together with the Expert Group, the legal, technical, operational and financial implications of the longer term development of a common repository of data.
- Commission and eu-LISA to engage in ongoing work towards a global Uniform Message Format for all relevant information systems.

8. CONCLUSION

This Communication launches a discussion on how information systems in the EU can better enhance border management and internal security, building on the significant synergies between European Agendas on Security and Migration. A number of information systems already provide border guards and police officers with relevant information, but these systems are not perfect. The EU is faced with the challenge of building a stronger and smarter data management architecture, in full compliance with fundamental rights, in particular the protection of personal data and its purpose limitation principle.

Where there are gaps in the EU's architecture of data management, they need to be addressed. Together with this Communication, the Commission has presented a proposal for an Entry-Exit System which should be adopted as a matter of urgency. The Passenger Name Record Directive also needs to be adopted in the coming weeks. The proposal for a European Border and Coast Guard should be adopted before the summer. In parallel the Commission will continue work to strengthen and where necessary streamline existing systems, such as developing an Automated Fingerprint Identification System functionality for the Schengen Information System.

Member States need to make full use of existing information systems and establish the necessary technical connections to all information systems and databases, in line with their legal obligations. Existing shortcomings, notably in the Prüm framework, need to be remedied without delay. While this Communication opens a discussion and starts a process for addressing systemic gaps and flaws, it is for Member States to urgently address persistent shortcomings in the feeding of EU databases and the exchange of information across the Union.

In order to structurally improve the EU's data management architecture for border control and security, this Communication initiates a process towards the interoperability of information systems. The Commission will set up an Expert Group on Information Systems and Interoperability to address the legal, technical and operational modalities of options to achieve the interoperability of information systems and address any shortcomings and gaps. Following the findings of the Expert Group, the European Commission will present further concrete ideas to the European Parliament and the Council as basis for a joint discussion on the way forward. The Commission will also seek the input of the European Data Protection Supervisor and national data protection authorities coming together in the Article 29 Working Party.

The goal should be the development of a joint strategy to make data management in the EU more effective and efficient, in full respect of data protection requirements, to better protect its external borders and enhance its internal security, for the benefit of all citizens.

ANNEX 1: ABBREVIATIONS

API	Advance Passenger Information
AFIS	Automated Fingerprint Identification System: system capable of capturing, storing, comparing, and verifying fingerprints.
CIS	Customs Information System
ECRIS	European Criminal Records Information System
EES	(proposed) Entry-Exit System
EIXM	European Information Exchange Model
EIS	Europol Information System
EPRIS	European Police Records Information System
EURODAC	European Dactyloscopy
EUROPOL	European Police Office (European Union's law enforcement agency)
ETIAS	(possible) EU Travel Information and Authorisation System
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
FIND	Fixed Interpol Networked Database
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
iARMS	(Interpol's) Illicit Arms Records and tracing Management System
INTERPOL	International Criminal Police Organization
MIND	Mobile Interpol Networked Database
PIU	Passenger's Information Unit: unit to be set up in each Member State to receive the PNR data from carriers.
PNR	Passenger Name Record
Prüm	Police co-operation mechanism for exchanging information on DNA, fingerprints and vehicle registration data
SafeSeaNet	European platform for maritime data exchange between Member States' maritime authorities
SBC	Schengen Border Code
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System (sometimes referred to as of the 2nd Generation – SIS II)
SLTD	(Interpol's) Stolen and Lost Travel Documents database
sTESTA	secured Trans European Services for Telematics between Administrations (to be upgraded to TESTA-NG (next generation))
UMF	Uniform Message Format: format of messages to allow compatibility between information systems
VIS	Visa Information System
VRD	Vehicle Registration Data

ANNEX 2: INVENTORY OF EXISTING INFORMATION SYSTEMS FOR BORDER MANAGEMENT AND LAW ENFORCEMENT

1. 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[29] and four Schengen associated countries[30], 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,[31] 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.

2. 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 2000) and all their external border crossing points (in total some 1800) 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 20 million visa-applications and, at peak-times, it handles over 50.000 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 allows the identification of a person who applied for a visa in the last five years and who may not carry identity documents.

---

29 All, except Ireland, Cyprus, Croatia.

30 Switzerland, Liechtenstein, Norway, Iceland.

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

3. EURODAC

EURODAC (European Dactyloscopy) contains fingerprints of asylum applicants and third-country nationals crossing irregularly the Schengen external borders. Its primary purpose currently is to determine which EU country is responsible for the processing of an asylum application, in line with the Dublin Regulation. 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 irregular migrants found in EU 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 allows the identification and monitoring of their secondary movements[32] within the EU, until an application for international protection has been submitted or a return decision has been issued (in the future, with a corresponding alert in SIS). More generally, the identification and monitoring of irregular migrants is required to ensure re-documentation by authorities in their countries of origin and thus facilitates their return.

4. 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[33], 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.

5. Advance Passenger Information (API)

The objective of API is to collect information about a person's identity ahead of boarding inbound flights to the EU and to identify irregular migrants upon arrival. API data consist of information held in a travel document, and relates to a traveller's full name, date of birth, nationality, number and type of travel document, as well as information on the border crossing point of departure and entry as well as transportation details. The API data related to the passenger is usually collected at the moment of check-in.

---

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

[33] 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

Pre-arrival information concerning transport by sea has to be transmitted under the Convention on Facilitation of International Maritime Traffic 24 hours prior to the scheduled arrival of the vessel. Directive 2010/65/EU[34] provides for an electronic transmission of data via a single window linking SafeSeaNet, e-Customs and other electronic systems.

There is no central EU system to record API data.

6. Europol information systems

The Europol Information System (EIS) is a centralised criminal information database for investigative purposes. It can be used by Member States and Europol to store and query data on serious crime and terrorism. The information stored in the EIS 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 EIS supports law enforcement cooperation and is not available for border control authorities.

Information exchange is channelled using the SIENA[35] platform, which is a secure electronic communication network between Europol, the Liaison Bureaux, the Europol 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 will enter into application. This framework will allow for an enhanced operational ability for Europol to conduct analysis, and to better identify links between available information.

7. The Prüm framework

The Prüm framework is based on a multilateral agreement[36] between Member States that enables the exchange of DNA, fingerprints and Vehicle Registration Data (VRD). The concept is based on the interconnection of a national system to the national systems of all other EU Member States, in order to enable remote cross-searching. Where a search generates a positive match in the database of other Member States, the details of the positive match are exchanged through bilateral exchange mechanisms.

---

[34] Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC:

[35] Secure Information Exchange Network Application.

[36] Prüm Convention of 2005. The Convention was integrated into EU Legislation in 2008 through Council Decision 2008/615/JHA.

8. 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.