European Parliament

European information systems in the area of justice and home affairs

An overview

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service
Author: Costica Dumbrava
Members' Research Service
May 2017 — PE 603.923

EN

This EPRS publication provides an overview of the existing and proposed European information systems in the area of justice and home affairs. It discusses the legal basis, the purposes, the scope of data and access, the utilisation and the proposed changes for each information system, including issues of interoperability. The analysis draws on a wide range of publications by EPRS.

PE 603.923
ISBN 978-92-846-1057-0
doi:10.2861/179068
QA-04-17-453-EN-N

Original manuscript, in English, completed in April 2017.

Disclaimer

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

EXECUTIVE SUMMARY

High levels of irregular migration and the increase in transnational terrorist activities have pushed the EU to take concerted measures to strengthen its external borders and to enhance internal security. The revision and development of information systems for border management and law enforcement has been a key aspect of this response.

As identified by the European Commission, the European information systems in the area of justice and home affairs have a number of important shortcomings related to: suboptimal functionalities, persistent information gaps, limited utilisation, fragmented overall architecture, and limited interoperability. To address these shortcomings, the Commission has put forward a series of proposals to revise existing information systems and to establish new ones.

A general trend has been the expansion of the law enforcement components of information systems, including of those that were not originally intended for such purposes. The recast Eurodac Regulation, which came into force in July 2015, allows for the use of the Eurodac database of asylum-seekers' fingerprints for preventing, detecting and investigating terrorist offences and other serious crimes. Similarly, access to the Visa Information System was given to national law enforcement authorities and to Europol.

While the use of information systems has improved in most cases, the full potential has not yet been reached. For example, alerts on foreign terrorist fighters are still not systematically inserted and checked in the Schengen Information System. Only a minority of Member States make use of Eurodac and the Visa Information System for law enforcement purposes. Member States' contributions to databases remain uneven. For example, just five Member States have reported almost all the cases of verified foreign terrorist fighters recorded in the Europol Information System. Some Member States are not yet connected electronically to the Interpol stolen and lost documents database, as they have not yet implemented the Prüm framework. Although Europol was given access to most databases, it has not yet made full use of its access rights.

Apart from taking measures to maximise the use and benefits of the information systems, the Commission has put forward legislative proposals aimed at expanding the scope of the existing systems. The proposals revising the Schengen Information System oblige Member States to issue alerts on persons related to terrorist offences and to introduce information about entry bans and return decisions in the system. The recast Eurodac Regulation makes it mandatory for Member States to collect data on third-country nationals or stateless persons who have been apprehended crossing EU borders irregularly or remaining illegally on EU territory. The proposal for a revised criminal records information system enables authorities to determine which Member State holds criminal records of a third-country national.

In view of closing information gaps concerning persons who might pose a security threat but are not covered by the existing systems, the Commission has presented proposals to establish two new information systems. The entry/exit system will record entry and exit data from all third-country nationals (including from visa-exempt third countries) crossing Schengen borders. The European travel information and authorisation system will collect pre-arrival information on third-country nationals (including family members of EU citizens) travelling to the EU. The new information systems will be built to ensure interoperability with other relevant information systems, while ensuring data protection rules are respected.

TABLE OF CONTENTS

List of main acronyms

API:	Advanced passenger information
CMS:	Case management system
EASO:	European Asylum Support Office
ECRIS:	European Criminal Records Information System
ECTC:	European Counter-Terrorism Coordinator
EES:	Entry/exit system
EIS:	Europol Information System
ETIAS:	European travel information and authorisation system
Eurodac:	European dactyloscopy database
eu-LISA:	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
Eurojust:	European Union Judicial Cooperation Unit
Europol:	European Police Office
Frontex:	European Border and Coast Guard Agency
FTF:	Foreign terrorist fighters
HLEG:	High-level expert group on information systems and interoperability
LIBE:	European Parliament Committee on Civil Liberties, Justice and Home Affairs
PNR:	Personal name records
SIS:	Schengen Information System
SLTD:	Stolen and lost travel documents database
VIS:	Visa Information System

List of figures

1. Introduction

A strong and efficient management of external borders is a prerequisite for the proper functioning of the Schengen Area. The interconnections between border management, migration and internal security have become more apparent recently in the context of high inflows of refugees and irregular migrants and of increasing terrorist activities in the EU. To address these challenges, the EU has taken steps to improve and expand the European information systems that enable authorities to collect, analyse and share data for the purposes of border control and law enforcement.

In the aftermath of the Paris terrorist attack, in February 2015, the EU Heads of State or Government called on Member States to reinforce and modernise control of EU external borders and to step up information sharing and operational cooperation among law enforcement and judicial authorities, including through Europol and Eurojust. The European agenda on security, put forward by the European Commission in April 2015, underlined the links between internal and external security and called for enhanced information exchange between law enforcement authorities. In the European agenda on migration, presented in May 2015, the Commission maintained that strengthening external borders requires making better use of the opportunities offered by IT systems and technologies. In its conclusions on the renewed European Union internal security strategy, of June 2015, the Council called for measures 'integrating the internal and external aspects of the fight against terrorism, improving information exchange and accessibility, especially by ensuring the interoperability of different information systems'. In the context of an unfolding migration crisis and another terrorist attack in Paris, in November 2015, the Council urged Member States to carry out systematic registration of third country nationals illegally entering the Schengen area and to perform systematic security checks by using relevant databases. The Council instructed the Commission to undertake efforts to achieve interoperability between the relevant databases with regard to security checks.

Together with adopting a series of operational and technical measures to improve the functioning and utilisation of information systems, the Commission put forward legislative proposals aiming to revise the legal bases of several European information systems, including the European dactyloscopy database, the Schengen Information System and the European Criminal Records Information System. In view of addressing information gaps with regard to persons who are not covered by existing databases but who might constitute security risks, the Commission proposed two new information systems. In November 2016, the Commission presented a proposal for a European travel information and authorisation system, which will contain data on visa-exempt third-country nationals travelling to the Schengen area. Within the revised smart borders package of April 2016, the Commission presented a new proposal to establish an EU entry/exit system for recording data on the entry and exit of all third-country nationals crossing the EU's external borders.

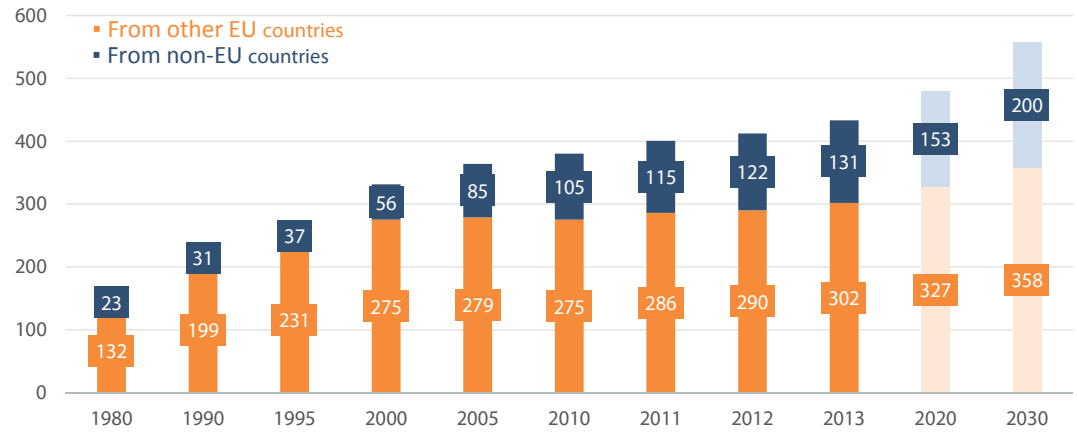
In January 2016, the European Counter-Terrorism Centre was launched at Europol to enhance EU operational cooperation and information sharing on terrorism. A high-level expert group on information systems and interoperability was subsequently established in June 2016 to work on a joint strategy to make data management in the EU more effective and efficient and to provide recommendations on the future development of European information systems. The work of the high-level expert group is essential to ongoing efforts to revise and update the European informational architecture in the area of justice and home affairs.

2. Migration and security challenges

2.1. External borders under pressure

The EU external borders have come under strain from a surge in the number of border crossings, both regular and irregular. According to a Commission communication of April 2016, the number of non-EU citizens travelling to the EU increased from 49 million (191 million border crossings) to 50 million (200 million border crossings), between 2014 and 2015. According to a study by the UN World Tourism Association (UNWTO),[1] the number of international tourist arrivals (not persons, who may be counted multiple times) in the 28 EU grew from 331 million to 433 million, between 2000 and 2013 (see Figure 1). In about one third of cases, the travellers arrived from non-EU countries. According to a report by PwC,[2] the number of non-EU travellers to the EU is estimated to rise to 76 million by 2025. The UNWTO study forecasts that the number of international tourist arrivals to the EU will grow to reach 558 million by 2030 (of which, 200 million arrivals from non-EU countries).

Figure 1 – International tourist arrivals in the EU, including projections (in millions)



Data source: UNWTO, 2016.

Ongoing visa liberalisation processes contribute to the growth in numbers of incoming EU travellers. Currently, the citizens of 57 countries and of 3 special regions or territories are exempted from the requirement to be in possession of a visa when crossing the external borders of a EU Member State for stays of no more than 90 days in any 180 day period. According to PwC's report, the number of visa-exempt third country nationals who travel to Schengen countries is expected to grow by almost one third between 2014 and 2020 (from 30 million to 39 million).

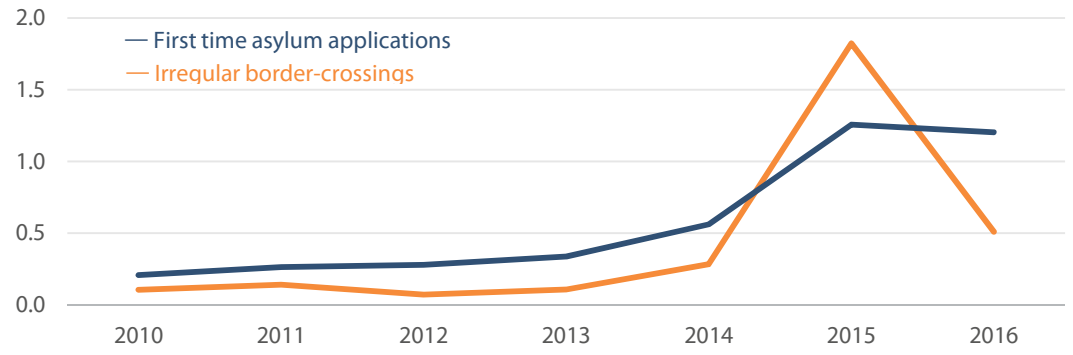
In 2016, Frontex detected 0.5 million illegal crossings between border crossing points. While the number of detections is significantly lower than in 2015 (1.8 million), it is still four times higher than the average number of detections recorded between 2010 and 2014. The number of (first time) asylum applications increased progressively from 0.2 million to 1.2 million between 2010 and 2015 and decreased only slightly in 2016 (see figure 2).

---

1 World Tourism Organization, International tourism trends in EU-28 Member States – current situation and forecast for 2020-2025-2030, May 2016.

2 PwC, Technical Study on Smart Borders. Final report, October 2014.

Figure 2 – Illegal border crossings and first time asylum applications (in millions)

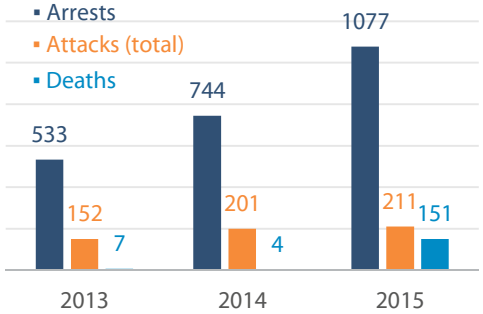


Data source: FRONTEX, 2014, 2015, 2016 and 2017; Eurostat, 2017.

2.2. Threats to EU internal security

The number of terrorist attacks per year in the EU increased from 152 to 211 between 2013 and 2015 (including foiled, failed and completed attacks), while the number of persons arrested on terrorism related charges doubled for the same period (see figure 3). A total of 151 persons were killed in terrorist attacks in 2015. Although the majority of perpetrators of these attacks were EU citizens, many had links with terrorist organisations from outside the EU, and some entered the EU irregularly by exploiting weaknesses in EU external borders. According to Europol, the perpetrators of the *Charlie Hebdo* attacks in Paris had links to Al-Qaeda in the Arabian Peninsula in Yemen, while a number of the suspects involved in the November 2015 Paris attacks had previously travelled to and been trained in Syria.

Figure 3 – Terrorism related arrests, attacks and deaths



Data source: Europol, 2014; 2015 and 2016.

The link between cross-border movement and crime is illustrated by the phenomenon of foreign fighters – EU citizens travelling to conflict zones abroad to engage in fighting. According to Europol, in 2015, around 5 000 EU citizens travelled abroad to engage in terrorist activities. The crackdown against ISIL/Da'esh in Iraq and Syria has raised concerns about the return to Europe of many of these foreign fighters.[3] Some 2 000 foreign fighters are expected to return[4] if ISIL/Da'esh continues to lose ground in Syria. While evidence suggests that only a minority – one in 360 returnees from Syria[5] – get involved in terrorist attacks upon their

[3] Mehra, T., Foreign Terrorist Fighters: Trends, Dynamics and Policy Responses, International Centre for Counter-Terrorism, December 2016.

[4] Reed, A., Pohl, J., Disentangling the EU Foreign Fighter Threat: the Case for a Comprehensive Approach, International Centre for Counter-Terrorism, Newsbrief 37(1), February 2017.

[5] Hegghammer, T., Nesser, P. Assessing the Islamic State's Commitment to Attacking the West, Perspectives on terrorism, 9(4), July 2015.

return to Europe, important challenges remain with regard to the reintegration of these persons.

2.3. Revision of European information systems

In its communication on stronger and smarter information systems, presented in April 2016, the Commission identified a series of key shortcomings of the existing European information systems in the area of border management and law enforcement:

- Partial utilisation of the existing information systems by Member States and EU agencies;
- Suboptimal functionalities and technical limitations, such as poor use of biometric data and low data quality;
- Persistent gaps in the EU informational architecture, meaning that certain categories of persons are not sufficiently covered by the existing database (e.g. visa-exempt third country nationals);
- Complex legal and policy landscape governing the various European information systems, given that not all EU Member States are connected to all existing systems;
- Overall fragmentation of EU data management architecture and limited interoperability between information systems.

In June 2016, the Dutch Presidency of the Council put forward a roadmap to enhance information exchange and information management, including interoperability solutions in the justice and home affairs area. The roadmap defined a series of principles to improve information management, information exchange and intelligence-led follow-up actions, based on:

- Full respect of fundamental rights and data protection rules, which requires embedding personal data protection in the technology basis;
- An information centred approach based on process analysis;
- A practitioner centred approach building upon trust and operational needs;
- Full implementation and use of existing information exchange instruments – and taking informed decisions on new initiatives – requires continuous monitoring;
- Ensuring effective interconnectivity of European initiatives with national processes;
- Pursuing systematic sharing of information between Member States, EU agencies and bodies;
- Using information management and information exchange as a means to an end.

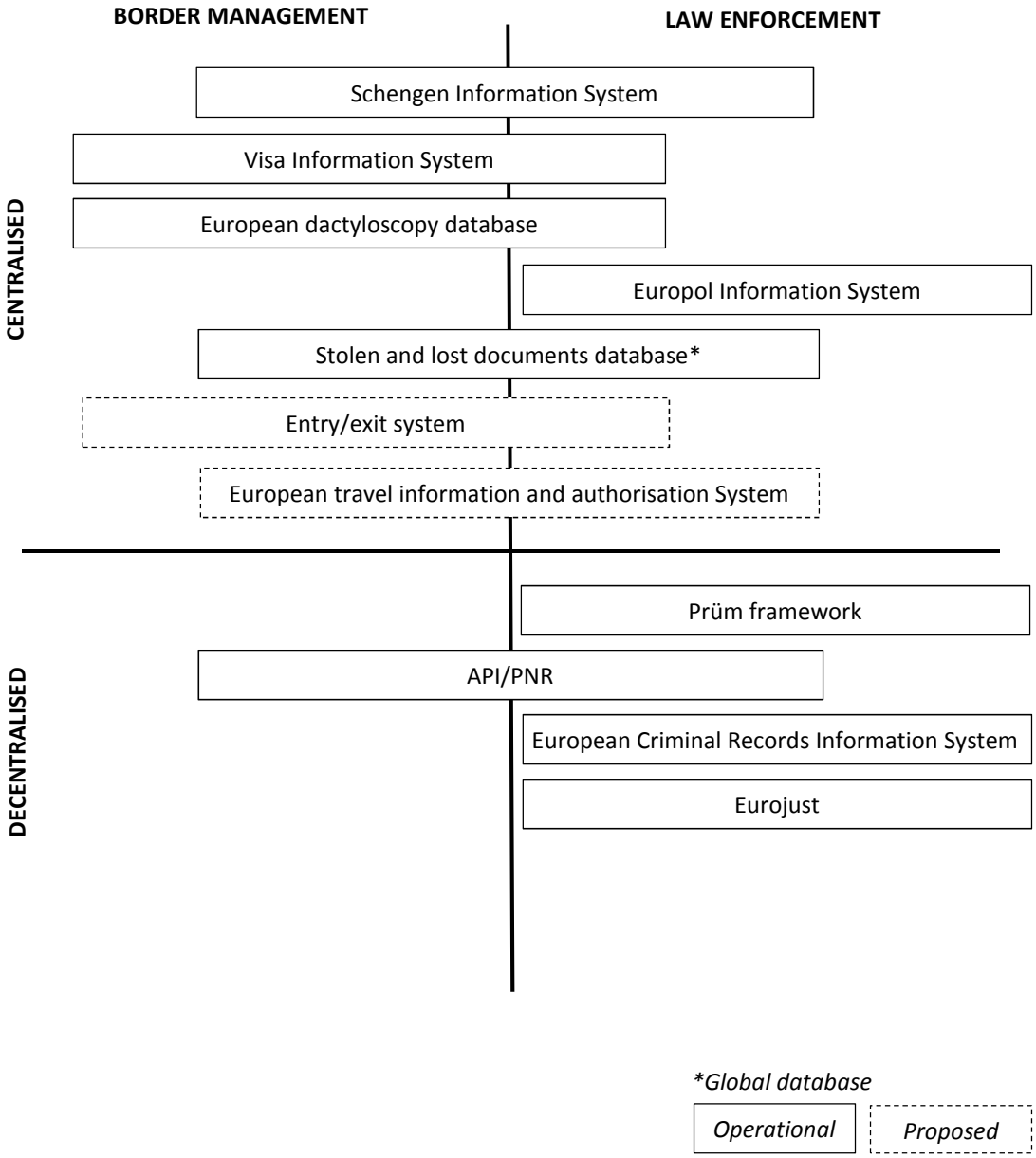
The high-level expert group on information systems and interoperability (HLEG) was set up in June 2016 to work on ways to strengthen and develop European information systems. The HLEG gathers high-level representatives from the Commission, Member States, associated members of the Schengen area, EU and the European Counter-Terrorism Centre (ECTC).

In its interim report, published in December 2016, the HLEG emphasised the need to raise the data quality and data usage standards and identified several priority options to be considered in promoting the interoperability of information systems, including establishing a single search interface (see section 4). The expert group is expected to present its final report in April 2017.

3. Overview of European information systems

The various European information systems in the area of justice and home affairs can be classified according to their primary purpose – border management or law enforcement – and according to whether or not they are centralised at the EU level (see figure 4).

Figure 4 – European information systems in the area of justice and home affairs



3.1. Schengen Information System

3.1.1. Purposes

Legal basis

Regulation (EC) 1987/2006; Regulation (EC) 1986/2006; Council Decision 2007/533/JHA.

The Schengen Information System (SIS) is the largest centralised European information system. The SIS supports external border management and law enforcement cooperation in the Schengen area by enabling border and law enforcement authorities to create and check alerts regarding certain persons and objects. It is a key instrument to combating terrorism through facilitating information exchange between Member States. The SIS was established in 1990 as a primary compensatory measure for the abolition of controls at the EU's internal borders. The current version of the SIS (SIS II) was established in 2006 and became operational in April 2013. The 22 EU Schengen Member States and 4 Associated Countries (Iceland, Liechtenstein, Norway, and Switzerland) are full participants in the SIS. Bulgaria, Romania and the United Kingdom participate in the SIS only with respect to law enforcement cooperation.

3.1.2. Data and access

SIS contains the following categories of alerts on:

- Third-country nationals banned from entry or stay in the Schengen Area (Article 24 of Regulation 1987/2006);
- Persons wanted for arrest – for whom a European Arrest Warrant or Extradition Request has been issued (Article 26 of Decision 2007/533);
- Missing persons (Article 32 of Decision 2007/533);
- Persons sought to assist with a judicial procedure (Article 34 of Decision 2007/533);
- Persons regarding whom discreet or specific checks are necessary – for the purposes of prosecuting criminal offences and for the prevention of threats to public or national security (Article 36 of Decision 2007/533);
- Objects for seizure or use as evidence in criminal procedures, such as vehicles, aircraft, boats, banknotes, firearms (Articles 36 and 38 of Decision 2007/533).

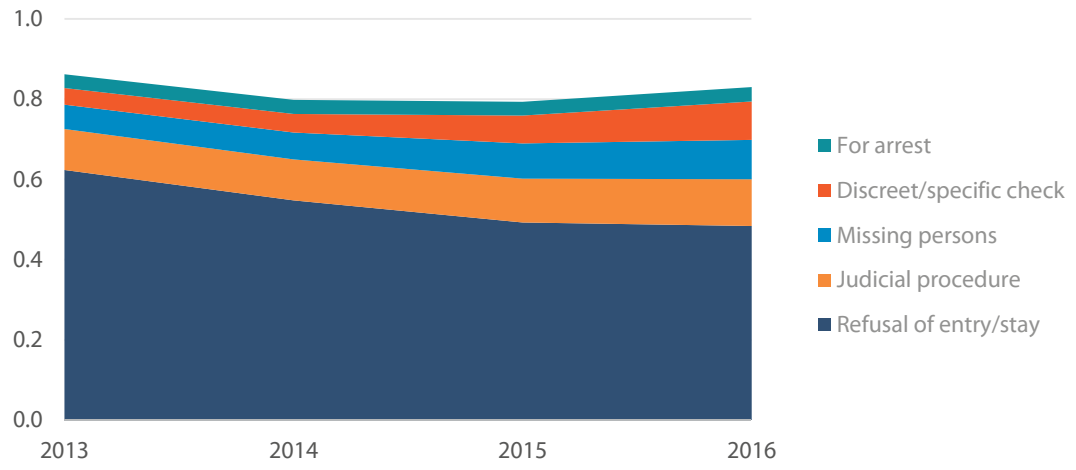
Member States can enter, update, delete and search data in the SIS via national systems and can exchange supplementary information via a dedicated supplementary information request made to the National Entry bureau (SIRENE). Access to SIS data is given to national authorities responsible for border control, police, customs, visas, and vehicle registration and, by extension, to national judicial authorities, when this is necessary for the performance of their tasks. The European Police Office (Europol) and the European Union's Judicial Cooperation Unit (Eurojust) have limited access rights to carry out certain types of searches.

3.1.3. Utilisation

According to the European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the agency in charge of managing SIS II, the total number of alerts inserted in the SIS increased from 50 million to almost 71 million between December 2013 and December 2016. However, the number of alerts on persons has remained low (about 0.8 million) in the period of reference. The majority of alerts on persons concern refusals of entry or stay (see figure 5). Currently, the SIS does not have specific alerts on foreign terrorist fighters (FTF). The number of alerts regarding persons for whom discreet or specific checks,

which are relevant for detecting foreign terrorist fighters, are necessary, has increased only slightly, from 41 097 to 69 475, between December 2013 and December 2015. According to a note presented by the ECTC in April 2016 not all Member States insert data on FTF into the SIS systematically and, when they do, the information recorded is often incomplete. For example, although all perpetrators of the Paris and Brussels attacks were subjects of SIS alerts, the information entered was insufficient and, in the absence of biometric identifiers, the attackers were able to travel under a false identity and thus avoid being stopped at the border.

Figure 5 – Alerts on persons in the SIS (in millions)

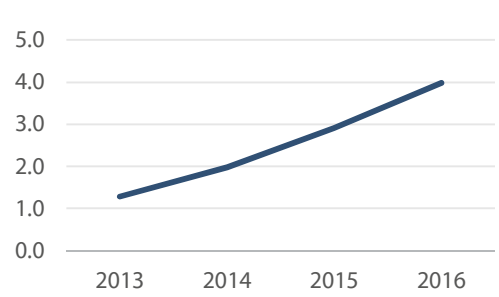


Data source: eu-LISA reports.

The share of alerts inserted in the SIS varies greatly among Member States. As of December 2016, more than half the alerts in the SIS were inserted by three member states: Italy (28%), Germany (14%), and France (13%).

The number of searches in the SIS increased from 1.2 billion to 3.9 billion, between April 2013 and December 2016 (see figure 6). A total of 200 778 hits on foreign alerts were reported for 2016, which represents an increase of 30 % compared to 2015. Over 74 % of hits generated in 2016 were triggered by alerts on persons. Member States' use of the SIS is uneven. In 2016, four Member States performed more than half of the searches in the SIS: France (20.1 %), the UK (12.9 %), Spain (11.9 %) and Germany (10 %). According to a report presented by the ECTC in March 2016, although Europol has had the right to access and search SIS data on arrests, discreet and specific checks and on objects for seizure, it had carried out only a limited number of searches.

Figure 6 - Searches in the SIS (in billions)



Data source: eu-LISA reports.

3.1.4. Proposed changes

In its evaluation of the SIS, the Commission found that, although the system was a 'highly successful tool', a number of improvements were necessary. Aiming to reinforce the SIS to better fight terrorism and cross-border crime, the Commission put forward three

proposals for reform in December 2016. The proposal for the revision of SIS in the field of police cooperation and judicial cooperation in criminal matters introduces new alerts and checks, extends the use of biometrics and enlarges access to the SIS for law enforcement authorities. It also makes it mandatory for Member States to issue alerts on persons related to terrorist offences. The proposal for a regulation on the establishment, operation and use of the SIS in the field of border checks provides for the more effective use of fingerprints and facial images in the SIS, introduces the obligation for Member States to introduce entry bans issued to illegally staying third-country nationals in the system. Lastly, the proposal for a regulation on the use of the SIS for the return of illegally staying third country nationals introduces the obligation for Member States to enter all return decisions in the system in view of enhancing their enforcement and contributing to reducing incentives to irregular migration.

Within the European Parliament, the three proposals have been assigned to the Committee on Civil Liberties, Justice and Home Affairs (LIBE). A joint debate on the proposals took place in the LIBE Committee on 30 March 2017.

3.2. Visa Information System

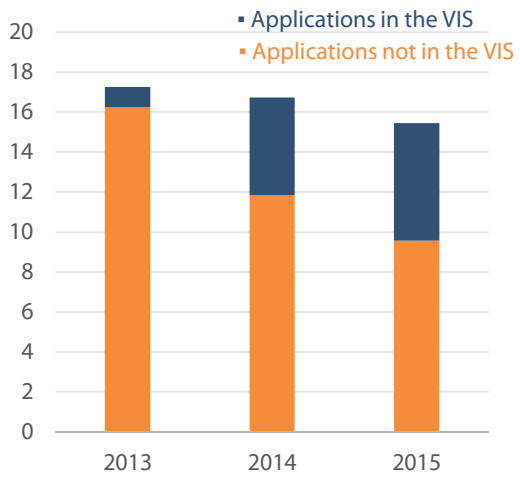
3.2.1. Purposes

Legal basis

Council Decision 2004/512/EC; Regulation (EC) 767/2008; Regulation (EC) 810/2009; Council Decision 2008/633/JHA.

The Visa Information System (VIS) is the EU's information system dedicated to the exchange of data on persons applying for short-stay visas to enter the Schengen area. The primary role of the VIS is to support the implementation of the common EU visa policy. However, because it gathers a large amount of data on persons entering the Schengen area, the VIS also plays a role in supporting asylum procedures, combating irregular migration and preventing threats to EU internal security. The VIS began operations in October 2011 and its worldwide roll-out was completed in December 2015. As of October 2014, the verification of visa holders based on fingerprints (where available) became mandatory at the Schengen borders. The 22 EU Schengen states and the 4 associated Schengen states are connected to the VIS.

Figure 7 – Applications for Schengen visa (in millions)



Data source: European Commission, 2016; eu-LISA, 2014; 2015 and 2016.

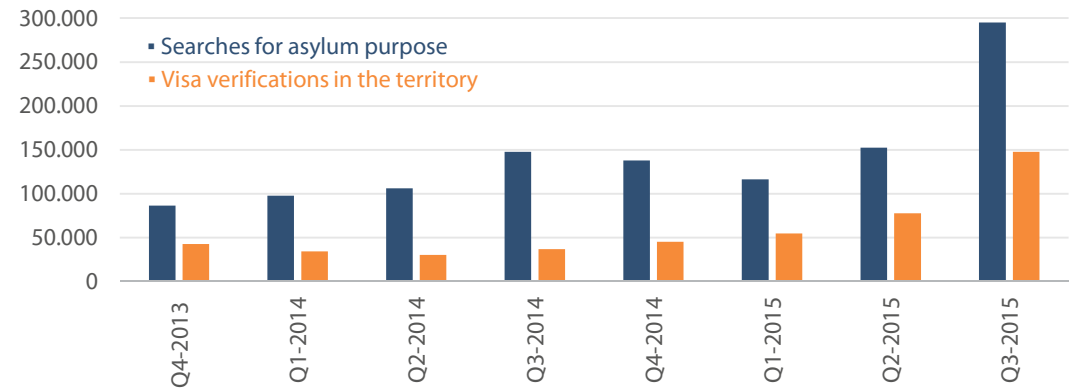
3.2.2. Data and access

The VIS contains data related to visa applications by third country nationals who require a visa to enter the Schengen area, including biometrics (fingerprints and a digital facial image). Each time a visa holder enters the Schengen area, their fingerprints will be checked against the database. Access to the VIS is given to national visa authorities when examining Schengen visa applications, border authorities upon entry into the Schengen area, and by migration and asylum authorities within the Schengen area charged with verifying the identity of visa holders. National law enforcement authorities and Europol can access the VIS to prevent, detect and investigate terrorist offences and other serious crimes.

3.2.3. Utilisation

According to data from the European Commission, the total number of applications for short-stay EU visas in 2015 was 15.4 million, decreasing from 16.7 million in 2014 (see figure 7). According to eu-LISA data, the number of visa applications registered in the VIS in 2014 was 5.5 million, while in 2015 (January-September) it was 6.5 million. Between September 2013 and September 2015, Member States made over 52.5 million searches in the VIS. The overwhelming majority of searches (98 %) took place at the borders. The general increase in the number of consultations of the VIS for visa verifications in the territory and for asylum purpose (see figure 8) indicates a greater role for the VIS in combating irregular migration and asylum abuse.

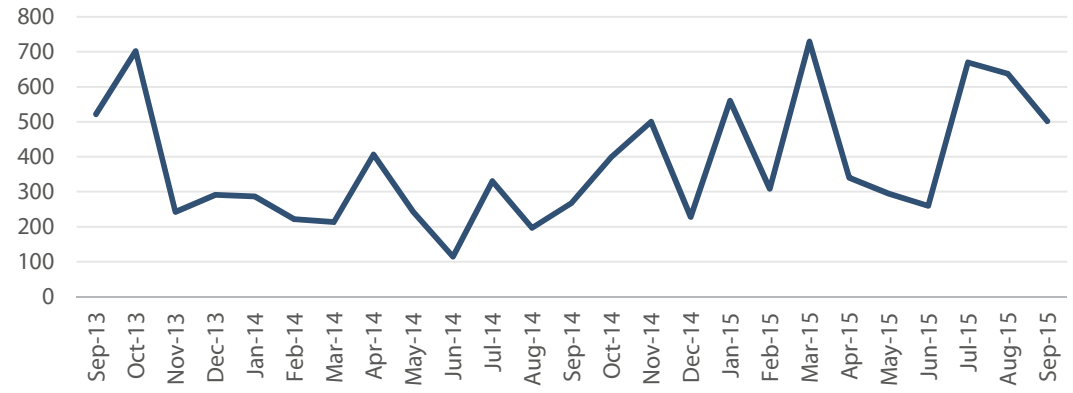
Figure 8 –VIS searches for asylum purposes and for visa verification in the territory



Data source: eu-LISA, 2016.

The Commission evaluation report of October 2016 found that the VIS has played a supportive role in the application of the Dublin Regulation. However, according to the eu-LISA, only a minority of Member States make use of the VIS for asylum purposes: Germany performed almost 45 % of the total searches reported, followed by Sweden with 34 % of all searches for asylum purposes.

Figure 9 – VIS searches for law enforcement purposes



Data source: eu-LISA, 2016.

The role of the VIS in the field of internal security remains limited, partly due to the current lack of access to the VIS for this purpose in EU Member States. According to a eu-LISA report, between September 2013 and September 2015, only 11 Member States granted access to the VIS to designated law enforcement authorities, which resulted in around 9 400 searches (see figure 9). Although, as of 1 September 2013, Europol gained access to the VIS, its connection to the database has not yet been established.

In September 2015, 20 % of the visa applications processed in the VIS did not contain fingerprints. According to the evaluation report by the Commission, in March 2016, there were 23 million visa applications stored in the VIS and 18.8 million fingerprints. There are three main reasons for the lack of fingerprints in the VIS: applicants, such as children under the age of 12, Heads of State or Government, sovereigns and other senior members of a royal family were legally exempted from the requirement (Article 13(7) of the Visa Code); it was physically impossible to provide fingerprints (Article 13(7) of the Visa Code), or the application was lodged in a region where the VIS had not yet been implemented. As reported by the eu-LISA, Member States do not always comply with the rules on how to indicate the reasons for not collecting fingerprints, which affects the quality and the accuracy of the data stored in the database.

3.2.4. Proposed changes

Based on its evaluation report, the Commission recommended developing the VIS, in particular, in view of improving its interconnectivity with other information systems. A number of recent legislative proposals make reference to the VIS. The proposal for a recast of the Dublin Regulation provides for an obligation on Member States to conduct searches in the VIS. The proposal for establishing a entry/exit system provides for the interoperability between the VIS and the new entry/exit system, which would enable direct consultation between the two systems in both directions at border crossing points and in consulates. The proposal for establishing a European travel information and authorisation system provides for the interoperability between the new system and the VIS. In view of these developments, a revision of the VIS is envisaged for 2017.

3.3. European dactyloscopy database

3.3.1. Purposes

Legal basis

Regulation (EU) 603/2013.

The European dactyloscopy database (Eurodac) facilitates the application of the Dublin Regulation by helping to determine the country responsible for the assessment of asylum claims through establishing the point of entry into the EU. Eurodac was established in 2000 and became operational in 2003. As of July 2015, when the new Eurodac Regulation came into force, it can be used for the purpose of preventing, detecting and investigating terrorist offences and other serious crimes, providing access to law enforcement authorities under certain conditions. All EU Member States and the four Associated Schengen States participate in Eurodac.

3.3.2. Data and access

Eurodac contains fingerprints from three categories of persons (older than 14 years):

- applicants for international protection (Article 9 of the Eurodac Regulation);
- third-country nationals or stateless persons who are apprehended in connection with the irregular crossing of a Member State's border having come from a third country and who are not turned back (Article 14 of the Eurodac Regulation);
- third-country nationals or stateless persons found illegally staying within the territory of a Member State (Article 17 of the Eurodac Regulation).

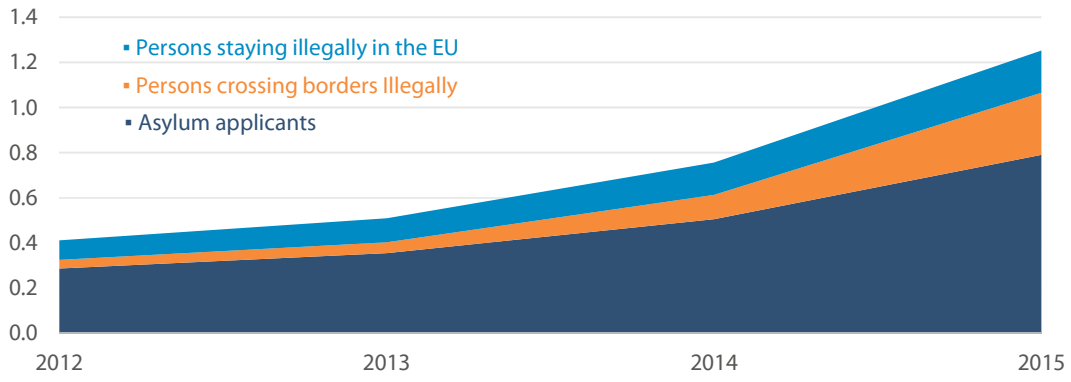
Access to Eurodac is given to Member States' authorities responsible for asylum applications. As of July 2015, Eurodac is accessible to designated national authorities that are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. The use of Eurodac for such purposes is permitted only when other law enforcement means have been exhausted, given that: there is an

overriding public security concern at stake, the search is for a specific case and not for systematic comparison, and there are reasonable grounds to expect that a search will contribute substantively to preventing, detecting and investigating criminal offences.

3.3.3. Utilisation

According to eu-LISA, the total number of data subjects (persons whose fingerprints were taken/checked) in Eurodac increased progressively between 2012 and 2015 (see figure 10).

Figure 10 – Data subjects in Eurodac (in millions)

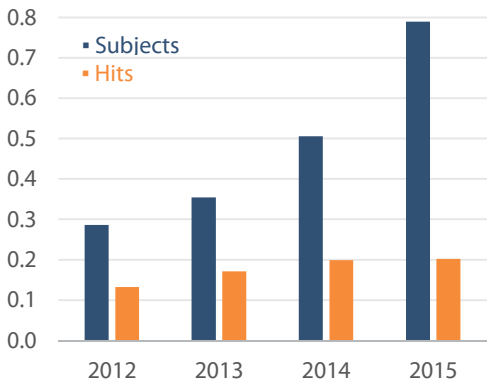


Data source: Commission, 2013; eu-LISA, 2014, 2015 and 2016.

Between 2014 and 2015, the number of Eurodac datasets on third-country nationals who lodged an asylum application in the Schengen area increased by 56 % (from 505 221 to 789 872). For the same period, the number of Eurodac datasets on third-country nationals apprehended in connection with the irregular crossing of a Member State's border increased by 156 % (from 106 980 to 274 936), while the number of Eurodac datasets on third-country nationals found staying illegally within the territory of a Member State increased by 30 % (from 144 167 to 187 478).

Between 2014 and 2015, the number of hits related to applicants for international protection (persons who had already lodged an application for international protection in the same or another Member State) increased slightly from 198 871 to 202 552 (see figure 11). Following verifications in Eurodac, in 2015, one in four applicants for international protection were found to have previously lodged applications for international protection. In the same year, verifications in Eurodac yielded that more than 90 % of the persons apprehended crossing a Member State's border irregularly had lodged applications for international protection elsewhere (see figure 12).

Figure 11 – New data subjects related to asylum claims and corresponding hits in Eurodac (in millions)



Data source: Commission, 2013; eu-LISA, 2014, 2015 and 2016.

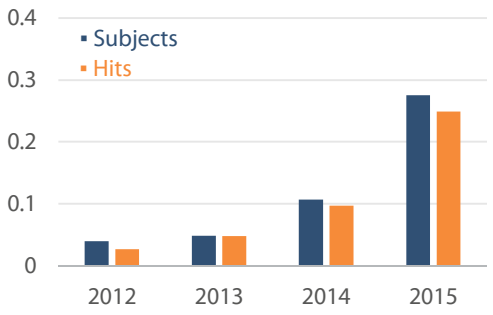
The Eurodac Regulation recast in 2013 allows the use of Eurodac for law enforcement purposes. However, as reported by eu-LISA, between July and

December 2015, only five Member States used Eurodac for such purposes (Austria, Germany, Finland, France, and the Netherlands) – performing 95 searches in total. Europol has not yet been connected to the database.

3.3.4. Proposed changes

In May 2016, the Commission put forward a proposal for a recast Eurodac Regulation, as part of the reform of the Common European Asylum System. The proposal introduces the obligation to collect data on third-country nationals or stateless persons who have been apprehended crossing EU borders irregularly or staying illegally on EU territory. It expands the range of data collected (fingerprints and an additional biometric identifier – a facial image) and lowers the age of persons subject to fingerprints checks to six years old.

Figure 12 – New data subjects related to illegal stay and corresponding hits in Eurodac (in millions)



Data source: Commission, 2013; eu-LISA, 2014, 2015 and 2016.

On 9 February 2017, the rapporteur for the European Parliament's LIBE Committee, presented a draft report on the proposal. The rapporteur welcomed the expansion of the Eurodac's scope and proposed to further extend the role of Eurodac in the area of law enforcement by simplifying Europol's access to the database and by providing for better tracking of unaccompanied minors.

3.4. Europol Information System

3.4.1. Purposes

Legal basis

Council Decision **2009/371/JHA** (until 30 April 2017); Regulation **2016/794** (from 1 May 2017).

The European Police Office (Europol) is the European Union's law enforcement agency. The Europol Information System (EIS) is the agency's central criminal information and intelligence database. Europol was established in 1995 and the EIS became operational in 2005. All EU Member States are members of Europol.

3.4.2. Data and access

The EIS contains information on serious international crimes, suspected and convicted persons, criminal structures, and offences and the means used to commit them. The data are stored within different online entities corresponding to various 'objects', such as persons, cars, and identity documents. These objects can be linked to create a structured picture of a criminal case. The newest version of the EIS, launched in 2013, can store and automatically cross-check biometrics and cybercrime related data. Issuing authorities have full control of the data inserted in the EIS and are responsible for checking, updating and deleting data.

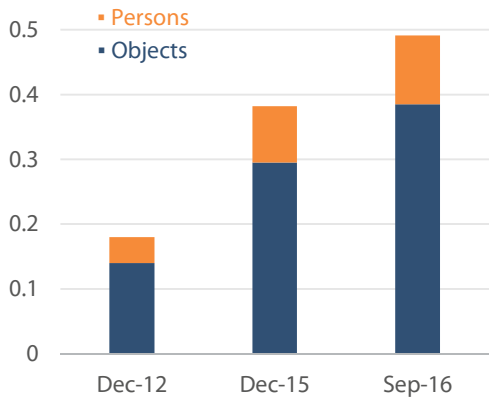
Access to the EIS is given to Europol officials, Member State liaison officers, seconded national experts stationed at Europol's headquarters, as well as to staff working in the Europol National Units and in the competent national authorities. In addition, some of Europol's cooperation partners can store and query data via Europol's operational centre. Designated authorities of Member States can run searches in the system and, in case of a hit, can request additional information via the secure information exchange

network application (SIENA), Europol's message-exchange system. SIENA is also used to exchange information between EU law-enforcement agencies, cooperating partners such as Eurojust and Interpol, as well as cooperating states outside the EU, such as Australia, Canada, Norway, Switzerland and the United States. Europol and Frontex have concluded an operational agreement allowing for data exchange.

3.4.3. Utilisation

According to Europol, between 2006 and 2012, the number of objects in the EIS increased from under 50 000 to more than 150 000. In December 2015, the EIS contained information on 295 347 objects and 86 629 suspected criminals (see figure 13). The number of cases of foreign terrorist fighters increased from just 18 in December 2014 to 6 506 in September 2016 (see figure 14). This number more than tripled between December 2015 and September 2016. However, according to a report by the ECTC, Europol's Focal Point Travellers, which is used to investigate FTF cases, contained only 2 786 verified foreign terrorist fighters. The ECTC noted a discrepancy between the higher number of relevant alerts in the SIS and the limited number of FTF cases in the EIS and Europol's Focal Point Travellers. In fact, all entries in the SIS II concerning FTF should, by default, be transferred to the EIS and more sensitive additional information should be shared for analysis purposes with Europol's Focal Point Travellers. According to a note presented by the ECTC in April 2016, more than 90 % of the contributions by Member States regarding verified FTF came from just five member states.

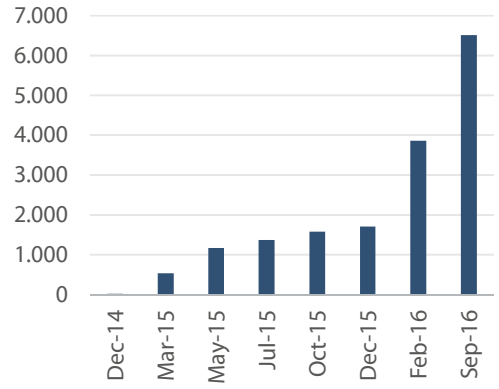
Figure 13 – Data subjects in the EIS (in millions)



Data source: EUROPOL, 2013; 2016; and 2017.

As reported by the ECTC, between 2014 and 2015, the number of queries in the EIS increased from 367 922 to 598 652. By the third quarter of 2016, the number of queries reached 1 025 052, according to Europol's work programme for 2017.

Figure 14 – Foreign terrorist fighters in the EIS



Data source: Europol, 2016, and 2017.

3.4.4. Proposed changes

While there are no proposals to revise the legal basis of Europol or the EIS, a number of proposals regarding other information systems will affect Europol. For example, the revision of the SIS will expand Europol's access rights, giving it full access to alerts on missing persons, on alerts issued for a criminal judicial procedure, and on future alerts on unknown persons. In its communication on stronger and smarter information systems, the Commission announced in April 2016 that it will explore, together with Europol, ways to 'promote synergies between the EIS and other systems, notably the SIS'.

3.5. Interpol's stolen and lost travel documents database

3.5.1. Purposes

The stolen and lost documents database (SLTD) was established in 2002 at the International Criminal Police Organization (Interpol). The database supports participating countries in their efforts to secure borders and fight against terrorism and other cross-border crimes involving the use of fraudulent travel documents. The SLDT is a global database, serving the 190 states that participate in Interpol. All EU Member States are members of Interpol.

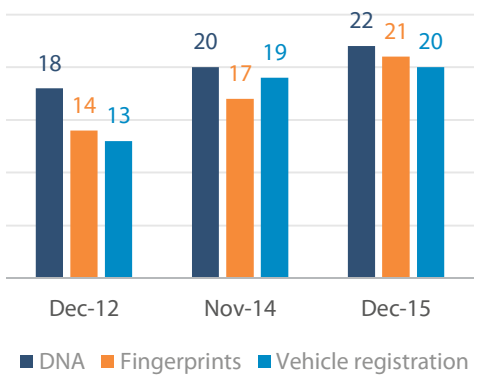
3.5.2. Data and access

Access to the SLTD is given to Interpol National Central Bureaus, established in each participating state, and to authorised law enforcement entities responsible for ascertaining the validity of travel documents (passports, identity documents, visas). Only the country that issued a document can add it to the database. Interpol is not automatically notified of all passport thefts occurring worldwide, and the SLTD database is not connected to national lists of stolen or lost passports.

3.5.3. Utilisation

According to Interpol's website, currently, the SLTD contains more than 68 million records from 174 countries. In November 2015, Interpol had records on around 12 000 suspects of terrorist offences and on around 5 000 suspected foreign terrorist fighters. Between January and September 2016, the database was searched 1.2 billion times, which resulted in more than 115 000 positive responses. However, member countries do not use the database evenly. As reported by the ECTC in March 2016, the number of searches in the SLTD by the authorities of EU Member States increased from 280 million to 360 million between 2014 and 2015. At the time, not all EU Member States were connected to the SLTD.

Figure 15 – Member states implementing the Prüm Decisions on key types of data



Data source: European Commission; 2015, ECTC, 2016.

3.6. The Prüm framework

3.6.1. Purposes

The Prüm framework is an instrument enabling participating states to exchange information for the purpose of preventing and investigating criminal offences. The framework was originally a multilateral treaty signed in 2005 in Prüm, Germany, by Austria, Belgium, Germany, France, Luxembourg, the Netherlands, and Spain. All EU Member States are now bound by the Prüm framework and should have implemented its provisions by August 2011. In June 2016, the Council authorised the Commission to start negotiations for the conclusion of agreements between the EU, on the one hand, and Liechtenstein and Switzerland, on the other hand, on the application of certain provisions of the Prüm Decisions.

Legal basis

Council Decision 2008/615/JHA; Council Decision 2008/616/JHA.

3.6.2. Data and access

The Prüm framework allows Member States to consult each other's data on DNA profiles, fingerprints, certain data related to vehicle registration and data in connection to events with a major cross-border dimension. For example, authorities in a Member State can compare DNA profiles or fingerprints found at a crime scene with profiles held in the databases of other Member States.

3.6.3. Utilisation

Although Member States have received financial and technical support from the EU to implement the Prüm Decisions, not all of them have done so (see figure 15). According to ECTC's report, by January 2016, 22 Member States had implemented the Prüm Decision with regard to DNA data, 21 Member States complied with the Prüm Decision with regard to fingerprinting and 20 Member States with regard to vehicle registration data. According to a study,[6] by November 2016, Croatia, Denmark, Greece, Ireland, Italy, and the UK had not yet implemented the Prüm Decisions on DNA data.

3.6.4. Proposed changes

The Council's roadmap recommended exploring the possibilities to associate Europol to the Prüm framework in view of enabling cross-matching of DNA fingerprints and vehicle registration with third countries.

3.7. Advanced passenger information and passenger name records

3.7.1. Purposes

Legal basis

Council Directive 2004/82/EC (API); Directive (EU) 2016/681 (PNR).

In view of improving border controls and combating irregular immigration the EU, in 2004, imposed an obligation on air carriers to communicate advanced passenger information (API), concerning their passengers travelling to the EU by air or sea, to the authorities responsible for carrying out border checks in the destination Member State. The API can also be used for law enforcement purposes, such as in proceedings aimed at the enforcement of the laws and regulations on entry and immigration, including the protection of public order and national security. Member States are also allowed to request API data from carriers for EU inbound flights.

In 2016, the EU obliged air carriers to transfer passenger name record (PNR) data from flights entering or departing from the EU. The Member States had to establish Passenger Information Units to be in charge of processing and analysing the PNR for the purpose of preventing, detecting, investigating and prosecuting serious crime and terrorist offences. The Member States can collect PNR concerning selected intra-EU flights, provided that they notify the Commission in this regard.

3.7.2. Data and access

API concern data from the machine-readable zone of the passport, including name, date of birth, passport number and nationality. PNR consist of booking information stored by airlines in their reservation and departure control systems: travel dates, travel itinerary, ticket information, contact details, means of payment used and baggage information. API and PNR serve different purposes: while API can be used to identify known terrorists and criminals by using alert systems, PNR allows for a risk assessment of unknown individuals through identifying specific behavioural patterns and associations between people. There is no central EU system to record API. PNR are collected by the Passenger

[6] Santos, F., Overview of the implementation of the Prüm Decisions, November 2016.

Information Units of the Member State and can be retained for a period of five years (they are anonymised after six months). Europol is entitled to access PNR or the result of data processing on a case-by-case basis and within the limits of its competences and for the performance of its tasks. The EU has concluded international agreements on the processing and transfer of PNR data with Australia, Canada and the United States. A previous PNR agreement with the United States was annulled by the European Court of Justice on the grounds of inadequate scope.

3.7.3. Utilisation

All Member States have implemented (API) Directive 2004/82/EC in national law. The (PNR) Directive 2016/681 has applied since May 2016. EU countries have to incorporate the directive into national law by 25 May 2018. By November 2016, only four Member States had functioning or nearly functioning PNR systems, while twelve other Member States were at different stages of implementing the PNR Directive.

3.8. European criminal records information system

3.8.1. Purposes

Legal basis

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

The Criminal Records Information System (ECRIS) is a decentralised information system that facilitates the exchange of information on criminal records between Member States. ECRIS was established in 2012. All Member States but Malta, Portugal and Slovenia participate in ECRIS.

3.8.2. Data and access

ECRIS enables judges and prosecutors to access information on a person's criminal history from other Member States, thus preventing offenders from concealing past criminal convictions by moving from one Member State to another. The criminal records data is stored in national databases and exchanged electronically between the central authorities of the Member States upon request. The Member State of nationality of a person is the central repository of all convictions handed down to that person. The convicting Member State must notify the authorities of the Member State of nationality, which are required to store and update all information received and retransmit them when requested.

3.8.3. Utilisation

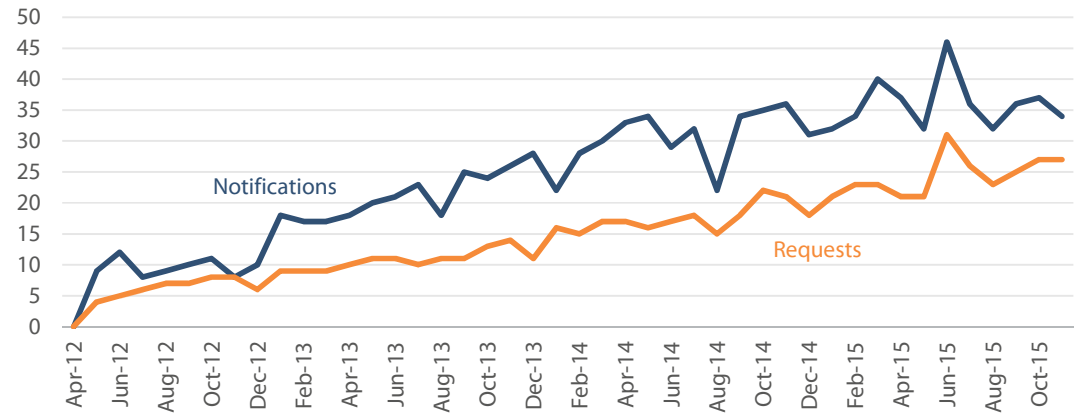
As reported by the Commission, the number of requests and notifications sent through ECRIS has increased gradually since the establishment of the system (see figure 16). By October 2015, the total volume of exchanges was about 35 000 notifications and 25 000 requests. Although it is possible to exchange information on third-country nationals through the ECRIS, the system does not allow determination of whether third-country nationals were previously convicted elsewhere without consulting the records of all Member States.

According to an impact assessment study by the Commission, although there were 558 000 third-country nationals convicted in 19 Member States in 2014, only 23 000 requests related to convictions of third country nationals were made in ECRIS in that year. This means that less than 5 % of convictions of third-country nationals took their criminal records in other Member States into account.

3.8.4. Proposed changes

In January 2016, the Commission adopted a proposal to upgrade ECRIS by establishing an index system enabling national authorities to determine which Member State holds criminal records of a third-country national. In its report on the proposal, the Parliament's LIBE committee insisted that all criminal records data should be stored solely in databases operated by the Member States within the territory of the Union, and proposed to grant Europol and Frontex access to the database. In its conclusions of June 2016, the Council expressed its support for a centralised automated system for the storage and exchange of both fingerprints and alphanumeric data and encouraged further discussion at the level of experts. The Commission has committed to put forward a revised proposal in June 2017.

Figure 16 – Requests and notifications sent through ECRIS (thousands)



Data source: European Commission, 2016.

3.9. Eurojust's case management system

3.9.1. Purposes

Legal basis

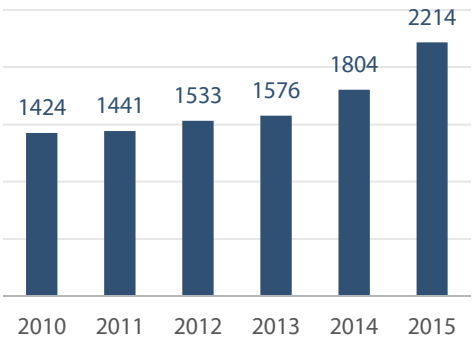
Council Decision 2002/187/JHA; Council Decision 2003/659/JHA; Council Decision 2009/426/JHA.

Eurojust is an EU body established in 2002 to stimulate and improve the coordination of investigations and prosecutions among the competent judicial authorities of the Member States when dealing with serious cross-border and organised crime. The case management system (CMS) is a database designed to store and process Eurojust's case-related data.

3.9.2. Data and access

According to Article 13 of Council Decision 2009/426/JHA, Member States are under a general obligation to exchange with Eurojust 'any information necessary for the performance of its tasks'. This allows for the exchange of personal data of suspects and offenders in cases of serious crime affecting two or more Member States, which may include biographical data, contact details, DNA profiles, fingerprints, photographs and

Figure 17 – Eurojust's cases



Data source: Eurojust; 2016.

telecommunication traffic and location data.

3.9.3. Utilisation

Eurojust has been increasingly involved in coordinating exchanges of information and the facilitation of legal requests between Member States. According to its 2015 annual report, the number of cases related to terrorism increased from 14 to 41 between 2014 and 2015 (see figure 17). According to ECTC's report, in 2015, 18 Eurojust cases concerned FTF. In the same year, Eurojust organised its first coordination centre on FTF and held 15 coordination meetings on operational terrorism cases, of which six were related to FTF. Between 2014 and 2015, the number of concluded court proceedings on terrorist offences reported to Eurojust increased from 180 to 217.

3.9.4. Proposed changes

In July 2013, the Commission put forward a proposal for a regulation on Eurojust, seeking to improve Eurojust's operational effectiveness. At the same time, the Commission presented a closely linked proposal on the establishment of a European Public Prosecutor's Office (EPPO). So far the negotiations on the two proposals have not met with success. In the European Parliament, the LIBE committee withheld its position on Eurojust while awaiting clarifications on the relations between Eurojust and the EPPO. In a non-legislative resolution, adopted on 5 October 2016, the Parliament reiterated its call on the Council to clarify its views on the matter.

3.10. Entry/exit system

On 6 April 2016, the Commission presented a proposal for establishing a new system for registering the entry and exit of non-EU nationals (including from visa-exempt third countries) crossing Schengen borders. The proposed regulation is a revised version of a legislative package presented by the Commission in 2013. The Commission explains that the new entry/exit system (EES) will facilitate border crossing of bona fide travellers, and will help detect over-stayers and identity fraud. It will also help to identify suspects, perpetrators or victims. If adopted, the system is expected to become operational by 2020.

The EES will replace manual stamping of passports at border checks with registration in a database. According to the proposal, the system will collect data about a traveller's identity, combinations of four fingerprints and facial images, and information about the date and place of entry and exit. The system will also record refusals of entry. Besides border, visa and immigration authorities, access to data will be given to Member States' law enforcement authorities and, under strict conditions, to Europol. The EES data will complement the information in the SIS. In order to achieve more efficient and rapid border checks, a connection will be established between the EES and the VIS.

The proposal is currently under discussion by the co-legislators. On 27 February 2017, the European Parliaments' LIBE committee adopted its position and decided to enter negotiations with the Council and the Commission. On 2 March 2017, the Council's Permanent Representatives Committee agreed on a negotiating mandate to start negotiations with the European Parliament. Some of the key issues raised during the discussions in the Council were related to the conditions of access to the database by law enforcement authorities and of transfer of data to third countries or non-participating EU Member States. In its report of 8 March 2017, the LIBE committee agreed to grant access to the EES to law enforcement authorities, but pushed for stronger data protection provisions. The co-legislators and the Commission share the objective of reaching a political agreement by the end of June 2017.

3.11. European travel information and authorisation system

On 16 November 2016, the Commission presented a proposal to establish the European travel information and authorisation system (ETIAS) as an automated system collecting pre-arrival information about non-EU citizens travelling to the EU. The aim of the ETIAS is to identify irregular migration, security or public health risks associated with visa-exempt third-country nationals travelling to the EU. According to the feasibility study for the ETIAS, over 1.2 billion people from 61 countries fall into this category. Registration in the ETIAS will also be mandatory for family members of EU citizens and for third-country nationals enjoying the right to free movement but who do not hold a residence card issued by a Member State.

The data in the ETIAS will be collected through an online application, in which applicants fill in their biographical and passport data, contact details, information on intended travel, as well as answers to background questions relating to public health risks, criminal records, presence in war zones and previous refusals of entry or an order to leave the territory of a Member State. The data provided by applicants will be checked against all relevant databases. While the possession of a valid travel authorisation is a precondition for entering the Schengen area, the final decision for granting or refusing entry will rest with the border guards at the border point of arrival.

The proposal is currently being discussed by the co-legislators. The key issues that emerged in the discussions in the Council related to the division of responsibilities between Member States, the conditions of access to data, and the interoperability of ETIAS with other systems. The Maltese Council Presidency has committed to reach an agreement by June 2017. In the Parliament, the proposal was assigned to the LIBE Committee.

4. Interoperability of information systems

The interoperability of information systems has been highlighted as a priority challenge in the European Agenda on Security. In its fourth report towards an effective and genuine security union, the Commission stated that there was a 'clear need for existing and future EU information systems to be searchable simultaneously using biometric identifiers to close off this avenue for terrorists and criminals.'

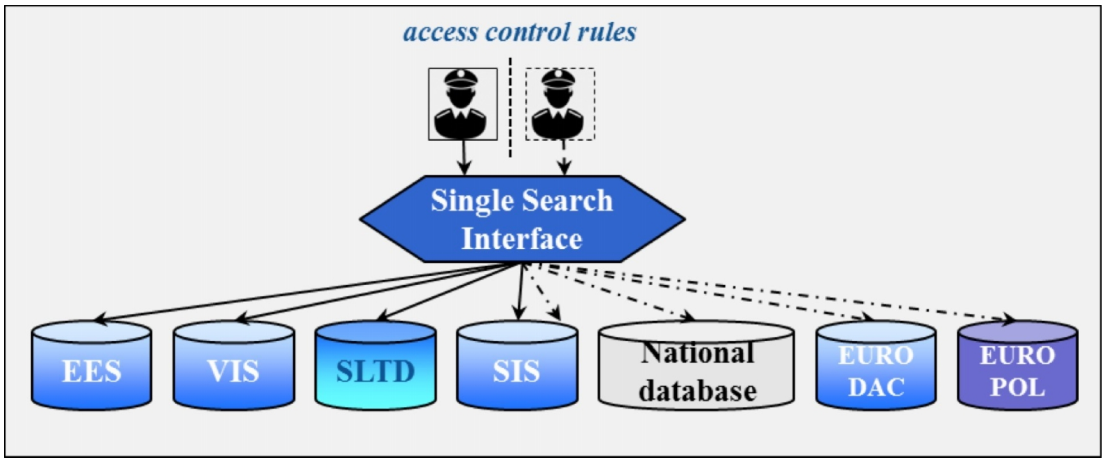
The Commission communication on stronger and smarter information systems explored options on how existing and future information systems could enhance external border management and internal security. It outlined four dimensions of interoperability:

1. Introducing a single search interface for accessing different information systems simultaneously;
2. Interconnecting information systems to allow data registered in one system to be automatically consulted by another system;
3. Establishing a shared biometric matching service that will support various information systems;
4. Establishing a common repository of data to be used by different information systems.

The single search interface will enable competent authorities to query several information systems simultaneously. The Council's roadmap to enhance information exchange identified the implementation of a single search interface as a priority action. In its interim report, the HLEG recommended the Commission start working on

establishing a single search interface that could be used without changing existing access rights (see figure 18).

Figure 18 – Single search interface for European information systems



Source: European Commission.

The HLEG expressed reservation with regard to interconnecting information systems. It decided to consider this option on a case-by-case basis, while evaluating whether data from one system could be automatically reused by another system. The proposal on establishing the EES envisages such an interconnection between the EES and the VIS.

According to the HLEG, sharing a biometric matching service would offer financial, maintenance and operational benefits and would enable single searches with biometric data. However, establishing a shared biometric matching service raises important legal issues related to the fact that each database serves specific purposes. A shared common repository of data implies the relocation of all alphanumerical identity data from existing information systems into a common repository. As this solution will have a significant impact on data protection, the HLEG recommends further reflection and the involvement of the EDPS and the FRA. The Commission announced a second set of proposals on interoperability for mid-2017.

5. European Parliament's position

The European Parliament has consistently advocated more effective cooperation between Member States' law enforcement authorities and to increase the use of European information systems, provided that appropriate safeguards on data protection and privacy are maintained.

In its resolution of 12 September 2013, the Parliament stressed that new IT systems in the area of migration and border management should be analysed carefully, in the light of the principles of necessity and proportionality. In its resolution of 17 December 2014, the Parliament called on the Member States to make better use of valuable existing instruments, including through 'more expeditious and efficient sharing of relevant data and information'. In its resolution on anti-terrorism measures of 11 February 2015, the Parliament restated its call on the Member States to make optimal use of existing databases and reiterated that 'all data collection and sharing, including by EU agencies such as Europol, should be compliant with EU and national law and based on a coherent data protection framework offering legally binding personal data protection standards

at an EU level'. In its resolution of 9 July 2015, the Parliament called for 'greater use of the existing instruments and databases such as SIS and ECRIS' and for 'the integration and further development of all aspects of judicial cooperation in criminal matters'.

In its resolution on the situation in the Mediterranean and the need for a holistic EU approach to migration of 6 April 2016, the Parliament stressed that the integrity of the Schengen Area and the abolition of internal border controls are dependent on having effective management of external borders and efficient exchange of information between Member States. In its resolution of 6 July 2016, the European Parliament called on the European Commission to present proposals to improve and develop existing information systems, to address information gaps and to move towards interoperability, accompanied by necessary data protection safeguards.

6. Main references

Bąkowski, P., Puccio, L., Foreign fighters: Member States' responses and EU action in an international context, EPRS, February 2015.

Bąkowski, P., Voronova, S., The proposed EU passenger name records (PNR) directive Revived in the new security context, EPRS, April 2015.

Dalli, H., Exchange of Information on Third Country Nationals – European Criminal Records Information System (ECRIS), EPRS, March 2016.

Dumbrava, C. Revision of the Schengen Information System for law enforcement, EPRS, March 2016.

Dumbrava, C. Revision of the Schengen Information System for border checks, EPRS, March 2016.

Dumbrava, C. Use of the Schengen Information System for the return of illegally staying third-country nationals, EPRS, March 2016.

Gatto, A., Carmona, J., European Border and Coast Guard System, EPRS, October 2016.

Gatto, A., Goudin, P., Niemenen, R., Schengen area: Update and state of play, EPRS, March 2016.

Ivanov, D., Reform of the Dublin System, EPRS, March 2017.

Maiani, F., The Reform of the Dublin III Regulation, European Parliament, Policy Department C, June 2016.

Malmersjo, G., Remáč, M., Schengen and the management of the EU's external borders, EPRS, April 2016.

Orav, A., Recast Eurodac Regulation, EPRS, March 2017.

Orav, A., Fingerprinting migrants: Eurodac Regulation, EPRS, November 2015.

Orav, A., D'Alfonso, A., Smart Borders: EU Entry/Exit System, EPRS, July 2016.

Radjenovic, A., European Travel Information and Authorisation System (ETIAS), EPRS, March 2017.

Voronova, S., Combating terrorism, EPRS, July 2016.

Wagner, M., Baumgartner, P., The Implementation of the Common European Asylum System, European Parliament, Policy Department C, May 2016.

QA-04-17-453-EN-N

The interconnections between border management, migration and internal security have become more apparent recently in the context of high inflows of refugees and irregular migrants and of increasing terrorist activities in the EU. To address these challenges, the EU has taken steps to revise and develop the European information systems in order to improve the collection, processing and sharing of data among Member States and relevant EU agencies.

This publication provides an overview of the existing and proposed European information systems in the area of justice and home affairs. It discusses the legal basis, the purposes, the scope of data and access, the utilisation and the proposed changes for each information system, including issues of interoperability.

This is a publication of the
Members' Research Service

Directorate-General for Parliamentary Research Services, European Parliament

PE 603.923
ISBN 978-92-846-1057-0
doi:10.2861/179068