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

July 2017

This report has been produced pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Council Decision 2007/533/JHA with the purpose of providing information on Central SIS II and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.

eulisa.europa.eu

ISBN 978-92-95208-58-2
ISSN 2443-8294
doi:10.2857/039227
Catalogue number: EL-AE-17-001-EN-N

Table of contents

Summary

SIS II plays a crucial role in facilitating the free movement of people within the Schengen area, and ensuring a high level of security supporting border controls at the external Schengen borders as well as law enforcement and judicial cooperation throughout Europe.

During the reporting period[1], the SIS II Central System was functioning in a stable manner in compliance with the agreed response time. The system was highly available, registering only a few incidents not preventing the normal use of the system. Similarly to what was reported in the previous report, in 2015 and 2016 SIS II remained the main and most powerful platform for cooperation and information exchange in the EU, heavily utilised by the Member States as a result of increased terrorist threats in Europe and growing information exchange between law enforcement agencies. On 31 December 2016, there were over 70 million alerts[2] stored in the system, showing a net increase of 51% in alerts stored since the entry into operation of the system in April 2013. In 2016, SIS II was searched almost 4 billion times, a billion more than in 2015.

Taking into account the observed increase in SIS II usage as well as the recent and upcoming changes which will lead to additional searches, the decision was taken to increase the capacity of the SIS II database as well as to extend the querying capacity of Central SIS II (CS-SIS) to avoid degradation of the service. The database capacity upgrade to 100 million alerts was put into production in the last quarter of 2016. By April 2017, the Agency had implemented a short-term solution by upgrading the infrastructure in order to increase the querying capacity. In the long term, further upgrades will be implemented based on future capacity needs.

In 2016, the implementation of a project on the biometric matching capabilities for SIS II Automated Fingerprint Identification System (AFIS) was initiated. The deployment of the first phase at Central level of this new functionality, which will allow a person to be identified based on fingerprints stored in SIS II, is planned for February 2018. During the reporting period, different studies were carried out in order to identify the best technology for a future Central System simulator, further improve the availability of the system and prepare for the implementation of state-of-the-art user access management architectures. In February 2015, the European Data Protection Supervisor (EDPS) carried out an inspection of Central SIS II and no critical findings were reported.

In a continuous process to further improve the usability and effectiveness of SIS II, eu-LISA in cooperation with the Member States has defined requirements and reports to support data quality efforts. As of summer 2016, a first set of reports on data quality was made available. By the end of 2016, the second phase of the project was launched, with an emphasis on alerts on persons. As from May 2017, an exhaustive set of monthly reports is now available to Member States. In addition, statistical reports to support Member States in the data amnesty[3] activity were provided as from August 2015.

Integration projects to connect the UK and Croatia to SIS II, necessitating an upgrade of the SIS II Central system, were successfully carried out during the reporting period, thus increasing the number of countries using the system to 30. The UK started entering alerts into the system and consulting it on 13 April 2015, and from 27 June 2017 Croatia has been able to enter alerts and perform searches against SIS II.

In line with the increased usage of the system already reported, the exchange of supplementary information

[1] From 1 January 2015 to 31 December 2016.
[2] 'Alert' means a set of data entered in SIS II allowing the competent authorities to identify a person or an object with a view to taking specific action (http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533).
[3] Data amnesty refers to data migrated from SIS 1+ to SIS II that still required intervention in order to satisfy SIS II legal requirements.

between Member States also grew. In 2016, Member States reported 200,778 hits on foreign alerts for 2016, which represents an increase of almost 30% compared with data reported for 2015.

On 21 December 2016, following its overall evaluation[4] of SIS II carried out in early 2016, the Commission presented three legislative proposals[5] aimed at strengthening the operational effectiveness and efficiency of SIS II. The triple structure of the SIS reform package reflects the different patterns of participation of the Member States in the Schengen *acquis* insofar as the different fields of border checks, police and judicial cooperation and return are concerned. The proposed improvements will further enhance the ability of the system to fight terrorism and cross-border crime, improve border and migration management and ensure effective information exchange between Member States to increase the security of European citizens.

[4] COM(2016) 880 final, 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.

[5] Proposal in the field of police cooperation and judicial cooperation in criminal matters *COM(2016) 883 final*; Proposal in the field of border checks *COM(2016) 882 final*; Proposal in the field of return of illegally staying third country nationals *COM(2016) 881 final*.

1. Introduction

The Schengen Information System (SIS) entered into operation in 1995, initially in six Member States, as the main measure to compensate for lifting the internal border checks in the Schengen area. Several upgrades of the system were implemented through the years, allowing the integration of new countries as well as enhancing technical performance. In particular, on 9 April 2013, the new generation of SIS II was brought into operation as per the implementation of Regulation (EC) No 1987/2006[6] of the European Parliament and of the Council on the establishment, operation and use of SIS II (hereafter referred to as the 'SIS II Regulation') and Council Decision 2007/533/JHA[7] on the establishment, operation and use of the second-generation SIS II (hereafter referred to as the 'SIS II Decision').

SIS II was developed under the supervision of the Commission in cooperation with the Member States. In 8 May 2013, at the end of an intensive one-month monitoring period following the entry into operation of SIS II, eu-LISA took over the 24/7 operational management of SIS II, as defined in Chapter III of the SIS II Regulation and the parallel provision of the SIS II Decision.

At the time of writing, SIS II was used by 30 Member States[8] as well as consulted by Europol[9] and Eurojust[10]. The UK began entering alerts into the system and consulting it on 13 April 2015, as established by Council Implementing Decision (EU) 2015/215[11]. Croatia's integration process was also successfully completed and, as from 27 June 2017, Croatia has been able to enter alerts and perform searches into SIS II as planned in Council Decision (EU) 2017/733[12]. The integration process with Ireland to connect to SIS II is currently ongoing.

SIS II plays a crucial role in facilitating the free movement of people within the Schengen area and ensuring a high level of security supporting border controls at the external Schengen borders as well as law enforcement and judicial cooperation throughout Europe. The system enables competent authorities to enter and consult data[13] on wanted persons, persons who may not have the right to enter or stay in the EU, missing persons – in particular, children – and objects that may have been stolen, misappropriated or lost.

The increase in the usage of SIS II is clearly visible in the statistics published annually by eu-LISA. On 31 December 2016, there were over 70 million[14] alerts stored in the system, showing a net increase of over 7 million (12%) compared with 31 December 2015. Since the second generation of the system was brought into operation on 9 April 2013 – when there were almost 47 million alerts stored in the database – there was a net increase of 51% in alerts stored.

As per the data reported by Member States, in 2016 SIS II was searched almost four billion[15] times, a billion more than in 2015 – an increase of 39% – when the number of reported queries was 2.8 billion. Searches performed in

[6] OJ L 381, 28.12.2006.
[7] OJ L 205, 7.8.2007.
[8] By the term 'Member States' the current document refers to the Member States of the EU and Associated Countries which are bound under Union law by the legislative instruments governing SIS II, if not further explained. Member States of the EU currently connected to SIS II are Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. Associated Countries connected to SIS II are Iceland, Liechtenstein, Norway and Switzerland.
[9] Article 41 SIS II Decision.
[10] Article 42 SIS II Decision.
[11] OJ L 36, 12.2.2015.
[12] OJ L 108, 26.4.2017.
[13] A data set in SIS II is referred to as an alert allowing competent authorities to identify and/or locate a person or an object with a view to taking specific action.
[14] For more information, see *SIS II – 2016 statistics* (http://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%20Statistics%202016.pdf).
[15] Total queries reported by Member States were 3,959,957,304.

2016 increased by 81% compared with in 2014, the first year with full reporting available. Along with the increase in searches, there was also an increase in the number of reported hits[16] on foreign alerts. In 2016 200,778 hits were reported, showing an increase of 30% compared with hits reported for 2015.

Access to SIS II data is limited to national border control, police, customs, judicial, immigration and visa-issuing authorities and vehicle registration services[17]. Every year, eu-LISA publishes an updated list of the Member States' competent authorities, specifying, for each authority, what data it may search and for what purposes, together with an updated list of N.SIS II Offices and the national SIRENE Bureaux. Pursuant to Article 31(8) of the SIS II Regulation and Article 46(8) of the SIS II Decision, the updated lists are published in the Official Journal[18] of the EU.

1.1 Legal basis and scope of the report

Pursuant to Article 50(4) of the SIS II Regulation and Article 66(4) of the SIS II Decision, two years after SIS II is brought into operation and every two years thereafter the Management Authority (eu-LISA) shall submit to the European Parliament and the Council of the EU a 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.

The report, the second one since SIS II was brought into operation, covers the period from 1 January 2015 until 31 December 2016. The report was drafted with information available at central level (operational activities, availability and performance, change management, releases, test activities, etc.) together with statistical data provided by the Member States in the framework of the annual statistics exercise.

This report, in conjunction with the other SIS II reporting obligations[19], aims to enhance both transparency and visibility, as per the goal sought by the SIS II legislator.

1.2 Legal and policy developments

On 21 December 2016, following its overall evaluation[20] of SIS II carried out in early 2016, the Commission presented three legislative proposals[21] aimed at strengthening the operational effectiveness and efficiency of SIS II. The triple structure of the SIS reform package reflects the different patterns of participation of the Member States in the Schengen *acquis* insofar as the different fields of border checks, police and judicial cooperation and return are concerned. The proposed improvements will further enhance the ability of the system to fight terrorism and cross-border crime, improve border and migration management and ensure effective information exchange between Member States to increase the security of European citizens.

[16] SIS II is a hit/no-hit system based on searches. A 'hit' in SIS II means that the person or object has been located in a Member State and thus further actions are required.

[17] As per Regulation (EC) No 1986/2006 regarding access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates, OJ L 381, 28.12.2006.

[18] OJ C 228, 14.07.2017.

[19] The SIS II annual statistics are regularly published on eu-LISA's website (http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx). The annual updated lists of competent authorities authorised to access and search the data contained in SIS II and the annual updated N.SIS II Offices and SIRENE Bureaux are published in the Official Journal of the EU.

[20] COM(2016) 880 final, 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.

[21] Proposal in the field of police cooperation and judicial cooperation in criminal matters *COM(2016) 883 final*; Proposal in the field of border checks *COM(2016) 882 final*; Proposal in the field of return of illegally staying third country nationals *COM(2016) 881 final*.

Throughout the reporting period considered here, eu-LISA actively participated in a number of fora and workshops to support the Commission in carrying out the overall evaluation of SIS II as well as in providing input on technical aspects of possible changes and new requirements. In particular, the Agency contributed to legal negotiations with technical expertise and supported the execution of impact assessments.

The new proposals provide for implementation of some of the improvements set out in the Commission's Communication of 6 April 2016 on *Stronger and Smarter Information Systems for Borders and Security*[22], which highlights the need for the EU to strengthen and improve its IT systems, data architecture and information exchange in the areas of law enforcement, counter-terrorism and border management. The appropriate means to implement the identified necessary improvements were elaborated by the High Level Expert Group (HLEG) on Information Systems and Interoperability established by the Communication.

The Agency played a very active role within the HLEG from its first meeting in June 2016, providing concrete and positive input and supporting discussions with appropriate expertise, data and information to ensure evidence-based decision making. Concrete suggestions were made regarding improvement of data quality in SIS II in non-papers submitted and in presentations provided during discussions on this topic. The Agency presented a comprehensive Action Plan on Data Quality, which was approved by the DAPIX Working Party[23] on 1 December 2016 in the context of the fifth Action List of the revised Information Management Strategy. The Action Plan forms the basis for actions on improving data quality in the HLEG's final report[24]. Implementation of interoperability of SIS II with other large-scale IT systems – for example, through its interfacing with a European Search Portal – was also discussed in depth. The Agency continues the follow-up work with the Commission and other stakeholders with a view to its implementation.

On 7 April 2017, Regulation (EU) 2017/458[25] on the reinforcement of checks against relevant databases at external borders entered into force. The new legal provision requires Member States to carry out systematic checks against relevant databases on all persons, including those enjoying the right of free movement under EU law, when they cross the external borders (at entry and at exit). SIS II is one of the databases in which systematic checks began to be carried out. The obligation, which applies to all external borders (air, sea and land borders), has already led to a significant increase in the usage of SIS II.

1.3 Governance

Several stakeholders – the Commission, the Member States and eu-LISA – have responsibilities when it comes to SIS II governance. The Commission holds responsibility for any legislative initiatives linked to the system as well as the correct application and implementation of the SIS II legal framework. The Commission chairs the SISVIS Committee[26], which regularly brings together representatives of the Member States with the aim of harmonising operational procedures, supporting the effective application of the rules and the optimised use of SIS II. eu-LISA is always invited to participate in the SISVIS Committee and provide updates in relation to the operational management of the system as well as report on a number of topics (e.g. major development projects, critical changes, training strategies and planning, annual statistics, etc.).

eu-LISA is responsible for the operational management of SIS II and it is supported in carrying out this task by the administrative and management structure as laid down in Article 11 of the Agency's establishing

[22] COM(2016) 205 final.
[23] Working Party on Information Exchange and Data Protection.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
[25] OJ L 74, 18.3.2017.
[26] As per Article 51 of the SIS II Regulation and Article 67 of the SIS II Decision.

Regulation[27], namely the Management Board and the SIS II Advisory Group. The SIS II Advisory Group met systematically during the reporting period[28], providing technical expertise to the Management Board of the Agency, in particular in the context of the preparation of the Annual Work Programme and the Annual Activity Report.

The SIS II Advisory Group is composed of a representative of the Commission and a representative of each Member State, with appointed observers from Europol and Eurojust being present. The group represents the regular forum where Member States and the Agency together with the Commission agree on changes to be endorsed before implementation in SIS II, report on availability of the Central System and of the national ones, approve release plans, discuss and plan developments, assess training plans, present annual statistics, etc. In addition, Member States have, along the reporting period, constantly supported the work of the Agency in a number of *ad hoc* fora and workshops, in particular to improve the Data Consistency Checks, further customise statistical reports and gather requirements for further developing data quality reports.

Member States are also participating in a number of regular fora – specific to SIS II or across all systems – such as the AFIS Project Management Forum (PMF), the Security Officers Network (SON), the National Contact Points for training (NCP) and the Change Management Group (CMG).

The SIS II Advisory Group, together with the VIS (Visa Information System) and Eurodac (European Asylum Dactyloscopy database) Advisory Groups, is also engaged in the Agency's annual operational planning. In particular, the group discusses and provides input to the Agency's Single Programming Document and is requested to give an opinion on the Agency's Annual Activity Report. The groups are involved in the planning cycles at an early stage, allowing time for discussions, consolidation and prioritisation of input.

2. Operational management of Central SIS II

eu-LISA is responsible for the operational management of Central SIS II, ensuring uninterrupted access to the system 24/7 and allowing the continuous exchange of data between national authorities, in accordance with the legal provisions. The operational management is achieved, to a large extent, through application management services, supervision, and implementation of appropriate corrective, adaptive and evolutionary maintenance.

External technical support has been guaranteed during the reporting period by the contractor as per the SIS II Maintenance in Working Order (MWO) Framework Contract signed on 13 March 2014[29], which entered into force on 1 April 2014. In 2015 and 2016, the majority of the work packages were active, including:

- corrective maintenance, consisting of reacting to the anomalies noticed during the operation of SIS II, by implementing their correction and/or temporary bypassing measures;
- adaptive maintenance, consisting of updating the configuration of the hardware equipment and the software products of SIS II;
- evolutionary maintenance, ensuring the appropriate alignment of the Central System with Member States' utilisation and business needs by upgrading the CS-SIS in order for the system to continue to perform and operate as expected; these developments include, since the summer of 2016, the implementation of the state-of-the-art biometric functionality AFIS;

[27] Regulation (EU) No 1077/2011, OJ L286, 1.11.2011.
[28] Meetings were held in Tallinn in February, June, October and December 2015; in February, June, October and December 2016.
[29] Operated by Atos, Accenture and HP.

- training, technical assistance and support to Member States.

In the framework of the MWO, eu-LISA holds the responsibility for the operational management of Central SIS II and it is directly accountable for the performance of the system with the support of the contractor.

The current MWO Framework Contract will expire in March 2018, so eu-LISA has already started working on the new contract. The first phase of the restricted procurement procedure was launched in February 2017[30].

On 29 February 2016, the Commission presented a report to the European Parliament and the Council on the availability and readiness of technology to identify a person based on fingerprints held in SIS II[31]. The current legal basis, in particular Article 22(c) of the SIS II Decision and Article 22(c) of the SIS II Regulation, provides the legal grounds for developing an AFIS for SIS II when technically possible, and also provides for the possibility to search fingerprints to identify a person. The new SIS II legislative proposal in the field of police and judicial cooperation in criminal matters[32] makes this search mandatory if the identity of the person cannot be ascertained in any other way.

The report presented by the Commission was supported by a study conducted by the Commission's Joint Research Centre (JRC) confirming that the fingerprint identification technology is available and ready for its integration into SIS II.

With the completion of the study and the submission of the abovementioned report to the European Parliament for consultation, the first steps towards the implementation of an AFIS functionality in the SIS environment were taken. This major upgrade of the system was launched[33] in 2016 with the signing of a Specific Contract related to AFIS, due to be implemented mainly in 2017 and put into operation in early 2018.

Being responsible for the operational management of Central SIS II, the Agency is building up relevant technical expertise and has become a recognised player, in particular in supporting the Commission and the Member States in the context of the Schengen Evaluation Mechanism[34].

2.1 Technical infrastructure of Central SIS II

Article 4 of the SIS II Decision and Regulation defines the technical architecture of SIS II, which includes (a) a central system (Central SIS II); (b) a national system (N.SIS II) in each of the Member States; and (c) a communication infrastructure between CS-SIS and NI-SIS (the Communication Infrastructure).

Central SIS II is composed of the SIS II database – where alerts on persons and objects are stored – and a uniform national interface (NI-SIS) consisting of an access point to the network and the uniform definition of the interaction between the N.SIS II and the CS-SIS, described in the Interface Control Document (ICD)[35].

Practically speaking, Central SIS II communicates with national systems (N.SIS II) through the secure Communication Infrastructure, used to provide online services such as searches and creation/update/deletion (CUD) of alerts. Alerts are managed, created, modified and deleted by Member States. CUD operations of alerts are sent by the N.SIS II to Central SIS II, which, after technical checks, within three minutes broadcasts the alerts

[30] More information available at http://ted.europa.eu/udl?uri=TED:NOTICE:60835-2017:TEXT:EN:HTML.
[31] COM(2016) 93 final.
[32] Proposal in the field of police cooperation and judicial cooperation in criminal matters *COM(2016) 883 final*.
[33] In order to implement this project in a timely manner, a number of SIS II activities planned for 2016 were postponed to 2017 in agreement with the Member States.
[34] In line with Regulation (EU) No 1053/2013, the Commission has invited eu-LISA to participate as an observer in SIS/SIRENE evaluations as from 2015. During the reporting period, eu-LISA experts supported ten evaluation missions (5 in 2015 and 5 in 2016).
[35] The ICD provides Member States with the technical specifications needed to implement the XML schemas used to interact with the CS-SIS. National Interfaces need to be compliant with the ICD specifications to ensure dialogue between CS and NS. The NS's compliance with ICD is tested before a Member State can connect to the CS-SIS.

to all N.SIS II with a national copy or sends a notification to countries without a national copy.

As indicated in Article 4(1)(b) of the SIS II legal basis, Member States may have a national copy containing a complete or partial copy of the SIS II database. Twenty-five Member States own a national copy, whereas Denmark, Finland, Liechtenstein, Norway and Slovenia do not have a national copy, so they query only Central SIS II. Pursuant to Article 9(2) of the SIS II legal basis, if a Member State uses a national copy, it shall ensure, by means of the services provided by CS-SIS, that data stored in the national copy are, by means of automatic updates, identical to and consistent with the SIS II database. This technical compliance is requested to make sure that a search in a national copy produces a result equivalent to that of a search in the Central SIS II database. CS-SIS regularly performs Data Consistency Checks to assure just this.

In 2016, a study was successfully conducted with the aim of replacing the outdated Central System simulator. The new Central System simulator will be used by the Member States for testing and training purposes at their premises. Following a workshop for gathering Member States' requirements in April 2016, and a webinar in December, the project was initiated at the beginning of 2017. The new simulator will provide almost all functionalities of the Central System, and it will be delivered in two phases as agreed with the Member States. The first delivery, planned for the end of 2017, will provide the main requirements, and the final delivery is currently planned for early 2018.

In order to ensure effective backup of all functionalities of the main CS-SIS in the event of failure of the system and full redundancy, as laid down in Article 4(3) of both SIS II legal instruments, the CS-SIS has two data centres. The CS-SIS central unit (CU) is located in Strasbourg (France), whereas the CS-SIS backup CU (BCU) is located in Sankt Johann im Pongau (Austria). In the event of failure of the CU, the BCU will be able to take over all the necessary services required for continuity of operations. This implies that the data contained in the CU and BCU remain synchronised at all times.

During the reporting period, a study on SIS II development to an active-active set-up was commissioned. The aim of the study was to investigate how the system could benefit from a database active-active technology, to provide better system resilience while optimising data centres' resource utilisation. More specifically, the study looked at whether the system could evolve towards a set-up where the stand-by system also handled requests that did not alter the live business data[36] (e.g. queries, scheduled jobs and any other operations that could benefit from this set-up). In addition, the study assessed what the impact of a similar change would be at multiple levels, including the switchover/failover time.

Being able to simultaneously use an additional copy of the SIS II database in active operations is also considered in the new legal proposals for the reinforcement of SIS II presented by the Commission in December 2016[37].

Some time will be needed before a conclusion can be reached, but this may be that a larger view is needed for integrating the active-active mode into the broader context of the Agency's horizontal strategy[38]. Meanwhile, the Agency will aim to deliver an impact assessment on the active-active mode of operations in 2017.

2.2 Monitoring and operational activities

Central SIS II monitoring is carried out at the operational centre in Strasbourg:

- A 24/7 monitoring regime by the eu-LISA Service Desk is active and enables event-triggered incident

[36] The scenario considered in the study assumed that offloading CUD operations would continue to be run only at the CU site.
[37] Article 4(3) of the proposals in the field of border checks as well as in the field of police and judicial cooperation.
[38] This will require not only a revision of the Agency's establishing Regulation, but also allocation of additional financial and human resources for the technical implementation.

management. This monitoring system is continuously analysed and assessed for business impact.

- The business activity is represented by a status overview screen giving the actual status of the queues for each Member State and agency connected to SIS II.
- The operational status of the exchange between Central SIS II and the national copies (the bridge) is continuously monitored. Any system unavailability is reported and escalated on a 24/7 basis.

The eu-LISA Service Desk is the single point of contact where users can report incidents[39] or request a service. Any request or incident is registered in a central incident management tool[40] for follow-up. Based on the initial analysis – impact, urgency and priority are defined[41] – the relevant assistance is provided and functional and/or managerial escalation is triggered. During the reporting period, 1,257 interactions[42] were created for SIS II in the incident management tool. For comparison, during the previous reporting period the eu-LISA Service Desk recorded 1,352 user requests (including incidents, requests for information, etc.) related to SIS II[43]. Both in 2015 and in 2016, the critical interactions represented 4% of the total interactions. eu-LISA has defined and implemented an IT Service Management (ITSM) process following extended best practices[44] to assure quality of service. This is a continuous exercise to ensure efficient and cost-effective management of SIS II by continuously monitoring and developing operational processes.

Central SIS II provides functionalities for ensuring synchronisation and consistency of national copies, via the Data Consistency Checks[45] (DCCs), as well as their restoration, should this be necessary. Thanks to the regular monthly DCC campaigns, each month all national copies are checked at least once. Checks are performed on all alerts and links, and any discrepancies found are automatically repaired by the mechanism itself. Compared with the previous reporting period, significant improvements in reaching zero discrepancies, in particular for alerts, were visible. It should be emphasised that the majority of monthly DCC campaigns resulted in zero discrepancies for alerts. Furthermore, continuous efforts to reach zero discrepancies as far as links are concerned are undertaken by both Member States and eu-LISA.

In addition to the regular DCC campaigns, a DCC can be requested by a Member State or by eu-LISA in cases of need (e.g., in the event of failures of the synchronisation process, DCC is launched after disconnections due to maintenance or incidents).

During the reporting period, a total of 873 DCCs were launched[46]. This is one of the regular topics discussed at the SIS II Advisory Group. In addition, dedicated workshops[47] have been organised for sharing best practices and improving the mechanism's implementation and execution time.

In the spring of 2015, following the works performed in the second half of 2014 a revised version of the SIS II Operator Manual (OPM) entered into force after adoption by the SIS II Advisory Group. In 2016, a revision was needed, and on 15 November 2016 the new version was rolled out. The major novelty in the revised OPM was the introduction of the so-called 'political escalation'. An additional step was introduced in the already existing

[39] An incident is opened by the service desk following an exchange/interaction with Member States or following eu-LISA monitoring activities (abnormal observations).

[40] In March 2016, the Agency's Service Desk upgraded the incident management tool in use from SM7 to SM9. Member States performed several test campaigns (connectivity tests started in December 2015 and functional tests in January 2016) with dedicated training activities organised as well.

[41] All along the process, eu-LISA's technical staff reviews the status and reassesses the severity of the incident.

[42] 585 in 2015 and 672 in 2016.

[43] http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx#k=#s=21.

[44] The Agency follows the Information Technology Infrastructure Library (ITIL version 3) best practices.

[45] Data Consistency Check is an exercise run to support Member States to achieve technical compliance as requested by Article 9(2) of the SIS II Decision and the parallel provision in Article 9(2) of the SIS II Regulation.

[46] 439 in 2015 and 434 in 2016. During the previous reporting period and since the entry into operations of the SIS II on 9 April 2013, over 500 DCCs were performed successfully (http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx#k=#s=21).

[47] In April 2016 and in February 2017.

escalation procedure, to address the possibility of having to reach the political level in the event of an incident at central or national level lasting more than eight hours.

Once a year, the Agency carries out a customer satisfaction survey covering the performance of the eu-LISA Service Desk, incidents and problem management, operational communication and technical assistance, as well as support to national activities. The participation of the SIS II community was very high in both years (86% of SIS II Member States participated in 2015 and 90% in 2016). In addition, the overall satisfaction rate of the community increased in 2016 (96% were satisfied or very satisfied) compared with 2015 (92%). Every year, the results of the survey are analysed and the lessons learned are regularly applied.

2.3 Performance and availability

Central SIS II was designed and optimised for a specific usage, which includes search distribution, traffic rate, maximum load and volume. Those indicators should be taken into account when measuring performance and availability[48] indicators for the system.

In order to have up-to-date estimations from Member States in terms of usage of the system, and thus for planning timely upgrades of the system, regular volumetric exercises for capacity planning in terms of queries, binaries and alerts were carried out in 2015 and in 2016 using questionnaires.

As per its design, the SIS II database had a size of 70 million alerts. Because of the permanent and stable increase in the amount of data stored[49] – on 31 December 2015 there were over 63.4 million alerts stored in the system, showing a net increase of over 7.5 million (13%) compared with 31 December 2014 – a storage capacity upgrade was deemed necessary. The project for the database capacity upgrade to 100 million alerts was initiated in the fourth quarter of 2015[50]. All necessary activities were performed during 2016 and, after the successful final test phase, the 100 million alerts upgrade of the Central System database was put into production in the last quarter of 2016. By the end of the reporting period, on 31 December 2016, the system contained over 70.8 million alerts, which represents 7.3 million alerts more than on 31 December 2015.

In 2015, over 20.7 million create/update/delete (CUD) transactions[51] were performed, 19% more than in 2014. In 2016, the CUD operations performed were over 23.5 million, an increase of 14% compared with the previous year. During the reporting period, the majority of the transactions – 95.5% in 2015 and 95.7% in 2016 – were performed in less than 3 minutes, in line with the design requirements of the system.

Central SIS II was designed to handle up to 250 million standard queries per year. Since its entry into operation until the end of 2016, a maximum of around one million queries were handled daily by the Central System without problems. In the spring of 2016, an analysis confirmed that there was a change in the search distribution, and the observed usage no longer reflected the distribution of queries among the Member States as per the designing and testing phases[52].

[48] The system's availability is defined in Section 7 ('Availability') of Commission Decision of 16 March 2007 laying down the network requirements for the Schengen Information System II (1st pillar) (notified under document number C(2007) 845) (2007/170/EC): 'The CS-SIS and the LNI and BLNI must be able to deliver an availability of 99,99 % over a 28-day rolling period excluding the network availability. The availability of the Communication Infrastructure must be 99,99 %.' In order to measure the CS-SIS availability and response time, two Key Performance Indicators were adopted by the Agency's Management Board in March 2017.

[49] Annex, I. Graph: total amount of alerts stored in the SIS II central database since 9 April 2013.

[50] Note that, in parallel with the capacity upgrade of the Central System database, alignment was also required from the Member States. Thus an increase of the databases of all national copies was needed, requiring national budget and infrastructure planning.

[51] Annex, II. Table: response time for CUD operations processed during the reporting period.

[52] Figures at design phase were 99.5% exact searches (SLA1 queries) and 0.5% fuzzy and partial searches (SLA2 queries). On the other hand, usage as per March 2016 showed a significant increase in the complex queries, which are much more costly in terms of database resources (55% exact searches/SLA1 queries and 43% fuzzy and partial searches/SLA2 queries).

Taking into account the analysis, as well as the recent and upcoming changes[53], it was decided to extend the query capacity to avoid degradation of the service. In 2016, a study investigated the possibility of extending the query capacity of Central SIS II up to eight times its initial load. The study concluded that the current architecture and design are not able to dynamically adapt to the changing load profiles and to scale up to meet the higher demand for complex queries. The solution envisaged was to replace the current search engine with a new one. Considering all currently ongoing SIS II projects[54], the project for the replacement of the search engine is planned to start implementation at the end of 2018. Meanwhile, by April 2017, the Agency had implemented a short-term action upgrading the infrastructure[55]. Thanks to this enhancement, the system will be able to sustain at least twice the initially designed query load.

As had been the case in 2013 and in 2014, the majority of SIS II searches were also performed on national copies during the reporting period. In 2015, over 281 million queries – representing 9.9% of the total queries for 2015 – were performed on Central SIS II. In 2016, the central queries were more than 361 million, 9.1% of the total searches reported by the Member States. Depending on the criteria selected by the end-user to perform a search, there is a different impact on the Central System and therefore a shorter or longer response time can be expected, as per the design. The most used types of searches are first-line searches, known as category 1/Service Level Agreement (SLA) 1 searches[56], and back office searches, known as category 2/SLA2 searches[57].

Over 59% of the central searches performed in 2015 were SLA1 searches, whereas almost 40% were SLA2 searches. In 2016, confirming the result of the analysis, the proportions changed slightly and the SLA1 type of search decreased to 54.3% of the total searches performed on Central SIS II, whereas the proportion of SLA2 type of searches increased, reaching 44.4% of the total searches performed[58].

In 2015, 99.97% of the total amount of queries on Central SIS II received a reply within three seconds or less. Taking into account only SLA1 searches, 99.99% of them were answered in three seconds or less in 2015. In 2016, 99.93% of the total queries performed against the SIS II were answered in three seconds or less, and when it comes to SLA1 queries this goes up to 99.94%[59].

SIS II was highly available during the reporting period. The availability is calculated against critical SIS II functionalities, such as searching the system or properly processing and broadcasting the alerts received from the Member States. Furthermore, only unavailability in all Member States is used in the calculation.

In 2015, the overall availability of the SIS II Central System including the associated connectivity network was over 99.96%. The total unavailability was 3 hours and 4 minutes. Like the previous reporting period, this does not take into account maintenance activities, which were announced in advance.

The methodology for calculating the availability was slightly modified in 2016, so that the unavailability of the system included outages due to planned maintenance. Thus, in 2016 the availability of the SIS II Central System and the associated connectivity network was 99.89%, with the outage time amounting to 9 hours and 56 minutes. The outages were due to planned maintenance and to two incidents[60] affecting the whole community.

[53] Such as the systematic checks of all travellers at the external borders enforced since 7 April 2017, the implementation of the Passenger Name Record (PNR) and the increasing use of Automatic Number Plate Recognition (ANPR) systems. In addition, an increase in the number of SIS II queries should be expected in the light of the legal proposals currently under negotiations, for example the European Travel Information and Authorisation System (ETIAS) and the SIS reform, as well as the interoperability dimension.

[54] In particular the implementation of AFIS as well as the availability of testing facilities suffering a heavy workload.

[55] The Central Processing Units (CPUs) on the query nodes were doubled.

[56] Category 1 searches are performed by police officers and border guards directly in front of the person, document or object to be checked; therefore, they need to be performed very quickly.

[57] Category 2 is the type of search that does not have the need to receive an answer immediately and deals with inexact information.

[58] In 2015, there were 112,354,034 SLA2 searches whereas in 2016 there were 160,476,856.

[59] Annex, III. Table: response time for central searches during the reporting period.

[60] One in March in relation to a release and one in December related to a connectivity issue.

As soon as the incidents were detected by the 24/7 monitoring system, actions were taken as per the OPM and solutions applied.

2.4 Data quality and reporting

Data quality is a key element to ensure and maintain the efficiency of SIS II. As per Article 34 SIS II Regulation and Article 49 SIS II Decision, a Member State issuing an alert shall be responsible for ensuring that the data are accurate, up to date and entered lawfully in SIS II.

In September 2015, the SIS II Advisory Group mandated eu-LISA to perform the necessary checks at central level in order to support the Member States in complying with their legal obligations in the matter. The European Data Protection Supervisor (EDPS) endorsed the request, clarifying that in eu-LISA's role of management authority, it can develop functionalities, e.g. for reporting, that make it easier for the Member States to comply with their own obligations (e.g. on self-monitoring, data quality) under the relevant legal basis.

eu-LISA started a project to develop a technical solution[61] for supporting the Member States. During the reporting period, several working groups dedicated to data quality were convened to gather requirements, discuss reports presented, and enhance and refine them based on the feedback from Member States. The first set of reports[62] was made available as from the summer of 2016, and further adjusted in the autumn. By the end of 2016, the second phase of the project was launched, with an emphasis on alerts on persons. A comprehensive assessment was performed[63], with discussions being held on specific technical verifications required for different checks to be performed. As from May 2017, a new set of reports are made available to Member States on a monthly basis.

Following a request from the Commission, starting in August 2015 the Agency provided Member States and the Commission with targeted statistics on the data migrated from SIS 1+ to SIS II that still required intervention in order to comply with the SIS II legal requirements[64]. Member States had three years from the entry into operation of SIS II (namely until 9 April 2016) to cleanse amnestied SIS 1+ data. Through the regular reporting, which proved to add transparency to the exercise, improvements were traceable and the number of non-compliant alerts steadily decreased. Eventually, the Member States affected made compliant – deleted or updated – all migrated alerts.

As per the practice already established, during the reporting period eu-LISA continued to provide Member States as well as the Commission with a set of daily and monthly statistics on the business usage of SIS II. Statistics are provided via a secure dedicated environment with controlled access. Following new requirements, in particular aimed at monitoring the usage of alerts for immediate reporting as per the changes introduced in February 2015, additional regular reports were made available from the spring of 2015 onwards. In addition, eu-LISA provided statistics on an *ad hoc* basis, in particular supporting the Commission in its task of implementing the SIS II legal framework.

As already mentioned above, pursuant to Article 50(3) of the SIS II Regulation and Article 66(3) of the SIS II Decision, eu-LISA collects annual statistics from Member States and, together with data available at central level, publishes[65] a set of statistics showing the number of records per category of alert, the number of hits per category of alert and how many times SIS II was accessed, in total and for each Member State.

[61] Creating an automated reporting system that did not affect the Central System's performance.
[62] With the 'Light check reports', alert categories for firearms, vehicle and issued documents were monitored.
[63] In the context of the HLEG as well as the DAPIX working party; see above.
[64] As per Article 70(1) of the SIS II Decision and parallel provision in Article 54(1) of the SIS II Regulation.
[65] http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx.

2.5 AFIS for SIS II

As per Article 22 of SIS II's legal basis, on 29 February 2016 the Commission presented a report to the European Parliament and the Council on the availability and readiness of technology to identify a person based on fingerprints held in SIS II. The report was supported by a study conducted by the JRC confirming that the fingerprint identification technology is available and ready for its integration into SIS II.

Upon the release of the report and related study, and based on the Communication from the Commission COM (2016) 205 final[66], which mandated eu-LISA to develop and implement an AFIS functionality for SIS II, the Agency carried out a complementary study, considering different scenarios and aiming to assess the resources needed for the project's implementation. Based on both studies and on the Commission Decision[67] on minimum data quality standards for fingerprint records within SIS II, eu-LISA launched the AFIS project in mid-2016[68]. The Agency considered a two-step approach in which all necessary preparatory works, including design of the AFIS solution, were carried out in 2016, implementation is carried out in 2017 and entry into operation of phase 1 is planned for February 2018.

In June 2016, the AFIS Project Management Forum (PMF) was established with the aim of providing the necessary coordination for the successful implementation of AFIS at central and national levels. As the project has a tight timeline, it requires well-coordinated efforts, alignment of planning and good communication among all stakeholders involved in order to succeed. The PMF is composed of eu-LISA SIS II AFIS project team members, National Project Managers of all SIS II Member States and representatives of the Commission. The forum has been meeting on a monthly basis[69] since its establishment and reports directly to the SIS II Advisory Group.

To ensure that the developed solution will be consistent with Member States' needs, requirements for phase 1 were gathered in Q2 and Q3 2016. On 31 October 2016, the SIS II Advisory Group adopted the User Requirements Document. Following completion of the requirements stage, the specifications of the system were further defined. At the beginning of February 2017, the detailed analysis and design phase was completed with the endorsement, by both the Advisory Group and the SISVIS Committee, of the SIS II AFIS ICD.

Together with SIS II Release 8.2.0 scheduled for July 2017, a NIST checker will be implemented at Central System level. From the deployment onwards, Member States will receive notifications on the compliance of their fingerprints NIST container based on defined specifications.

Member States[70] participating in phase 1 will have integration tests in the second half of 2017, whereas training activities are planned for November 2017. Member States will have to convert (update/adapt) the fingerprints already stored in the system to the format that is required for the AFIS, ideally before the data migration planned for January 2018.

[66] Communication from the Commission to the European Parliament and the Council *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final.

[67] Commission Implementing Decision (EU) 2016/1345 on minimum data quality standards for fingerprint records within the SIS II; OJ L 231, 6.8.2016.

[68] The Agency had to re-align its planning to incorporate the AFIS project to its activities for 2016. For that reason, a number of SIS II activities, planned in 2016, had to be re-prioritised for 2017, as agreed with the Member States on the Management Board (the Annual Work Programme 2016 was amended to include the SIS II AFIS project).

[69] Mainly by web conference. Live meetings also took place for the main project milestones. In addition to the regular meetings, several *ad hoc* meetings were organised, including working groups on the ICD specifications and the NIST definition. The PMF will continue meeting with the same regularity.

[70] At the time of writing, those Member States were Austria, Germany, Switzerland, the Netherlands, Liechtenstein, Latvia, Luxembourg, Poland and Portugal.

2.6 Change management and releases

eu-LISA, being the operational management authority in charge of Central SIS II, has also been responsible for the continued development of the system, technologically and functionally. Developments and changes related to the Central System are discussed and formalised within the Change Management Process (ChMP) [71], ensuring agreement with Member States and coordinated implementation of all changes having an impact on national systems (functional changes and changes affecting the ICD).

In mid-2015, in order to optimise the ChMP already applied by the Agency, eu-LISA launched a survey among the Member States to review the process. The complex ChMP was revised to ensure proper coordination among all stakeholders involved on the technical and business side, as well as the decision makers if needed. The process was streamlined and earlier involvement of the SISVIS Committee was introduced for operational assessment, in particular for all functional/ICD changes.

In 2015, the Change Management Group (CMG) met nine times by means of online webinars. In 2016, the CMG met eight times both online and in person. In addition, other subgroup meetings and discussions were carried out online to assess the proposed Change Requests submitted by Member States or by the Commission, for example to work on the improvement of SIS II Data Quality, in a continuous process to further improve the usability and effectiveness of SIS II.

During the reporting period, almost all pending Change Requests, some of which were pending since before SIS II entered into operation in 2013, were implemented and made available to Member States[72]. Specifically, the following SIS II Releases were implemented:

- On 29 January 2015, Release 7.3.3 was implemented, as an emergency release to implement the changes requested by the Commission in the context of the Foreign Terrorist Fighters phenomenon. The changes related to relevant code tables, definition of new business rules and the check on compatibility of alerts. The release was planned and implemented by eu-LISA in the Central System and fully tested with Member States in less than 60 calendar days, with a great effort from all stakeholders involved, Member States and the Agency.
- On 9 June 2015, SIS II Release 7.4.0 was implemented. This release focused mainly on changes related to the UK's integration into SIS II, in particular the adaptation of CS-SIS in relation to alerts under Article 24 of the SIS II Regulation (refusal of entry/stay in the Schengen area) that are filtered for the UK[73]. In addition, an upgrade of Oracle completed the release. The release was deployed with a CU-BCU switchover/switchback[74].

[71] eu-LISA has adopted a standardised ChMP in order to guarantee the application of a common process in line with international standards for the applications used by Member States. The ChMP applies equally to all systems under eu-LISA's responsibility, in a uniform manner.

[72] For instance, in 2016 eu-LISA completed the implementation of 195 new SingleCategory Standard Queries and 34 new MultiCategory Standard Queries, for the benefit of those Member States querying the central system (with and without a national copy).

[73] This was introduced to ensure the overall coherence of the system taking into account the compatibility rules and the fact that the UK does not participate in the SIS II Regulation.

[74] In order to ensure the functioning of the system, eu-LISA plans the implementation of maintenance, a process based on releases. The installation of a release (or system patches used in emergencies) cannot be performed when the system is in operation. To reduce the downtime of the CS-SIS services to the minimum, eu-LISA performs a 'switchover' of operations from the CU to the BCU. When maintenance activities are completed, the operations are transferred back to the CU. MSs are always informed in advance, when a maintenance activity is planned for Central SIS II. To enhance further the maintenance process and to minimise the impact on the SIS II services, the Agency is currently assessing the possibility of implementing a new configuration for SIS II that allows both the CU and the BCU to be active at the same time. This new active-active configuration should minimise even further the impact on SIS II services during the installation of a release.

- On 16 March 2016, SIS II Release 8.0.0 was implemented. Among the changes was a new Change Request from the Commission related to 'Conveyance of Objects' in order to enforce counter-terrorism measures related to Article 36 alerts. The implementation of this Change Request implied the adoption of some new business rules[75].

  Furthermore, the enhancements of security elements for stolen/lost credit cards were also part of the release, solving an issue discussed and analysed within the CMG for several months.

- On 31 May 2016, SIS II Release 8.0.1 with corrective items for several queries was implemented. The release was deployed with a CU-BCU switchover/switchback.

- On 28 November 2016, SIS II Release 8.1.0 was deployed. The release encompassed the implementation of additional MultiCategory query for any logical combination[76] and the change to support alerts related to lost/stolen EU laissez-passer. A critical change raised by the Commission about adding new entries in the code table for type of offence to make information about a person's sexual offences immediately visible to law enforcement officers in the event of a 'hit' was implemented. In addition, a new software version was deployed and bugs were corrected, including the Orphan link bug that had previously caused some problems during the DCCs. The release was deployed with a CU-BCU switchover/switchback.

In addition to the three CU-BCU switchovers and switchbacks performed during releases, four other CU-BCU switchovers and switchbacks were carried out during the reporting period[77]. The switch between the CU and the BCU is transparent to the users regarding the network addressing.

Another critical change proposed by the Commission related to SIS II – update of the applicability of 'type of offence' for which a suspect is wanted – was discussed extensively within the CMG in Q4 2016. The CMG's final recommendation was not to implement the change. The first release in 2017, Release 8.2.0, took place on 4 July and included, in particular, improvements to the DCC functionality and the implementation at central level of a NIST checker as part of the AFIS project.

Release 8.2.0 also implemented a new check to detect the file type of the files attached to SIS II alerts, with the aim of further enhancing the data quality. Release 8.2.0 also implemented an update in code tables ST118_FILETYPE by adding '.DOCX' and '.XLSX' file types, which are used by MS Office 2007 and later versions.

2.7 Test activities

2.7.1 Internal testing

As with any major information system, Central SIS II has to undergo regular system maintenance to ensure its continuous operation. The role of eu-LISA's test team is to test that activities under corrective, adaptive and evolutionary maintenance do not adversely affect the system.

During the period, a test campaign for each release of SIS II was conducted to confirm the release. The campaigns were aimed at ensuring that the releases required for corrective, adaptive and evolutionary maintenance would not add regression to the system as a whole as well as at validating the updates.

Extensive tests, both functional and non-functional, are conducted prior to a release being deployed in

[75] Aiming to modify an existing SIS II business rule to make a code table available for alerts on discreet and specific checks (for persons and objects under Article 36 of the SIS II Decision) as a 'non-mandatory' field.
[76] Standard and MultiCategory Queries.
[77] In December 2015 and in March, October and December 2016.

production. Functional testing is the type of testing done against the business requirements of the application and it verifies compliance with all business and system use-cases. Non-functional tests are performed against the non-functional requirements, which are not related to any specific function or user action, such as performance, scalability, security or behaviour of the application under certain constraints. When performing these tests, special attention is paid to the actual release procedure to ensure that ongoing business processes are impacted as little as possible.

In Q1 2016, eu-LISA successfully tested and deployed SIS II Release version 8.0, allowing the integration of the Croatian national SIS II system into Central SIS II. In addition, tests of a new version of the DEBS (Data Exchange between SIRENEs 'SIS II') were also carried out, with the version successfully deployed. During the second half of 2016, eu-LISA also qualified the Central System for handling up to 100 million alerts. After successful internal tests, Member States were involved in order to ensure that their national systems (for those with a national copy) could cope with the increased capacity. Special emphasis was put on guaranteeing that there were no degradations in the response time for create/delete/update (CUD) or DCC operations or for queries.

In Q3 2016, eu-LISA proceeded with all necessary internal tests qualifying a higher version of WebLogic (Java 2 Platform Enterprise Edition Application Server). The internal qualification campaign lasted three months. The deployment of the newer version of WebLogic was performed simultaneously with the qualification of a new release. For the first time, infrastructure aspects together with the application layer of Central SIS II were successfully changed at the same moment.

All evolutions are thoroughly tested by eu-LISA in order to ensure the integrity of SIS II and the absence of regression once deployed.

2.7.2 Testing with Member States and Europol

eu-LISA is also responsible for coordinating tests, determining test requirements and planning; this covers integrating new Member States and new or substantially changing national systems. Member States assist eu-LISA in the overall performance of all tasks related to test execution. The test results executed by Member States and organisations connected to SIS II are, after approval by the SIS II Advisory Group, endorsed by the SISVIS Committee. The major test campaigns performed in the reporting period were:

- **The United Kingdom:** following the testing campaigns, the UK successfully joined SIS II and created its first alert on 13 April 2015, based on the relevant Council Implementing Decision.

- **Switzerland, Austria and Germany:** following successful tests, both functional and non-functional, the new national system of Switzerland (SNI 3.0) entered operation in February 2015. The validation led to similar campaigns in Austria and Germany. Tests were performed between September and November 2015. The successful deployment in production took place for both countries in early 2016.

- **Finland:** following the successful SIRENE tests performed in 2014, in 2015 Finland proceeded with the qualification of the new national system. The connectivity tests were conducted in Q1 2015, whereas the compliance tests were carried out in Q2. Following successful conclusion of the test campaigns, Finland deployed a new system.

- **Romania:** Romania ran extensive tests with eu-LISA in order to qualify the backup system, intended to perform queries against Central SIS II only if both the primary and secondary systems were unavailable because of data corruption issues. These tests started in Q3 2015 and ended successfully in Q2 2016. Since the successful qualification, Romania has activated its backup solution on several occasions without compromising the integrity and the continuing operation of Central SIS II.

- **Bulgaria:** extensive test campaigns, of both functional and non-functional natures, took place in May and December 2015 between eu-LISA and Bulgaria, leading to a successful upgrade of the Bulgarian Oracle infrastructure. In the course of Q4 2015, Bulgaria also successfully qualified the possibility of linking alerts.

The functionality was activated by the end of the year.

- **The Czech Republic:** between September 2015 and August 2016, eu-LISA conducted connectivity, compliancy, comprehensive and resilience tests with the Czech Republic for the successful deployment of a new version of the Czech national system.
- **Italy:** between September and December 2015, eu-LISA conducted various test campaigns in order to validate the virtual Message Oriented Middleware set up by Italy. The successful tests led Italy to proceed with deployment into production in Q2 2016.
- **Latvia:** between September and December 2015, eu-LISA conducted various test campaigns in order to validate the N.SIS release set up by Latvia. These tests were of both a functional and non-functional nature. As per the original project plan, two different test campaigns were conducted: connectivity and compliance tests; and comprehensive tests. In 2016, Latvia migrated towards a new Message Oriented Middleware.
- **Slovenia:** in Q1 2016, Slovenia successfully qualified the possibility of linking alerts, and functionality was activated.
- **Norway:** during October and November 2016, eu-LISA conducted a test campaign in order to validate the new Message Oriented Middleware implemented in the Norwegian SIS II national system. These tests were of both a functional and non-functional nature. Norway successfully qualified and put into operation the new Message Oriented Middleware solution.
- **Belgium:** during Q3 and Q4 2016, eu-LISA successfully qualified a new release of the Belgian national system. The new release went into operation at the end of 2016.
- **Denmark:** during Q4 2015 and Q1 2016, eu-LISA supported Denmark with tests in relation to the implementation of an ANPR (Automatic Number Plate Recognition) solution that would also ensure the preservation of the integrity of Central SIS II and the related throughput.
- **Estonia:** in Q4 2016, Estonia successfully qualified the possibility of linking alerts. The feature was activated in Q1 2017.
- **Europol:** in Q4 2016, Europol successfully qualified and implemented batch querying against Central SIS II.
- **Dual encryption layer:** in order to support the migration towards TESTA-ng as the new network provider as well as to align the production and the pre-production environments, eu-LISA conducted tests with three pilot Member States implementing the secondary encryption layer also on the pre-production network. The tests ran in Q2 2015 with the support of Germany, Hungary and Luxembourg.
- **Message Oriented Middleware:** eu-LISA continued to support the adaptive maintenance for the Message Oriented Middleware, allowing Member States to connect to Central SIS II. During the reporting period, five new versions of middleware were successfully tested and introduced as potential solutions for Member States.
- **Capacity increase of Central SIS II:** during the second half of 2016, eu-LISA qualified the systems used by Member States in order to ensure that their national systems (for those with a national copy) could cope with the increased capacity. Particular attention was put into guaranteeing that there was no SLA degradation for CUD or DCC operations or for queries.
- **WebLogic upgrade:** in the course of Q3 2016, prior to its deployment in production, the upgrade to a higher version of WebLogic was extensively tested with Member States. Special emphasis was put on verifying that the different types of Member States' interfaces (WebLogic, Oracle, Websphere, OpenMQ) were all covered and supported.
- **Integration of Croatia:** in April 2015, eu-LISA started the project for the Croatian integration into SIS II. Several testing activities were needed: Croatia needed to be added to the core of Central SIS II; and heavy

internal testing activities were carried out at Central System level, including a User Acceptance Test with Member States. Following the successful test campaigns, in Q4 2015 eu-LISA started a series of campaigns with Croatia: connectivity and compliancy tests; comprehensive tests; tests with all Member States verifying their capability to handle alerts from Croatia; robustness and resilience testing for the Croatian national system; and SIRENE tests (see also next point). All tests were run within a six-month period[78], including the approval by the SIS II Advisory Group and endorsement by the SISVIS Committee.

2.7.3 SIRENE testing

The SIRENE tests aim to validate all functional aspects of the SIRENE workflow system – including the underlying Communication Infrastructure – used by the Member States with respect to the specifications of the interaction with Central SIS II. Those tests address the functioning of the national SIRENE workflow system and the exchange of information between the SIRENE Bureaux[79] using this system, entering, modifying, flagging and deleting corresponding alerts in SIS II and attaching/detaching relevant additional information to/from SIS II alerts.

- **SIRENE Bureau Poland:** in March 2015, eu-LISA, assisted by experts from Member States, executed SIS/SIRENE functional tests with Poland. The purpose of this test campaign was the evaluation of the correct implementation of the SIS II CUD and other functions as well as the correct functioning of the SIRENE Bureaux workflow (operationality of the systems, compliance with SIS II, and SIRENE's ability to follow the procedures described in the SIS II legal basis and SIRENE Manual). Poland successfully performed the global SIRENE forms test with all Member States connected to SIS II and the functional tests with the four volunteer countries Switzerland, Latvia, Slovakia and Germany.
- **SIRENE Bureau Croatia:** in June 2016, with the assistance of Member States' experts, eu-LISA executed SIS/SIRENE tests with Croatia. The purpose of the SIS/SIRENE functional tests is the evaluation of the correctness of the implementation of the SIS II CUD and other functions together with the functioning of the SIRENE Bureaux workflow. During those tests, both the Communication Infrastructure as well as the business process flow were successfully tested.

2.8 Training activities

eu-LISA provides training for the benefit of the SIS II community as per the Agency's establishing Regulation. Training topics and target groups are specified in particular, in recital 11[80] as well as in Article 3(b)[81]. In addition to being a legal requirement for eu-LISA, training activities for national IT operators and technical SIS II experts facilitate the operational management of the system supporting technical maintenance and communication via the single point of contact (SPOC), as well as ensuring data consistency and synchronisation.

Furthermore, training on SIS II is required prior to the integration of new Member States and/or organisations into the system to ensure their capacity to develop and operate their national systems.

2.8.1 Training activities for 2015

[78] All validation procedures were completed before mid-July 2016, allowing Croatia to access the Schengen Accession Funds before the deadlines.
[79] Through forms sent via the SIRENE Mail infrastructure according to the specifications provided in the SIRENE Manual.
[80] 'The Agency should perform tasks relating to training on the technical use of SIS II, VIS and Eurodac and other large-scale IT systems which might be entrusted to it in the future.'
[81] 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.'

The delivery of the eu-LISA training activities in 2015 was an integral part of eu-LISA's efforts to support Member State national authorities in the technical use of the systems. The 2015 Training Plan was discussed and agreed with national representatives – the NCP Network – and corresponding financial resources were allocated. The training budget in 2015 covered the organisational and logistical costs of the training delivered. All twelve training courses envisaged by the Training Plan, in addition to five *ad hoc* training sessions, were successfully delivered during the year[82].

The general average satisfaction rate of 4.5 on a five-point scale confirmed the appreciation towards eu-LISA trainees and provided programmes[83]. Compared with 2014, the number of eu-LISA trainers increased by approximately one third, the training curricula were updated and new training courses (e.g. SIS II for SIRENE, SIS II Operational Training) were created.

In 2015, the development of appropriate and modern training tools was finalised, by establishing eu-LISA's Training Platform LMS (Learning Management System). The majority of eu-LISA training courses rely on a blended learning methodology, which includes an online phase (studying the eLearning materials during the pre-course phase), followed by face-to-face sessions (classroom courses). The eLearning Platform allows smooth communication with trainees and trainers and it is an essential tool for any eLearning-based training activity (it also includes other LMS features: distribution of training materials, course evaluation, forums, etc.).

eu-LISA's Training Platform offers access to three thematic sub-platforms, one for each system[84]. The platform for SIS II contains eLearning modules for self-study, SIS II course supporting documents and training materials from the SIS II classroom course – Train the trainer. The platform is open to all registered SIS II IT operators, SIRENE officers and Schengen evaluation team members.

In 2015, eu-LISA took over the annual Chairmanship of the Justice and Home Affairs (JHA) agencies Training Coordination Network[85], during which several activities were organised with the objective of enhancing cooperation with the JHA agencies in the field of training.

2.8.2 Training activities for 2016

In 2016, eu-LISA delivered 33 training sessions on various scales and in various formats on all three large-scale IT systems. Special focus was given to the enhancement of the eLearning component by creating a number of eLearning training materials and providing additional, webinar-oriented training sessions on specific related technical topics. More than 1,000 trainees, from all Member States, attended eu-LISA training in 2016.

A total of 141 trainers from eu-LISA and experts from JHA agencies, the Commission and the Member States were engaged in preparing and delivering the training. In addition to the 27 training activities covering all the systems envisaged in the Annual Training Plan, six additional training sessions were requested by Member States and eu-LISA and subsequently successfully delivered[86]. Furthermore, a series of new curricula (pilot training courses) were delivered as well.

[82] Annex, IV. Training courses related to SIS II provided in 2015 and graph on the number of participants.

[83] In 2015, eu-LISA organised 17 training events (for all systems) with 447 participants in total.

[84] The other two platforms, for the VIS and for Eurodac, contain the same type of training materials (eLearning modules for self-study, course supporting documents and training materials from classroom courses – Train the trainer) and are open to registered national IT operators managing VIS and Eurodac.

[85] The JHA Training Coordination Network consists of eu-LISA, the European Union Agency for Law Enforcement Training (CEPOL), the European Asylum Support Office (EASO), the European Union Agency for Network and Information Security (ENISA), Eurojust, Europol, the European Union Agency for Fundamental Rights (FRA) and the European Agency for the Management of Operational Cooperation at the External Borders (Frontex). The JHA Training Coordination Network is a part of the Network of JHA Agencies aiming to coordinate information exchange among the JHA Agencies and between the JHA Agencies and the Commission. The Network also serves as a platform for enhanced visibility of the activities of the JHA Agencies to the EU institutions.

[86] Annex, IV. Training courses related to SIS II provided in 2016 and graph on the number of participants.

The general average satisfaction rate of 4.45 on a five-point scale confirms the high level of satisfaction among attendees at the training delivered by the Agency. The total number of eu-LISA training events increased by 94.1% over 2015.

Regarding training-related activities, in 2016 the Agency continued its successful cooperation with the Member States through the activities of the NCP Network and the partners from JHA agencies and the Commission. The cooperation with CEPOL and EASO was particularly productive, resulting in the delivery of eight joint training activities in 2016, of which two were completely newly created training curricula on technical topics.

The regular annual meeting of the NCP Network was held in October. The training needs analysis for 2017 was successfully concluded, with the identification and agreement on topics for the training curricula and Annual Training Plan for 2017. Finally, in order to further enhance the learning experience of eu-LISA's trainees, in 2016 the preparatory work for the delivery of a Moodle-based Learning Management System started. The delivery of the new eu-LISA LMS is envisaged for 2017.

3. Communication Infrastructure

According to Article 4(1)(c) of the SIS II legal instruments, one of the three elements comprising SIS II will be a communication infrastructure between the Central System (CS-SIS) and the national interfaces (NI-SIS) which provides an encrypted virtual network dedicated to SIS II data and the exchange of data between the authorities responsible for the exchange of all supplementary information (SIRENE Bureaux).

The Communication Infrastructure is provided via a European private secure network named Secure Trans European Services for Telematics between Administrations (sTESTA) implemented under the IDABC programme (2005-2009) by the European Commission's Directorate-General for Informatics (DIGIT). The SIS II Network is a community under sTESTA and was implemented by DG JLS[87] to support the second-generation Schengen Information System.

The scope of services covered by the sTESTA network includes (a) the provision of a Core Management Team, responsible for the overall vision, design and security of sTESTA and the leadership, communication and management of the service delivery team; (b) a dedicated centralised Support and Operations Centre (SOC), responsible for ensuring the operational management and the quality of the network by the provider on a 24/7 basis; (c) consultancy services; (d) connectivity; (e) network; and (f) security. These services relate to the provision, set-up and operation of a dedicated centralised management, monitoring and support infrastructure. Additional services cover the provision of monitoring tools, reporting and SOC staffing.

According to Article 7 of the eu-LISA establishing Regulation[88], tasks regarding the Communication Infrastructure (including operational management and security) are divided between eu-LISA and the Commission. In June 2014, a Memorandum of Understanding (MoU) was concluded between eu-LISA and the Commission in relation to the operational working arrangements.

As specified in Article 19 of the MoU, the Agency is responsible for supervision, security and coordination of relations between the Member States and the network provider for the Communication Infrastructure of

[87] DG JLS stands for the Directorate-General for Justice, Freedom and Security, nowadays replaced by DG Home Affairs.
[88] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011R1077.

SIS II[89]. The Agency is also responsible for the security measures in respect of the exchange of supplementary information through the Communication Infrastructure of SIS II[90].

On the other hand, the Commission is responsible for all other tasks relating to the Communication Infrastructure, in particular tasks relating to the implementation of the budget, acquisition and renewal and contractual matters. As regards SIS II, the Commission is also responsible for adopting the security measures including a security plan in relation to the Communication Infrastructure.

3.1 Technical functioning of the Communication Infrastructure

The SIS II network provides a secure wide-area network for the exchange of data between central and national systems. The architecture of the network can be described as a 'star topology with resilience'. The central unit (CU in Strasbourg) and backup central unit (BCU in Sankt Johann im Pongau) contain the systems to which each national network connects. The central unit and backup central unit are interconnected by a dedicated point-to-point connection.

Confidentality of SIS II communication over the sTESTA network between the Central System and national systems is ensured by a secondary encryption layer, made up of dedicated encryption devices. It is fully managed by eu-LISA in order to ensure that third parties cannot gain access to clear text data. The secondary encryption layer originally covered only the production part of the Communication Infrastructure, so it represented a certain risk to the availability of the service, as, for example, testing was not possible. Therefore, during 2015 and 2016 the secondary encryption layer was deployed in the pre-production part of the Communication Infrastructure as well.

The SIS II Mail Relay service, operated within the SIS II network, provides Simple Mail Transport Protocol (SMTP) relay functionality in a hub-and-spoke topology to national systems (NS) for the purposes of supporting the communications of the SIRENE network, namely the exchange of supplementary information.

The SIS II mail SPOC servers consist of two mailbox servers, one at the CU site and one at the BCU site, which host the SIS II central SPOC mailbox. This allows NS SPOC mailboxes to send email messages to the central SPOC mailbox, and the central SPOC mailbox to send messages to the NS SPOC addresses.

The SIS II network is permanently monitored in order to ensure continuous service availability, while strict performance service level requirements have been established. During the reporting period covered in this report – 1 January 2015 to 31 December 2016 – there were no incidents with a critical impact[91] on the functioning of the overall SIS II community. There were in total three incidents affecting the overall service availability with less than critical impact, caused by hardware and software malfunctioning, including incidents with the second encryption layer. These incidents caused in total one hour and 15 minutes' unavailability of the Central System[92]. Every one of these incidents was analysed to identify the root cause, and appropriate measures were implemented to prevent recurrence of the incident.

During the reporting period, the technical complex project for the migration from the current sTESTA network to the new TESTA-ng (New Generation) network was ongoing. The migration[93] concerns the set-up and installation of the TESTA-ng network by a different legal entity, the continuation of the sTESTA services until the TESTA-ng network is operational, and the transfer of all existing sTESTA services – and therefore also those

[89] As well as for VIS and Eurodac.

[90] And for establishing the technical procedures necessary for the use of the Communication Infrastructure for Eurodac.

[91] A critical impact is considered to be when the service is not available for more than 8 hours and the entire community is affected.

[92] This unavailability is already considered in the unavailability mentioned above in section 2.3, 'Performance and availability'.

[93] First migration on production sites for Member States started in early 2017, outside the reporting period. During the writing of this report, the TESTA-ng migration was delayed because of contractual concerns.

related to SIS II – from the old sTESTA network to the new TESTA-ng network.

In this respect, several activities were organised during the reporting period: definition of migration processes and approaches, hardware deliveries, software deployments, several testing campaigns and technical workshops held with Member States. In total, 47 sites concerning the SIS II community are to be migrated.

4. Security and data protection

4.1 Security

The overall security framework for SIS II and its Communication Infrastructure provides assurance that, at central level, the system will protect the information it stores and will function as and when it needs to, under the control of designated authorities, relying on the core principles of information security, namely confidentiality, integrity and availability.

Article 16(1) of the SIS II legal basis establishes roles and responsibilities for the adoption of the necessary security measures at CS-SIS level and the Communication Infrastructure. The corresponding security measures applicable to CS-SIS have been defined within the SIS II Security Plan and SIS II Security Policy, both of which were adopted by eu-LISA's Management Board on 13 March 2013. The measures described by the Security Policy[94] implement the principles of least privileges, security by default, defence in depth and segregation of duties.

At the physical security boundary, the SIS II Central System is protected by a very strong set of physical controls including multi-layer external perimeter; 24/7 monitored CCTV; intrusion detection; biometrics access control; and the permanent presence of security guards. The security guard service is outsourced to an external company and this service is supervised and monitored by internal security staff.

In the event of a disaster situation, operations can be switched to the backup site in Austria, where a permanent presence of eu-LISA's staff is ensured.

All persons having logical or physical access to the production systems (central or backup sites) have a valid personnel security clearance at 'EU Secret' level. Operational and administrative access to the central and backup systems is allowed for duly authorised persons, who have clearly defined roles and responsibilities, be they Agency staff, contractors or other staff involved in operational management. The roles and responsibilities are also documented and communicated to the persons concerned.

Confidentiality and secrecy agreements are concluded with all persons to whom no European Union or Member State public service rules apply. Staff and contractors required to work with Central SIS II are required to possess a valid EU national personal security clearance.

All activities carried out within SIS II are strictly controlled, monitored and logged. All communication with Member States is protected with multiple layers of encryption and network security controls with several layers of firewalls and integrity checks. CS-SIS is located in an isolated, controlled and secure environment, physically

[94] The measures to be provided for in the security policy, according to Article 16(1) of the SIS II Decision, include restrictions of access to data-processing facilities, personnel security requirements, controls on removable media containing data and any other important assets, data-storage controls, passwords, access to SIS II hardware and software, communication controls for the Communication Infrastructure, monitoring and security incident management.

isolated from the internet. A Security Incident Management Process is in place to detect, handle and respond to security incidents, which may compromise SIS II operations and data.

In terms of security audits and assessments, the Agency Security Policy mandates that all Agency information systems including technical and non-technical security controls are subject to regular security assessments, vulnerability and penetration testing to provide security assurance and to verify that the implementation, integration and configuration are compliant with defined security requirements. CS-SIS undergoes periodic technical vulnerability testing and baseline security self-assessments and is subject to vulnerability testing on a regular basis.

Finally, in order to increase the level of cooperation in the area of security operations, an informal network of security contact points, the SON, was established by eu-LISA's Management Board to facilitate more effective information exchange among Member States' experts. The SON met four times in 2015 and 2016.

In 2015, the EDPS carried out an inspection of SIS II, with the aim of checking:

- the security of Central SIS II and its Communication Infrastructure: information security, management system, security incident management, physical security, backups, disaster recovery, access control, logging, auditing and monitoring;
- the impact of operational management of SIS II on its security in the sense of Article 22 of Regulation (EC) No 45/2001 – Central System and its Communication Infrastructure: change management, release management, problem management.

The EDPS's report was finalised in 2015 and shared with the Council, the European Parliament, the Commission, the national data protection authorities and eu-LISA. No critical findings were reported. The main recommendations in terms of security included to fully define and document the security framework under which eu-LISA operates, perform the relevant risk assessments in order to define the most appropriate controls to implement, document or update all security policies and procedures applying to eu-LISA, and finalise notifications related to security processes.

Regarding the findings of the EDPS, eu-LISA is maintaining an Action Plan addressing the recommendations.

The SIS II security plan and business continuity plan are currently being updated to account for the development of the AFIS, with the first internal draft, including the updated risk assessment, to be ready at the start of Q4 2017.

The security unit coordinated a study on the implementation of a Central User Repository for SIS II, which was completed in Q4 2015. The agency subsequently procured the implementation services for the new security architecture for SIS II in 2016, planned to be integrated into the development of the SIS II AFIS. The implementation work is planned to be initiated in May 2017.

The implementation of the security documentation framework also follows a roadmap starting with the development and approval of the Agency's rules on information security based on Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission[95], followed by the finalisation and approval of the supporting standards and guidelines. A first internal draft of the Agency's rules on information security is planned for the end of Q4 2017. The standards and guidelines are scheduled for completion on a rolling schedule between Q4 2017 and Q2 2018.

The relevant notifications have been provided to eu-LISA's Data Protection Officer.

[95] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.006.01.0040.01.ENG.

4.2 Data protection

At both central and national levels, the SIS II technical solution complies with strict data protection requirements. The European Data Protection Supervisor (EDPS), in close cooperation with eu-LISA's Data Protection Officer (DPO), monitors the implementation of the data protection provisions, in particular concerning the processing of personal data by Central SIS II, as per Regulation (EC) No 45/2001[96], Chapter VI of the SIS II Regulation and the parallel provision of Chapter XII of the SIS II Decision.

As mentioned above, the EDPS inspected Central SIS II on 25-26 February 2015. On this occasion, the DPO acted as a liaison between the Agency and the EDPS during the entire exercise (from the preparation phase, through the on-site visit, the post-visit document requests and comments, to the draft Report[97]). The EDPS's recommendations in terms of data protection included measures such as the introduction of training and awareness sessions for the Agency's staff as well as the introduction of timely notification to eu-LISA's DPO if an operation processing personal data is carried out.

During the reporting period, the DPO was involved in projects concerning data quality and data amnesty[98] reports. Although Member States as owners of the data are liable, eu-LISA has been fully committed to providing monitoring capabilities and technical solutions to support Member States in improving the quality of the data inserted in the system.

Close cooperation between the EDPS, eu-LISA's DPO and the Commission was achieved in the interpretation and application of the SIS II legal framework, in order to draw up harmonised proposals for a joint solution for the data quality reporting process.

The Supervision Coordination Group of SIS II (SCG SIS II), consisting of representatives of national data protection authorities of Member States integrated with SIS II, together with the EDPS, meets regularly twice a year[99]. eu-LISA's DPO is regularly invited to the meetings.

The group aims to enhance the cooperation between the national supervisory authorities and coordinate the supervision of Central SIS II and the national systems, contributing to the exchange of relevant information and implementation of common practices. In addition, the SCG SIS II assists national supervisory authorities during inspections and audits, and provides support in the event of difficulties pertaining to the interpretation or implementation of the SIS II legal provisions.

In October 2015, the SCG SIS II published an updated version of the Guide for exercising the right of access[100]. The Guide[101] describes the procedures for exercising the right of access by persons whose personal data is collected, held or processed in SIS II[102].

[96] 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.

[97] The report is not a public document, due to legal restrictions. The recipients of the report are eu-LISA, the European Commission, the European Parliament, the Council of the EU and the national data protection authorities.

[98] Data amnesty refers to the process needed for assuring that the contents of the alerts transferred from SIS 1+ to SIS II were compliant with the legal basis of SIS II. As per Article 54(1) of the SIS II Regulation and parallel provision of Article 70(1) of the SIS II Decision, Member States had three years – as from the entry into operations of SIS II – to ensure this process.

[99] The SCG SIS II met on 25 March 2015, 7 October 2015, 14 April 2016 and 22 November 2016.

[100] Available at the functional link: https://edps.europa.eu/sites/edp/files/publication/15-10-12_sis_guide_of_access_summary_en.pdf verified on 12 April 2017.

[101] For the correction of inaccurate data and deletion of unlawfully stored data in SIS II.

[102] Anyone wishing to exercise these rights should submit the request to the competent national authority of his/her choice where SIS II is operated, regardless of the Member State issuing the alert, and not to eu-LISA.

5. Exchange of supplementary information between Member States

As part of the collection of SIS II annual statistics, eu-LISA collects statistical data on the exchange of supplementary information between Member States and in particular on the number of forms exchanged as well as on hits achieved. The exchange of supplementary information through SIS II has a crucial role, as concluded by the Commission's evaluation report[103], as it has contributed greatly to effective law enforcement cooperation and border management in Europe. Furthermore, the efficient cooperation structure set up within the framework of the SIRENE Bureaux is an indispensable factor in the operational success of SIS II.

This section presents data on forms and hits reported by Member States for the reporting period.

5.1 Exchange of forms

SIS II contains the indispensable information (i.e. alert data) allowing the identification of a person or an object and the necessary action to be taken. In addition, according to the SIS II legal instruments, Member States shall exchange supplementary information[104] related to an alert, which is required for implementing certain provisions of the SIS II legal instruments, and for SIS II to function properly, on either a bilateral or a multilateral basis.

Forms	2015		2016	
	Outgoing	Incoming	Outgoing	Incoming
Forms A	22,689	553,772	22,050	578,317
Forms E	315	329	554	570
Forms F	18,078	18,066	17,686	17,336
Forms G	118,735	120,027	169,128	169,797
Forms H	17,044	19,468	18,835	21,426
Forms I	9	6	41	33
Forms J	571	584	792	821
Forms K	570	583	863	825
Forms L	5,319	7,061	5,807	6,548
Forms M	226,243	597,718	294,255	710,227
Forms N	4,666	4,767	4,585	4,541
Forms O	2,145	2,169	3,576	3,569
Forms P	14,739	14,974	14,679	15,023
Forms Q	156	512	123	466
Total	**431,279**	**1,340,036**	**552,974**	**1,529,499**

In every Member State connected to the system there is a SIRENE Bureau, which is responsible for the coordination and verification of the quality of the data entered in SIS II and the facilitation of the necessary information exchange with other Member States via exchanged forms. Rules and procedures governing the bilateral and multilateral exchange of supplementary information are laid down in the SIRENE Manual[105].

The table on the side provides the breakdown of *outgoing* and *incoming* forms[106] for the reporting period[107].

In relation to 2015 *outgoing* forms, Member States reported that they had also sent 57,807 forms A and M

[103] COM(2016) 880 final.

[104] As per Article 3(b) of the SIS II Regulation and Article 3(1)(b) of the SIS II Decision, supplementary information is exchanged: in order to allow Member States to consult or inform each other when entering an alert; following a hit, in order to allow the appropriate action to be taken; when the required action cannot be taken; when dealing with the quality of SIS II data; when dealing with the compatibility and priority of alerts; when dealing with rights of access.

[105] OJ L44, 18.2.2015.

[106] Form A exchanging supplementary information on alerts for arrest; form E consultation in case of incompatible alerts; form F requesting to add or remove a flag; form G matching (hit) of alert; form H if procedures cannot be followed; form I if original objective of the alert is altered; form J for data that are legally or factually inaccurate; form K exercising the right to access or rectify data; form L supplementary information on a person's identity; form M miscellaneous information; form N consultation procedure as pursuant to Article 25(1) of the Schengen Convention; form O consultation procedure as pursuant to Article 25(2) of the Schengen Convention; form P further information to be supplied when a vehicle, boat, aircraft, container or industrial equipment is recovered; form Q misused identity.

[107] At the beginning of 2017, while collecting data for 2016, some Member States updated their data on forms for 2015.

to the UK for the initial load, prior to its connection to SIS II[108]. Those forms are not counted in the table above.

In 2015, there were in total 1,829,122 forms exchanged bilaterally or multilaterally between Member States. In 2016, there was an increase of 14%, with 2,082,473 forms exchanged.

As a counting rule, any SIRENE form that was sent to several or all SIRENE Bureaux was counted only once by the sending SIRENE Bureau (for the *outgoing* forms); on the other hand, this same form was counted as an *incoming* form by each of the SIRENE Bureaux receiving it. Each form, whether *outgoing* or *incoming*, represents a workload for the sending or receiving Bureau.

5.2 Hits

A 'hit' occurs in SIS II when a user conducts a search and the search reveals a foreign alert[109], i.e. the alert in SIS II matches the searched data. As a result of the hit, further actions are requested in accordance with the legal provisions. A distinction is made between hits achieved on alerts issued by other countries (i.e. hits on foreign alerts) and hits achieved by other countries on alerts issued by the reporting country (i.e. hits abroad on own alerts).

The table below provides the breakdown of *hits abroad on own alerts* and *hits on foreign alerts* for the reporting period[110].

		2015		2016	
		hits abroad on own alerts	hits on foreign alerts	hits abroad on own alerts	hits on foreign alerts
Art 26 SIS II Dec		10,595	10,998	11,330	12,003
Art 24 SIS II Reg		21,741	30,465	20,514	29,746
Art 32 SIS II Dec		5,366	5,711	6,918	7,687
Art 34 SIS II Dec		28,748	34,506	34,736	47,931
Art 36 SIS II Dec		32,103	32,839	60,548	60,867
Art 38 SIS II Dec	vehicles, trailers, caravans	13,317	15,285	13,010	14,794
	boats	12	19	18	19
	aircraft	0	0	0	1
	industrial equipment	199	197	109	106
	boat engines	55	74	79	71
	containers	1	0	0	3
	firearms	332	295	224	185
	blank docs	1,826	1,533	1,293	1,198
	vehicle registration certificates	999	1,377	1,212	1,371
	number plates	2,043	2,732	2,448	2,842
	issued docs	13,277	18,560	15,674	21,868
	banknotes	528	150	30	53
	securities and means of payment	29	27	21	33
	Total Art 38 SIS II Dec	32,618	40,249	34,118	42,544
TOTAL		**131,171**	**154,768**	**168,164**	**200,778**

[108] The UK started using SIS II on 13 April 2015.

[109] SIS II contains only those categories of alerts that are entered by each of the Member States as required for the purposes laid down in Articles 26 (persons subject to arrest for surrender or extradition), 32 (missing persons (adults and minors)) 34 (persons to assist with a judicial procedure), 36 (persons for discreet or specific checks) and 38 of the SIS II Decision and Article 24 (third country nationals to be refused entry into or stay within the Schengen Area) of the SIS II Regulation. Alerts can relate to persons in relation to whom an alert has been entered or to objects referred to in Articles 36 and 38 of the SIS II Decision (vehicles, aircraft, banknotes, blank official documents, boats, boat engines, containers, firearms, industrial equipment, issued documents, vehicle licence plates, securities and means of payment, vehicle registration documents).

[110] At the beginning of 2017, while collecting data for 2016, some Member States updated their data on hits for 2015.

The *hits abroad on own alerts* reported by Member States in 2016 showed an increase of over 28% compared with data for 2015. Similarly, the *hits on foreign alerts* reported by Member States in 2016 showed an increase of almost 30% compared with data for 2015.

6. Conclusion and looking forward

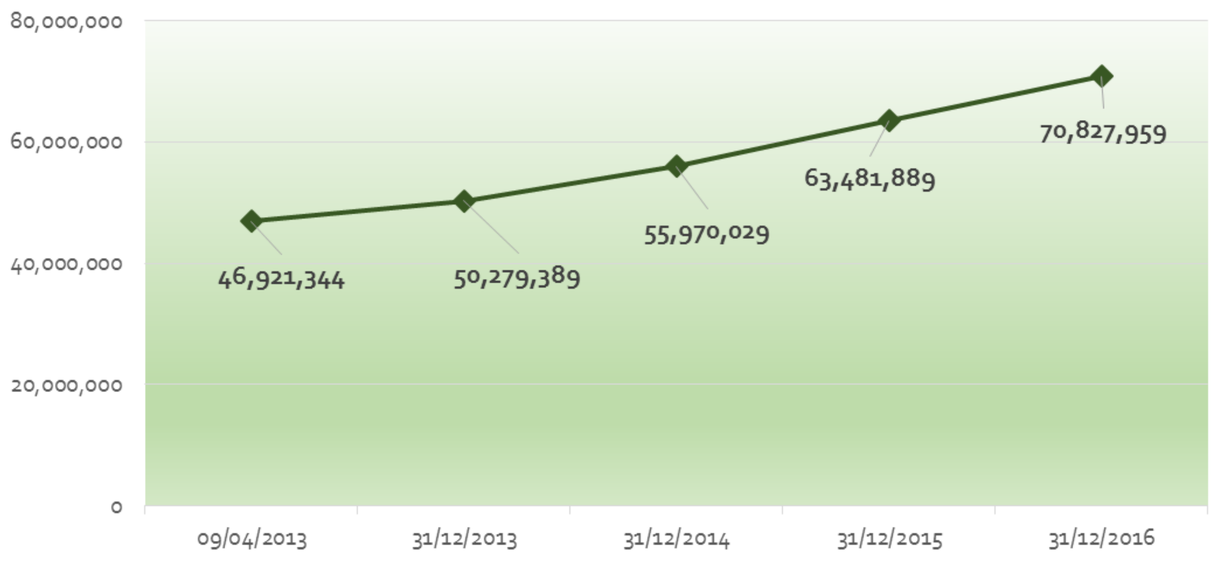
SIS II – the most used IT system in the area of freedom, justice and security in the EU – has been performing well during the reporting period. No critical incidents were reported. An increase in the usage in terms of data stored, searches performed and hits achieved is clearly visible.

Close cooperation with the Member States and the Commission has been instrumental for the Agency to ensure the operational management and proper evolution of Central SIS II during the reporting period. eu-LISA is implementing several SIS II projects, e.g. the AFIS, and others are in the planning stage, to be launched in the near future. The Agency remains strongly committed to maintaining the SIS II Central System in operation on a 24/7 basis.

The system will certainly evolve in the future because of various initiatives, including ongoing discussion and follow-up works with a view to considering interoperability with other systems. Furthermore, the new legislative proposals presented in December 2016 and currently under negotiation contain a series of measures aimed at maximising the effectiveness and efficiency of SIS II by technical enhancements, focusing on end-users and giving access to more national authorities and extending the access of EU agencies.

Annex

I. Graph: total number of alerts stored in the SIS II central database since 9 April 2013



II. Table: response time for CUD operations processed during the reporting period[111]

1/01/2015 - 31/12/2015			
Total CUD	Broadcasts < 3 min	Broadcasts 3-5 min	Broadcast > 5 min
20 742 738	19 804 242	119 030	819 466
	95.5%	0.57%	3.95%

1/01/2016 - 31/12/2016			
Total CUD	Broadcasts < 3 min	Broadcasts 3-5 min	Broadcast > 5 min
23 559 407	22 538 117	103 184	918 106
	95.7%	0.44%	3.90%

[111] Internal analysis concluded that broadcasts > 5 minutes were due to national systems being disconnected.

III. Table: response time for central searches during the reporting period

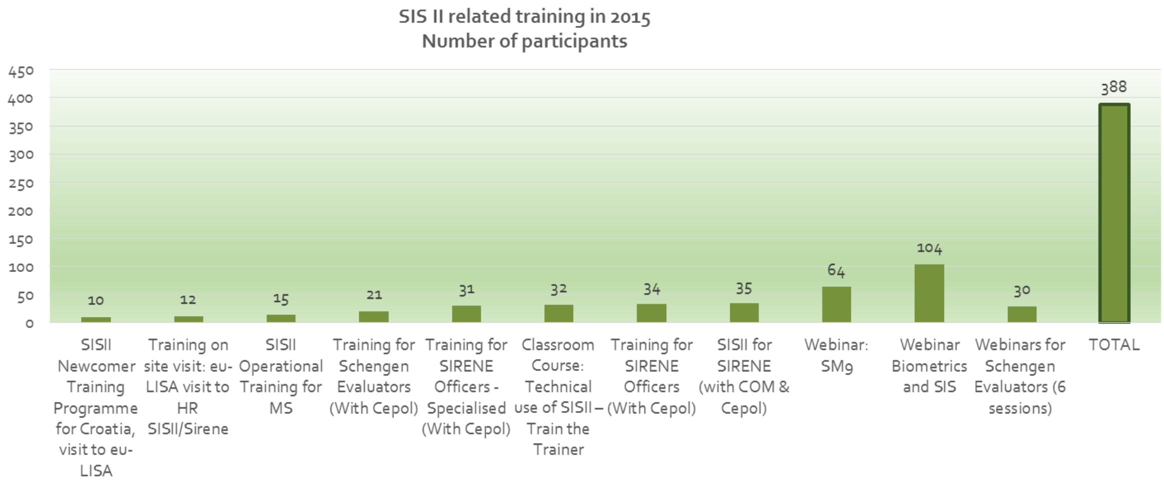
2015 Central searches - response time in seconds				
Type of search	Amount of search	Response ≤ 1 sec	Response > 1 sec, < 3 sec	Response > 3 sec
SLA1	166 328 075	99.78%	0.21%	0.01%
SLA1 - response ≤ 3 sec		**99.99%**		
All searches	281 415 738	99.82%	0.15%	0.03%
All searches - response ≤ 3 sec		**99.97%**		

2016 Central searches - response time in seconds				
Type of search	Amount of search	Response ≤ 1 sec	Response > 1 sec, < 3 sec	Response > 3 sec
SLA1	196 209 565	99.86%	0.08%	0.06%
SLA1 - response ≤ 3 sec		**99.94%**		
All searches	361 387 327	99.85%	0.07%	0.07%
All searches - response ≤ 3 sec		**99.93%**		

IV. Training activities

Training courses related to SIS II provided in 2015:

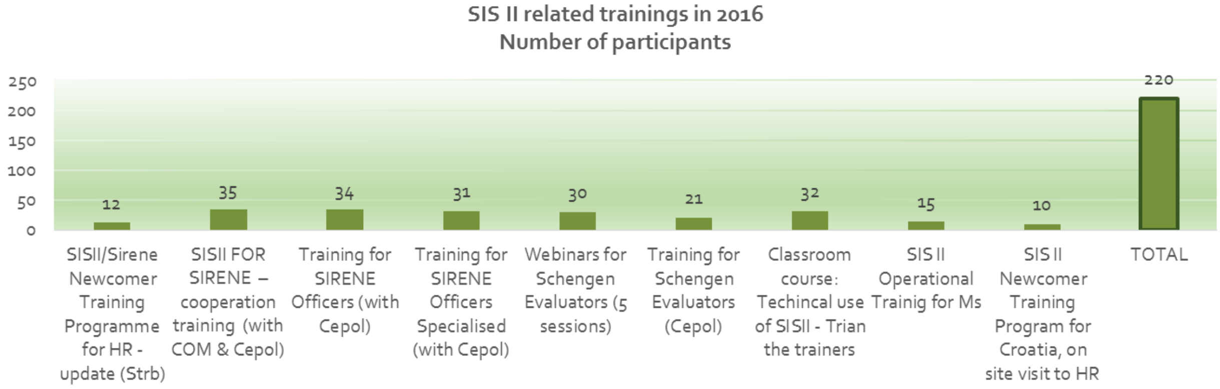
1. SIS II Newcomer Training Programme for Croatia – visit to eu-LISA
2. SIS II Newcomer Training Programme for Croatia – on-site visit to N.SIS/SIRENE Croatia by eu-LISA
3. SIS II operational training for MSs
4. Training for Schengen Evaluators (with CEPOL)
5. Training for SIRENE Officers – specialised (with CEPOL)
6. Classroom course: Technical use of SIS II – Train the trainer
7. Training for SIRENE Officers (with CEPOL)
8. SIS II for SIRENE (with Commission and CEPOL)
9. Webinar: ITSM tool HP Service Manager 9
10. Webinar: Biometrics and SIS
11. Webinar for Schengen Evaluators (six sessions)



Training courses related to SIS II provided in 2016:

1. SIS II/SIRENE Newcomer Training Programme for Croatia – update
2. SIS II for SIRENE (with Commission and CEPOL)
3. Training for SIRENE Officers (with CEPOL)
4. Training for SIRENE Officers – specialised (with CEPOL)
5. Webinar for Schengen Evaluators (LU, IT, EL, MT, FR)
6. Training for Schengen Evaluators: SIS/SIRENE (with CEPOL)
7. Classroom course: Technical use of SIS II – Train the trainer
8. Operational training for MSs – hands on, session I, session II
9. SIS II Newcomer Training Programme for Croatia – on-site visit

In addition, several workshops on change management were organised.



EL-AE-17-001-EN-N

ISBN 978-92-95208-58-2 ISSN 2443-8294 doi:10.2857/039227