EUROPEAN
COMMISSION

Brussels, 21.12.2016
SWD(2016) 450 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and articles 59 (3) and 66 (5) of Decision 2007/533/JHA

{COM(2016) 880 final}

TABLE OF CONTENTS

1. INTRODUCTION

The SIS II legal instruments[1] describe the system, how it is managed and how it must be used. The legal instruments also specify which aspects of SIS II must be evaluated and the timescales for that evaluation. Due to the wide-ranging nature of this evaluation, covering legal, operational, procedural and technical issues, a large part of this document is dedicated to the overall evaluation as described in section 2.1. The objectives of the two more tightly focused areas on alerts for refusal of entry or stay and remedies are also described below and subsequently addressed in dedicated sections in the report. The summaries below set out the evaluation objectives of each subject area.

1.1 OVERALL EVALUATION (ART 50 (5) SIS II REGULATION AND ART 66 (5) SIS II DECISION)

> *Three years after SIS II is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS II and the bilateral and multilateral exchange of supplementary information between Member States. This overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Decision in respect of Central SIS II, the security of Central SIS II and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.*

The evaluation objectives can be summarised as:

- evaluation of Central SIS II;
- the bilateral and multilateral exchange of supplementary information between Member States;
- an examination of results achieved against objectives;
- an assessment of the continuing validity of the underlying rationale;
- evaluation of the application of this Decision/Regulation in respect of Central SIS II; the security of Central SIS II;
- implications for future operations.

1.2 ALERTS ON REFUSAL OF ENTRY OR STAY (ART 24 (5) SIS II REGULATION)

> *The Commission shall review the application of this Article three years after the date referred to in Article 55(2). On the basis of that review, the Commission shall, using its right of initiative in accordance with the Treaty, make the necessary proposals to modify the provisions of this Article to achieve a greater level of harmonisation of the criteria for entering alerts.*

The evaluation objectives can be summarised as:

- review the application of this Article;

---

[1] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).
Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).
Although the evaluation is not covered in a third legal instrument its impact should also form part of the evaluation: Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).

- make the necessary proposals to modify the provisions of this Article to achieve a greater level of harmonisation of the criteria for entering alerts.

1.3 REMEDIES (ART 43 SIS II REGULATION AND ART 59 SIS II DECISION)

The evaluation objectives can be summarised as to collate and review the provisions in each Member State on: (a) a person's ability to bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him, and (b) the mutual enforcement of decisions in other Member States[2].

1.4 SCOPE

This evaluation covers all Member States as they all use SIS II (25 MS), will join imminently (Croatia) or intend to use it in the future (Cyprus and Ireland). The UK started using SIS II during the evaluation process (13 April 2015). The evaluation also covers four associated countries which use SIS II (Norway, Iceland, Switzerland and Liechtenstein) as well as the two agencies which are permitted access, namely EUROPOL and EUROJUST.

1.5 STRUCTURE OF THE STAFF WORKING DOCUMENT

In line with the principles of Better Regulation, this Staff Working Document follows the structure set out in Tool #47 of the European Commission's Better Regulation Toolbox. Section 1 contains an Executive Summary. Section 2 introduces the purpose and scope of the overall evaluation of SIS II and describes the structure of this paper. Section 3 sets out the background of the initiative, its components and how they fit together. Section 4 explains the evaluation concept and lists the evaluation questions. Section 5 provides information with regards to the method used in the overall evaluation. Sections 6 to 21 describe the answers to the evaluation questions. Within this, Sections 14 and 15 set out particular implementation challenges highlighted by respondents, related to the new functionalities in SIS II and the Automated Fingerprint Identification System. This maintains the internal logic of the document. Finally, section 22 summarises the findings and conclusions of the SIS II overall evaluation and these are listed in full in Annex 1.

2. BACKGROUND TO SIS II AND BASELINE

2.1 BACKGROUND TO SIS II AND BASELINE

The Schengen area was established by the 1985 Schengen Agreement that set out the gradual abolition of checks at common borders. The Agreement was supplemented by the 1990 Schengen Implementing Convention that set out the final abolition of internal border controls, as well as a series of necessary accompanying measures. The Schengen Agreement made passport-free travel possible for over 400 million Europeans. From the initial five Member States, the Schengen area without internal border controls now includes 26 countries. The participating countries apply common rules for checks at the external borders of the Schengen area, as well as rules on issuing visas and cooperation between law enforcement and judicial services in criminal matters.

In the absence of internal border controls, Member States had to address the issues of cross-border crime and irregular migration. This included assessing the most effective way for Europe-wide information sharing and legal assistance for the carrying out of national law enforcement, immigration and judicial decisions. It was clear that these could no longer be

[2] Note: Due to the date of entry into operation of SIS II it was not feasible to carry out this evaluation within the legally foreseen timescale. Accordingly, it is appropriate to include it in the overall evaluation.

achieved with traditional bilateral agreements and mutual legal assistance requests, due to the rapid movement of criminals and the need to act promptly. In order to effectively maintain a high level of security, Member States had to create a tailor-made instrument to:

- share security-related information in a centralised, structured way and move away from fragmented bilateral cooperation;
- make such information immediately available to all competent national authorities; and
- empower competent authorities in other Member States to act on behalf of requesting Member States.

However, the first generation of the Schengen Information System, which entered into operation in the mid-1990s, was not able to serve the needs of increasing number of Member States of the EU after its enlargement. Due to this, and in order to benefit from the latest IT developments and to provide end-users with new functionalities[3], it was decided that it was necessary to establish a new, second generation Schengen Information System (SIS II). As acknowledged in Decision SCH/Com-ex (97) 24 of the Executive Committee of 7 October 1997, "only SIS II will be able to meet a certain number of essential operational demands"[4].

2.2 THE SECOND GENERATION OF SIS (SIS II)

SIS II entered operations on 9 April 2013. New functionalities for operational end-users are:

- Enhanced alerts on persons and objects: vehicles, firearms, issued documents, blank documents, bank notes.
- New categories of alert: stolen aircraft, boats, boat engines, containers, industrial equipment, securities and means of payment.
- The ability to conduct direct queries in the central system, as opposed to the previous practice of all queries being carried out in a national copy of the data.
- Linking of alerts on persons, objects and vehicles (e.g. alerts on a wanted person and the stolen vehicle he/she is using).
- Biometric data (fingerprints and photographs).
- A copy of the European Arrest Warrant (EAW) attached directly to alerts for persons wanted for arrest for surrender or extradition.
- Information on misused identity preventing the misidentification of the innocent party in identity fraud.

Data on persons stored in SIS II are:

- the data necessary to locate a person and confirm his/her identity (now including a photo and fingerprints, where available);
- relevant information about the alert (including the action to be taken).

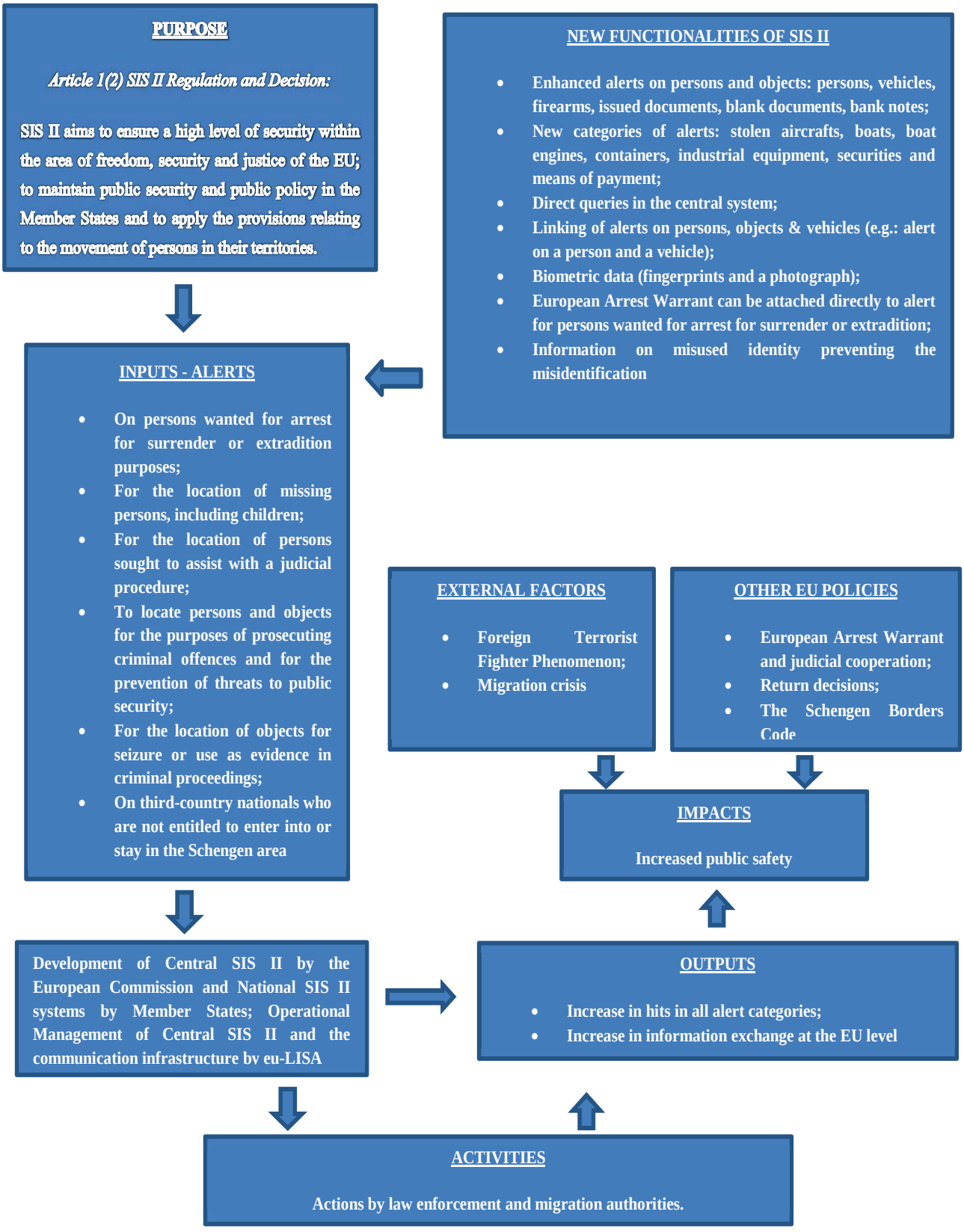
Fingerprints are currently used to confirm an identity but in the future they may also be used to establish the identity of a person.

2.3 INTERVENTION LOGIC

[3] Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II) (OJ L 328, 13.12.2001, p. 4).
Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II) (OJ L 328, 13.12.2001, p. 1).

[4] Decision of the Executive Committee of 7 October 1997 on the development of the SIS (SCH/Com-ex (97) 24) (OJ L 239, 22.9.2000, p.442).

As set out in the SIS II legal instruments, the purpose of the system is to contribute to the maintenance of a high level of security within the area of freedom, security and justice of the European Union. It enables law enforcement and migration authorities to enter and consult alerts on persons and objects and provides end-users with new functionalities in order to facilitate their operational needs. Essentially, a significant increase in information exchange at the EU level has been witnessed since the establishment of SIS II. The system has also demonstrated its flexibility in responding to the dynamic security and migration environments, exacerbated by the foreign terrorist fighter phenomenon and the migration crisis. The simplified intervention logic diagram below explains how the different components of SIS II fit together.



Simplified Intervention Logic

3. THE EVALUATION QUESTIONS

3.1 THE EVALUATION PROCESS

The evaluation was carried out by Commission staff supported by external supporting studies in four areas: remedies, use of alerts for refusal of entry or stay and consultation procedures where a residence permit and an alert for refusal of entry or stay may co-exist as well as about the role of the SIRENE Bureaux in the European police information exchange. The list of studies are set out in Annex II.

The evaluation followed an iterative process: issues were raised in the questionnaire phase and clarified through interviews so that all issues could be raised in a comprehensive and transparent way. These issues were shared in dedicated meetings/workshops aiming to arrive at a shared understanding and assessment. Moreover, the Commission has set up an Inter-service Steering Group with the participation of the General Secretariat, DG HOME, DG JUST, DG HR and DG DIGIT which monitored the evaluation process and provided the necessary guidance. The dates of the relevant meetings are attached in Annex III.

The analysis was based on both qualitative and quantitative evidence. A qualitative assessment was carried out, outlining a number of initiatives designed to solve issues or improve guidance on the use of SIS II. Quantitative data were collected in order to provide the statistics needed for the reports, benefiting from the fact that SIS II was designed legally and technically from the outset to provide statistics on its use and effectiveness, which is an unusual feature amongst law enforcement cooperation systems.

The intention of many of the questionnaire elements was to establish effectiveness, relevance and coherence, with a view to identifying potential improvements in these three areas and thereby increase EU added-value. Where inefficient procedures were identified or had already been eliminated, this was also highlighted.

The evaluation made use of the extensive figures on the use of SIS II and the performance of the system itself, gathered and published (to a restricted audience) by eu-LISA. It also used Member State statistics on the exchange of supplementary information and hits on alerts.

3.2 EVALUATION QUESTIONS

3.2.1 Evaluation of Central SIS II and the application of the Decision/Regulation in respect of Central SIS II

The evaluation of the technical and operational management aspects of SIS II incorporates the findings of the report prepared by eu-LISA under Article 66(4) of the SIS II Decision[5]. This report describes the technical functioning of the Central SIS II and the network, including the security thereof, between its entry into operation on 9 April 2013 and 31 December 2014. It sets out how SIS II performed against expectations, addressing issues related to SIS II effectiveness, efficiency, relevance, coherence and EU added-value.

3.2.2 Security of Central SIS II

The evaluation of the security of Central SIS II was based on the eu-LISA report mentioned above and on relevant sections from a European Data Protection Supervisor audit carried out on Central SIS II in 2014[6].

[5] eu-LISA document 2015-094 Rev 1.

[6] Report on inspection pursuant Article 47(2) of Regulation (EC) N. 45/2001 on the Schengen Information System II (SIS II) managed by the EU Agency for large-scale IT systems (eu-LISA) case reference: 2014-0953.

3.2.3 Alerts

The questions on the technical and operational aspects of the SIS II covered the following operational and legal issues:

A. What problems are experienced in operational work that are caused by the wording of the relevant Article? (*What does not work as well as it might?*)
B. What are the obvious gaps in operational capability that are not covered by the legal instruments? (*What do you need to do but cannot?*)
C. Which concrete proposals, if any, could improve the text to overcome these issues? (*What do you propose to overcome these problems or gaps?*)

3.2.4 Other provisions of the SIS II legal instruments

A. What problems are experienced in your work that are caused by the wording of the relevant Article? (*What does not work as well as it might?*)
B. What are the obvious gaps that are not covered by the legal instruments? (*What do you need to do but cannot?*)
C. Which concrete proposals could improve the text to overcome these issues? (*What do you propose to overcome these problems or gaps?*)

3.2.5 Use of Art 24 of the SIS II Regulation on refusal of entry or stay

The following questions were addressed to the Member States via the Commission-chaired European Migration Network.

1. Do Member States have statistics on how many entry bans are entered into SIS II due to the non-compliance with national migration laws and as a sanction of a criminal offence (national grounds for the imposition of entry bans)?
2. What duration of overstaying on the territory of a Member State is sanctioned with an entry ban entered into SIS II?
3. What is the major ground for the consultation procedure pursuant to Section 4.5 of the SIRENE Manual[7] (namely (i) the procedure provided under Art. 25 (1) of the Schengen Convention, (ii) the procedure provided under Art. 25 (2) of the Schengen Convention, (iii) procedure in cases falling under Art. 6(5) (a) of the Schengen Borders Code[8], or (iv) procedure in cases falling under Art. 6(5) (c) of the Schengen Borders Code)?
4. Do Member States use the consultation procedure?
5. How many successful consultation procedures were conducted in 2013 and 2014?
6. What are the national deadlines for a consultation procedure?
7. What sorts of difficulties have Member States encountered with the consultation procedure?
8. Are there special procedures for such consultation with regard to persons enjoying the right of free movement?

3.2.6 Bilateral and multilateral exchange of supplementary information between Member States

This section was completed through:

---

[7] Commission Implementing Decision (EU) 2016/1209 of 12 July 2016 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2016) 4283) (OJ L 201, 28.07.2016, p.35).

[8] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

- a statistical assessment of the exchange of supplementary information between the Member States;
- a questionnaire survey to all Heads of SIRENE Bureau on their ability to comply with the requirements of the SIRENE Manual;
- identification of any gaps in operational needs which should be addressed; and
- discussion papers addressed at workshops in Brussels with delegates to the SISVIS Committee.

3.2.7 Examination of results achieved against objectives and any implications for future operations

This section was completed through:

- a statistical assessment of the use by Member States of the categories of alerts and the hits achieved (this included the use of SIS II by the Member States' authorities responsible for the registration of motor vehicles);
- a questionnaire survey to all Heads of SIRENE Bureau on:
  - the capacity of existing alert categories to meet operational needs
  - the identification of under-used alert categories
  - the reasons for under-use
  - the identification of operational needs which are not met by current alert categories
- discussion papers addressed at workshops in Brussels with delegates to the SISVIS Committee;
- a statistical assessment on the implementation of alerts for refusal of entry or stay;
- a questionnaire survey to the relevant authorities in each Member State seeking a description of national procedures leading to the creation of alerts for refusal of entry or stay and the ongoing management, updating and deletion of alerts.

3.2.8 Assessment of the continuing validity of the underlying rationale

This element was completed through:

- a questionnaire survey to Heads of SIRENE Bureau, Heads of N.SIS II[9] and other relevant authorities on aspects of the SIS II legal instruments which are viewed as not fully fit for purpose on whatever grounds;
- discussion at workshops in Brussels with delegates to the SISVIS Committee;
- a conclusion to the evaluation report which answers the question on the continuing validity of the underlying rationale and sets out concrete proposals from the Commission.

3.2.9 Remedies

This section contains the key points of the report provided by the SIS II Supervision Coordination Group[10] and the information gleaned from the targeted questionnaire. Detailed questions on specific areas were forwarded to the national contact points.

1. Please describe the procedures in your Member State for any person to bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert

[9] N.SIS II is the term used for the national side of SIS II in each country connected to Central SIS II.

[10] Report from the chair of the SIS II Supervision Coordination Group on the exercise of the rights of the data subject in SIS and Guide for exercising the right of access in SIS of 16 December 2014 - Council document 16807/14 SIRIS 82 COMIX 668.

relating to him. Include procedures: (a) within your country; (b) where the applicant is in another Schengen State; (c) where the applicant is in a third country.
2. In the cases described above (a-c), are there any fees or costs involved or implied for the applicant?
3. If the applicant is in a third country how do you verify their identity and right to make the application?
4. Please provide any available annual statistics covering 2013 and 2014 on the use of such remedies by any person (if possible the total number of cases per year; the number of cases per year where the court or authority ruled in favour of the applicant; the number of cases per year where compensation was paid; the financial value, in total per year of the compensation paid).
5. Please describe your provisions for mutual recognition and enforcement of final decisions handed down by the courts or authorities of other Schengen States on alerts created by your country.

The evaluation report outlines findings for areas where improvement is required on the basis of the exhaustive report and questionnaire.

4. METHOD

4.1 TIMESCALE

Due to the need to evaluate key elements of the functioning of SIS II after three years of operation, the evaluation started in February 2015 and covers the period from April 2013 to the end of 2015.

4.2 METHODOLOGY AND DATA COLLECTION

The methodology for the evaluation followed a three phase approach:

1. a design phase where the evaluation team structured questions and activities, described in the evaluation mandate and presented to the inter-service steering group;
2. a data gathering phase to collect the evidence required;
3. the analysis, judgment and reporting phase, where the evidence was analysed in order to identify observations and recommendations.

4.2.1 SIS II technical architecture

In order to evaluate the effectiveness and efficiency of the complex technical architecture of SIS II, a study was launched with the following objectives:

- Assess the implications for efficiency and cost-effectiveness of the national ICT architectures in relation to Central SIS II, with a view to making observations and recommendations on developments at central level which could make the national technical implementation of SIS II more efficient and cost-effective. The impact of the architecture of the central system on the Member States' choice of technology was assessed, without entering into an assessment of Member States' chosen solutions as this was out of the scope of the evaluation.
- Assess the existing central SIS II infrastructure and, in particular, its interactions with national systems, with a view to making recommendations to improve efficiency and cost effectiveness at both central and national level.

Further work was carried out with an ICT impact assessment on possible improvements to the SIS II architecture. The assessment studied the cost and complexity of possible change scenarios by looking at the impact at central level and also in several Member States.

4.2.2 Responsibilities of the 'Management Authority' (eu-LISA) for Central SIS II

The SIS II legal instruments require eu-LISA to submit a report on the technical functioning of Central SIS II and the network, including security, and on the bilateral and multilateral exchange of supplementary information between Member States[11]. The first report was published in June 2015[12]. To complement this information, the Commission requested an amended set of information from eu-LISA specifically for the evaluation. However, it should be noted that as eu-LISA is the subject of separate evaluation mechanisms, its evaluation was out of scope for this document.

4.2.3 SIS II security and data protection

The security provisions relating to the processing of personal data for the Central SIS II are set out in Article 16 of both the SIS II Regulation and Decision. The legal instruments set out the responsibilities of the European Data Protection Supervisor (EDPS) with regard to checking that the personal data processing activities carried out by eu-LISA are in accordance with the legal instruments. The EDPS ensures that personal data processing activities are audited at least every four years in accordance with international auditing standards. The EDPS audit was taken into consideration in addition to the report from eu-LISA.

4.2.4 SIS II alerts and procedures

The most important source of information for evaluating the use of SIS II by Member States is the Schengen Evaluation Mechanism. Since the entry into operations of SIS II, the use of SIS II and the functioning of the SIRENE Bureaux[13] has been evaluated in 18 Member States[14] under this mechanism.

Member States were consulted through the SISVIS Committee, which includes the Member States' representatives on both operational SIRENE and technical matters on SIS II and the related SIRENE application. 21 Member States responded (of the 28 Member States and Associated Countries using SIS II at the time of distributing the questionnaire; the UK commenced use on 13 April 2015).

4.2.5 Alerts for refusal of entry or stay under Article 24 of the SIS II Regulation

Different sources of data were used:

- Questionnaire to the delegates of the SISVIS Committee.
- Two queries launched by the European Migration Network (EMN): No 2014.628 on registering entry bans in the SIS II (20 responses received) and No 2015.662 on entry bans entered into the SIS II and consultation procedures in the Member States (25 responses received).
- Data collected within the context of the external study on the use of SIS II for return purposes. The study set out to analyse the feasibility and the legal, operational and practical implications of the incorporation of return decisions and all entry bans in SIS II. Although the study is a forward-looking exercise it revealed information on the current application of Article 24 of the SIS II Regulation.

---

11 Articles 66 (4) of the SIS II Decision and 50 (4) of the SIS II Regulation.

12 eu-LISA document 2015-094 Rev 1 http://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20Technical%20Report%202015.pdf

13 SIRENE stands for Supplementary Information Request at the National Entries. Each state operating the SIS II has established a national SIRENE Bureau, operational 24/7, which is responsible for any supplementary information exchange and coordination of activities connected to SIS II alerts.

14 Old mechanism: Slovenia, Malta, Slovakia, the Czech Republic, Hungary, Poland, Estonia, Latvia, Lithuania, Switzerland, the United Kingdom. New mechanism (Council Regulation (EU) No 1053/2013 of 7 October 2013): Austria, Belgium, Germany, the Netherlands, Liechtenstein, Luxembourg and Italy.

- Statistics collected by eu-LISA and Eurostat.
- Synthesis Report for the EMN Focused Study 2014. Good practices in the return and reintegration of irregular migrants: Member States' entry bans policy and use of readmission agreements between Member States and third countries.
- Evaluation on the application of the Return Directive (2008/115/EC). Final Report. European Commission — DG Home Affairs. 22 October 2013.

4.2.6 Remedies

In December 2014, the Chair of the SIS II Supervision Coordination Group presented a report to the Council (doc 16807/14) on the exercise of the rights of the data subject in SIS II and a guide to the right of access. The report provided a comprehensive overview on rights of access, correction and deletion of data and the right to have data checked in SIS II. To update the report with more recent information, the members of the SIS II Supervision Coordination Group were consulted in June 2015.

5. FINDINGS OF THE EVALUATION CONCERNING THE CENTRAL COMPONENTS OF SIS II AND THE APPLICATION OF THE LEGAL INSTRUMENTS IN RESPECT OF CENTRAL SIS II

5.1 CENTRAL SIS II

Effectiveness

The key mechanism for checking data consistency between Central SIS II and national copies of SIS II data works effectively but is a relatively heavy mechanism, largely due to the differences in implementation at national level causing inconsistencies. Approximately 15 % of data consistency campaigns with the Member States ran without any discrepancy on both alerts and links between related alerts. Some Member States have no issue; this confirms that it is possible to reach zero discrepancies and the design of the system, *i.e.* having a central database and national copies, is not the root cause per se. An update to the analysis and reporting mechanism resulted in more accurate identification of discrepancies and a lower overall total. This made the data consistency monitoring more effective and efficient to both eu-LISA and Member States, as Central SIS II had the means to detect and repair discrepancies found during data consistency campaigns. This allows a good level of confidence in the accuracy of alerts in the national copies of a large majority of Member States. Central SIS II is reaching the limits to its capacity to carry out data consistency campaigns, as the architecture only permits one campaign with one Member State at a time.

eu-LISA has outlined eleven technical options and three procedural options to improve data consistency. Some of these have only minimal financial, technical and procedural impact, while some are quite radical. Given that the impacts will always be balanced and shared between all the SIS stakeholders, a study would be the best vehicle to assess which option or combination of options would improve the data consistency process.

Due to Central SIS II's ability to report on data discrepancies, there has been no need to restore a national copy.

The provision of a back-up site for Central SIS II has demonstrated effectiveness due to the ability to switch operations during either maintenance or incidents. Since the entry into operations five switchovers have taken place: four were planned due to upgrades to the central system and one was unplanned, after a database upgrade. These switchovers covered, in total, 97 hours of operational time. Effectiveness could be improved; the current technical set-up requires the passive back-up site to be started and shut down. As a result, any month that requires a switch to the back-up site risks taking the system below its availability

requirement of 99.99 % availability to the Member States. An active-active technical set-up with the back-up site running constantly in the background would be more effective.

Efficiency

A few Member States still need to improve their national technical implementation in order to reach zero discrepancies. Much of this could be achieved by the Member States in question implementing the technical specifications (the Interface Control Document — ICD) as envisaged. This would allow data consistency campaigns to run more smoothly against a frozen snapshot of the data in order to avoid detecting 'false discrepancies' caused by alert updates taking place in the middle of a consistency campaign. This situation still leads to an inefficient and unexpected burden for monitoring the campaigns and the repair activity to ensure synchronisation between national and central systems. The persistence of this issue in some Member States requires eu-LISA to plan additional resources to support them. The variation in interpreting the ICD at Member State level is a major cause of this inefficiency. For example, some Member States send a deletion notification to Central SIS II but then only carry out the deletion later that day in a batch. This can represent nearly 60 % of the discrepancies in a data consistency check, causing unproductive work at both eu-LISA and national level.

Central SIS II has a functionality which corrects the inconsistencies. However, this does not prevent investigation after the repair to seek an avoidance of repetition.

Due to the diversity of national systems, a standardised solution to resolve all national data consistency issues cannot be put in place. This is a logical outcome of the choice to pursue different technical solutions at Member State level. eu-LISA has increased efficiency at both central and national levels, by raising issues with Member States when automatic reports for restoring consistency have not been acted upon. Through consistently pursuing each issue, Member States repaired the elements of their national systems which had prevented repair. This type of incident has now been eradicated.

Relevance

Given the detailed description of the work carried out in order to support the three key roles of Central SIS II, the relevance of the legal instruments remains high.

Coherence/Consistency

Variations in interpreting the technical specifications at national level cause some internal inconsistency which could be reduced or removed.

EU added-value

The architecture of SIS II, *i.e.* having a central database and national copies, has a substantial EU added value as due to the centralised solution Member States can perform one query via Central SIS II and it does not need to send queries to all other Member States which would be necessary in case of a decentralised system. Moreover national copies ensure business continuity in case of the unavailability of Central SIS II or the network.

5.2 SIS II TECHNICAL ASSESSMENT

Although it has been a significant operational success, SIS II is perceived by some Member States as being a complex system that is difficult to use efficiently and requires high development and operational costs. One of the primary reasons for this complexity is the flexibility offered to Member States in implementing their national solutions. This has resulted in diverse systems that require an increased support overhead and pose concerns with regards to business continuity. In addition, expected future needs, especially with regards to increased use of the system, might benefit from the current architecture being adapted to address issues in a forward-looking manner. This technical assessment identifies the key

current issues and future needs that should be addressed, identifying concerns with regards to maximising business continuity and ensuring that the overall architecture can adapt to meet increasing capacity requirements.

5.2.1 Identified issues

Business continuity — effectiveness, efficiency and coherence/consistency with the legal base

In the past years of operation of SIS, loss of business continuity has been experienced rarely, and has been related primarily to failover issues at the national level. Cases where Central SIS II has been unavailable are primarily due to network issues, whereas planned upgrades of Central SIS II are largely transparent to the Member States with the effect limited to increased alert processing time for the duration of the Central Unit (CU) and Backup Central Unit (BCU) switchover. Certain types of planned upgrades however are foreseen to cause full unavailability of Central SIS II resulting in both the CU and BCU being unavailable for limited periods. In such cases the main impact is on the N.SIS II without a national data copy, resulting in complete loss of business continuity, with a more limited, but still considerable effect on the N.SIS II with partial data copies or partial query functionality. National implementations with full data copies are affected to the extent of data desynchronisation that is later addressed through the message queue handling, albeit with delayed processing. Albeit infrequent, potential business continuity loss is recognised as a key area where all possible solutions are considered taking into account the critical nature of SIS.

Data consistency— effectiveness, efficiency and coherence/consistency with the legal base

There are no significant problems with regards to data consistency between central data and national copies. Cases where Data Consistency Check (DCC) campaigns have resulted in extensive synchronisation requirements are typically isolated to specific national implementations, indicating a localised problem. The causes of failed consistency checks are investigated by eu-LISA, in discussion with the national authorities. National DCC campaigns are an area with potential for improvement. This depends entirely on national implementations and is outside central control. One area that should be considered in particular is the overall complexity of the DCC campaigns. Even though the campaigns do not currently suffer from technical problems, they are perceived as being complex to set up and follow up, and are a potential bottleneck if SIS II data increase significantly.

Data consistency problems do occasionally appear between the alert data recorded in the Central SIS II and their representation in national source systems (e.g. law enforcement systems). This may be due to incomplete implementation in the N.SIS II where updates to a national source system may not trigger alert updates in SIS, and inversely, where updates received from the Central SIS II related to data recorded in the national source system (i.e. not limited to a national SIS copy) are not correctly reflected in the national source system.

Inefficient handling of biometric data — efficiency

Fingerprints and photographs are currently stored in the Central SIS II to allow them to be included in relevant query responses. Apart from being used in responding to queries however, biometric image data recorded in this way cannot be otherwise analysed for matching purposes. A specialised biometric data handling system such as an AFIS would be more appropriate. An additional consideration regarding biometric data is the large storage capacity that would be required in the Central SIS II database if biometric data use increases, especially for any future use of photographs for facial recognition, if legally permitted. An increase in use of biometric data is expected, making the necessity of processing and storing in a more effective manner, increasingly important.

Data quality — effectiveness and coherence/consistency with the legal base

Data quality problems have been cited by numerous Member States as a frequent and recurring issue. Example cases that have been raised include:

- basic information missing from alerts such as a person's gender or date of birth;
- inconsistent encoding of information, such as placing a date of birth in the name field or using the text 'Unknown' for missing values;
- problems regarding the consistent transliteration of textual information, notably person names, with respect to ICAO standards to allow effective searching of non-Latin characters by Member States where they are not supported;
- the image quality of fingerprints and photographs that impairs biometric data matching.

Incomplete national ICD implementation — effectiveness and coherence/consistency with the legal base

The SIS Interface Control Document (ICD) details the data exchange between the N.SIS II and Central SIS II, driving the implementation of national solutions. The interpretation of this technical document offers a degree of flexibility to Member States with regards to the implementation of their N.SIS II. This can result in inconsistent national implementations that do not cover fully some features in Central SIS II, such as complex search options. This results in potentially missed opportunities when carrying out queries.

National systems with local copies that are configured to use the Central SIS II for certain searches effectively rely on Central SIS II for the full set of SIS features, with no back-up scenario in case of Central SIS II unavailability. A case where this is considered currently unavoidable is the fuzzy searching of alerts where query results depend on the specific tool or algorithm used. The possibility of national implementations using central services should ideally be a source of flexibility to Member States in balancing their query needs between Central SIS II and N.SIS II. An incomplete national ICD implementation, however, would mean that this flexibility could manifest itself as a loss of business continuity if the Central SIS II becomes unavailable.

Excessive query logging at national level — efficiency and coherence/consistency

Article 12(3) of the SIS II Decision stipulates that all searches performed on alerts need to be logged, including the data that was used for the search. This has implications for both Central SIS II and the N.SIS II, in terms of additional processing to record the log entry but also in terms of storage capacity to maintain the log information. Several Member States have raised the concern that with solutions that perform large numbers of automated queries such as Automatic Number Plate Recognition (ANPR), the number of queries can reach the level of millions per day. It is clear that maintaining a log of all such automated queries will increase storage requirements for the N.SIS II and, even if performed asynchronously, will affect their overall processing capacity.

Alert history logging at national level — efficiency and coherence/consistency

As with the logging of queries, Article 12(3) of the SIS II legal instruments requires N.SIS II to log the history of alerts. As all alert modifications are channelled through Central SIS II, the alert history log is also maintained centrally. Article 9(2) nonetheless stipulates that an N.SIS II holding a national data copy needs to ensure it is identical to the central data. Maintaining national copies of the alert history log increases storage capacity requirements and processing for the N.SIS II, leading to suggestions from Member States that the alert history should be recorded and queried at central level only. However, a national alert history copy currently represents a key information source for national data protection authorities.

Removing the alert history at national level would require an alternative means of obtaining the required information when carrying out data protection checks at national level.

Consistent network management — efficiency

The SIS II legal instruments split network management between the Commission and eu-LISA along the lines of financing and contracting versus supervision, security and provider-relations. It is advisable to confer the sole responsibility to eu-LISA for managing the network as the entity in charge of the operational management of Central SIS II and the communication infrastructure.. Furthermore, it is advisable that network decisions are made commonly, covering the possibility of a common network access point for additional systems including VIS and EURODAC. Consolidating network responsibilities is expected to streamline network management, provide a single point of contact to Member States, and allow for more effective reactions to networking problems.

Inefficient change management procedure — efficiency

The change management procedure for SIS II has been raised on several occasions in the SISVIS Committee meetings. One of the main issues relates to when and how the SISVIS Committee is involved in the change management process, notably regarding initiating and endorsing changes before changes are implemented and ensuring that interest of the end-users is duly taken into account throughout the process. The analysis of the change requests from technical point of view is carried out by eu-LISA assisted by Member States in the SIS II Advisory Group and in particular in its sub-group, the Change Management Group. The recommendations of the Change Management Group must be adopted with consensus by the Advisory Group. The SISVIS Committee must deliver an opinion on the changes which require national implementation. Strong coordination is required from eu-LISA and the Commission to ensure the full consistency of the process.

Moreover, the change management process must remain flexible concerning SIS by allowing changes to be made rapidly if operational needs require so. During the operation of SIS II changes related to foreign fighters have been implemented very quickly by eu-LISA and Member States, other changes (e.g. adding laissez-passer issued by the European Union to the code tables, shortening the expiry date for credit card alerts, etc.) however, very subject of a very long procedure. An additional challenge of the process relate to the complexity of making changes in SIS II at national level which requires national systems and relevant end-user applications to be updated in addition to the central system. Therefore, it is rather difficult to set a target date when all Member State can implement the change at the same time. It necessitates strong coordination and discipline from eu-LISA as well as from Member States.

5.2.2 Future needs

The key future technical challenge is the expected increase in use of SIS II. This increased use could be the result of expansion of its user base, e.g. including national immigration and naturalisation service authorities that are responsible for decisions regarding requests of admission and naturalisation of third-country nationals, or wider access for Europol as well as a new access to the European Border and Cost Guard Agency. The addition of an AFIS would increase the number of transactions; for example, visa applicants would be checked in SIS II using fingerprints as well as name and date of birth to ensure that they have not tried to use an alias.

The highest source of use for SIS II is expected to come from automated checks such as automatic ANPR, and facial recognition (if legally permitted) at border control points such as airports. Automated checks such as these generate millions of queries per day and huge increases in query requests can be experienced when Member States introduce such systems.

The underlying concern, however, for the future capacity of SIS II is the need to increase storage capacity.

Increased alert information — effectiveness and efficiency
Future changes are expected to increase the amount of information held in alerts. As well as including additional information, alerts will also include coding that allows the national and central systems to treat information differently. This will:

- provide as much information as possible in the alert, minimising supplementary information exchange through SIRENE forms;
- allow alerts to be better categorised (e.g. on missing person cases); and
- improve alert flagging so that alerts can be temporarily suspended or deleted.

Extended use of biometric data — effectiveness and efficiency
One of the new functionalities in SIS II is the use of biometric data, including the impending automatic matching of fingerprints and, later, facial recognition (if legally permitted).

Extension of automated tasks on alerts — efficiency
As part of the feedback provided to the evaluation, Member States commented on additional automation in handling alerts. This includes the automatic update of alerts (for missing person cases when a child becomes an adult) and automatic deletion (when the executing Member State forwards a valid address to the issuing Member State in relation to alerts on persons sought to assist with a judicial procedure). Automated processes and scheduling are already implemented in SIS II; the extension of these is not considered likely to have an effect on the overall system architecture.

5.2.3 Conclusions
This assessment began by establishing a baseline of issues to consider in developing technical solutions, drawing on currently highlighted issues and expected future needs with technical implications. The key needs identified in this process are: (i) ensuring maximum business continuity, taking all possible steps to address current limitations and (ii) ensuring that SIS II is capable of handling the increased usage, especially in terms of querying, expected in the near future.

Central SIS II and overall architecture
- The 'read capacity' and performance of Central SIS II should be increased.
- There should be a back-up site update and upgrade process to ensure minimal business continuity loss.
- There should be increased central system test capabilities.
- There should be the possibility to develop N.SIS II implementations, shared between Member States.

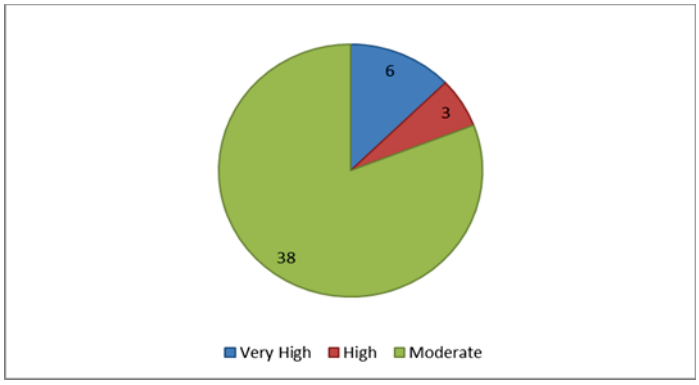
National optimisation and harmonisation (a distinct N.SIS II developed by each Member State)
- The logs on alert history, retained at national level should be optional.
- Query logging should be selective, especially in cases such as ANPR, and subject to standardised rules.
- XML messages should be replaced with JSON objects (technical change on data exchange format).
- ICD national implementation should be complete implementation of the ICD.
- National copies (partial) for N.SIS II should be mandatory.
- Each N.SIS II should have a mandatory back-up system.
- There should be a common blueprint for consistent N.SIS II configuration.

5.3 THE SECURITY OF CENTRAL SIS II

The European Data Protection Supervisor (EDPS) carried out a security audit in relation to SIS II (the subject was also covered in the evaluation of eu-LISA). This made recommendations that, when addressed by eu-LISA, will improve overall SIS II security and compliance with ISO/IEC 27 001 and CD(2006)3602. While all of the EDPS recommendations are important, recommendations on 'security policy' and 'risk assessment' should be implemented as a priority. No recommendations were made in relation to the architecture of SIS II and the services offered by the central unit of the system, although several procedural issues were highlighted. eu-LISA should make sure that when implementing the EDPS recommendations, it covers all provisions relating to the security of Central SIS II, which are mentioned in Regulation (EC) No 1987/2006

5.3.1 Coherence — network security

Security is provided effectively and is consistent with the legal instruments. The Commission asked eu-LISA to provide a detailed breakdown of the most critical network incidents affecting the availability of the SIS II between its entry into operations and the date the information was provided.



Overall breakdown of the incidents by their severity

5.3.2 Conclusions

No recommendations were made in relation to the architecture of SIS II or the services offered by Central SIS II. Taken together with the results of the analyses of incidents in Central SIS II and the network, which showed that there had been no incidents where the integrity of SIS II data was compromised, the overall conclusion is that Central SIS II security is highly effective.

6. THE RESULTS ACHIEVED BY SIS II AGAINST THE ORIGINAL OBJECTIVES AND THE CONTINUING VALIDITY OF THE UNDERLYING RATIONALE OF SIS II

6.1 NUMBER OF VALID (NON-EXPIRED) RECORDS 2013-2015[15]

Distribution and trends

In 2014 and 2015, the competent authorities of the Member States created more than 13 million alerts, a clear demonstration of the system's importance for border control and facilitating law enforcement cooperation within the Schengen area and, thus, its EU added-value. It would have been impossible to achieve these results at regional or national level.

[15] Valid (non-expired) records are the alerts in SIS II which can be searched by end-users.

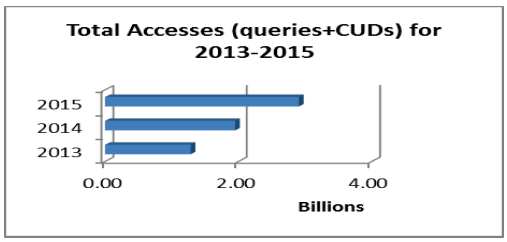
Alert	2013	2014	2015
Person	861 900	797 764	793 878
Vehicle	3 241 809	3 298 541	3 401 517
Aircraft	7	10	19
Banknote	265 968	267 123	271 893
Blank document	768 620	981 211	1 107 569
Boat	1 046	3 288	6 608
Boat engine	1 691	9 735	19 815
Container	18	96	302
Firearm	431 121	457 059	486 154
Industrial equipment	4 252	42 783	84 426
Issued document	39 836 478	43 552 428	48 357 109
Licence plate	2 157 328	2 470 227	2 786 092
Security	394 918	1 432 409	3 123 969
Vehicle registration document	2 314 233	2 657 355	3 035 305
Total alerts	**50 279 389**	**55 970 029**	**63 474 656**

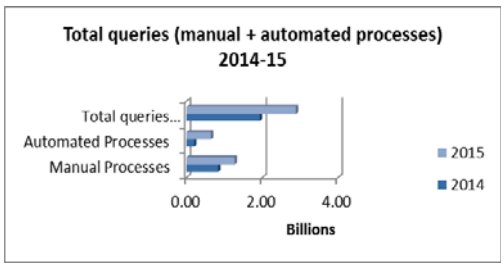
6.2 THE NUMBER OF TIMES SIS II HAS BEEN ACCESSED BY END-USERS

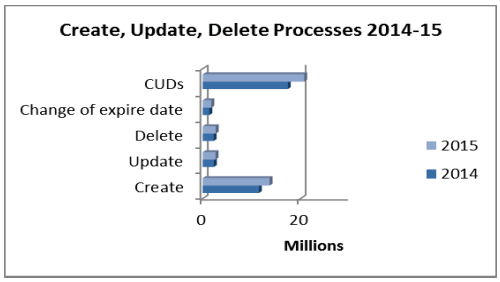
The legal instruments require statistics to be kept on the number of times SIS II data were accessed by end-users in the Member States.

Queries in SIS II cover all checks of persons and objects. Most people will think of a law enforcement officer or border guard carrying out a check on a person, a document or a vehicle; a manual check. However, there are situations where checks are carried out in an automated fashion. This can be carried out on the licence plates of vehicles by ANPR systems, on cruise ship manifests or on lists containing Passenger Name Records. Member States can report on these automated checks, if their computer systems allow such separation.

In 2013 an overall figure per Member State was recorded but it became clear that this picture did not provide sufficient detail to assess how SIS II was being used. As a result, the SISVIS Committee agreed to a more detailed break-down of the annual statistics. The statistics for 2014 and 2015 show queries carried out in SIS II, 'create, update and delete' transactions for alerts and transactions which change the expiry date of an alert, thereby prolonging its life in SIS II.







The usefulness of SIS is diminished, however, that in certain Member States the national police or immigration databases are not searched in parallel with SIS therefore the SIS search must be carried out with a separate search transaction depending on the consideration of the end-users. It has been noticed in the course of Schengen evaluations that the number of SIS searches was significantly lower if the SIS was not incorporated in a parallel search mechanism. In such cases the cross-border dimension of a crime may be missed.

6.3 OVERALL HITS

A hit on an alert is defined in the SIRENE Manual as follows:

> *A hit occurs in SIS II when:*
> *(a) a search is conducted by a user,*
> *(b) the search reveals a foreign alert in SIS II,*
> *(c) data concerning the alert in SIS II matches the search data, and*
> *(d) further actions are requested as a result of the hit*

The figures used reflect the hits achieved by Member States on their own territory on alerts issued by other Member States.

HITS	2013	2014	2015	TOTAL
Art 26 of the SIS II Decision	5 777	8 774	11 156	25 707
Art 24 of the SIS II Regulation	22 702	25 888	30 501	79 091
Art 32 of the SIS II Decision	2 667	3 961	5 713	12 341
Art 34 of the SIS II Decision	18 068	31 255	34 511	83 834

Art 36 of the SIS II Decision	14 169	23 942	34 313	72 424
Art 38 of the SIS II Decision	23 439	34 115	40 253	97 807
Total	**86 822** [16]	**127 935**	**156 447**	**371 204**

Note: In this report when counting hits, the figures used are those reported by Member States on hits achieved on their individual territories on alerts issued by another Member State. This provides the most reliable data. Due to the entry into operations of SIS II on 9 April 2013, the figures for 2013 are part-year figures. Accordingly, percentage increases will only be calculated on the difference between 2014 and 2015 in order to avoid distortion. The raw figures for the 267 days of 2013 when SIS II was running have been provided.

6.4 MAIN IDENTITIES, ALIASES AND MISUSED IDENTITIES

There was an increase in the total number of all identities**.** Given the overall fall in the total number of alerts on persons and a 3 % drop in main identities, this figure indicates an increase in the use of additional identities. These are either an alias (a false identity) or a misused identity (a potentially innocent person's real identity being misused by another person; although it has been known for co-conspirators to re-use one identity, based on the availability of documents for unlawful use). The number of aliases increased by almost 19 %.

	2014	*2015*
Main identities	756 391	737 515
Alias	244 272	290 443
Misused identities	115	142
TOTAL	**1 000 778**	**1 028 090**

6.5 AUTHORITIES HAVING A RIGHT TO ACCESS ALERTS

Access to data entered in SIS II and the right to search such data directly or in a copy of SIS II data is reserved to the authorities responsible for border control, other law enforcement and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities. National judicial authorities, including those responsible for launching public prosecutions in criminal proceedings and for judicial inquiries prior to charge, may also access these data in carrying out their tasks, as provided for in national legislation, as can their coordinating authorities.

The right to access and directly search data entered in SIS II and data on documents relating to persons entered in accordance with Article 38(2)(d) and (e) of the SIS II Decision may be exercised by:

- the authorities responsible for issuing visas;
- the central authorities responsible for examining visa applications and
- the authorities responsible for issuing residence permits and administering legislation relating to third-country nationals when applying the EU *acquis* relating to the movement of persons.

The use of SIS II by customs authorities varies. A questionnaire sent out on 11 January 2016 to the experts on the SISVIS Committee showed that, in most Member States, customs officers have read-only access to SIS II. In many Member States, SIS II is mainly used within the course of a customs-related criminal investigation. SIS II is not systematically consulted

[16] Part-year figures.

by customs officers performing surveillance and customs control tasks. Checks against the SIS II are only carried out manually. No Member State applies automated processes for cross-checking customs information systems with SIS II, even though it is clear that some categories of object alerts (such as containers, vehicles, firearms, boat engines and industrial equipment) fall largely within the competence of customs control at the external border.

There is significant EU added value to the transparency requirement for Member States to forward to eu-LISA for publication the list of national authorities empowered to search and insert alerts to SIS II, as it facilitates the rights of individuals to access their data and allows the monitoring of the purpose limitation of those authorities.

6.6 INSTITUTIONAL USERS: EUROJUST AND EUROPOL

Eurojust and Europol are granted access to SIS II data under Article 41 of the SIS II Decision (Europol) and Article 42 (Eurojust).

- Europol has access to alerts under the following Articles:
  - 26 — alerts for arrest;
  - 36 — alerts for discreet and specific checks;
  - 38 — objects sought for the purposes of seizure or use as evidence in criminal proceedings.
- Eurojust has access to alerts under the following Articles:
  - 26 — alerts for arrest;
  - 32 — alerts on missing persons;
  - 34 — persons sought to assist with a judicial procedure;
  - 38 — objects for seizure or use as evidence in criminal proceedings.

Both agencies can carry out queries in the central SIS II, but neither has a copy of SIS II data. Equally, neither agency can create alerts in SIS II. The two agencies are not covered by the evaluation framework on the use of SIS II. Therefore, in order to assess use of the system the Commission carried out a fact-finding visit. The findings are set out in a specific section of Annex 1.

7. REVIEW OF THE APPLICATION OF ALERTS FOR THE REFUSAL OF ENTRY OR STAY UNDER ARTICLE 24 AND 26 SIS II REGULATION

7.1 A BRIEF OVERVIEW

This category of alert is only applicable to third-country nationals.

Where a competent court or authority has decided that a third-country national should not be allowed to enter or stay in the Schengen territory (generally for criminal, state security or migration/visa irregularity reasons), the authority either must or may enter an alert in SIS II with EU/Schengen-wide effect. Upon a hit, the person will be refused entry at the external border or will be removed from the Schengen area if found on the national territory of any Member State. Due to the duration of the refusal of entry or stay, this category of alert is retained in SIS II after a hit as the ban is still active up to its date of expiry. Article 24(2) and (3) describe the two grounds for issuing an alert: Article 24(2) relates to third-country nationals who pose a threat to public or national security, whereas Article 24(3) relates to third-country nationals who have not complied with immigration legislation. Article 26 of the

SIS II Regulation establishes that SIS II must also contain alerts relating to third-country nationals who are the subject of a restrictive measure.

Alerts under Article 24 are only used by the 26 EU Member States which are part of the Schengen area without internal border controls. Romania and Bulgaria are allowed to see but not to enter refusal of entry alerts and they are not obliged to give effect to alerts issued by other MS. The UK receives a notification of refusal of entry alerts issued by other Member States if it wants to create an alert on the same person which would be incompatible with an existing refusal of entry alert.

The number of alerts has decreased since SIS II began operating, falling from 623 203 (31 December 2013) to 492 727 alerts (31 December 2015) – a decrease of 21 %. The reasons for this decrease are that certain Member States have regularised many of the third-country nationals who were subject of a refusal of entry alert and they granted them residence permits. Other Member States have started with a systematic quality control targeting this specific alert category as it happened that several authorities in the same Member State created a refusal of entry alert on the same person as they did not consult the system or were negligent.

Alerts in SIS II	***2013***	***2014***	***2015***
Third-country nationals to be refused entry or stay into the Schengen Area	623 203	547 492	492 727

Hits	***2013***	***2014***	***2015***
	22 702	25 888	30 501

In accordance with Appendix 5 of the SIRENE Manual the following are considered a hit for refusal of entry alerts:

(a) refusals of entry at the external border as a result of a foreign alert;
(b) following a hit on a foreign alert for refusal of entry under Article 24, refusals to issue a short-stay visa (including at embassies and consulates) or a residence permit, withdrawals of a residence permit or a long-stay visa.

7.2 KEY THEMES EMERGING

Legal aspects

An alert for refusal of entry issued by one Member State applies throughout the Schengen area. The legal consequences of the presence of the alert in SIS II within the context of border checks on persons are laid down in two other EU instruments that are part of the Schengen *acquis*:

- Schengen Borders Code (SBC)[17]: the existence of an alert in SIS II for the purposes of refusing entry is a ground for refusing entry to the Schengen area, in accordance with Article 6(1)(d) and 14(1) of the SBC. Consultation of SIS II is therefore a mandatory part of the entry border checks on third-country nationals, as set out in Article 8(3)(a)(vi) of the SBC.

[17] OJ L 77, 23.3.2016, p. 1.

- Visa Code: Article 32(a)(v) of the Visa Code[18] states that a short stay visa shall be refused to a person for whom an alert has been issued in SIS II for the purpose of refusing entry.

The EU-wide effect of the alerts is not unconditional as, in particular circumstances, a person subject to a refusal of entry alert may still be allowed to enter. These circumstances include:

- Article 32 (1) of the Visa Code establishes that a visa with limited territorial scope may be issued despite the existence of a refusal of entry alert, on humanitarian grounds, for reasons of national interest or because of international obligations.
- Article 6(5)(a) of the SBC allows Member States to authorise transit for a person subject to an alert who holds a residence permit or long stay visa issued by another Member State. In this situation, a consultation procedure should be initiated under Article 25(2) of the Schengen Implementing Convention. The Member States that issue the alert nevertheless retain the right to include the third-country national on their national list of alerts and to refuse him/her entry at their external borders.
- Article 6(5)(c) of the SBC provides that a Member State may, despite the alert, authorise a person to enter its territory on humanitarian grounds, on grounds of national interest or because of international obligations. In these cases, consultation with the Member State(s) that issued the alert is not required but the latter must be informed by the Member State authorising the entry.

There is no EU legislation laying down the EU-wide effect of a refusal of entry or stay alert for third-country nationals who are staying on a Member State's territory. This might result from several situations:

- **A third-country national is staying illegally on a Member States territory and is the subject of an alert in SIS II**. In accordance with Article 6(1) of the Return Directive, a return decision needs to be issued. However, the executing Member State may grant the person the right to stay in accordance with Article 6(4) of the Return Directive for compassionate, humanitarian or other reasons. In this case, Article 25(1) of the Schengen Implementing Convention (SIC) applies. It states that that where a country considers issuing a residence permit to a third-country national for whom an alert has been issued for the purposes of refusing entry, it must first consult the country that has issued the alert and take account of its interests. The residence permit can only be issued for serious reasons, in particular cases of a humanitarian nature or arising from international obligations. Where the Member State decides to grant a residence permit, the other Member State must withdraw its SIS II alert but may nevertheless put the person in question on its national list of alerts.
- **A third-country national is staying illegally on a Member State territory but holds a residence permit issued by another Member State**. In accordance with Article 6(2) of the Return Directive, the executing Member State shall require the person to go back to the Member State that issued the residence permit or authorisation to stay, unless the person's immediate departure is required for reasons of public policy or national security. In case of non-compliance, the executing Member State shall issue a return decision in accordance with Article 6(1) of the Return Directive. Article 25(2) of the SIC applies when the person is subject to a return decision, while holding a residence permit or other authorisation to stay from another Member State, and an alert for refusal of entry or stay is issued. This Article states that the country issuing the alert must consult the country which

[18] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

issued the residence permit to determine whether there are sufficient reasons for withdrawing the residence permit. If the residence permit is not withdrawn, the country issuing the alert must withdraw the alert but may nevertheless put the person in question on its national list of alerts.

- **A third-country national is the subject of an alert in SIS II but holds a residence permit issued by the Member State where he is staying**. In this case the Return Directive does not apply, as the person is not staying illegally on the Member State territory. Article 25(2) of the SIC applies in this situation and the consultation procedure described in the previous bullet point needs to be carried out.

The decision to grant a residence permit always takes priority over the decision to issue an alert for refusal of entry or stay as, in all situations under Article 25 of the SIC, the alert needs to be withdrawn if it is decided to allow the residence permit to continue. This obviously has an impact on the alert's effectiveness.

Lack of comprehensive statistics - effectiveness

A lack of comprehensive EU-wide statistics makes it difficult to assess the effectiveness of Article 24. Hit numbers cover situations in which the alert has taken effect, but not the situations in which entry was allowed or a right to stay was granted despite the existence of an alert. Furthermore, there is no distinction in the statistics between hits achieved during an application process for a visa, at an external border or on the Member State territory. Member State statistics collected by Eurostat in 2014 show that 12 205 third-country nationals were refused entry on the basis of an alert in SIS II in 2014. The overall hit number for 2014 was 25 888. This might indicate that fewer than half the hits occur at an external border.

Cases in which the required action was not taken

The measure's effectiveness can be partly demonstrated using SIRENE G and H forms. A 'G form' is sent when the required action is taken in the event of a hit. An 'H form' is sent when the action was not taken (either at the external border or within the territory). However, the figures relating to the forms unfortunately do not disclose a complete picture as Member States may choose not to be informed about hits on their Article 24 alerts. Therefore, the number of G forms sent does not correspond to the number of hits reported and the number of H forms does not reflect the total number of cases where the action was not taken at entry or on the territory.

	2014	***2015***
Number of outgoing G forms	11 623	12 007
Number of outgoing H forms	7 056	7 264
Total	18 679	19 271

In both years, G forms accounts for approximately 60 % of cases and H forms account for approximately 40 %. This can be used as an indication of the ratio of cases where the alert has taken effect in comparison to the cases where the alert has not taken effect. The table below demonstrates that, in comparison with other alert categories on persons, the number of H forms compared to the number of G forms is very high – i.e. that the number of cases where action is not taken is comparatively high with this kind of alert.

2015	Alert for refusal of entry		Alert for arrest		Alert on missing person		Alert for discreet or specific check		Alert for judicial procedure	
G forms sent	12 007	62 %	9 804	96 %	4 923	94 %	24 027	99 %	26 200	99 %

H forms sent	7 264	38%	450	4%	337	6%	233	1%	270	1%
Total	19 271		10 254		5 260		24 260		26 470	

The simultaneous increase in the number of G forms and H forms in 2015 may indicate that the increase in the number of hits in 2015 is not due to improved effectiveness but rather to an increase in the number of checks and improved data quality for Article 24 alerts leading to more positive matches.

Use of the consultation procedure - effectiveness, efficiency and coherence/consistency -

Article 25 of the SIC sets out a mechanism for ensuring that Member States consult each other and take into account each other's assessment when deciding whether to grant a residence permit and for avoiding situations in which an alert co-exists with a valid residence permit. Article 25(1) sets out the process to follow if an alert exists in SIS II but another Member State is considering granting a residence permit. Article 25(2) sets out the process if an alert has been issued for a person who already holds a valid residence permit. The table below shows the number of outgoing and incoming consultations reported by Member States within the context of an SIS II alert:

	2014	***2015***
Number of outgoing consultations	5 945	6 043
Number of incoming consultations	6 884	6 608
Total	12 829	12 651

Note: the numbers do not completely tally as it may occur that one consultation is sent to several Member States.

In an ad hoc query launched by the EMN at the request of the Commission, all Member States confirmed their use of the consultation procedure in cases falling under Article 25(1) of the SIC. Member States reported some examples of when they had used the consultation procedures through SIS II. Nine Member States out of 26 provided statistics on successful consultation procedures. The statistics include consultations made to other Member States and the replies sent to Member States who had made their own requests. These nine Member States reported a total of 5 352 successful consultation procedures. Statistics on the use of the consultation procedure should be considered in conjunction with statistics on the exchange of SIRENE N and O forms. In the SIRENE Manual the consultation procedure is implemented as follows:

- Procedure under Article 25(1): *If a Member State that is considering granting a residence permit or visa discovers that the applicant concerned is the subject of an alert for refusal of entry or stay issued by another Member State, it shall consult the issuing Member State via the SIRENE Bureaux.* ***The Member State considering granting a residence permit or visa shall use an N form*** *to inform the issuing Member State about the decision to grant the residence permit or visa. If the Member State decides to grant the residence permit or visa, the alert shall be deleted. The person may, nevertheless, be put on the issuing Member State's national list of alerts for refusal of entry.*
- Procedure under Article 25(2): *If a Member State that entered an alert for refusal of entry or stay finds out that the person who is the subject of the alert has been granted a residence permit or visa, it shall instigate a consultation procedure with the Member State that granted the residence permit or visa, via the SIRENE Bureaux.* ***The Member State which granted the residence permit or visa shall use an O form*** *to inform the issuing Member State about the decision whether or not to withdraw the residence permit or visa. If this Member State decides to maintain the residence permit or visa,*

the alert shall be deleted. The person can, nevertheless, be put on a Member State's national list of alerts for refusal of entry.

	2014	***2015***
Number of N forms sent = number of outgoing consultations under Article 25(1) SIC	5 277	4 666
Number of O forms sent = number of replies to consultations under Article 25(2) SIC	2 232	2 145
Total	7 509	6 811

These figures may indicate that:

a) most consultations take place within the context of Article 25(1) of the SIC. This is confirmed by the replies to the ad hoc query by the EMN: 11 Member States reported mostly using the consultation procedure under Article 25(1) of the SIC, while 8 Member States reported applying mainly Article 25(2) of the SIC;
b) in at least 5 000 cases per year, a Member State considered granting a residence permit despite the existence of an alert;
c) in at least 2 000 cases per year, there was a situation where a residence permit co-existed with a refusal of entry alert. This number may be much higher as an M form or H form may also be used in such cases. It should be noted that these figures do not cover the situation under Article 6(5)(c) of the SBC, where an H form will be sent if entry was granted despite the existence of an alert.

Need for additional data in the alert to allow field officers to take the requested action - effectiveness

In their replies to the questionnaire, several Member States mentioned as a weakness of the system that the information contained in the alert does not reflect the specific reasons it has been issued. The SIS II Regulation provides for four possible reasons:

1. Article 24(2)(a): 'conviction';
2. Article 24(2)(b): 'security threat';
3. Article 24(3): 'illegal stay';
4. Article 26: 'restrictive measure'.

It may also be useful to indicate whether an alert relates to a third-country national who has the right of free movement within the EU (Article 25 of the SIS II Regulation).

Member States expressed the opinion that additional information in the alert would increase efficiency and allow quick and correct decision-making. The following responses to the questionnaire were received:

- Sub-division of the categories of alerts for refusal of entry, suggesting a clear distinction between refusals of entry based on: i) national security; ii) criminal reasons; iii) immigration law. Such a move would facilitate the gathering of statistics on reasons for refusals of entry and provide an indication to the officer on the ground of the background to a case when a hit is achieved.
- The inclusion of a remark on the underlying reason for a refusal of entry alert.
- The alert itself should hold the information of the basis of the decision underlying the alert, that is, a field indicating whether the alert was created due to criminal conviction, non-respect of visa/migration procedures, against a person benefiting from the right of free movement or due to restrictive measures.

- The importance of knowing whether the alert subject had been informed of the refusal of entry alert or not (when the person is in a third country it is not always feasible).
- A copy of the refusal of entry notice to be attached to the alert.
- More information in the alert to reduce exchange of supplementary information.

The consultation procedure and delays in the exchange of information - efficiency -

In their replies to the questionnaire and the EMN ad hoc query, Member States reported many flaws in the exchange of supplementary information and the consultation procedure. A key issue is the delay in receiving information from other Member States, including after a hit on the reason for the alert. Responses routinely do not arrive within the 12-hour deadline required by the SIRENE Manual. In order to be able to answer within the timeframe, SIRENE Bureaux should have direct access to the relevant national databases.

Quality of information - effectiveness

It is difficult to gather evidence to identify an individual (fingerprints, photos, copies of ID documents or residence permits) from other Member States. Documents provided in the system are sometimes not of good quality. This causes difficulty in identifying the third-country national, especially when names are written in other alphabets.

Difficulties with the consultation procedure - effectiveness and efficiency

Member States reported specific operational difficulties with the SIC consultation procedure:

- Responses to consultation procedures do not provide enough detail, such as the reasons, validity and duration of the alert or of the residence permit/visa to be granted. Introducing common guidelines on the compilation of a response to consultation procedures may be useful.
- Requests to delete an SIS II alert after issuing a residence permit to the concerned individual are often not processed or are delayed by the competent Member State.
- There are cases where one Member State imposed an entry ban on a third-country national while another Member State had issued him/her a residence permit.
- Complexity of the N and O Schengen forms used in the consultation procedure. Revision of the forms used for consultation between the Member States would assist, as different procedures adopted by Member States in completing the forms cause delays and problems in consultation. Standardised procedures are already set out in the SIRENE Manual. Revising the N and O forms in line with harmonised procedures would also simplify the considerable workload of the SIRENE Bureaux in their role as a conduit for consultation.

Similar issues were reported to the EMN for the purpose of the 2014 study. In one Member State, authorities have experienced problems when wanting to impose an entry ban on an individual who poses a risk to public security, but who holds a residence permit in another (Member) State. In these cases, information provided does not always lead to withdrawal of the residence permit.

Lack of harmonisation in the deadlines for the consultation procedure - effectiveness, efficiency and coherence/consistency -

- Long waiting periods for responses are experienced by most Member States, even after several reminders. This may delay administrative procedures for issuing residence permits. A binding response time for consultation procedures would assist. An example of two weeks was given.
- Member States have different provisions with regard to deadlines for consultation procedures through SIS II. Most of them do not provide for a deadline. However, some Member States reported that the reply to a consultation procedure is normally expected within a short timeframe. One Member State sets a limit of 24 hours.

- Only a few Member States set deadlines for SIS II consultation procedures, either by law or by administrative practice. Some of them set a deadline for replies to launched consultations corresponding to the deadline in the procedure to issue a residence permit. One Member State replied that responses to consultation requests are sent within 24 hours.

Finding new models for the exchange of supplementary information - effectiveness and efficiency

In many Member States the immigration authorities are the competent authorities for issuing, updating and deleting refusal of entry or stay alerts. They also take decisions on the return and removal of third-country nationals apprehended on the Member State territory. The exchange of supplementary information (notification of a hit, request for supplementary information to confirm the identity of a person etc.) between Member States takes place via the SIRENE Bureaux, which are usually situated within the structure of the police authorities. As a consequence, when information is being exchanged on Article 24 alerts, the SIRENE Bureaux function mainly as letter boxes between the relevant immigration authorities. This brings two major risks: (1) unnecessary delays in information exchange (as the information source is outside SIRENE control) and, as a result, the decision-making process; (2) a loss of efficiency of SIRENE communication could cause other channels of communication to be used.

The Commission launched a study on the use of SIS II for return purposes. One of the tasks carried out in the study was to analyse two models for organising the exchange of information on migration-related SIS II alerts more efficiently and allowing immigration authorities to be directly involved. In the study, two models were examined: seconding migration officers to the SIRENE Bureau (model A); or setting up a separate single point of contact (SPOC) (model B).

The main findings of the study were:

(a) Costs would be higher for model B. The model would require the implementation of new infrastructure(s), including IT, while model A would require only minor changes to the current infrastructure and IT system;
(b) As model B would require new infrastructure, it would probably take more time to implement than model A;
(c) If model B were chosen, field officers would need to determine which of the two coordinating authorities (SIRENE Bureau or new migration SPOC) should be contacted.

Member States did not express a clear preference for either of the proposed models, as any preference will depend on the division of responsibilities at national level.

7.3 INCONSISTENCY WITH THE RETURN DIRECTIVE – COHERENCE/CONSISTENCY

The Return Directive provides the EU with common standards and procedures for returning persons staying illegally on Member States territories. It determines that Member States may not tolerate third-country nationals staying illegally on their territory but must either issue a return decision or grant them a right to stay. A return decision is sometimes accompanied by an entry ban, prohibiting entry into or stay on EU territory for a specified period. An entry ban is always issued if: (1) no period of voluntary return has been granted, or (2) the person has not complied with the return decision within the granted period of voluntary departure. In other situations, an entry ban is optional. Entry bans issued under the Return Directive have EU-wide effect and are binding on all Member States bound by the Return Directive. The length of entry bans issued under the Return Directive is determined on a case-by-case basis but must not exceed five years, unless the person represents a serious threat to public policy,

public security or national security. If that is the case, entry bans issued under the Return Directive may exceed five years. An entry ban forms the basis for issuing a refusal of entry or a stay alert in SIS II.

There are links but also inconsistencies between the SIS II Regulation and the Return Directive:

Article 24 of the SIS II Regulation has a broader scope than the entry bans under the Return Directive

According to the Return Directive, an entry ban relates to third-country nationals who have stayed illegally on a Member State's territory, and is always linked to a return decision. A refusal of entry alert under Article 24 (2) of the SIS II Regulation, on the other hand, may also cover third-country nationals who are not present on the Schengen territory. The Return Directive also offers, in Article 2(2), the option of not extending its provisions to:

(a) third-country nationals who are the subject of a refusal of entry in accordance with Article 13 of the SBC, or who are apprehended in connection with irregular border crossing and
(b) third-country nationals who are subject to a removal procedure as a criminal law sanction under domestic law.

There are no clear links between both instruments, in either the Return Directive or the SIS II Regulation

Recital 18 of the Return Directive states that Member States should have rapid access to information on entry bans issued by other Member States and that this information-sharing should take place in accordance with the SIS II Regulation. Recital 14 of the Return Directive makes clear that entry bans have a European dimension, as they should prohibit the entry into and stay on the territory of all Member States. There is no obligation laid down in the Return Directive to enter all entry bans in SIS II, thereby causing incoherence with the goal of the measure.

Legally and practically, an entry ban can only be effective in other Member States if accompanied by a SIS II alert

The entry ban can only achieve its EU-wide effect if it is inserted as a refusal of entry or stay alert in SIS II, as only the alert – not the decision itself – forms the basis for refusing entry in accordance with the SBC or for refusing a short stay visa in accordance with the Visa Code (see above). A complication occurs when considering the geographical scope of the Return Directive and the SIS II Regulation. All Member States and Associated Countries participating in the provisions of the Schengen *acquis* are bound by the Return Directive, and the SIS II Regulation. There is, however, a particular situation in Romania, Bulgaria, Cyprus and Croatia.

These EU Member States already apply the provisions of the Return Directive but they are not yet part of the border-free Schengen area. This means that they cannot issue any alerts in SIS II for refusal of entry or stay. These Member States cannot create EU-wide entry bans through SIS II.

There is no obligation in the Return Directive to enter all entry bans as an alert in SIS II

The SIS II Regulation only requires an alert to be issued in some circumstances: when the underlying decision is based on a threat to public policy, public security or national security (Article 24(2)) an alert is required (subject to the general proportionality principle of SIS II); if the decision is based on non-compliance with immigration legislation (Article 24(3)) there is no such requirement. In their 2014 study, the EMN came to the conclusion that '*not all (Member) States systematically enter an alert into the SIS following the imposition of an entry ban. If not informed about the entry ban imposed on a specific individual, (Member)*

States will not be able to ban entry of that individual into EU territory. The entry ban thereby essentially loses its effect and will in practice only apply to the territory of the (Member) State that imposed it.'.

The evaluation of the application of the Return Directive (October 2013) concluded that '*almost all Member States register every entry ban decision in SIS. However, there are a few exceptions. According to a government body, there is some variation among different police districts. In some police districts the entry bans are not systematically registered in SIS. Moreover, in another Member State not all entry ban decisions are registered in SIS. In another Member State, entry bans are issued on a national level and also on a Schengen level. Only those entry bans that are applicable to the whole Schengen area are registered in SIS.*'

The maximum retention period of a refusal of entry or stay alert in SIS II does not correspond to the maximum length of an entry ban issued in accordance with the Return Directive

Alerts can be retained for three years, whereas an entry ban lasts for up to five years (and potentially longer in cases of threats to public policy, public security or national security). A SIS II alert may be prolonged after a re-assessment. The maximum retention period set out in the SIS II Regulation should be harmonised with the length of an entry ban in the Return Directive.

There is an inconsistency in terminology between the Return Directive and Article 24 of the SIS II Regulation

An entry ban is defined in Article 3(6) of the Return Directive as an administrative or judicial decision or act prohibiting **entry into and stay** on the territory of the Member States for a specific period, accompanying a return decision. Article 24 on the other hand covers alerts for the purpose of refusing **entry or stay**.

The Return Directive does not include provisions on direct enforceability of alerts for refusal of entry or stay

The same conclusion was reached in the feasibility study on creating a new alert category in SIS II for return decisions. The study concluded, among other issues, that the EU-wide follow-up and enforcement of return decisions and entry bans could more successfully be achieved with a system of mutual recognition of return decisions and entry bans.

7.4 LACK OF HARMONISATION WHEN ENTERING ENTRY BANS IN SIS II - EFFECTIVENESS AND COHERENCE/CONSISTENCY

When considering the grounds for issuing alerts laid down in Article 24, a distinction should be made between alerts relating to third-country nationals who pose a threat to public or national security (Article 24(2)) and alerts relating to third-country nationals who have not complied with immigration legislation (Article 24(3)). There is limited quantitative data available on the volume of alerts split along these lines, due to the fact that the alert itself does not contain this information. In the EMN query, only five Member States reported making a distinction between these categories in their national statistics.

Member States reported the following issues with registering entry bans in SIS II:

Not all Member States systematically register all entry bans in SIS II

An entry ban is intended to have an EU-wide effect and the only way of achieving this effect is to enter the ban in SIS II. One Member State pointed out that the wording of Article 24 (3) is unhelpful in that it proposes that an alert '*may*' be entered. Different national interpretations of this text have resulted in some Member States entering alerts whilst others do not, even though this negates the EU-wide effect. The text should be modified to '*an alert shall be entered*'.

There are different practices with regard to the timing of registration of entry bans in SIS II

In eleven Member States, entry bans can only be registered in SIS II once the decision is final or immediately enforceable. Three Member States also require that the person leaves the territory before recording the entry ban. In another Member State, the decision imposing the entry ban may be registered in SIS II and enforced before it is final and non-appealable, if the third country national does not have the right to stay during the appeals process, e.g. because s/he did not have a residence permit prior to the decision or because s/he represents a danger.

In contrast, in six Member States, entry ban alerts are inserted in SIS II as soon as the decision is taken, without it needing to be final or enforceable. If the decision is repealed by the competent national authority or reviewed by a court, the alert will be also deleted from the SIS II. As explained above, an entry ban only can have EU-wide effect from the moment it is entered as an alert in SIS II. Therefore, the moment of registration in SIS II should coincide with the moment the entry ban is enforceable.

7.5 ENTERING TRAVEL BANS CONSTITUTING A RESTRICTIVE MEASURE IN SIS II - EFFECTIVENESS AND COHERENCE/CONSISTENCY

Travel bans constituting a restrictive measure adopted as Council Decisions, including those issued by the United Nations, are given effect via the creation of a refusal of entry alert in SIS II. In accordance with Article 26(3) of the SIS II Regulation and section 4.1 of the SIRENE Manual, alerts are created in SIS II by the Member State holding the Presidency of the Council of the EU. This Member State is also responsible for updating and deleting the alert as required. There are several practical problems with this, including:

- **Data quality**. Travel bans are entered in SIS II using the personal data set out in in the Annex to the relevant Council Decision. Usually it contains last name, first name, date of birth and place of birth, but sometimes the data available are not sufficient to enter an alert in SIS II (for example, if only the name of the person, or even an alias, is known). If this happens, the travel ban cannot be entered in SIS II, as the technical rules do not allow an alert to be created for a person without at least a last name and a year of birth. However, the SIS II Regulation waives the minimum data quality requirements for these alerts and so there is an inconsistency between the legal basis and the technical possibilities, even though such minimal data will not lead to hits. Alerts created on the basis of only a name are not effective, as they do not provide sufficient information to identify a person. In these cases, Member States should include as much as data as possible (such as photographs) in the alert in order to ensure that the travel ban can have effect.
- **Lack of coordination**. Each Member State is responsible for creating, updating and deleting alerts relating to restrictive measures adopted during the period of its presidency. Due to the six monthly rotation of presidencies, there is no centralised responsibility. Some Member States proposed a centralised solution for creating and following-up these alerts.

7.6 CREATION OF A EUROPEAN BORDER AND COAST GUARD AGENCY

On 14 September 2016, the European Parliament and the Council adopted the Regulation on a European Border and Coast Guard Agency[19] establishing a European integrated border

[19] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Cost Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p.1).

management and significantly strengthening the mandate of Frontex, renaming it a European Border and Coast Guard Agency. The enhanced Agency will have expanded tasks and responsibilities, including the possibility to deploy European Border and Coast Guard Teams on a Member State's territory in case of an urgent situation and will have a stronger role in the return of irregular migrants. Within the scope of these competences, the Agency will need access to refusal of entry and (future) return decision alerts in SIS II.

7.7 CONCLUSIONS

There are many situations in which a Member State may decide to grant a person the right to enter into or stay on the territory despite the existence of an Article 24 alert issued by another Member States. As a consequence, the EU-wide effect of alerts is not systematically achieved. Furthermore, despite the obligation to enter refusal of entry alerts in the SIS, the EU-wide effect of these alerts is not systematically achieved. .This limits the EU added value of the measure, as the Return Directive does not include provisions to directly enforce alerts for refusal of entry or stay.

Incomplete statistics mean there is a lack of transparency on the effectiveness of the measure. An analysis of the G and H SIRENE forms demonstrates that refusal of entry or stay is the least effective alert category among alerts on persons. The alert achieved its effect in just 60 % of cases, whereas for other alert categories on persons, this is true in more than 90 % of cases. There is a lack of comprehensive statistics on the use of the consultation procedure. However, it may be deduced that most consultation take place within the context of Article 25(1) of the SBC and that there are, on an annual basis, at least 2 000 cases in which a residence permit coexists with a refusal of entry or stay alert. It is very difficult to avoid these situations as, in many cases, the Member State issuing the alert may even not be aware of the existence of a residence permit due to the lack of an EU-wide system.

Member States reported shortcomings in the processes for and quality of information exchange on alerts for refusal of entry or stay, especially in the context of the consultation procedure. These flaws highlight a significant procedural weakness as the deadline for all other forms of SIRENE response is twelve hours. It is clear that the lack of harmonisation in consultation processes and tardy responses cause operational staff and the individual concerned considerable problems. In some cases, the need to exchange supplementary information through the SIRENE Bureaux may be removed by adding additional data to the alert itself, leading to more efficient and reliable identification and decision-making processes.

There are links but also inconsistencies between the provisions on entry bans (as set out in the Return Directive) and refusal of entry or stay alerts (as set out in the SIS II Regulation). Both instruments were drafted from different perspectives and therefore are not fully aligned. This leads not only to limits on the EU-wide effect of entry bans but also to a lack of harmonisation in the criteria for issuing alerts. More harmonisation could be achieved by making it mandatory to enter an entry ban in SIS II from the moment the decision is enforceable.

8. ALERTS FOR ARREST FOR EXTRADITION OR SURRENDER UNDER ARTICLE 26 OF THE SIS II DECISION

Alerts in SIS II	***2013***	***2014***	***2015***
Arrest for extradition or surrender	34 263	34 651	34 590

Hits	*2013*	*2014*	*2015*
	5 777	8 774	11 156

8.1 KEY THEMES EMERGING

Non-disclosure of fact that a person has been located - efficiency

The Commission should raise with the Member States the problem of creating SIS II alerts when the whereabouts of the subject of the alert are already known and confirmed. Member States should improve their procedures for ensuring that, when an EAW has been created for a person whose whereabouts are known and confirmed, the correct field of the SIRENE A form is used to highlight that fact so that needless work on checking whether the person is known or present on the territory is avoided.

Flagging and the need for coordination in multiple arrest cases - effectiveness

The legal instruments and technical specifications of SIS II should be amended to allow Member States to temporarily make an alert 'non-searchable' by end-users without the need to delete the alert.

Increasing the amount of information held in the alert - effectiveness

Alerts in SIS II carry sufficient information to identify a person or object and provide a text on the 'action to be taken' by the officer locating the person or object. Additional information, such as fingerprints, photographs or a copy of the European Arrest Warrant can be attached to an alert. Any other information related to the alert is deemed supplementary information and is held in the SIRENE Bureau, having been exchanged bilaterally or multilaterally between the Bureaux. Several Member States, across the range of alerts, raised the issue of including more information in the alert itself for the benefit of the operational officer on the ground.

Post-hit procedures - EU added-value

The Commission should raise with Member States the problems related to transfers, working with judicial and law enforcement authorities to find areas where common practice can be established and procedures can be harmonised.

9. ALERTS ON MISSING PERSONS UNDER ARTICLE 32 OF THE SIS II DECISION

Alerts in SIS II	*2013*	*2014*	*2015*
Missing persons (minors)	36 476	42 623	56 886
Missing persons (adults)	24 344	24 552	31 167
Total Missing persons	**60 820**	**67 175**	**88 053**

Hits	*2013*	*2014*	*2015*
	2 667	3 961	5 713

9.1 KEY THEMES EMERGING

The inability to create 'preventive alerts' for children at risk of abduction - effectiveness

In the area of parental abduction, the current wording of the SIS II Decision only allows the creation of an alert once a child is missing. In the early stages of a case, the only fact that is known is that a child is missing. Accordingly, an alert should be created in the SIS II. Given that parental abductions often take place in highly planned circumstances, with the intention of rapidly leaving the legal jurisdiction under which custody arrangements had been agreed, the Member States pointed out that it is preferable to be able to have "preventive alerts" in the SIS II so that a border guard checking a child leaving will see that the child has been entered in SIS II as at risk of abduction and can inquire further into the circumstances of the child leaving the Schengen area. Naturally, such an initiative would require very careful case management and re-structuring of the information within the alert to minimise the possibilities of the child and parents being inconvenienced in situations which are perfectly ordinary and lawful. It is always possible to delete an alert later once the child is found and legal proceedings (under The Hague Convention, for example) can take place.

Categorisation of missing person cases - EU added-value and effectiveness

Member States asked about the possibility of receiving more information in the alert itself about the cases they face. This would include the categorisation of missing children, involving the use of concepts such as 'runaway', 'abduction', so that officers have information about the background to a case. Although SIS II is not primarily a statistics gathering tool, many bodies – from the police through to child welfare agencies – would wish to have an overview of the problem of cross-border missing children cases. At present, SIS II can only provide raw figures on the number but not the types of cases. Most Member States have a categorisation system but they are not harmonised. A respected categorisation has been developed by the organisation Missing Children Europe, described in the 2013 Commission report, *Missing Children in the European Union — mapping, data quality and statistics*.

Repatriation of missing minors – coherence/consistency

Historically, many vulnerable missing persons were citizens of the Member State issuing the alert. Accordingly, there was no question regarding costs of repatriation. However, in cases of missing illegal migrant children or trafficked children in care who then abscond, repatriation is not always requested by the issuing Member State and it may not even be in the child's best interests. It is not efficient for SIRENE Bureaux to find themselves in a situation where the responsibility for the ongoing care and custody of a vulnerable missing person is in dispute with another Member State. It would be more efficient to review the wording of the action to be taken and to provide more background information on cases where repatriation may not be sought.

10. ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE UNDER ARTICLE 34 OF THE SIS II DECISION

Alerts in SIS II	***2013***	***2014***	***2015***
Persons sought to assist with a judicial procedure	102 517	101 918	108 988

Hits	***2013***	***2014***	***2015***
	18 068	31 255	34 511

10.1 KEY THEMES EMERGING

Failure to delete alerts at the national level - efficiency

These alerts are frequently requested by judicial authorities to finalise court cases by providing an address for the service of judicial documentation. Although judicial authorities can access SIS II, the practice at national level is often that they ask the police to create the alert. There is a fundamental problem in this approach, in that the police officer entering the alert is not, in reality, the officer in the case. Even if it is clear that an alert should be deleted, the officer would need the agreement of the judge or prosecutor. Repeated hits and exchange of the same supplementary information are clearly inefficient — alerts which are still stored, despite the fact that this is obviously unnecessary, cause needless work for authorities in Member States.

11. ALERTS FOR DISCREET AND SPECIFIC CHECKS UNDER ARTICLE 36 OF THE SIS II DECISION

11.1 A BRIEF OVERVIEW

These alerts are used to check the movements of serious travelling criminals and threats to security. They can be used for a person and for related modes of transport (vehicle, boat, plane or container). This category of alert is often kept in SIS II after a hit, due to the fact that the further movements of the person may be of interest.

Alerts in SIS II	***2013***	***2014***	***2015***
Discreet checks Art 36(2)	31 888	33 566	48 124
Specific checks Art 36(2)	8 164	11 103	13 451
Discreet checks for national security Art 36(3)	1 042	1 809	3 744
Specific checks for national security Art 36(3)	3	50	4 201
Total number of alerts for discreet and specific checks	**41 097**	**46 528**	**69 520**

Hits	***2013***	***2014***	***2015***
	14 169	23 942	34 313

Hits (breakdown)	***2014***	***2015***
Persons	18 394	27 810
Vehicles	5 548	6 502
Boats	0	0
Aircraft	0	1
Containers	0	0
Total	**23 942**	**34 313**

Note: due to the different categorisation of objects in the 2013 statistical report, this and the following section compare results exclusively from 2014 and 2015.

11.2 USE OF SIS II FOR COUNTER-TERRORISM PURPOSES

Measures to increase use for counter-terrorism - effectiveness and EU added-value

Since 2013, the Commission has undertaken intensive awareness-raising with Member States to overcome the reluctance of the national security services to use SIS II. The system has been shown to be capable of holding confidential, sensitive information while disseminating this information to law enforcement officers and border guards in 29 Schengen States.

Following these initiatives, SIS II is now the sole information exchange platform through which the state security authorities cooperate. It is capable of offering a well-tailored solution to tackle persons (and related objects such as documents) travelling to conflict zones with a view to joining terrorist organisations. The Commission has encouraged Member States on several occasions to use all possibilities of SIS II.
There are several actions that improve use of SIS II in these cases. First of all, the alert subjects should be sufficiently identifiable, therefore Member States should add photographs and fingerprints, when available, to the alerts. Where there is sufficient evidence, they can issue a EAW together with an alert for arrest. If the person should be observed, especially entering the Schengen area, a discreet check alert is appropriate. Such an alert can also be issued on his or her vehicle. If there is an operational need, the person's belongings can be also searched if a specific check alert has been issued. If the suspect is still a minor, Member States should issue a missing person alert which will require officers on the ground to place the person under protection and question him or her. These procedures were included in the SIS II and SIRENE *Catalogue of Best Practices and Recommendations*[20].

In addition to awareness-raising, the Commission has made legal and technical improvements to SIS II to provide for real-time communication from the ground to the competent services in other Member States on hits on persons and objects that are the subject of discreet and specific checks, in cases requiring special urgency and attention. These measures were introduced on 1 February 2015. In December 2015, there were 5 300 such alerts in SIS II, of which 5 200 were related to persons. As of 1 February 2015, SIS II also clearly displays if an identity document has been invalidated by the issuing Member State for travel purposes. This includes passports, ID documents, visa stickers and residence permits. In February 2016, there were over 9 000 such alerts in SIS II. In some Member States, there is no national legislation allowing for the invalidation of citizens' personal identification documents. The SIS II code tables were updated on 23 February 2015 to display the 'terrorism related activity' of a person. Since 17 March 2016, the system also shows this information for vehicles and other means of transport.

The ability to link alerts in SIS II is key, as it allows a connection between two alerts to be identified, e.g. linking a discreet or specific check alert with an alert on the invalidated travel document or with an alert on the vehicle used by the suspect.

To date there are more than 70 000 alerts for discreet and specific checks, a 300 % increase compared to the situation in June 2013. Of these, 8 000 were created by the state security services. These latter alerts must be accompanied by an exchange of supplementary information which creates significant extra workload for the SIRENE Bureaux, which have clear capacity difficulties. New amendments in the SIRENE Manual will be introduced to allow discreet and specific check alerts to co-exist with other alert categories – this is not currently permitted.

Legal, technical and operational challenges
The Dutch Presidency issued a questionnaire to Member States (doc 15537/1/15) on the use of SIS II with regard to foreign terrorist fighters, to which 24 Member States and Schengen associated countries replied (doc 5722/1/16 REV1). SIS II has proven to be the most effective

[20] Commission Recommendation of 16 December 2015 establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS (C(2015) 9169).

information exchange tool for counter-terrorism purposes with an immense EU added-value, allowing national security services to cooperate quickly, confidentially and efficiently. Several issues, as listed in Section 12.3, however, hinder more effective use of the system, requiring further action by Member States and the Commission.

11.3 KEY THEMES EMERGING

Increasing the amount of information held in the alert - effectiveness

Member States reported that it would be helpful to include more information in the alert itself, especially when the request is for a specific check. Where this is permitted by national law, a search of the person takes place. The alert currently does not specify what the grounds of the search might be nor what is being sought. During discussions in SISVIS Committee on the response to foreign terrorist fighters, it was agreed that the code table on 'type of offence' should be updated and its use extended to Article 36 alerts. This feature could be further reviewed to provide more information to officers on the ground to assist them in their searches.

The use of identity documents by criminals and persons posing threats to national security - effectiveness

Although modes of transport connected to travelling criminals can be circulated as alerts, it is not possible to create alerts on identity documents, in particular, passports, linked to them. Given that passports can be used by several people and can therefore 'take on a life of their own', it would be more effective to be able to create alerts monitoring the use of such documents when seizure is not the operational action required. A field relating to the identity document(s) of a person should be added to alerts on persons so that documents can be queried too.

Lack of provision on issuing alerts on persons in the framework of execution of criminal penalties - effectiveness

The current wording of the Article does not allow for an alert to be issued following a measure imposed by a court, e.g. supervision of conduct after a sentence has been served, although Member States are using this alert category to trace dangerous criminals after they have served their sentence.

Alerts on aircraft, containers, boats - effectiveness

Police officers do not routinely check containers, boats and aircraft. When there is an alert for discreet or specific check on such an object, there is need to raise awareness, otherwise there is little likelihood of a hit. This could be done by means of a procedure for an issuing Member State to inform one or more Member States of a request to check containers, boats or aircraft within the framework of these alerts. As noted previously, at the external border, it is much more likely that such checks would be carried out by a customs officer but more needs to be done on supporting customs checks in SIS II.

Inability to detain a person who is subject of a discreet check - effectiveness

In many circumstances a person posing a significant threat to national security may be the subject of an alert for a discreet check. In ideal circumstances, the person would be stopped by police or border guards and thoroughly checked and quizzed regarding his/her movements and activities. Sometimes the alert-issuing Member State does not have the legal ability to create an alert for a specific check (a physical search of the person) or the Member State achieving the hit only has the legal power to carry out discreet checks instead of specific. In these cases, a discreet check will be carried out and the person rapidly allowed to continue. This is not ideal. It would be more effective for the person to be temporarily detained in order

to gain more information about their movements and activities — essentially, a check which is not as limited as a discreet check, but which does not involve a full physical search of the person solely on the basis of an alert.

Indication of sexual offences in the SIS II code tables - EU added-value, efficiency and effectiveness

One Member State issued discreet check alerts for persons previously convicted for serious sexual offences. These alerts were issued for the two top categories of sexual offenders considered to continue to be most dangerous. Due to discreet check alerts, the authorities ascertained if the person breached travel restrictions and could warn other Member States about the arrival of a dangerous sexual offender on their territories. Since the SIS II code tables do not specify sexual offences, the Member State sends SIRENE forms to the other SIRENE Bureau describing the risk. This creates additional workload for the Bureaux and problems on potential follow-up to the notifications. Therefore, the categories of offences displayed should be updated to cover sexual offences and child sexual abuse material. It would increase the effectiveness of SIS II by informing officers on the ground about the nature of the discreet and specific checks and it would also increase the efficiency of the system by reducing SIRENE communication.

New category of alert for travel bans - EU added-value and effectiveness

When considering the use of alerts to combat foreign terrorist fighters, unless a European Arrest Warrant could be obtained, the SIS II legal instruments allow the use of alerts for discreet or specific check to report on movements and of alerts for seizure (Art. 38 of the SIS II Decision) where an identity document had been invalidated for travel purposes and its seizure requested. The legal provisions however do not allow an EU-wide exit ban on a person therefore exit bans can be imposed only concerning the territory of a certain Member State subject of national legislation.

With regard to foreign terrorist fighters and children at risk, provision could be made for an alert on persons lawfully banned from leaving the Schengen area or their own Member State. This would require mutual recognition of national exit bans. This concept requires further exploration, as not all Member States may be able to take action on their territory regarding a national exit ban imposed by another Member State.

12. ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS UNDER ARTICLE 38 OF THE SIS II DECISION

12.1 A BRIEF OVERVIEW

Alerts in SIS II	**2013**	**2014**	**2015**
Alerts on vehicles (inc. trailers and caravans)	3 241 809	3 298 541	3 401 517
Alerts on banknotes	265 968	267 123	271 893
Alerts on firearms	431 121	457 059	486 154
Alerts on issued documents	39 836 478	43 552 428	48 357 109
Alerts on blank documents	768 620	981 211	1 107 569
Alerts on licence plates	2 157 328	2 470 227	2 786 092
Alerts on vehicle registration documents	2 314 233	2 657 355	3 035 305

New alert categories introduced by SIS II			
Alerts on aircraft	7	10	19
Alerts on boats	1 046	3 288	6 608
Alerts on boat engines	1 691	9 735	19 815
Alerts on containers	18	96	302
Alerts on industrial equipment	4 252	42 783	84 426
Alerts on securities and means of payment	394 918	1 432 409	3 123 969

Hits	***2014***	***2015***
Vehicles (inc. trailers and caravans)	14 103	15 288
Blank documents	1 274	1 533
Vehicle registration certificates	773	1 378
Number plates	2 416	2 729
Issued documents	14 793	18 558
Boats	32	19
Aircraft	1	0
Industrial equipment	258	197
Boat engines	27	75
Containers	1	0
Firearms	213	296
Securities and means of payment	6	27
Banknotes	218	153
Total number	**34 115**	**40 253**

12.2 KEY THEMES EMERGING

12.2.1 Alerts on vehicles, industrial equipment and licence plates

Distinguishing between industrial equipment and road vehicles - efficiency and effectiveness

Regarding industrial equipment, another new category in SIS II, some Member States have experienced difficulty in distinguishing between road-going industrial equipment and vehicles, especially as the registration of such objects is not harmonised across the Member States, or where only a component is recovered. During Schengen evaluations, the recommendation is given to carry out multi-category searches in order to ensure hits can be achieved. Including a description of the original offence (if any) in the alert, would help the officer finding the object and increase their ability to seize the object requested. It would increase efficiency and effectiveness if guidelines clearly set out the category into which the road-going industrial equipment falls, so that checks stand a better chance of achieving the objective of the alert.

Deletion of vehicle alerts: lack of consistency - efficiency and coherence/consistency

The SIRENE Bureaux are not normally responsible for repatriating recovered vehicles, but they can find themselves involved in exchanging information on handing back vehicles and other objects. Due to a lack of harmonisation of procedures and the timing of deletion of alerts, alerts may be deleted shortly after a hit, upon arrangement to recover the object or upon repatriation. Deleting alerts on repatriation can cause problems for the owner; as the

alert still exists in SIS II, when the vehicle arrives in the country, it can be re-seized from its legitimate owner.

The most difficult cases arise when a stolen vehicle from one Member State is re-registered in another Member State and then sold in the open market. These 'good faith' purchases cause significant problems which can result in court judgments in the Member State where the new owner resides. Where the new owner is awarded title to the vehicle, due to lack of mutual recognition of court decisions in such cases, the alert – created in the Member State where the original theft took place – can remain in SIS II. As a result, every law enforcement check on the vehicle will result in the vehicle being stopped and potentially seized, unless the new owner carries the court decision around with him/her. The inconvenience is disproportionate to the goal of the alert. Some Member States, especially those which have been affected by such cases, have demanded a solution. One suggestion has been to flag the alert in the Member State of the new owner. The effect of this would be to make the alert invisible to the end-users in that Member State. This would reduce the inconvenience in that country, but not if the person crossed a border as, in the neighbouring country, the vehicle would be seized.

The only practicable solution is to introduce stricter alert deletion rules, so that the alert is deleted once a vehicle or other object is recovered by law enforcement officers in the Member State achieving the hit or safe storage of the object has been arranged (some objects are very large or, in the case of a good faith purchase, the vehicle may indeed be left in the hands of the new owner pending a court case). As cases can take time, if the alert is deleted prematurely and there is a need to communicate on the recovery of objects, the SIRENE workflow systems should be amended to ensure that Schengen Identity Numbers of deleted alerts are still recognised and SIRENE forms can be sent. Several Member States have introduced this functionality. One Member State asked for the facility to 'recall' a deleted alert in order to check the details in such cases. If this option were considered, access would have to be strictly limited in order to avoid errors by officers in the field.

A Member State reported problems with disposal of seized property where it is not collected by the owner or insurer. A solution could be for national rules on disposal of property to be forwarded with the initial G form (report of a hit where the action has been taken), so that the deadline for recovery is made clear to the owner or insurer.

With regard to effectiveness, the lack of mutual recognition of court decisions and the fact that every law enforcement check on the vehicle might lead to its seizure is certainly inconvenient for the owner and is not the desired effect of the intervention. This situation causes inefficiencies and SIRENE Bureaux are involved in time-consuming activities, which are not their responsibility.

Combating cloning of cars - effectiveness

Just as human identity can be misused, the cloning of car identities is common. Where it is clear that this has happened, an equivalent of the misused identity extension to person alerts could be created for object alerts, in order to allow officers on the ground to distinguish the vehicles. The system is not as effective as it could be in responding to this problem. Furthermore, a misused identity extension on object alerts would also render the system more efficient, as it would reduce the workload of the SIRENE Bureaux who currently have to carry out this task through sending SIRENE forms. Member State cooperation is crucial in addressing the cloning of cars and SIS II can support greater coordination and, potentially, more results in the field, demonstrating the EU added value in this situation.

Vehicle parts - effectiveness

The SIRENE Manual sets out the procedure for dealing with circumstances in which a stolen vehicle is dismantled and identifiable component parts are recovered by the law enforcement authorities, but the whole vehicle is not. There may be several hits on components from one stolen vehicle, recovered over time. There is currently no provision for circulating stolen vehicle components that have not ever been built into a vehicle. A new alert category or new fields could cover readily identifiable vehicle parts such as the engine or the gearbox. The lack of an alert category or fields for vehicle parts renders the system incapable of addressing a serious criminal activity and goes to the heart of its effectiveness. The circulation of stolen vehicle components must be addressed appropriately by the system, as this issue is also critical to the relevance of SIS II in responding to this type of criminal activity. At the external border, customs agencies have competence for checking imported or exported vehicle parts.

Updated definition of 'motor vehicle' – coherence/consistency

The current definition of a motor vehicle in the SIS II is outdated, as it relies on a minimum 50cc cylinder criterion. Electric cars do not meet this criterion, which should now be revised. It is crucial for SIS II to adapt to technological developments in order to remain relevant and effective.

Post-hit procedures on vehicles and similar objects - EU added-value

When an object, such as a vehicle, is seized by law enforcement authorities due to an alert in SIS II, the post-hit procedures entail a SIRENE G form (hit) to be sent, which the issuing Member State will respond to with a SIRENE P form (further information to be supplied when a vehicle etc. is recovered). The two mandatory fields in the section 'further information concerning the alert' describe the date(s) or period(s) the offence(s) was/were committed and the place(s) of offence(s). This information, and possibly more, could be included in the alert itself, which might reduce the exchange of supplementary information. This could improve efficiency. The impact on ease of access for the end-user to the extra information that would be entered in the alert would need to be considered. More harmonisation on the extent of the responsibility of SIRENE, thereby setting expectations on the exchange of supplementary information, would help maintain the efficiency and effectiveness of the SIRENE Bureaux.

Automatic Number Plate Recognition (ANPR) systems and SIS II - effectiveness and relevance

Several Member States have implemented camera-based systems which can scan vehicle number plates and carry out a check against databases. These are usually databases of stolen, unregistered or uninsured vehicles or vehicles that are being sought by the law enforcement authorities in the course of investigations.

A key concept of SIS II is that checks on objects in the relevant national databases should also check SIS II. As a result, the Commission recognised the potential for large numbers of searches in SIS II carried out automatically. The SIRENE Manual was updated to include procedures on how to handle the exchange of supplementary information in such cases, especially as implementations vary widely between Member States.

Several Member States pointed out that the provisions of Article 9.2, concerning logging of all queries, are difficult in the context of automatic number plate recognition (ANPR) systems and other solutions which carry out large numbers of automated queries. Such systems may carry out millions of queries per day, requiring considerable technical resource to store logs

of all checks. The Netherlands proposed that only hits should be logged. Belgium asked for clarity on ANPR as it is easier to make a technical copy of limited information on vehicles (such as the vehicle registration number) for such purposes rather than all the vehicle data. This should be possible under current legal provisions but needs to be clarified. The Netherlands also requested further work on logs on the history of alerts, asking whether the central system logs and reports (such as 'load history') could be used instead of all Member States having to make such technical provision. Data quality itself remains the responsibility of the data's owner. It is inefficient to store all these data as logs, as a large amount will not be needed for the intervention. The current provisions of Article 9(2) of the SIS II legal instruments are not practicable when considering systems such as the ANPR, which carry out millions of automated queries per day.

Use of vehicle licence plates to locate persons - effectiveness

Law enforcement officers know that one of the most effective ways of finding a wanted or missing person is to circulate details of the person's vehicle. It is not currently possible to issue an alert on objects with the purpose of finding a person without seizing the object to secure property or evidence. This is an operational shortcoming. The suggested solution is to change the wording of Article 38(1) of the Council Decision, so that it reads:

> *'Data on objects sought for the purposes of:*
> *a) seizure or use as evidence in criminal proceedings; or*
> *b) establishing the whereabouts of a person for whom an alert has been issued on the basis of Art. 26, 32 or 34 of the Council Decision or Art. 24 (possibly Art. 25 (f)) of the Regulation shall be entered in SIS II.'*

It would be operationally more efficient and effective for law enforcement officers to be able to locate people through sharing information which they already possess on licence plates, which they have used at national level to locate people for many years.

12.2.2 Checks carried out by the authorities responsible for issuing vehicle registration certificates

The SIS II legal instrument[21] allowing direct or indirect access to certain SIS II data so as to avoid re-registering vehicles stolen in another Member State does not technically fall within the scope of this evaluation. However, as the Regulation's overall objective aligns it closely with the SIS II Decision, it was felt it would be an oversight to exclude it.

Distribution and trends — Searches

There was a considerable increase in the number of searches for motor vehicles — rising from 18.5 million in 2014 to 32.3 million in 2015, an increase of more than 75 %. Similarly, a rise can be seen in searches for number plates — there were 1 123 897 such searches in 2014, compared to 13 355 236 in 2015, an increase rise of more than 1 080 %.

It is important to stress that more could be done by some Member States with regard to implementing the Regulation and reporting statistics. For example, Belgium, Finland, France, Greece, Iceland, Norway, Italy, Switzerland and the United Kingdom recorded neither searches nor hits. Germany, Austria, Slovakia and Slovenia only reported hits, not the searches that were carried out. Implementation therefore appears to be incomplete. As a result, there may be potential for more success in tracing stolen vehicles.

---

[21] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).

Coherence/consistency

Several Member States do not make use of the stolen vehicle number plate alerts, as the plate re-issued to the victim is identical to the stolen plate. Accordingly, the victim would be likely to be inconvenienced by being repeatedly stopped by the law enforcement authorities. This is certainly disproportionate to the objectives of the intervention and could therefore affect its effectiveness.

Effectiveness

The checking of SIS II data by the authorities responsible for issuing vehicle registration certificates has resulted in over 37 000 hits since the entry into operations of SIS II. This access has proved highly effective, where it is used. The lack of full data indicates that implementation is incomplete or reporting is not enforced. This suggests that effectiveness could be increased.

EU added-value

The legislation remains coherent with its goals and relevant, given the ongoing success generated. SIS II has addressed the issue of duplicate licence plates and the intervention is still relevant, given the extent of cross-border vehicle theft. The mechanism to share information on stolen vehicles, registration and number plates has demonstrated significant EU added value.

12.2.3 Alerts on containers and boats

National procedure for checking containers and boats - effectiveness

The Schengen evaluation on-site visits revealed that many Member States do not have effective procedures in place to carry out checks on containers and boats in SIS II. The contents of containers and boats are checked based upon previous information or risk assessment. As a result, the new object categories of boat and container cannot be used effectively in Member States, as the competent authorities are not sufficiently aware of the new categories. Customs authorities generally have competence for checking maritime traffic, even traffic between Member States (where the EU-status of goods needs to be verified). If customs authorities could use SIS II for daily routine checks, this could further increase the effectiveness of use of the system.

12.2.4 Alerts on issued and blank documents

Lack of harmonisation in seizure of documents – coherence/consistency and effectiveness

Alerts on issued documents form the largest volume of alerts in SIS II. The action to be taken on alerts for documents is seizure. However, it is clear that this does not always happen, due to lack of harmonisation of national procedures. A common scenario is that a person loses their identity document, reports the loss and receives a duplicate. The person then finds the original and does not report this to the competent authorities. The issue of the duplicate document automatically triggers the creation of an alert in SIS II, requesting seizure of the document. Some Member States consider a reported lost/stolen document to be invalid once a duplicate has been issued. Problems arise when the person uses this document to travel. Border guards in several Member States see that the person is the original holder of the document and, not wishing to spoil the person's travel plans, hand back the document and allow the person to proceed.

This will remain a problem whilst there is no harmonisation on the seizure or not of documents entered in SIS II. The Commission issued a factsheet to the Member States about the national laws and requirements in each Member State in respect of lost, stolen and invalidated documents. This helps border guards be informed about the legal situation for a

document reported in SIS II for seizure which is held by the lawful owner. They will be in a better position to decide whether to seize the relevant document.

This lack of harmonisation harms the effectiveness of the system to address specific problems (the foreign fighter phenomenon is a good example) — certain objectives of the intervention cannot be achieved. Steps to achieve harmonisation in the field would demonstrate EU added-value.

Counterfeit documents: proposal for a new category within the alert - effectiveness and EU added-value

There are some documents which do not fall under any of the existing categories as they are entirely falsified, i.e. counterfeit documents. Sometimes batches or part-batches of such documents are seized by law enforcement authorities. This allows the serial numbers to be ascertained and checked. Once the authorities have decided that there are documents missing from the batch seized, they should be able to enter the documents in SIS II. The present system is not as effective as it could be as it cannot handle counterfeit documents. The criterion of relevance should also be considered here — SIS II is currently not well-equipped to address this issue.

A new option should therefore be created in this alert category to cover counterfeit blank and 'issued' documents.

Proposal to include details of identity chips in alerts - effectiveness and coherence/consistency

Technical developments in documents need to be reflected in SIS II. A decision should be taken on whether information contained a document's identity chip should be included in alerts. The inclusion of this information in SIS II alerts would render the system more effective in identifying the person and any potential misuse of documents. The ability to use SIS II to check that the document holder is indeed the genuine holder, on the basis of the security features in the document, would make SIS II more consistent with the goal of better document security.

Possible interconnection between SIS II documents section and SLTD - effectiveness and coherence/consistency

Article 55 of the SIS II Decision provides for a connection between SIS II and Interpol's stolen and lost travel documents (SLTD) database. This would allow details of passport numbers, country of issue and document type for stolen, misappropriated, lost or invalidated passports entered in SIS II to be exchanged with Interpol members and Member States would be able to access the SLTD database through SIS II. A connection like this would ensure that: (1) all passport data available in SIS II are also uploaded in the SLTD database; (2) all consultations of passports in SIS II also consult the SLTD database.

However, there are a number of preconditions that need to be met before this technical connection can be made, including an agreement between Interpol and the EU that the data shared will only be accessible to members of Interpol from countries that have an appropriate level of protection of personal data. The Council will seek the Commission's opinion on Interpol's protection of personal data and respect of fundamental rights and liberties when automatically processing personal data, and that of countries that have delegated members to Interpol.

SIS II has not yet been connected to the SLTD database. On 31 March 2015, a questionnaire was sent out to 28 EU Member States and four Associated Countries, to which 29 responses were received. The results of the questionnaire revealed the following:

- the majority (17 out of 29) of respondents do not enter or modify data automatically through one transaction in their national database, SIS II and SLTD, largely due to cost, technical or legal reasons;
- a large majority of respondents (28 out of 29) indicated that they upload data regarding stolen and lost travel documents into Interpol's SLTD database, either automatically (16 MS), manually (nine MS) or semi-manually, using Interpol's 'Push & Pull' solution (three Member States);
- a large majority of countries (22 out of 29) are using Interpol's FIND/MIND tools to check travel documents through a single automated search in different databases (national, SIS II and SLTD). It could not be distinguished whether these tools are solely used for border checks or also for law enforcement checks on Member States' territory.

This demonstrates that many Member States have implemented national solutions ensuring that all passport data that are entered in SIS II are also entered in the SLTD database and that the SLTD database is consulted simultaneously with SIS II.

In order to ensure that data on stolen or lost travel documents are entered in SIS II and the SLTD database at the same time, the following options could be considered:

Option 1: Member States implement national solutions to simultaneously add and consult travel documents in SIS II, SLTD and national databases.
Option 2: implement Article 55 of the SIS II Decision and exchange data between SIS II and the SLTD database.

There are some difficulties with option 2:

- The SLTD database covers travel documents including passports, identity documents and visas. Article 55 of the SIS II Decision is limited to passports. Limiting the data exchange to passports would be counter-productive, as it would not cover all types of travel documents that are now being entered in the SLTD database.
- Only the country which issued a document can add it to the SLTD database - this limitation does not exist for SIS II.
- 170 Interpol members contribute to the SLTD database. It is not clear how the Commission would be able to identify for each of those members the appropriateness of their protection of personal data and respect of fundamental rights and liberties when automatically processing personal data. It is also not clear how Interpol would be able to prevent access to EU documents in the SLTD database by members that do not provide an appropriate level of protection and respect.

Therefore, option 1 seems to be more practicable.

Based upon Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol[22], Member States are required to upload travel documents to the SLTD database and search it. Thanks to the FIND search software Interpol developed, Member States can search the SLTD database and their national systems in parallel. As there

[22] OJ L 27, 29.1.2005, p. 61.

is a common search interface, SIS II is also searched. Member States are the largest contributors of alerts in the SLTD database. In addition, following several initiatives by the Commission and the Council, the number of searches in the SLTD database has recently increased substantially.

The existing mechanism is effective. The Commission should explore the potential added value of linking the document section of SIS II with the SLTD database at central level. It should also address the technical and the legal difficulties identified and take action to ensure that document alerts are automatically entered in the SLTD database.

12.2.5 Alerts on banknotes, securities and means of payment

Counterfeit banknotes - effectiveness and relevance

Article 38(2)(g) of the SIS II Decision states that alerts may be issued only on banknotes that are registered. In practice, alerts are also entered in SIS II on counterfeit money. There have been few or no hits on genuine banknotes. Operationally, it is ineffective to limit this alert category to real money, and counterfeit should be included if the alert category is retained. However, on the basis of hits achieved there appears to be limited value in retaining alerts on banknotes in SIS II.

As a result, the Commission and Member States should consider whether alerts on banknotes should be deleted from the legal instruments and technical specification. If they are retained, the legal instruments and technical specifications should be updated in order to accommodate counterfeit banknotes.

Securities and means of payment - relevance and efficiency

The number of hits in this area has increased from six in 2014 to 27 in 2015. However, there are a very large number of alerts on securities and means of payment, and a very low number of hits. This raises issues pertaining to the added value of including them as separate sub-categories under Article 38 of the SIS II Decision and, whether this is efficient. As a result, the alert category 'securities and means of payment' should be deleted from the SIS II legal instruments and the technical specifications.

12.2.6 Broadening the scope and use of object alerts

Extension of the object alert categories - effectiveness

Member States welcomed the extension of the categories of objects that can be entered in SIS II. Several Member States asked for further extension of the categories, to include technical or electronic equipment such as computers and smartphones. High value jewels and watches were also mentioned; however, this would require a method for uniquely identifying these objects as SIS II has always used serial numbers. Watches may have unique serial numbers (but do not always), but photographs are more effective for jewellery. There is no sub-categorisation or search facility in SIS II to permit searches of photographs.

Use of alerts when law enforcement measures are deemed 'administrative' not judicial - effectiveness and coherence

Alerts under Article 38 of the SIS II Decision concentrate on « *alerts on objects for the purposes of seizure or use as evidence in criminal proceedings* ». During procedures carried out by law enforcement personnel, administrative measures regularly take place before or in parallel to a judicial procedure (such as an exit ban from the national territory – an administrative measure). To ensure the effectiveness of such procedures operationally, the text of the Decision should clearly spell out the possibility of creating SIS II alerts on the

objects covered by such measures. This would increase consistency with the goal of the judicial process.

13. NEW FUNCTIONALITIES IN SIS II — CHALLENGES IN IMPLEMENTATION

13.1 IMPLEMENTING FUNCTIONALITIES

This section sets out the changes in the use of new features in SIS II — the inclusion of fingerprints, photographs, copies of the European Arrest Warrant (EAW) and links between alerts which are related (e.g. a wanted person in a stolen car could result in two alerts but with a link between them to give the officer on the ground the full picture).

The inclusion of the European Arrest Warrant - efficiency and coherence

All alerts for arrest resulting from an EAW must contain a copy of the EAW. This has required enormous efforts by Member States to upload copies of warrants relating to the alerts that already existed before SIS II went live. Article 70 of the SIS II Decision provided for a three-year transition period for Member States to ensure compliance. The 30 000 EAW's held in SIS II in January 2016 indicate the move to compliance. We are only now reaching the efficiency gain intended by this feature. Under previous provisions, each hit on an alert for arrest would have necessitated at least two SIRENE business transactions: upon arrest, a request for a copy of the EAW and, from the issuing Member State, the forwarding of that EAW. Given the number of EAW's now in SIS II and over 11 000 hits on alerts for arrest in 2015, we can estimate that in excess of 20 000 SIRENE business transactions per year can be avoided through this measure.

Fingerprints and photographs - efficiency and effectiveness

Where fingerprints and photographs are available, they must be added to an alert. The statistics show the move towards compliance. More must be done, on two fronts:

1. ensuring compliance with legal instruments, in that fingerprints and photographs are indeed uploaded;
2. ensuring the quality of the fingerprints and photographs, through compliance with existing standards and ensuring those standards are extended, especially in the light of the proposed automated fingerprint identification system in SIS II and any future need to use facial recognition technology.

Efficiency and effectiveness gains based on fingerprints will not be realised until an automated fingerprint identification system has been installed in SIS II. In those Member States where end-users can see a photograph of the alert subject, the increase in effectiveness is clear.

Links between alerts - effectiveness

Member States choose to use links on the basis of operational assessment. The Schengen evaluation mechanism checks on the use of links. One area for possible future development might be the ability for two or more Member States to cooperate on linking alerts. Currently, this is not legally or technically possible and a business case would be necessary.

13.2 CONCLUSIONS

When SIS II began operating, some Member States had not implemented the new functionalities. By the time of writing this report, this situation had largely been resolved but it is too early to fully evaluate the effectiveness of, for example, the introduction of fingerprints, as the technology to make use of this functionality is not yet in place. It is currently only possible to report on the use of new functionalities, as no statistics are yet available on results.

14. USE OF FINGERPRINTS IN SIS II

It is becoming increasingly difficult to establish the identity of a person due to name-changes and the use of aliases or fraudulent documents. The use of document fraud is an increasing modus operandi to illegally enter and move around the Schengen area. The *Frontex Annual Risk Analysis* for 2015 reported that in 2014 there were around 9 400 detections of document fraud cases on entry to the EU/Schengen area from third countries, which represents a slight decrease compared to the previous year. By contrast, cases reported on intra-EU Schengen movements showed a marked increase from 7 867 in 2013 to 9 968 in 2014 (an increase of 27 %). Document fraudsters not only undermine border security but also the internal security of the EU. The use of fingerprints would be an efficient way for both border guards and law enforcement officials to identify persons sought by the authorities and to detect cases of document fraud. The fraudulent use of travel documents in connection with the recent terrorist attacks in Paris also confirms the necessity for a tool that provides the possibility of identification of persons on the basis of fingerprints. To date there is no EU-wide system which would allow the checking of persons on the basis of fingerprints.

A new SIS II feature is the storage of fingerprints in Central SIS II. At present, prints are used to *confirm* the identity of a person located as a result of a search, usually on name and date of birth. This is a 'one-to-one' search — the person's prints are compared to one set of prints stored in SIS II. However, the possibility to *identify* a person on the basis of his/her fingerprints requires an evolution to the present law enforcement practice: the comparison of a person's prints to all sets of prints — a 'one-to-many' search — to identify the person solely on the basis of fingerprints. This functionality requires the implementation of an Automated Fingerprint Identification System (AFIS). AFIS has been successfully used in numerous national and cross-border cooperation databases. For the EU the obvious examples are the Visa Information System (VIS) and EURODAC. Articles 22(c) of the SIS II Decision and the SIS II Regulation provide a legal basis for using AFIS. Before this functionality is implemented, the Commission was required to report on the availability and readiness of the required technology, on which the European Parliament should be consulted.

On 29 February 2016, the Commission adopted a report[23] in line with Article 22 (c) of the SIS II legal instruments about the availability and readiness of the technology to use fingerprint for search. eu-LISA has launched the concrete implementation of a centralised AFIS, the first phase of which will be introduced in 2017. AFIS can be used by the same authorities that are entitled to carry out checks in SIS and it can be used in the same control situations when a SIS II check is performed, i.e at the time of a visa application, at border controls and at checks on the territory of a Member State.

[23] Report from the Commission 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) (COM/2016/093 final).

Effectiveness and relevance
SIS II, with only the ability to carry out alphanumeric searches, is currently not sufficiently effective as 28 % of the identities in SIS II are aliases. Many persons travel under different identities that cannot be revealed by searches only using a name and date of birth. Therefore, a fingerprint search is needed to increase effective law enforcement, allowing people to be identified beyond any doubt. The SIS II AFIS would represent significant EU added value, as it would be the first EU-wide criminal AFIS. To date, there is no such functionality comparable to SIS II's geographical coverage; this is problematic for the EU-wide security screening of irregular migrants. Consistency should be ensured with the Prüm mechanism on the bilateral exchange of fingerprints.

In order to ensure the maximum effectiveness of fingerprint searches it is necessary to set high standards for data quality. To this end on 4 August 2016 the Commission adopted a Commission Implementing Decision on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II)[24] pursuant to Art. 22(a) of the SIS II legal instruments.

15. OPERATIONAL PROCEDURES

As this section goes right to the heart of operations it brought out some very detailed comments on operational practices.

15.1 KEY THEMES EMERGING

Ensuring that end-users can gain full benefit from SIS II information - effectiveness and efficiency
The SIS II legal instruments set out the categories of information which may be held in SIS II. The provisions on 'additional data' in Article 3(1)(c) of the SIS II Decision[25] state that these data must be immediately available to the end-user, while the arguments for making other data available are present but less explicit. Experience from Schengen evaluation on-site visits shows that the legal instruments should be more explicit on making SIS II information available to end-users as, in some Member States, features such as photographs and links between alerts were not visible to the end-user. One Member State proposed that a third paragraph could be added to Article 9, stipulating that the authority designated pursuant to Article 7(1) (N.SIS II) is responsible for ensuring that all end-users can see the data provided to them via SIS II on their user interface.

It is inefficient and ineffective to provide enhanced data for end-users and for them not to have access to it. It is inconsistent to have explicit text on accessing data for some data but not others.

Automation of data insertion - efficiency
In order to ensure consistency with national police databases and improve data quality, when a national entry is created, it should be transferred automatically to SIS II without requiring a separate alert to be created in SIS II. This also applies to the update and deletion procedures.

---

[24] Commission Implementing Decision (EU) 2016/1345 of 4 August 2016 on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II) (notified under document C(2016) 4988) (OJ L 213, 6.8.2016, p. 15).

[25] 'additional data' means the data stored in SIS II and connected with SIS II alerts which are to be immediately available to the competent authorities where a person in respect of whom data has been entered in SIS II is located as a result of searches made therein.

Single query to query the national systems and SIS II - efficiency and effectiveness

SIS II is a compensatory measure that helps to maintain a high level of security within the area of freedom, security and justice by supporting operational cooperation between police authorities and judicial authorities in criminal matters (Decision 2007/533/JHA) and the implementation of policies linked to the movement of persons that are part of the Schengen *acquis* (Regulation 1987/2006). If SIS II is not systematically included in law enforcement checks on a Member State's territory, the Member State is unable to fully contribute to the very purpose of SIS II, as it will not access and act upon the information that is included in the alerts. This means that there is a flawed application of SIS II which could constitute a security gap in Europe.

Improving use of 'fuzzy' or 'any name' searches to obtain more hits - effectiveness and efficiency

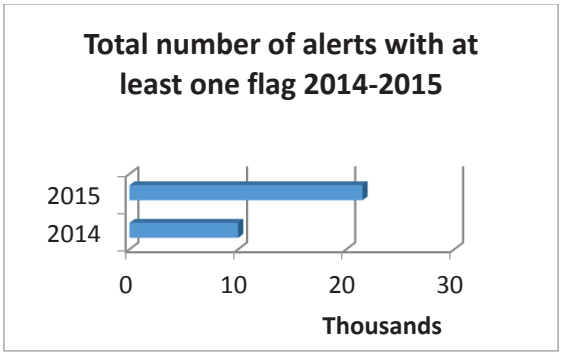
Member States can configure their queries to seek exact matches against SIS II data or seek varying amounts of 'fuzziness', or permutations of a name, to cater for misspelling or partial details. Exact match searching is only realistic in very controlled environments, such as airport checks, but even this will not cater for misspelling in the original alert. Exact match searching is inefficient for detection purposes as, although it provides a rapid response, it may miss the potential hit.

Flagging - effectiveness and coherence/consistency

Flagging is an exception to the principle of mutual recognition, and should not therefore be used extensively. It is a suspension of validity of an alert at national level that may be added to alerts for arrest, alerts on missing persons and alerts for discreet or specific checks, if a Member State considers that giving effect to a particular alert is incompatible with its national law, its international obligations or essential national interests. When the alert is flagged, the requested action is not taken on the territory of this Member State. Only a potential incompatibility with national law or international obligations can justify a flag. Formal errors in an EAW, such as the illegibility of a date or signature, cannot lead to a flag. A flag can only be added at the request of or by agreement with another Member State.

Number of alerts with at least one flag (distribution and trends)

There has been a substantial increase in the number of alerts with at least one flag — there were slightly more than 10 000 such alerts in 2014, rising dramatically to 21 497 in 2015, an increase of more than 100 %.



Flagging is used when a Member State informs (using a SIRENE F form) the Member State which issued the alert that it cannot take the action requested on an alert. The existence of a high number of flags on a Member State's alerts indicates that the Member State has a high number of requests for arrest that at least one other Member State cannot act upon. This indicates some inconsistency between national law and the Framework Decision on the European Arrest Warrant[26] (applicable only to EU Member States, not associated countries).

[26] Council Framework Decision of 13 June 2002 (2002/584/JHA) on the European arrest warrant and the surrender procedures between Member States OJ L 190, 18.7.2002, p. 1-20.

Two Member States 'own' 51 % of all alerts against which at least one flag has been set. Although no further conclusion can currently be drawn, this situation is statistically disproportionate and merits further investigation. Extensive use of flagging reduces the effectiveness of the system, as end-users will not act upon these alerts. Flagging should therefore remain an exception.

16. SIRENE BUREAUX AND THE EXCHANGE OF SUPPLEMENTARY INFORMATION BETWEEN MEMBER STATES

16.1 INTRODUCTION

SIS II only contains the information (i.e. alert data) required to allow a person or an object to be identified and the necessary action to be taken. In line with the SIS II legal instruments, Member States must, either on a bilateral or multilateral basis, exchange supplementary information related to the alert to implement certain provisions provided for in the SIS II legal instruments, and to ensure that SIS II functions properly.

The structure that has been built to deal with the exchange of supplementary information has been given the name 'SIRENE'. This is an acronym of the definition of the structure in English: Supplementary Information Request at the National Entries. Each Member State designates the authority which will host the SIRENE Bureau in their country. The Bureaux work in accordance with the provisions of the SIRENE Manual[27], an annex to a Commission Implementing Decision.

Supplementary information is exchanged via the SIRENE Bureaux for the following reasons:

(i) to allow Member States to consult or inform each other when entering an alert;
(ii) following a hit, to allow the appropriate action to be taken;
(iii) when the required action cannot be taken;
(iv) when dealing with issues relating to the quality of SIS II data;
(v) when dealing with the compatibility and priority of alerts;
(vi) when dealing with rights of data subjects to access, correct or delete his personal data.

The operation of SIS II is inseparable from the SIRENE Bureaux, as they are at the very heart of SIS II communication. The SIRENE Bureaux are the single contact point for all SIS II communication within a Member State and between Member States. The Bureaux manage all background information on a SIS II alert, which is indispensable for the officers on the ground to confirm hits and carry out the required action.

16.2 SIRENE COMMUNICATION

The SIRENE communication infrastructure operationally forms an integral part of SIS II and is operated by eu-LISA. The fact that SIS II is the most successful European security system is largely due to effective SIRENE communication, based upon structured information and solid procedures.

16.3 SIRENE COMMUNICATION WITHIN A MEMBER STATE

End-users in a Member State must contact the SIRENE Bureau to:

[27] Annex to Commission Implementing Decision (EU) 2016/1209 of 12 July 2016 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2016) 4283) (OJ L 201, 28.07.2016, p.35).

- confirm whether a search in SIS II has produced a hit
- receive supplementary information and instructions
- report a hit.

This contact can take place by telephone (in many Member States the end-user interface displays the telephone number), in a free-text message or via a dedicated, structured hit-reporting form. To ensure that supplementary information which is essential to take action (e.g. the missing person needs immediate medication) is sent rapidly, Italy put in place pop-up messages on the end-user screen which become visible only if there is a hit. This practice saves precious time for the officers as they have the necessary information immediately at their disposal. Many Member States have already implemented structured hit-reporting forms, which in some countries can be immediately transformed into a SIRENE G form. This saves time for the SIRENE Bureau and speeds up bilateral communication with the Member State that issued the alert. Internal hit reporting forms allowing structured and automatic communication between officers on the ground and the Bureau increase SIS II's effectiveness by speeding up communication. This boosts the system's overall efficiency, as it saves additional resources in Member States if this form is transformed automatically or semi-automatically into a G form.

16.4 Bilateral or multilateral SIRENE communication — the SIRENE Forms

Communication mainly takes place through 14 SIRENE forms, designed for specific purposes. Supplementary information exchange is the principal means of ensuring that outputs (hits) become successful outcomes, for example, the extradition of wanted people, the protection of the vulnerable and the correct seizure of stolen property. Each SIRENE form sent or received represents a piece of work for the SIRENE Bureaux in the Member States. In 2015, nearly 1.8 million forms were sent or received, an increase of 27 % on 2014. This reflects the 22 % increase in hits in the same period. The Bureaux carry out an average of 11.6 pieces of work per hit (incoming or outgoing forms) in order to achieve the tasks detailed above (ensuring data quality, following up on a hit, consulting to ensure that alerts do not conflict or when an alert is particularly important). This appears remarkably efficient. The key question remains: are such efficiency and effectiveness sustainable in the face of year-on-year workload increases?

There are several ways of approaching statistics on the exchange of supplementary information by SIRENE form. Since a form can be sent bilaterally from one Member State to another, this would count as one form sent and one received. This is most likely to happen when a hit is achieved and the executing Member State reports the hit to the issuing Member State using a G form. However, when an alert for arrest is created an A form is sent multilaterally to all Member States, i.e. one form is sent, but 28 received. In these examples, the G form represents two pieces of work (one Member State creating a form and one Member State receiving and processing the information on the hit), whereas the A form represents 29 pieces of work (one Member State creating a form and 28 Member States receiving and processing the information). Statistics are therefore provided on what Member States generated (outgoing forms), what Member States had to process (incoming forms) and the total number of pieces of work which the Member States' SIRENE Bureaux had to handle (incoming + outgoing forms).

From a statistical point of view, the growth in number of the Schengen states will have an impact on the exchange of forms. This has always been so. At the end of 2014 and start of 2015, all the existing Member States sent A forms for the existing 34 000 alerts for arrest to the UK for verification. A similar process will take place in 2016-17 for Croatia. However, even if the base were stable, there is a year-on-year workload increase for the SIRENE

Bureaux. For example, while the number of alerts for arrest has remained stable, between 2014 and 2015 there was a 27 % increase in hits. This cannot solely be explained by the addition of one Member State into SIS II and therefore must largely be due to an increase in operational 'productivity' by law enforcement and judicial authorities in Member States. Although very welcome, the effect is an increase in work, generally without an increase in resources. This is the major reason why the Commission asked Member States to highlight areas of potential inefficiency to ensure increases in productivity do not have a detrimental effect on the effectiveness and efficiency of the Bureaux.

16.5 'DATA EXCHANGE BETWEEN SIRENES (DEBS)'

SIRENE forms must comply with a set of technical standards in order for the correct information to be entered in the correct sections (fields) of the forms so that they are universally comprehensible. In 2015, the SISVIS Committee agreed that responsibility for ongoing maintenance of DEBS would pass from the Commission to eu-LISA, in order to effectively incorporate DEBS updates into the SIS II change management process. To date, eu-LISA has not acquired sufficient competence to manage DEBS and it is still highly dependent upon Member State expertise. Release 8 of the Central SIS II had to be postponed due to issues relating to DEBS. As changes in Central SIS II may have an effect on DEBS, appropriate centralised management is required to analyse the wider impact of changes to DEBS. Centralised management of DEBS that is not dependent solely on Member State expertise is required. eu-LISA taking over management of DEBS has had a substantial positive impact on the effectiveness and EU added-value. It also reflects the principle that SIRENE communication is an integral part of SIS II.

16.6 SIRENE FUNCTIONAL TESTS

SIRENE functional tests examine the functioning of the national SIRENE technical solutions and exchange of information between SIRENE Bureaux through forms sent via the SIRENE Mail infrastructure according to the specifications provided for in the SIRENE Manual. These include entering, modifying, flagging, deleting corresponding alerts in SIS II and attaching/detaching relevant additional information to SIS II alerts. As the SIRENE functional tests cover both the exchange of forms and core SIS II operations, eu-LISA took over the overall management of the tests, assisted by volunteer Member States. So far SIRENE functional tests have been run with Poland, Finland and the UK. Tests on exchanging forms also had to be run as a consequence of Release 8 of the Central SIS II. eu-LISA's stronger engagement in the SIRENE community helps eu-LISA to understand the nature of the business and the operational needs of SIS II end-users.

16.7 SIRENE WORKFLOWS AND WORKLOAD — MAINTAINING EFFECTIVENESS, EFFICIENCY AND COHERENCE WITH REQUIREMENTS

Other than installing automated workflow systems with the potential to significantly improve capacity, the formal elements of SIRENE information exchange must be respected. It has been recognised, in the framework of the European Information Exchange Model, that SIRENE Bureaux can work at high levels of intensity due to the formalisation of their working practices. However, even those Bureaux which have installed workflow systems have highlighted that the workload is at the limits of capacity. The SISVIS Committee has worked on generic requirements for workflow systems. The Commission carried out a survey to identify the highest areas of pressure, the areas where the Bureaux consider themselves to be strong and what changes they would envisage. Staffing levels have not increased in line

with the rapidly increasing workload. Better case management systems and workflows are required and procedures should be as automated as possible.

16.8 STRUCTURE OF THE SIRENE BUREAUX

Transparency

The Commission published a list of N.SIS II Offices and the national SIRENE Bureaux in the Official Journal C10 3, 9.04.2013, together with a list of competent authorities that are authorised to directly search the data in SIS II. Updated versions were published by the Agency in OJ C 278, 22.08.2014 and OJ C 208, 24.06.2015. Member States are responsible for ensuring that their SIRENE Bureaux are fully operational on a 24/7 basis. The implementation of this requirement differs throughout the Member States.

SIRENE Contact Person: solving problems — efficiency

In some cases, standard procedures may be insufficient. The SIRENE Contact Person (SIRCoP) deals with files on which progress is complex, problematic or sensitive and a degree of quality assurance and/or longer term contact with another SIRENE Bureau may be required in order to resolve the issue. The SIRCoP may formulate proposals to improve quality and set out options to resolve such issues in the longer term. An annual assessment is carried out as part of annual statistical reporting. There were 113 contacts initiated in 2014, rising to 167 in 2015 – an increase of almost 50 %. (No data on this were collected in 2013, therefore the statistics cover only 2014 and 2015.) The low number of complex or blocked files requiring SIRCoP intervention is remarkable when compared with the overall level of contact and information exchange between Bureaux and the total number of successful outcomes achieved.

Premature deletion of supplementary information and related issues — effectiveness and efficiency

Not all Member States make use of the provisions of Article 53 of the SIS II Decision. These state that:

> *2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS II.*
>
> *3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.*

In some Member States, the national system is configured to automatically trigger the deletion of any supplementary information when an alert is deleted. Any subsequent exchange of information between the Member States on the alert is hampered, as a result. This often happens in missing person cases and follow-up enquiries on recovered objects. This is especially problematic when a Member State's SIRENE system can only generate SIRENE forms relating to an existing Schengen ID number as the number will have ceased to exist.

Member States should therefore reconsider the automatic deletion of supplementary information, especially as the legislation permits longer retention. Alternatively, Member States should reconfigure their SIRENE systems to be able to generate forms using Schengen ID numbers that no longer exist.

17. SIS II- SIRENE TRAINING AT EUROPEAN LEVEL

17.1 SIRENE CEPOL COURSES

An enduring outcome of the 2008 French Presidency of the Council of the EU is the SIRENE Training Committee. With the growing number of Member States, training needed to become more structured and professional. Interested Member States and the Commission formed the Training Committee. Due to the inseparable link between interpretation of the legal instruments and ensuring that operational staff receives clear explanations of the legal instruments, the Training Committee, by common consent, came under the responsibility of the SISVIS Committee when SIS II became operational on 9 April 2013. The Committee decides on user needs for training. Through a partnership with CEPOL, Member States experts, the Commission and, more recently, eu-LISA (which has a statutory responsibility to provide training on technical aspects of SIS II, including to SIRENE staff and those involved in Schengen evaluations) the following courses are listed in the SIRENE Training Manual. They were developed by the three original partners.

- SIRENE I (or Basic) — The SIRENE I course is intended for SIRENE operators who:

  – already have some SIRENE work experience (at least 6 months); or
  – have already worked for a longer time in a SIRENE Bureau but need to update their knowledge in light of developments; or
  – come from candidate countries and need to understand the SIRENE's work.

  Participants should have knowledge of the SIS II legal instruments and the SIRENE Manual, and they should be able to apply the relevant articles within their national legislation. Usually, two courses are run per year.

- SIRENE II (or Advanced) — This advanced training activity is aimed at experienced SIRENE operators. They should have sound knowledge of the legal framework and operational practice, including national procedures. Their level of experience and knowledge should enable them to generate creative solutions within this complex environment. Outputs from these seminars include discussion documents and factsheets (see section 9.9.1.3). Usually, one course is held per year, unless the SISVIS Committee seeks a second course and this can be accommodated within CEPOL's schedule.

- SIRENE III (Train-the-Trainers) — This course is to provide SIRENE operators with some knowledge and skills in training methodology. They gain an understanding of the difference between the two categories of SIRENE training, in particular their aims and structure. This course is run when there is a need to increase the number of trainers.

17.1.1 The SIRENE online module and SIRENE platform

CEPOL, Member States and the Commission worked together to develop an online training module on SIS II and SIRENE. It is hosted on the CEPOL training platform, in a dedicated SIRENE area. Training and reference materials are therefore available 24/7 to staff throughout the Bureaux. The platform also holds all pre-course and training materials for training seminars. In parallel, the Commission manages the uploading and update of reference materials on the platform, such as the SIRENE factsheets and legal texts, which are useful for operational staff.

17.1.2 Statistics on the SIRENE CEPOL trainings

The trained SIRENE officers is 353 in total since 2013.

Divided per years:

2013 - 133 Participants (3 courses)

2014 – 64 participants (2 courses)

2015 – 85 participants (3 courses)

2016 – 71 participants (2 courses) - Still one course to be implemented in Latvia at the end of September 2016.

These figures do not contain the number of persons participating in webinars hosted by CEPOL. The Commission organised since 2013 altogether 11 webinars. The number of participants varied between 50 and 220 depending on the subject matter.

17.2 EU-LISA TRAINING

eu-LISA's mandate in providing SIS II training is based on the eu-LISA Regulation. Training topics and target groups are specified in:

- Recital 11: The Agency should perform tasks relating to training on the technical use of SIS II[28];
- Article 3(b): The Agency shall perform tasks relating to training on the technical use of SIS II, in particular for SIRENE staff, and training of experts on the technical aspects of SIS II in the framework of Schengen evaluation.

By joining the existing partnership between the Commission, the Member States and CEPOL, eu-LISA has improved the training offered by increasing the opportunities for SIRENE staff to learn about the technical aspects of SIS II. eu-LISA regularly delivers targeted training before each Schengen evaluation mission, focusing on the technical performance of the Member State under evaluation. In November 2015, eu-LISA organised the first technical course on SIS II for SIRENE operators. This is meant to close a gap, as efficient SIRENE work cannot be separated from a basic technical understanding of the system.

17.3 CONCLUSIONS

Regular SIS II-SIRENE training is one of the core achievements of SIRENE cooperation at European level and it substantially contributes to the consistent application of the system throughout the Member States. Member States explored the possibility of applying the SIRENE training model to other forms of European law enforcement cooperation, as regular training activities harmonise procedures and improve the working relationships between SIRENE operators. Common European training activity therefore has a clear EU added value. Schengen evaluation missions have shown the different levels, however, of end-user training. This falls under the competence of Member States and to-date there is no common European training curriculum. SIS II is less effective if end-users are not aware of the different functionalities, alert categories and, most importantly, actions to be taken. Carrying out discreet checks poses a particular challenge for end-users in particular at the external borders where the waiting queues are long therefore the border guards in certain Member States disregard the discreet nature of the check and take the person to the second line, in-depth check which jeopardises the secrecy of the check.

[28] And VIS, Eurodac and other large-scale IT systems that might be entrusted to the Agency in the future.

18. SIS II GOVERNANCE — ISSUES ALREADY ADDRESSED AND HARMONISATION OF PROCEDURES

18.1 GOVERNANCE

SIS II governance is provided by:

- the Commission;
- the SISVIS Committee;
- eu-LISA;
- the eu-LISA Management Board; and
- the SIS II Advisory Group.

Responsibilities of the Commission

The Commission's responsibility relating to SIS II is twofold: firstly, it manages any legislative initiative linked to SIS II and secondly, in its role as the guardian of the Treaties, ensures the correct application and implementation of the SIS II legal framework. The Commission takes a dual approach towards Member States to ensure that EU law is applied correctly. It pursues breaches of EU law via the 'EU-Pilot' procedure, with the further option of infringement, and it supports Member States' in developing capacity to optimise the use of the system. The Commission also works together with the Member States on the correct use of SIS II, as described later in this document. The Commission preserves its budgetary powers, as the EU general budget covers the costs of maintaining and operating the central system and the communication infrastructure, including continuous synchronisation with national systems.

The Commission's participation and active involvement in every training course and conference organised on SIS II (a minimum of five times per year on regular courses) ensures the correct interpretation and provision of the most up-to- date information on SIS II.

In SIRENE-related matters, the Commission is the primary point of contact for Member States, including for managing the SIRENE address book, organising meetings and managing and maintaining a dedicated website. The Commission monitors the implementation of the SIRENE Manual, oversees all training-related materials and products to ensure they are legally compliant and takes part in SIS II/SIRENE evaluation missions through the Schengen Evaluation mechanism.

Responsibilities of the SISVIS Committee — EU added-value, efficiency and effectiveness

The SIS II legal instruments set up the SISVIS Committee to assist the Commission in a number of key tasks. The committee is comprised of Member State delegations (including one technical and one operational expert) and is chaired by the Commission. The Commission coordinates and steers the committee's work and prepares the draft measures on which the committee is asked to give an opinion and any other working papers. The committee meetings provide transparency and an opportunity to address issues of concern, to put pressure on Member States to fix problems and to exchange best practice. The committee has evolved to become the main forum for harmonising operational procedures, supporting the effective application of the rules and the optimised use of SIS II. Implementing the SIS II legal instruments means that the Commission must adopt implementing measures with normative effect and, as set out in the SIS II legal instruments, it is assisted in this by the SISVIS Committee. Provisions with normative effect comprise mainly business rules on data processing, including biometrics, which have a direct impact on individuals whose data will be processed in SIS II, or rules which set or alter the underlying architecture of the system within the framework provided by the SIS II legal bases.

The committee originally met in three formations: SIS II technical, SIRENE and Visa Information System (VIS). In 2015, the SIS II technical and SIRENE formations were merged, as virtually all issues addressed had implications for both operational business and IT. The SISVIS Committee is can create working groups to examine particular issues, if needed.. The Training Committee (described above) is a sub group of the SISVIS Committee, and previous examples include the Test Advisory Group (TAG), the Change Management Board (CMB) and the National Project Managers meeting. These tasks are now carried out by eu-LISA, with the involvement of the SIS II Advisory Group.

There is significant EU added value, efficiency and effectiveness in providing a forum with a suitable and sufficiently broad legal basis to allow the end-users of SIS II, the Commission and eu-LISA to meet regularly to ensure clarity on interpretation of EU law, identify operational issues and technical improvement. The Commission is kept apprised of operational and technical matters at Member State level and the Member States have ready access to the Commission for interpretation of the legal instruments. This is especially important in the fluid situations of migration and security. There is internal consistency and effectiveness in ensuring close ties between the interpretation of the law and the explanation of the law through training, all coordinated within the Committee structure.

Responsibilities of eu-LISA

While the Commission develops technical rules and normative procedures (either alone or working with the SISVIS Committee, as described above), eu-LISA has responsibility for the operational management of the SIS II central system and its interconnection with the national systems. In order to ensure the highest technical and budgetary synergy between the activities, it is essential that the Commission works very closely with eu-LISA.

Responsibilities of the Management Board

The Management Board's role in SIS II governance is derived from the tasks reserved to the Board, under the eu-LISA legal basis, particularly relating to the annual programming and budgetary cycles. It also has to approve the final release plan concerning SIS, VIS and EURODAC.

Responsibilities of the Advisory Group

The SIS II Advisory Group was set up to provide the Management Board with expertise relating to the SIS II central system, in particular, relating to the annual work programme and the annual activity report. The Advisory Group comprises Member State representatives and the Commission. The procedures for the operation and cooperation of the Advisory Groups are laid down by the Management Board in eu-LISA's rules of procedure.

18.2 ISSUES ALREADY ADDRESSED AND THE HARMONISATION OF PROCEDURES

18.2.1 Issues addressed in the SISVIS Committee — EU added-value and effectiveness

The Commission's 2014 report on the *Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation* stated that:

> *Clear rules on data capturing, quality control, agreements on legal basis used when capturing and using the data, common procedures, etc. are not in place for all aspects relating to cross-border information exchange. SIS II and SIRENE were mentioned as a good example where detailed rules exist.*

The Commission convenes the SISVIS committee approximately every six weeks to address technical and operational matters. Accordingly, even while this evaluation report was being written, progress was being made on matters of common interest to the Commission and Member States. As an operational system, SIS II is under continuous review. The SIS II

governance model created a highly effective structure, able to respond to new operational requirements and challenges. The structure fosters mutual understanding amongst stakeholders and facilitates harmonisation in the operation of SIS II and SIRENE. The Commission and eu-LISA significantly benefit from this ongoing feedback from Member States, allowing them to better understand operational practice and reality. It also provides an opportunity for the Commission to monitor SIS II on an ongoing basis and raise issues in a more informal and educative manner.

18.2.2 Interim reviews of the SIRENE Manual

The statistics on hits in SIS II and the exchange of supplementary information between the SIRENE Bureaux show that this sphere is highly operational and use of SIS II evolves to face new operational challenges. As a result, although stability in the legal base is always desirable, periodic review is needed to ensure that the legal basis remains fit for purpose. No set of procedures will ever be perfect and from time to time, the SISVIS Committee needs to discuss common problems and adopt procedures to overcome these. Where necessary, these new procedures must be reflected in the SIRENE Manual. The need to respond to the issue of foreign terrorist fighters provided an opportunity, in 2014, to carry out an interim review of the SIRENE Manual in order to meet operational demands. The new version entered into force on 29 January 2015. On 12 July 2016 the Commission adopted the revision of the alert compatibility rules by providing for the possibility of the waiver such rules in case of serious threat.

18.2.3 The Catalogue of Recommendations and Best Practice — EU added-value

In 2015, a Commission Recommendation was adopted, creating a catalogue of recommendations and best practices for correctly using SIS II and exchanging supplementary information by the Member States implementing and using SIS II. The catalogue is used as a reference guide by Member States integrating into the SIS II, by Member States checking and reviewing their procedures, and by members of on-site teams carrying out evaluations under the Schengen Evaluation Mechanism.

18.2.4 Factsheets — Effectiveness

The SIRENE advanced seminars specifically focus on implementing SIS II and SIRENE procedures and, when appropriate, produce factsheets to provide an overview of the state of play in the Member States. The Commission checks the problem statement and legal references, and the respective Heads of SIRENE Bureaux validate the national content. The factsheet initiative began under SIS I. With the go-live of SIS II, the Commission initiated a review of all factsheets. Several issues which had proved problematic under SIS I were removed or reduced with the introduction of SIS II and, as a result, the factsheets could be amended or deleted. The factsheets provide an interesting fact-finding exercise in that they describe situations where national laws or procedures have an impact on the implementation of the SIS II legal instruments and there is value in describing these situations to other Member States, in order to avoid lengthy exchanges of messages. Factsheets are not static. They are revised, used as a basis for improving working procedures in the SIRENE Manual or the catalogue of recommendations and best practice (SIS II and SIRENE), and they are deleted when they have served their purpose. Factsheets are only retained in the longer term where national law and procedure are not harmonised at EU level, to explain differences in national implementation. The factsheets are uploaded by the Commission onto the secure SIRENE section of the CEPOL website, where other reference documents are placed for access by end-users.

The factsheets are effective as they highlight issues of national law or lack of harmonisation or consistency. They also provide an effective basis for action, as demonstrated by the deletion of factsheets once issues have been resolved. Pending deletion, the factsheet

provides a reference document to indicate national specificities which can reduce inefficiency caused by unnecessary correspondence.

19. REMEDIES

Remedies are the provisions in each Member State that allow a person to bring an action before the courts (or the authority competent under the law of any Member State) to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him and the mutual enforcement of decisions in other Member States.

In accordance with data protection principles, all individuals whose data are processed in SIS II have the following specific rights under Article 41 of the SIS II Regulation and Article 58 of the SIS II Decision:

- the right of access to data relating to them stored in the SIS II;
- the right to correct inaccurate data or have data deleted, if they have been stored unlawfully; and
- the right to bring proceedings before the courts or competent authorities to correct or delete data or to obtain compensation.

Anyone exercising these rights can apply to the competent authorities in the Schengen State of his/her choice. This is possible because all copies of data in the national databases (N.SIS II) are identical to the central system database (CS.SIS II). Therefore, these rights can be exercised in any Schengen country, regardless of who issued the alert. When an individual exercises his/her rights of access, correction of inaccurate data and deletion of unlawfully stored data, competent authorities must reply within a strict deadline. The individual must receive a reply as soon as possible and, in any event, not later than 60 days from the date on which he/she applies for access, or sooner if national law so provides. The individual must also be informed as soon as possible of action taken to correct or delete data as requested, and in any event not later than three months from the date on which he/she applies for correction or deletion, or sooner if national law so provides.

19.1 THE RIGHT OF ACCESS

The right of access allows anyone, on request, to have knowledge of the information relating to him/her stored in a data file as referred to in national law. This is a fundamental principle of data protection which enables data subjects to exercise control over personal data kept by third parties. This right is expressly provided for in Article 41 of SIS II Regulation and in Article 58 of SIS II Decision. The right of access is exercised in accordance with the law of the Member State where the request is submitted. These procedures differ from one country to another, as do the rules for communicating data to the applicant. When a Member State receives a request for access to an alert that it did not issue, it must give the issuing country the opportunity to state its position on disclosing the data to the applicant. The information must not be communicated to the data subject if this is required to carry out the legal task connected to the alert, or in order to protect the rights and freedoms of other people.

There are currently two types of system governing the right of access to data processed by law enforcement authorities, and thus which also apply to SIS II data. In some Member States the right of access is direct, while in others it is indirect. Direct access means the person applies directly to the authorities who process the data (police, gendarmerie, customs, etc.). If national law permits, the applicant may be sent the information relating to him/her. Indirect access means the person applies to the national data protection authority in the country where

the request is submitted. The data protection authority carries out the necessary checks to handle the request and replies to the applicant.

19.2 RIGHT TO CORRECTION AND DELETION OF DATA

People also have the right to correct factually inaccurate or incomplete personal data and to ask for personal data that have been unlawfully stored to be deleted. Only the Member State responsible for issuing an alert in the SIS II may alter or delete it. If the request is submitted in a Member State that did not issue the alert, the competent authorities in the relevant countries work together on the case, exchanging information and carrying out the necessary checks. The applicant should provide the grounds for their request to correct or delete the data and any relevant information to support the request.

19.3 REMEDIES: THE RIGHT TO COMPLAIN TO THE DATA PROTECTION AUTHORITY OR TO INITIATE A JUDICIAL PROCEEDING

Articles 43 of SIS II Regulation and 59 of SIS II Decision set out the remedies available to individuals if their request has not been complied with. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him. If they have to deal with a complaint with a cross-border element, data protection authorities should work with each other to guarantee the rights of the data subjects.

19.4 EVALUATION

The evaluation is based on a questionnaire to the members of the SIS II Supervision Coordination Group in June 2015 and evaluations by Member States on the application of the Schengen *acquis* in the field of data protection.

19.4.1 Questionnaire forwarded to the members of the SIS II Supervision Coordination Group

The questionnaire forwarded to the members of the SIS II Supervision Coordination Group in June 2015 sought responses to the questions described previously in Section 4.2.9. Sixteen responses were received.

Several Member States provided an overview of the initial subject access enquiry process (direct to the data controller or indirect to the DPA), the possibilities for seeking redress via the national data protection authority (DPA) and the appeal process through a tribunal or administrative court. In general, the approach adopted is that the DPA receives requests for rights of access, correction, deletion and obtaining of information relating to an alert on the data subject. The DPA then contacts the data controller to check the details of the subject access enquiry and ensure any corrective action is taken. If the alert was entered by another Member State, the DPA contacts its counterpart in that Member State. The views of the other Member State are sought prior to any disclosure of information to the data subject. Many Member States said that the subject access enquiry process is the same regardless of the location of the applicant. They described the list of identification information and identity documents required to establish the identity of the subject access enquirer.

The services of the DPA or the data controller are provided free of charge in all Member States that responded. Lithuania highlighted that one free right of access is provided in a calendar year. However, where a data subject decides to seek redress or appeal to the court, there are usually court fees to be paid. Even then, several Member States described schemes whereby those in financial need could apply for a fee waiver. If the applicant is in a third country, Member States generally require the data subject to apply in person unless he/she

provides sufficient proof of authorising a third party e.g. a lawyer, to carry out the request. The data subject must provide sufficient proof of identity, such as a copy of a passport or national identity card. Poland does not require the attachment of identity documents.

The amount of statistics available varies. This was a key finding of the questionnaire, as the inconsistency of statistics hindered effective evaluation of the measures. The detailed replies provided by Member States on the number of complaints and remedies are set out in Annex IV.

There are several approaches to mutual recognition and enforcement of final decisions handed down by the courts or authorities of other Schengen States. Some Member States considered that the provisions of Article 59(2) of the SIS II Decision or Article 43(2) of the SIS II Regulation are sufficient, stating that national courts are obliged to enforce such decisions.

19.5 THE EVALUATIONS OF CERTAIN MEMBER STATES ON THE APPLICATION OF THE SCHENGEN ACQUIS IN THE FIELD OF DATA PROTECTION

The evaluation and monitoring mechanism for verifying the application of the Schengen *acquis*, as established by Council Regulation (EU) No 1053/2013 of 7 October 2013[29], provides for a multi-annual[30] evaluation programme and more detailed annual evaluation programmes[31]. This analysis takes into account the evaluations carried out by the time of drafting the evaluation report. Generally, Member States evaluated to date implement and apply the EU's Schengen *acquis* in line with the data protection requirements. Examples of points for improvement and best practices are listed below.

Right of access, correction of inaccurate data and deletion of unlawfully stored data

Article 58 (6) of the SIS II Decision and Article 41(6) of the SIS II Regulation state that the time limit for replying to requests for access to data should be 'as soon as possible' and in any event 'not later than 60 days' from the date of the request. In certain Member States the national legislation provides for longer periods for the reply than 60 days. In several Member States, access requests were free of charge. A best practice example was that multiple data subject access requests can be exercised free of charge, with no limit on the number of access requests that can be made by a data subject. Other Member States, however, limit requests to one per year per requestor for a set of data, unless the data subject submits relevant justification, which does not seem to be the most suitable tool for guaranteeing the exercise of the data subject's rights.

Public awareness regarding data protection

It was noted in certain cases that the information provided to the public is not entirely up to date and could be more extensive and coordinated.

Supervision of N.SIS II

Article 44(1) of the SIS II Regulation and Article 60(1) of the SIS II Decision state that the authority or authorities designated in each Member State who have the powers referred to in Article 28 of Directive 95/46/EC (the 'National Supervisory Authority') must independently monitor the lawfulness of:

---

29 OJ L 295, 6.11.2013, p. 27.

30 Commission Implementing Decision of 18.6.201, establishing the multi-annual evaluation programme 2014-2019 in accordance with Article 5 of Council Regulation (EU)No 1053/2013 of 7 October 2013 (C(2014) 3683).

31 Commission Implementing Decision of 30.10.2014 establishing the first section of the annual evaluation programme for 2015 in accordance with Article 6 of the Council Regulation (EU) No 1053/2013 of 7 October 2013 (C(2014) 7781).

- the processing of SIS II personal data on their territory;
- transmission of those data from that territory; and
- the exchange and further processing of supplementary information.

An audit of the data processing operations in its N.SIS II should be carried out in accordance with international auditing standards at least every four years. Member States must ensure that their National Supervisory Authority has sufficient resources to fulfil the tasks entrusted to it under the SIS II legal bases. SIS II must be audited by 9 April 2017. This will necessarily cover all the data protection aspects of the structure and functioning of SIS II, including the quality of the data entered into the system. Regular comprehensive checks of SIS II alerts, especially on the basis of log file analysis, are required. These must take into account that SIS II related logs are kept just for one year. In several Member States, a lack of human resources in general and particularly for SIS II supervision is an issue. In one Member State, no specific supervision and monitoring of SIS II has been carried out. The main reason given for not carrying out checks and audits after SIS II came into force is limited human and financial resources coupled with the fact that the supervision of SIS II has not been considered a priority. A considerable weakness was noted regarding the lack of access to log records from the N.SIS II by the SIS II data controller.

A best practice example was where the mandatory Data Protection Officer worked as an in-house advisor, legally empowered to assist and monitor data processing activities within the police forces and formally incorporated in the legal system, ensuring independence and legal protection. This helped support an optimal enforcement of the applicable data protection rules. In another Member State, each police unit has a privacy officer. Together with the Data Protection Authority for the national police, they have set up a Privacy Platform as a forum to discuss all privacy-related issues and where privacy-by-design solutions are going to be developed.

Effectiveness

All Member States have well-developed frameworks allowing any person to bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him. Many Member States said that the subject access enquiry process is the same, regardless of the location of the applicant. They described the list of identification information and identity documents required to establish the identity of the subject access enquirer.

Member States were asked to provide available annual statistics covering 2013 and 2014 on the use of such remedies (the total number of cases per year; the number of cases where the court or authority ruled in favour of the applicant; the number of cases where compensation was paid; the financial value, in total of the compensation paid). In this sphere there is significant variation in the amount of statistics available. In order to be able to check on the use of recourse in Member States it is necessary to be able to receive statistics on data subject enquiries and subsequent actions from the data owner, the data supervisor and the Courts. This is not possible in all Member States and is ineffective in gaining an overview of the issues at the EU level.

Serious problem of non-recognition of court decisions is described in Section 13.2.1, second point concerning alerts on vehicle purchased by a third party acting in good faith.

Efficiency

Member States vary in their ability to provide statistics. In order to be able to check on the use of recourse in Member States, statistics on data subject enquiries and subsequent actions from the data owner, the data supervisor and the Courts must be available. Proper statistical

reporting would increase the efficiency to monitor the implementation of the data protection rules.

Relevance

The right to access one's personal data and the right to correction of inaccurate data or deletion when data have been unlawfully stored are key principles of EU data protection law. In the context of processing personal data such as in the SIS II, it is imperative that rules are in place at EU level to ensure the data subject's rights. Additionally, given the reported use of the rights of subject access enquiry, the rules in place are highly relevant.

Coherence/Consistency

Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[32] applies to the processing of personal data carried out in application of this Regulation. This includes the designation of the controller and the possibility for Member States to provide for exemptions and restrictions to some of the rights and obligations provided for in that Directive, including the rights of access and information of the individual concerned. The principles set out in Directive 95/46/EC are supplemented or clarified in the SIS II legal instruments, where necessary. The same applies to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

During the overall evaluation and in SISVIS Committee meetings, some Member States raised the issue of 'good faith' acquisition of motor vehicles which turn out to have been stolen in another Member State and re-registered. As acquisition in good faith can take place in many Member States, but there is a problem when a prosecutor in one Member State insists on leaving an alert for a stolen vehicle in SIS II even though a court in another Member State has awarded ownership to the new owner. The impact of the continued existence of the alert is disproportionate as the new owner risks being stopped by the law enforcement authorities every time the car is used (see recommendations on alert deletion).

EU added-value

It is not always obvious to an alert subject which Member State has created an alert related to him/her. The mutual recognition and procedures in place to allow a person to commence a subject access enquiry in any Member State provide considerable EU added value.

[32] OJ L 281, 23.11.1995, p. 31.

20. OVERALL COST EFFICIENCY OF SIS II

As a follow-up to the technical assessment a further study was commissioned to assess:

- the current operational costs of SIS II incurred by Member States; and
- the ICT impacts of proposed improvements to the SIS II architecture.

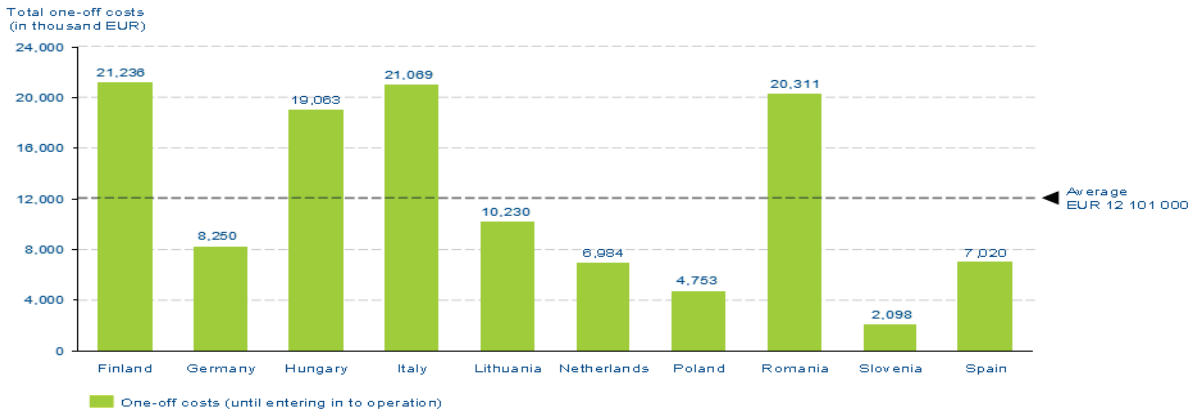
20.1 BUILDING THE ICT COST MODEL

This study assesses substantive compliance costs, according to the ICT cost categories specified in the Value Assessment Tool (VAST[33]) guidelines of the European Commission.

20.1.1. Operational costs

The technical architecture of SIS II has to be considered when calculating SIS development and operational costs incurred by the EU and the Member States, in particular the fact that it consists of the three major components: a central system, national systems, and a communication infrastructure.

This section provides an overview of the current operational costs incurred firstly by Member States and secondly by the EU for the Central SIS II. For the purpose of this study, the authors carried out a total costs of ownership (TCO) assessment to calculate the operational costs of SIS II incurred by Member States. This includes total one-off costs in terms of development and capital investment in hardware and software until N.SIS II came into operation in 2013, plus ongoing costs of infrastructure (hardware and software) maintenance, support, hosting facility and training for subsequent years (i.e. 2013, 2014, and 2015). The project team was able to draw on results received from ten sample Member States. It should be noted that, due to the flexibility in national implementation (e.g. whether a copy of SIS II data is kept at national level), costs can vary significantly between Member States.



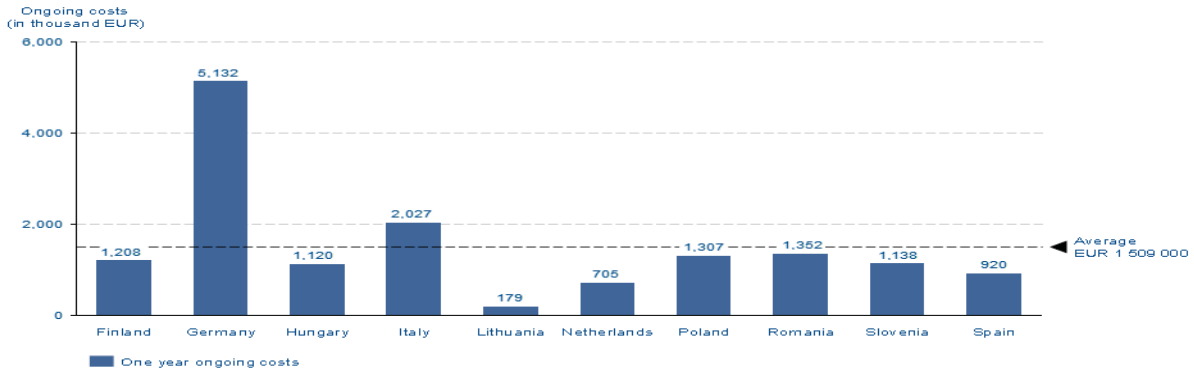
Total one-off costs until N.SIS enters into operation

Initial one-off costs in terms of development and capital investment in hardware and software for N.SIS II until it began operating in 2013 average out at approximately €12 000 000 per Member State, based on the ten Member States examined in this study.

Total one-off costs include the initial cost for updating the integration between national policing systems and N.SIS II application and the acquisition of a onetime software licence. The total one-off costs from the EU budget for development of Central SIS II between 2002 and the system going live in 2013are €152 961 319.

33 Value Assessment Tool guidelines, European Commission, Directorate-General for Informatics, 2010.

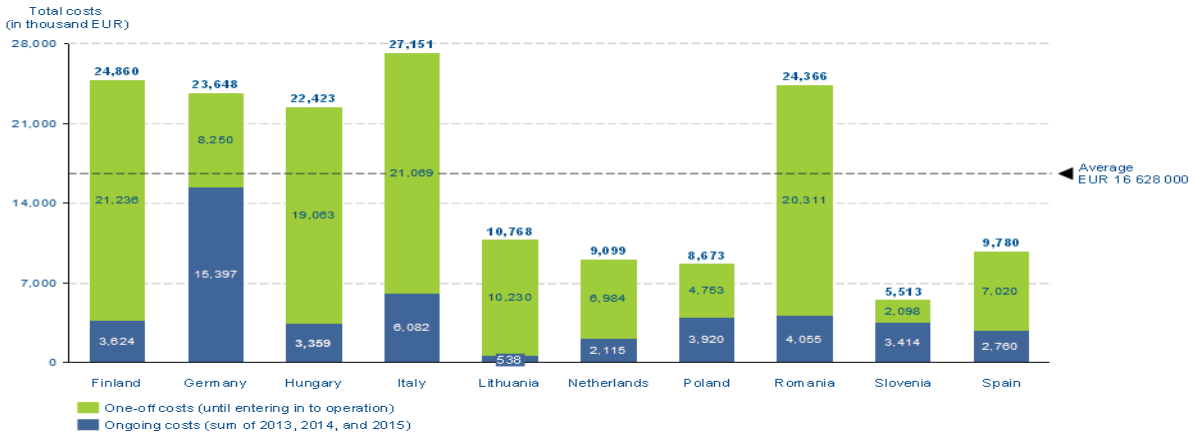
In addition to one-off costs, the national systems and Central SIS II incur yearly ongoing maintenance costs. The chart below shows the annual ongoing costs for N.SIS II for the period 2013-2015.



One year ongoing costs for maintaining N.SIS II for the period 2013-2015

In the ten Member States considered during this study, these ongoing costs average out at approximately €1 509 000. They include annual software licence fees and software updates, annual network costs, maintenance[34] of the N.SIS II infrastructure, user support (i.e. help desks), costs of the data centre facility (e.g. security, electricity, power supply), and costs for training end users. Annual maintenance costs of the Central System amounted to €7 794 732.35 in 2014 and €5 631 826.58 in 2015.

The chart below gives an overview of the total cost of ownership of N.SIS II, including one-off costs for 2007 until it came into operation in 2013, and the sum of the yearly ongoing costs for the subsequent years (i.e. 2013, 2014 and 2015). Overall, the total cost of ownership of N.SIS II including one-off and ongoing costs in the ten Member States considered in the study average out at approximately €16 628 000.



Total Cost of Ownership of N.SIS II

There are two broad ranges of TCO, with half of the interviewed countries (i.e. Italy, Finland, Germany, Romania, and Hungary) having TCO higher than €15 000 000 (averaging out at approximately €24 000 000) and the other half of the interviewed countries (i.e. Lithuania, Spain, Netherlands, Poland, and Slovenia) having TCO lower than €15 000 000 (averaging out at approximately €9 000 000).

---

34 Maintenance includes activities related to both corrective maintenance and evolving maintenance. (Source: VAST — Value Assessment Tool Guidelines of the European Commission, Directorate-General for Informatics, 2010).

The overall TCO (including one-off and ongoing costs) summing up the ten analysed Member States considered in this study is €166 280 508.

20.1.2 The costs of non-Schengen - efficiency

Development and operational costs incurred by the EU and Member States in respect of SIS II have been calculated taking into consideration the technical architecture of the system, mainly the fact that it consists of the three major components: SIS II central system (CS-SIS), national systems and a network.

The costs, however, had to be analysed taking into consideration that SIS II is the main compensatory measure for the abolition of internal border controls within the Schengen area. Without SIS II, keeping an area with no internal borders would be hardly feasible. The Commission clearly stated, in its Communication on the roadmap 'Back to Schengen' of 4 March 2016[35], that reintroducing temporary border controls not only hampers the free movement of persons, but also comes with significant economic costs. The Commission estimated that:

- full re-establishment of border controls within the Schengen area would generate immediate direct costs of €5 billion to €18 billion annually.
- Member States such as Poland, the Netherlands or Germany would face more than €500 million of additional costs for the road transport of traded goods. Spain or the Czech Republic would see their businesses paying more than €200 million in additional costs.
- Border controls would cost the 1.7 million cross-border workers between €1.3 billion and €5.2 billion in terms of time lost.
- At least 13 million tourist-nights could be lost, with a total impact of €1.2 billion.
- Between €0.6 billion and €5.8 billion of administrative costs would have to be paid by governments, due to the need for increased staffing for border controls.

21. CONCLUSIONS

SIS II operates against a background of serious concerns about security, cross-border crime and irregular migration. When considering the five key areas of evaluation, the following broad strategic conclusions can be drawn:

- SIS II is highly effective, as it achieves significant operational outcomes in the areas covered by the alerts.
- SIS II is highly efficient, as it achieves these outcomes via the simple expedient of information sharing and with limited follow-up communication between Member States.
- SIS II is broadly coherent, with some notable exceptions, with the overall policies at EU level in security, judicial cooperation and irregular migration.
- SIS II is highly relevant to operational need, having demonstrated its ability to address existing issues and evolve to meet new needs.
- SIS II provides significant EU added value as the key compensatory measure for the removal of internal borders between the Member States, in a way that could not be achieved without a pan-European approach.

[35] COM(2016) 120 final.

This study has identified a series of conclusions and findings for further consideration and reflection. The complete listing appears in Annex 1.

ANNEX I - FINDINGS AND RECOMMENDATIONS

The evaluation methodology as well as the specific questions are described in Section 3 of this Staff Working Document; the sources are listed in Annex II and Annex III and these form the basis of the following findings and recommendations.

All proposals marked with an asterisk (*) will require a legislative amendment to the existing legal bases; Regulation (EC) No 1987/2006 and/or Council Decision 2007/533/JHA.

SIS II Technical Assessment

Note: In the light of information also provided by eu-LISA to the evaluation and based upon Report ICT Impact Assessment of Possible Improvements to the SIS II Architecture[36], *the following recommendations should be viewed as a start point for further discussion with all stakeholders as any solutions will be predicated upon a balance of the amount of flexibility Member States require, the capabilities of SIS II to carry the load of transactions and the cost both at Member State and central system level.*

Proposals for the central system and overall architecture

1. The central system's read capacity and performance should be increased.
2. There should be a backup site update and upgrade process to ensure minimal business continuity loss*.
3. There should be increased central system test capabilities
4. There should be the possibility to develop N.SIS II implementations, shared between Member States*.
5. Proposals for national optimisation and harmonisation (option — distinct N.SIS II)*
6. The logs on alert history, retained at national level should be optional*
7. Query logging should be selective, especially in cases such as ANPR, and subject to standardised rules*.
8. XML messages should be replaced with JSON objects.
9. ICD national implementation should be complete implementation of the ICD*.
10. National copies (partial) for N.SIS II should be mandatory*.
11. Each N.SIS II should have a mandatory backup system*.
12. There should be a common blueprint for consistent N.SIS II configuration.*
13. There should be a common N.SIS II implementation in the Member States*

Authorities empowered to enter and search SIS II alerts

14. It should be considered to grant administrative access to authorities responsible for the registration of boats and aircraft to enable them to check the status of the craft prior to re-registration*
15. The Commission, together with the Member States, should investigate how the use of SIS II by customs shall be carried out more systematically, to achieve reinforcement of the capacity to detect all types of risks and analysis of trends involving all types of illegal movement of goods and cash, brought by persons crossing the external border
16. Member States should ensure that the statistical reporting on the SIS II checks carried out by vehicle registration services and the resultant hits is more efficient*

[36] European Commission, Directorate-General for Migration and Home Affairs — Report ICT Impact Assessment
of Possible Improvements to the SIS II Architecture 20 April 2016.

17. Harmonisation of licence plate design is outside the scope of this report. The Commission should highlight, to the competent national authorities, the problems linked to stolen licence plates and the success achieved by both law enforcement and vehicle registration authorities in detecting stolen licence plates. This should be viewed in the context of incomplete implementation of procedures or provision of statistics concerning SIS II checks on imported vehicles presented for re-registration

EUROJUST and EUROPOL

18. Eurojust and Europol should fully implement the SIS II functionalities as foreseen in the SIS II Decision
19. Europol should develop a batch searching tool to allow SIS II to be queried to cross-check information received from non-SIS II using countries and third party operational organisations. Each query in the batch must be capable of being justified. In principle, in the longer term perspective, coherence and complementarity between SIS II and Europol data must allow for appropriate instruments to pro-actively seek links and fill identified gaps in either of the data repositories at any time
20. Europol should extend the functionality of its end-user interface to allow access to fingerprints included in alerts and to download the prints for comparison in the Europol AFIS
21. Europol should describe its logging processes for SIS II queries especially in order to remedy the situation where log information has been considered unlawful copying of SIS II data*
22. During the proposals on the update of the SIS II legal instruments the wording of the data protection provisions of Europol and Eurojust should be revised to allow both agencies to effectively log their queries and carry out their core business without being at risk of suggestions of unlawful downloading and processing of data*
23. Europol should receive full access to all alert categories of SIS II, including data on missing persons and third-country nationals whose entry or stay is refused in the Schengen area*
24. Europol and Eurojust should carry out internal training in order to raise awareness on the improved SIS II functionalities and services available

Alerts on refusal of entry or stay under Article 24 SIS II Regulation

25. A review should be carried out on the collecting and reporting of statistics on all hits on refusal of entry alerts both at border crossing points and on a Member State territory
26. The Commission should make a proposal on a standardised statistics package on the use of the consultation procedure for completion by the Member State. This should include definitions and counting rules
27. The legal instruments and technical specifications should be updated to improve the possibilities for identifying a person, for example through the inclusion of details of identity documents*
28. The SIS II legal instruments and technical specifications should be updated so that additional information on the reasons for issuing the alert is immediately available to the end-user. The statistics on the volume of alerts should distinguish between the different categories in accordance with the reason for issuing the alert*
29. The Commission should assess the findings of the study on alternative models for the exchange of supplementary information on refusal of entry or stay alerts with the purpose of increasing its efficiency

30. The Commission should propose a review of the consultation procedure and should makes proposals for the harmonisation of use of the related SIRENE forms and describe the simplification of the procedures and the forms
31. In line with the review of the consultation procedure, the Commission should make proposals on a binding time limit for Member States to respond to a request for consultation. If the SIRENE Bureau remains the conduit for such consultation the staffing and access to systems should be ensured to achieve a response within 12 hours
32. In line with the review of the consultation procedure, staffing and access to systems should be ensured so that alerts which need to be deleted are deleted without delay
33. It should be mandatory for Member States to enter all entry bans issued in accordance with the Return Directive as a refusal of entry alert in SIS II from the moment the decision becomes enforceable*
34. In the SIS II Regulation it should be implemented as a legal obligation to issue an alert in SIS II when the underlying decision is related to a failure to comply with national immigration legislation*
35. The Commission should make a proposal on a standardised procedure and timing for the entry of alerts on refusal of entry or stay. Given that the creation of an alert implies that action is requested as specified in the alert, the basis of the timing of the entry should be that the alert is enforceable*
36. The retention period for refusal of entry or stay alerts in SIS II should be aligned with the maximum length of entry bans as established in the Return Directive*
37. The Commission, in the context of inter-institutional discussions, should seek agreement on more efficient and effective procedures for the insertion and maintenance of alerts based on restrictive measures against third countries
38. Also for alerts issued under Article 26 of the SIS II Regulation there should be a requirement to enter all available data for identification purposes (such as photographs) to the alert beyond the data that are strictly mentioned in the act constituting the restrictive measure*
39. For the effective performance of its task in the monitoring of returns, organising return operations and conducting return interventions, the European Border and Coast Guard Agency should receive access to alerts on third country nationals subject to a refusal of entry alert or a return alert (in the future)*

Alerts for arrest for extradition or surrender under Article 26 SIS II Decision

40. Together with other matters related to the EAW, the Commission should raise with the Member States the problem of creating SIS II alerts when the whereabouts of the subject of the alert are already known and confirmed
41. Member States should reinforce their procedures for ensuring that, when an EAW has been created for a person whose whereabouts are known and confirmed, the correct field of the SIRENE A form is used to highlight that fact so that needless work on checking whether the person is known or present on the territory is avoided
42. Together with other matters related to the EAW, the Commission should raise with Member States the problems related to transfers, seeking to find, with the judicial and law enforcement authorities, areas where common practice can be established and procedures harmonised
43. The legal instruments and technical specifications of SIS II should be amended to allow Member States to temporarily make an alert ‘non-searchable’ by end-users without the need to delete the alert*

44. The Commission should make a proposal on additional fields to be added to alerts for arrest for extradition or surrender in order to reduce the amount of information exchange via supplementary information but avoiding information that is not essential for officers carrying out the arrest

Alerts on missing persons under Article 32 SIS II Decision

45. The wording of the legal instruments should be amended in order to provide the opportunity to create preventive alerts on people who are at serious risk of abduction. The wording should be such that over-use of such alerts is controlled in order to avoid inefficiencies and inaccuracies in alerts. The correct action to be taken must be determined*
46. The legal instruments and technical specifications should be updated to permit end-users to mandatorily enter a category of missing person, not only for children but also to indicate vulnerability in adults. This is to ensure a correct first response by officers on the ground and follow-up care but also to give policy makers an overview of the phenomenon of missing persons*
47. The Commission should make a proposal on the categories of missing person cases which should be entered in SIS II and those which should not in order to avoid situations where officers are tasked to investigate cases where legally the person is not considered missing on that national territory
48. In line with the initiative on categorisation of missing person cases, the options for action to be taken should be expanded to clearly indicate cases where repatriation is not sought as it should not be assumed that this would be in the best interests of the child. This includes repatriation to the alert-issuing Member State, another Member State or a third country
49. The SIS II technical specifications should be updated so that upon achieving the age of eighteen the reason for request and action to be taken automatically change to those relevant for a missing adult. The end-user should have the option of specifying that the person remains vulnerable. This is to cope with cases where competent authorities have concerns about the person regardless of age. Alternatively, the alert can be set to expire on the eighteenth birthday*

Alerts on persons sought to assist with a judicial procedure under Art 34 SIS II Decision

50. Together with other matters related to judicial procedures, the Commission should raise with Member States the problems related to non-deletion of alerts on persons sought to assist with a judicial procedure*
51. The prompt deletion of alerts where a valid address has been provided is paramount. Once a valid address has been provided by a Member State and the alert not deleted, that Member State should not be obliged to report further hits. In order to prevent repeated work by officers on the ground the wording of the legal instruments should be amended to permit flagging of alerts on persons sought to assist with a judicial procedure in circumstances where a hit has been achieved in a Member State and a valid address forwarded to the issuing Member State. The effect of the flag would be to make the alert non-searchable by end-users*
52. Regular training should be provided to the judiciary on the use of SIS II with particular regard to alert updating procedures and alert deletion

Alerts for discreet and specific checks under Article 36 SIS II Decision

53. The Commission should make a proposal on fields/extensions to fields that should be added to alerts for discreet and specific checks in order to provide more information to the officer on the ground carrying out a check, especially a specific check
54. The wording of the legal instruments should be updated to allow the creation of alerts for discreet and specific checks on the basis of an identity or travel document only; that is, the alert is on a document which is not necessarily linked to a specific person*
55. As some criminal penalties require supervision to ensure that they are respected the Commission should amend the wording of the legal instruments to include '*executing criminal penalties*' within alerts for discreet and specific checks*
56. Even though specific checks are less discreet than a discreet check it is important not to unnecessarily divulge information on the existence of the alert. The Commission should propose new wording to be incorporated in the 'action to be taken' on specific checks to avoid improper divulging of the existence of the alert to the alert subject as required by Article 37.3 of the SIS II Decision*
57. The Commission should discuss with the Member States the ability of Member States to issue travel bans on their citizens and secondly, the mutual recognition of such travel bans. On the basis of these discussions, depending on the outcome, the wording of the legal instruments should be updated in order to add a new category of alert 'people subject of a national exit ban who are to be prevented from leaving the Schengen area'*
58. The Commission should discuss with the Member States whether the field 'type of offence' should become mandatory for alerts for discreet and specific checks
59. In at least eleven Member States no specific checks can be performed. Member States should adopt legislation to allow specific checks. Under the SIS II Decision the alternative action for a specific check, in case it cannot be performed under national law, is a discreet check. The Commission should consider defining another option for action which does not contain the same element of secrecy as the discreet check*
60. The Commission should increase the effectiveness of discreet and specific check on boats and containers and to this end should make a proposal for a procedure for an issuing Member State to inform one or more Member States of a request to check for containers, boats and aircraft within the framework of alerts for discreet and specific checks
61. It is advisable to revise code table 028 concerning the 'type of offence' by adding child pornography and sexual offence

Counter-terrorism

62. The Commission should consider introducing a specific alert and action for entering into SIS II a person under 'terrorism related activity' which would allow the detention and the specific check of a person for a limited period of time without a formal arrest*
63. The criteria for using the new 'immediate reporting' should be harmonised and it should be made clear in which cases this option should be used
64. In cases requesting immediate reporting the occurrence of a hit should be reported without delay to the SIRENE Bureau that issued the alert
65. A post-hit procedure should be agreed in order to clarify if the hit information should be sent only to the issuing Member State or to all Member States. Member States should share hit information with Europol allowing further analysis on terrorist travel routes and movements (in line with the "three tier information approach")
66. It is necessary to enhance national training activities on SIS II counter-terrorism measures for the SIRENE staff, national state security services as well as the end-users

67. There should be an automated notification mechanism between the SIRENE Bureau and the national security services

Alerts on objects for seizure or use as evidence in criminal proceedings under Article 38 SIS II Decision

68. The wording of the legal instruments should be updated to include 'technical equipment' in the alerts on objects for seizure or use as evidence in criminal proceedings. The technical specifications should be updated accordingly, including fields for 'type of technical equipment', 'technical equipment serial number' and 'make of technical equipment'. The latter two fields may have to be free text, firstly because the serial numbers will not be of a standard length or composition, and secondly due to the very wide range of makes of equipment which simply could not be managed by a code table*
69. The alert category 'securities and means of payment' should be deleted from the SIS II legal instruments and the technical specifications*
70. The Commission should make a proposal that all road-going industrial equipment should be entered in SIS II as a vehicle (sub-category 'industrial equipment')
71. Member States should ensure that when vehicles or industrial equipment are checked the check takes place against both vehicles and industrial equipment categories in the SIS II in order to avoid circumstances where a potential hit is not achieved
72. The Commission should address the problem where a person is awarded ownership of an object by a competent court or authority and yet an alert for the seizure of the object remains in the SIS II. *
73. The Commission should make a proposal for an extension to object alerts that will have the effect of providing more identification data on, for example vehicles, which will allow the identification of the vehicle even if it has been subject of cloning
74. The Commission should make a proposal to address the issue that an appropriate action, generally seizure, is consistently taken across the Member States in relation to the objectives of the alert
75. The technical specifications and legal instruments should be updated in order to allow Member States to enter alerts on counterfeit documents in SIS II*
76. On the basis of hits achieved, there appears to be limited value in retaining alerts on banknotes in SIS II. Accordingly, the Commission and Member States should consider whether alerts on banknotes should be deleted from the legal instruments and technical specifications. If not, the legal instruments and technical specifications should be updated in order to accommodate counterfeit banknotes within this alert category*
77. The wording of the legal instruments should be updated to ensure that when law enforcement officers carry out actions within their competence they should not be prevented from using SIS II merely because the national legal classification of the action is deemed administrative rather than criminal; an example would be the request for seizure of documents invalidated for travel purposes in support of a national exit ban. To this end, the wording of Article 38.1 of the SIS II Decision should be reworded to read, *'Data on objects sought for the purposes of seizure for law enforcement purposes or use as evidence in criminal proceedings shall be entered in SIS II'**
78. The SIS II technical specifications should be updated to allow the inclusion, in document alerts, of information held in a document's identity chip. This would typically include the full contents of the Machine Readable Zone, fingerprints and

photograph (if contained), and any other national specificity (such as national citizen register number, commune of registration)

79. The legal instruments and technical specifications should be updated so that significant, identifiable component parts of a vehicle can be entered as alerts in SIS II, instead of only complete vehicles being entered*
80. The legal instruments should be updated so that the definition of a motor vehicle is no longer dependent on it being equipped solely with an internal combustion engine as this no longer reflects reality*
81. The legal instruments and technical specifications should be updated so that, in order to be able to locate a person who is the subject of an alert under Articles 26, 32 or 34 of the SIS II Decision or Art. 24, 25 or 26 of the Regulation, there should be the possibility of entering the details of a vehicle that is in possession of, or being used by the alert subject*
82. The Commission should make a proposal on extra information fields that could be added to an alert in order to reduce the post-hit exchange of supplementary information on object alerts
83. The Commission should make a proposal on inclusion in SIRENE G forms on the national rules for retention of property in police storage prior to the disposal of the property. This is to prevent the unnecessary exchange of supplementary information on reminders to collect property or on requests for property disposal deadline information
84. The Commission should make a proposal so that rules on mandatory fields in problem areas such a non-standard VIN and firearms should be reviewed to make the use of the system more efficient
85. Member States should increase the awareness of the competent authorities on the possibility to check boats and containers in SIS II. They should describe the competence and responsibilities of the law enforcement authorities in this regard and put in place adequate procedures
86. The Commission should explore the added-value of a possible interconnection of the document section of SIS II with SLTD at central level. It should address the technical and the legal difficulties. The Commission should also address the automatic transmission of document alerts into SLTD*
87. The legal instruments should be updated to remove the requirement to log all queries on objects carried out through ANPR systems provided that a comparable solution is provided to trace the legality of queries. At the Member State level, when a hit is achieved using ANPR, a full query in SIS II should be carried out (not least to check which category of alert is involved) and the query and its result logged*

Biometric identifiers

88. There is no provision on checking latent fingerprints against SIS II fingerprint data.. The legal instruments should be updated to explicitly describe the storage and use of fingerprint data in SIS II. This should include the checking and storage of latent fingerprints*
89. The Commission should discuss and agree with the Member States the quality standards for fingerprint files in SIS II. eu-LISA should then implement a ‘checker’ of submitted files at the central level as an early action in the implementation of a central SIS II Automated Fingerprint Identification System (AFIS) in order to detect sub-standard fingerprint files
90. In order to ensure the effectiveness of SIS II at the external borders while checking EU citizens, SIS II should include a functionality to compare the facial image of the

person against the facial images stored in SIS (facial recognition). This would be also compliant with border checks carried out via electronic gates*

Operational procedures

91. The legal instruments should be updated to clarify the term 'use of data for purposes other than the purpose set out in the alert'*
92. Police officers at the national level should be trained to deal with cases of misused identity in alerts for discreet checks
93. The legal instruments and technical specifications should be updated to permit more personal identification information to be included in the misused identity extension of an alert*
94. Member States should implement, for each end-user, internal hit reporting forms on a mandatory basis
95. Member States should reconsider the automatic deletion of supplementary information, especially as the legal base permits longer retention. Alternatively, Member States should reconfigure their SIRENE systems to be able to generate forms on Schengen ID numbers that no longer exist. The Commission and the Member States should discuss whether the retention period should be more that the current one year*
96. The legal instruments should be updated so that all Member States are required to have a back-up technical solution to ensure business continuity of their N.SIS II*
97. The legal instruments should be updated so that all Member States are required to have a back-up technical solution to ensure business continuity of the national SIRENE Bureau*
98. The legal instruments and technical specifications should be updated so as to make it clear that all functionalities of SIS II are implemented in the Member States and available to the appropriate end-users including all the query options which are available in the SIS II Central system*
99. The Commission should continue its work with other interested bodies and agencies in ensuring that end-users, through one query, receive the relevant information from the systems which they have the rights to access. In parallel, the Commission should continue to support the establishment of Single Points of Contact so that the end-users have one point of call to support them regardless of the source of the information upon which they have acted
100. The Commission, the General Secretariat of the Council and the Presidency could represent the SIS II/SIRENE interests, possibilities and good practice at all meetings, where issues linked with SIS II/SIRENE are discussed (e.g. search for persons and objects, executing law enforcement and other checks and controls including border controls at external border, sharing of law enforcement information, sharing the intelligence, law enforcement cooperation, entry ban measures, cooperation in criminal matters, training of law enforcement officer for European tools, cooperation with Interpol)
101. The Commission should present on a permanent basis the successful stories of SIS II/SIRENE use
102. The Commission, the General Secretariat of the Council should make sure that in relevant documents, media releases and publications, SIS II and SIRENE are adequately mentioned and described (e.g. publications on free movement, publications on 25 years' celebration of open borders) including the SIRENE logo
103. The Member States should perform the tasks described in point 139) to 141) at national level and as well in international meetings including the use of SIRENE logo

104. eu-LISA will actively present the SIS II and its key role in international law enforcement (and judicial) cooperation in its documents, media releases, at relevant meetings and on its website (e.g. the SIS II statistics), but also mentioning the human interface — SIRENE
105. The Commission, the General Secretariat of the Council and the Presidency should make sure eu-LISA may take part in all relevant meetings to represent the SIS II
106. The SIRENE logo plays a substantial role in any presentation and awareness-raising. The logo should be kept and exploited to the maximum extent
107. A common training curriculum should be set up at European level for end-users defining minimum standards of SIS II expertise to be incorporated into the national training programs

Person related remark

108. The text of the legal instruments should be amended so that the content of the field 'person related remark' is no longer set in the main legal texts but is decided as an implementing or technical measure in order to reflect operational issues*
109. The number of 'person related' remarks should be extended with a view to protect end-users from the imminent threat posed by the alert subject. It should be also considered to make the person related remark mandatory with the option to indicate 'Not Applicable'*
110. In line with other recommendations on the field 'person related remark' the value 'terrorism related activity' should be an option for insertion by the end-user. Given the wide nature of terrorism there should also be the opportunity to include more than one person related remark in an alert so that if the person is also deemed to be armed or violent, for example, more than one person related remark can be included in an alert*
111. Member States with a high number of flags on their own alerts should start an internal analysis on the reasons of non-recognition of their alerts by other Member States. They should endeavor to eliminate the reasons leading to the non-recognition

Governance

Responsibilities of the Member States

112. The legal instruments should be updated to ensure that all the SIS II information that is intended for the end-user is made directly available to them by the N.SIS II Office which is deemed legally responsible for this task*
113. The legal instruments should be updated to ensure that all queries carried out in the national databases used for border management or law enforcement purposes also include a parallel query in SIS II*
114. In order to ensure the coherence with the national police database and data quality it is highly recommended that when a national entry is created it will be transferred in an automated way to SIS II without requiring a separate alert creation in SIS II. The same applies for the update and the deletion procedures
115. Member States should increase the efficiency of end-users in handling SIS II alerts and the related procedures. This can be achieved by regular end-user training and a clear end-user interface describing the action to be taken and all information available in the alert. It should be considered to provide a consistent minimum standard of end-user training via CEPOL
116. Member States should improve their workflows and case management systems to automate the operations and to reduce the necessity of human intervention

Responsibilities of the Management Authority

117. The Commission should evaluate the data protection implications of removing the requirement to carry out logging at the national level when a parallel log exists at the central level. This should include the legal provisions for a national supervisory authority to call for a central log to carry out its national responsibilities*
118. The legal instruments should be updated so that, with regard to the network, all responsibility for tasks relating to implementation of the budget; acquisition and renewal and contractual matters are handed to eu-LISA*
119. eu-LISA should develop a central monitoring tool for data quality and provide regular reports to the Member States as well as provide a statistical overview to the Commission about the issues encountered and the Member States concerned*
120. The legal instruments should distinguish between public statistical and other reports, such as performance, and reports available upon request*
121. The legal instrument should specifically refer to the Commission's entitlement to have access to the statistical reports of eu-LISA and to request such statistical reports which are available upon request*
122. Given the extensive use of the SIS II by Member States and the considerable success involved, it makes sense to be able to search the database for trends and statistical analysis at a strategic, not personal, level. The legal instruments and technical specifications should be updated in order for this to be possible. The legal instruments should also describe which authority at EU level would have the responsibility for the analysis*
123. The legal instruments should be updated to permit the analysis of trends with regard to hits reported via supplementary information. Although currently problematic, due to the recording of hits at SIRENE Bureau level, this step would be relevant should the exchange of supplementary information be undertaken in another way, for example, via the central SIS II. The legal instruments should also describe which authority would have the responsibility for the analysis*
124. Taking into consideration that the exchange of supplementary information is inseparable from the SIS II alerts and indispensable to ensure the effective action and follow-up of SIS II alerts and hits on the ground, eu-LISA should develop further expertise in SIRENE matters, including testing activities, updating DEBS and providing training to SIRENE staff on the technical use of SIS II. eu-LISA should engage stronger in SIRENE activities and establish a closer relationship with the SIRENE community*

Right to access and retention of alerts

125. The legal instruments should be updated so that the maximum expiry date for alerts on persons and different categories of objects is described in the legal instruments*

Data protection

126. The SIRENE Manual should describe a binding time limit and procedure for deletion/modification of alerts containing unlawfully stored, inaccurate or out of date information. This is to permit SIRENE Bureaux to be able to carry out their coordinating role in data quality verification
127. The wording of the legal instruments should be reviewed so that it reflects the new EU data protection directive and regulation once adopted*

128. The legal instruments should include a mandatory action for Member States to report security incidents affecting SIS II data*

Liability and penalties

129. The rules on alert deletion should be reviewed and included in the legal instruments to ensure that it is clear that when the underlying subject or object of the alert has entered another process, e.g. court procedure on ownership, the alert shall be deleted. Non-compliance should be reported to the Commission for consideration of infringement procedures*

Legal Remedies (including the rights of data subjects to access, correct or delete his personal data and the mutual recognition of judgments)

130. The legal instrument should be updated with a view to requiring the development of a standardised annual statistics package to allow consistent reporting on activities on remedies at the national level, including the activities of the data controller, the supervisory authority and the courts*

ANNEX II - SOURCES

SIS II Legislation

Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (*OJ L 381, 28.12.2006, p. 1)*

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) *(OJ L 381, 28.12.2006, p. 4)*

Commission Decision (2007/170/EC) of 16 March 2007 laying down the network requirements for the Schengen Information System II (1st pillar) *(OJ L 79, 20.3.2007, p. 20)*

Commission Decision (2007/171/EC) of 16 March 2007 laying down the network requirements for the Schengen Information System II (3rd pillar) *(OJ L 79, 20.3.2007, p. 29)*

Council Decision (2007/533/JHA) of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) *(OJ L 205, 7.8.2007, p. 63)*

Commission Decision of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure *(OJ L 112, 5.5.2010, p. 31)*

Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice *(OJ L 286, 1.11.2011, p. 1)*

Commission Implementing Decision 2013/115/EU of 26 February 2013 on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) *(OJ L 71 of 14.3.2013, p. 1)*

Commission Implementing Decision (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) *(OJ L 44, 18.2.2015, p. 75)*

Commission Implementing Decision (EU) 2016/1209 of 12 July 2016 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2016) 4283) *(OJ L 201, 28.07.2016, p.35)*

Commission Implementing Decision (EU) 2015/450 of 16 March 2015 laying down test requirements for Member States integrating into the second generation Schengen Information System (SIS II) or changing substantially their directly related national systems *(OJ L 74, 18.3.2015, p. 31)*

Additional sources

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) *(OJ L 77, 23.3.2016, p. 1)*

Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) *(OJ L 243, 15.9.2009, p. 1)*

Commission Recommendation of 16 December 2015 establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS (C(2015) 9169)

Communication of 4 March 2016 from the Commission to the European Parliament, the European Council and the Council — Back to Schengen — A Roadmap (COM(2016) 120)

DATA EXCHANGE BETWEEN SIRENES (DEBS) — SIS II Version 1.3.2 12 July 2013

Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals *(OJ L 348, 24.12.2008, p. 98-107)*

Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States (2002/584/JHA) *(OJ L 190, 18.7.2002, p. 1)*

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM/2012/010 final)

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM/2012/011 final)

eu-LISA statistical reporting

eu — LISA SIS II Statistics 2013 — June 2014

eu — LISA SIS II Statistics 2014 — October 2015 (revised version)

eu — LISA SIS II Statistics 2015 — March 2016

Studies and Reports

Council document doc 16807/14: A report from the chair of the SIS II Supervision Coordination Group on the exercise of the rights of the data subject in SIS and Guide for exercising the right of access in SIS — 16 December 2014

European Commission, Directorate-General for Migration and Home Affairs — Feasibility study on the use of the Schengen Information System (SIS) for return purposes 2016

European Commission, Directorate-General for Migration and Home Affairs — Independent external evaluation of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice — eu-LISA — March 2016

European Commission, Directorate-General for Migration and Home Affairs — Report ICT Impact Assessment of Possible Improvements to the SIS II Architecture 20 April 2016

European Commission, Directorate-General for Migration and Home Affairs — Report on the technical functioning of Central SIS II and the Communication Infrastructure, including the security thereof and the bilateral and multilateral exchange of supplementary information between Member States by European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) (2015-094 REV 1)

European Commission, Directorate-General for Migration and Home Affairs — SIS II technical assessment — 18 January 2016

European Commission, Directorate-General for Migration and Home Affairs — Study on the implementation of European Information Exchange Model for strengthening law enforcement (EIXM) cooperation

European Commission, Directorate-General for Migration and Home Affairs — Summary of European Migration Network (EMN) ad-hoc queries No 2015.662 on entry bans entered into the SIS and consultation procedures in Member States, and No 2014.628 on registering entry bans in the SIS — March 2015

JRC Science for Policy Report — Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II) — 2015 (EUR 27 473 EN) ISBN 978-92-79-51929-1

Report on Inspection Pursuant to Article 47 (2) of Regulation (EC) Number 45/2001 Schengen Information System II (SIS II) managed by EU Agency for large—scale IT systems (eu-LISA). EDPS case reference 2014 - 0953

Study on Departure from the Schengen Agreement — Macroeconomic impacts on Germany and the countries of the European Union by Global Economic Dynamics 2016

eu-LISA`s input for SIS II overall evaluation — February 2016

Schengen Evaluation Reports

Schengen SIS/SIRENE Evaluation Report of Slovenia (document 16704/13 (SCH-EVAL 134, SIRIS 97, COMIX 627) of 22 November 2013)

Schengen SIS/SIRENE Evaluation Report of Malta (document 16705/13 (SCH-EVAL 135, SIRIS 98, COMIX 628) of 02 December 2013)

Schengen SIS/SIRENE Evaluation Report of Slovakia (document 17101/13 (SCH-EVAL 142, SIRIS 100, COMIX 653) of 02 December 2013

Schengen SIS/SIRENE Evaluation Report of the Czech Republic (document 17100/13 (SCH-EVAL 141, SIRIS 99, COMIX 652) of 02 December 2013

Schengen SIS/SIRENE Evaluation Report of Hungary (document 7599/14 (SCH-EVAL 28, SIRIS 19, COMIX 157) of 11 March 2014)

Schengen SIS/SIRENE Evaluation Report of Poland (document 9369/1/14 (SCH-EVAL 50, SIRIS 33, COMIX 238) of 12 September 2014)

Schengen SIS/SIRENE Evaluation Report of Estonia (document 7229/14 (SCH-EVAL 25, SIRIS 13, COMIX 130) of 04 March 2014

Schengen SIS/SIRENE Evaluation Report of Latvia (document 7586/14 (SCH-EVAL 26, SIRIS 17, COMIX 154) of 11 March 2014)

Schengen SIS/SIRENE Evaluation Report of Lithuania (document 7587/14 (SCH-EVAL 27, SIRIS 18, COMIX 155) of 11 March 2014)

Schengen SIS/SIRENE Evaluation Report of Switzerland (document 12691/14 (SCH-EVAL 82, SIRIS 49, COMIX 424) of 11 September 2014)

Schengen SIS/SIRENE Evaluation Report of the United Kingdom (document 11780/15 (SCH-EVAL 20, SIRIS 57, COMIX 381) of 19 November 2015)

Commission Implementing Decision of 22 September 2015 establishing the report of the 2015 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by Austria (COM(2015)6300)

Commission Implementing Decision of 22 December 2015 establishing the report of the 2015 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by Belgium (COM(2015)9000)

Commission Implementing Decision of 01 February 2016 establishing the report of the 2015 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by Germany (COM(2016)24)

Commission Implementing Decision of 11 April 2016 establishing the report of the 2015 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by the Netherlands (COM(2016)5101)

Draft Schengen Evaluation Report of the 2015 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by Liechtenstein

Draft Schengen Evaluation Report of the 2016 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by Luxembourg

Draft Schengen Evaluation Report of the 2016 evaluation of implementation of the Schengen *acquis* in the field of the Schengen Information System by Italy

ANNEX III - MEETINGS

Meetings of the SISVIS Committee

2013

14 February

29 May

5 July

5 September

30 October

10 December

2014

4 February

28 March

15 May

15 July

9 September

3 November

16 December

2015

6 February

24 March

19 May

9 July

8 September

20 October

14-15 December

2016

3-4-5 February

17 March

10-11 May

30 June

15 September

Meetings of the Commission Inter-service Steering Group

17 April 2015

6 July 2015

6 November 2015

14 March 2016

ANNEX IV - DETAILED STATISTICS ON COMPLAINTS AND REMEDIES

In this sphere there is variation in the amount of statistics available.

- In Finland, during 2013 and 2014 no SIS remedy cases were submitted to the DPA.
- In Belgium the DPA received 26 access requests to the SIS II in 2013 and 22 in 2014. There was one deletion of a registration in 2013 and 2 deletions in 2014. The Privacy Commission has no data at its disposal related to the courts decisions.
- In France the DPA received 260 access requests to SIS in 2013 and 262 in 2014. In 2014, 310 individual checks on records were led by the "Commission nationale de l'informatique et des libertés" with the following outcomes:
  Person unknown (no alert in SIS) or "became unknown" (alert deleted during the process) – 212 (SIS alerts on 22 people, from France or another state, were deleted during the subject access procedure).
  Person known (SIS alert) – 98 (64 FR alerts, 34 alerts from other states).
- In Malta no applicants had recourse to the Court as the data controller and DPA handled all requests.
- In Slovenia the police received 88 access requests in 2013 and 89 in 2014. During this time the DPA received no complaints.
- In the Czech Republic the DPA received 9 access requests in 2013 and 10 in 2014. According to information available none of these requests resulted in Court action. The Supreme Administrative Court has heard one case where the applicant had not exhausted the remedies available to him, such as applying to the DPA. The Court ruled that it would not hear such a case as the applicant had not attempted to resolve the issue through the available mechanisms. The DPA has no information about compensation awarded by the Courts or other rulings mainly due to the low number of cases and complaints received.
- Similarly, Estonia reported that no court cases had taken place.
- In Denmark the DPA received 21 access requests to SIS in 2013. Most of the cases were forwarded to the data controller, the national police. Following appropriate action by the police no further action was necessary or requested. The police directly received 21 access requests and 10 cases regarding deletion.
  In 2014 the Danish DPA received 7 access requests. Most of the cases were forwarded to the data controller, the national police. Following appropriate action by the police no further action was necessary or requested. The police directly received 10 access requests and 5 cases regarding deletion.
- During 2013 and 2014 the Polish DPA did not directly receive any remedies or appeals concerning SIS.
- Lithuania reported that there were no statistics in this area.
- Hungary reported that in 2014 the SIRENE Bureau received 320 access requests and the DPA 10. At the date of receipt of the Hungarian response (September 2015) the SIRENE Bureau in 2015 had received 150 access requests and the DPA 10.
- Sweden reported that there are no available statistics from the Courts on access, correction, deletion or compensation. The DPA estimated that it receives less than 10 cases per year. In 2013 the police received 63 access requests. In one case information was corrected and in 4 cases it was deleted. In 2014 the police received 52 access requests. In one case information was corrected and 14 cases information was deleted.
- Latvia reported that its data inspectorate receives, on average, ten complaints per year. The majority of the complaints are forwarded to the SIRENE Bureau. Due to the

actions carried out by the Bureau there have been no decisions taken regarding appeal as the Bureau has ensured the rights of the data subject. There is no information available on cases taken to Court for compensation.

- Iceland reported no cases in either 2013 or 2014.
- The UK DPA does not hold information on cases taken to Court.
- Switzerland reported that there has only been one appeal against the Federal Police for refusing to disclose information. This took place in 2009 with the Court ruling in favour of the Police. In 2013 information was refused twice and no appeal was made. Switzerland is able to provide comprehensive statistics on access requests.