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

June 2015

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 the 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 978-92-95203-92-1
ISSN 2443-8294
doi:10.2857/567010
Catalogue number: EL-AE-15-001-EN-N

Table of contents

Summary

SIS II is the largest information system for public security in Europe and represents the primary compensatory measure following the abolition of controls at the internal borders of the Schengen area. While SIS II entered into operation on 9 April 2013, eu-LISA took over its operational management from the European Commission on 8 May 2013 at the end of the intensive monitoring period following the system's entry into operations.

This report - pursuant to Article 50(4) of Regulation (EC) No 1987/2006[1] 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") as well as to Article 66(4) of Council Decision 2007/533/JHA[2] on the establishment, operation and use of the second generation SIS II (hereafter referred to as the "SIS II Decision") - describes the technical functioning of the Central SIS II and the Communication Infrastructure including the security thereof from the entry into operations on 9 April 2013 until 31 December 2014. Change management and releases deployed as well as operational and testing activities performed during the reporting period are also covered.

eu-LISA ensures the operational management of SIS II guaranteeing the continuous, uninterrupted exchange of data between national authorities 24 hours a day, 7 days a week. eu-LISA is also responsible for providing training for national SIS II operators and SIRENE staff and Schengen evaluators, in specific fields, publishing statistics as well as producing the list of authorities accessing the system on an annual basis. Moreover, eu-LISA is tasked with managing the accession of new Member States and organisations to SIS II.

The present report provides statistical data in relation to the bilateral and multilateral exchange of supplementary information between Member States[3], in particular the number of forms exchanged between SIRENE Bureaux and the total hits generated from positive checks on SIS alerts. From 9 April until 31 December 2013, the countries connected to the system reported having had 86,822 hits on foreign alerts[4]; in 2014 for the entire calendar year, there were a total of 127,935 hits on foreign alerts reported.

There was an increase in the overall usage of the system as per the statistical data gathered for 2013 and for 2014. Taking the average of hits generated in a 30-day period, in 2014 the reported hits on foreign alerts – compared to data available for 2013 - increased on average by 7.8%. Using the same approach of the 30-day period, in 2014 the outgoing forms increased on average by 10% and the incoming forms on average by 19%.

The overall availability and performance of SIS II throughout the reporting period was excellent[5]; the few related incidents were properly managed following IT Service Management international standards minimising the operational impact.

Due to recent events impacting the EU's internal security, SIS II has been recognised as a key instrument in the fight against terrorism and its usage can be significantly enhanced. eu-LISA has reacted to the emerging threats by swiftly implementing critical changes to the Central SIS II, in cooperation with the countries connected to the system and the European Commission. The recent evolution of the system has shown that SIS II is an adaptable tool, which supports information exchange in the field of counter-terrorism.

[1] OJ L381, 28.12.2006, p. 4. It constitutes the legislative basis for governing SIS II with respect to matters falling under Title IV of the Treaty establishing the European Community (former first pillar).
[2] OJ L 205, 7.8.2007, p. 63. It represents the necessary legislative basis for governing SIS II for matters falling under Title VI of the Treaty on European Union (former third pillar).
[3] Under 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 connected to SIS II are: Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. The United Kingdom connected to SIS II on 13 April 2015. Associated Countries connected to SIS II are: Iceland, Liechtenstein, Norway and Switzerland.
[4] For more information, see the section on Exchange of supplementary information between Member States.
[5] For more details, see section on Availability and performance.

1. Introduction

The Schengen Information System[6], in both its first and second generation, has since its establishment been the main compensatory measure for the abolition of internal border checks in the Schengen area. The system plays an important role in ensuring a high level of security within the area of freedom, security and justice of the EU through maintaining and safeguarding security in the Member States, as well as facilitating the free movement of people within the Schengen area.

SIS II allows competent national authorities to issue and consult alerts[7] on persons who may have been involved in a serious crime or may not have the right to enter or stay in the Schengen area. It also contains alerts on missing persons, in particular children, as well as information on certain property, such as banknotes, aircraft, boats, cars, vans, containers, firearms and identity documents, that may have been stolen, misappropriated or lost.

Article 3(a) of Regulation (EU) No 1077/2011[8] establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereafter referred to as the "Agency" or eu-LISA) states that in relation to SIS II, the Agency shall perform the tasks conferred on the Management Authority by Regulation (EC) No 1987/2006 and Decision 2007/533/JHA, the two legal instruments[9] on the establishment, operation and use of SIS II.

SIS II was developed under the supervision of the Commission in cooperation with the Member States and entered into operations on 9 April 2013, replacing SIS1+ which was operated under inter-governmental arrangements. The central section of SIS 1+ was managed by France on behalf of the Member States. The migration of data from SIS 1+ to SIS II took place prior to the entry into operation which was followed by a switchover of the national applications from SIS 1+ to SIS II on 9 April 2013. During an intensive monitoring period of 30 days both SIS 1+ and SIS II co-existed and remained synchronised via a convertor which allowed the conversion of data in both directions. At the end of the intensive monitoring period, SIS 1+ and the convertor were turned off and only SIS II continued to operate. Since 8 May 2013 eu-LISA has ensured the 24/7 operational management of SIS II.

SIS II has enhanced functionalities compared to its predecessor, such as the possibility to enter biometrics (fingerprints and photographs), new types of objects (stolen aircraft, boats, containers, means of payment), as well as the possibility to link[10] different alerts (such as an alert on a person and a vehicle). SIS II contains copies of European Arrest Warrants (EAW) attached directly to alerts for persons wanted for arrest for the purposes of surrender or extradition.

SIS II is a hit/no hit system based upon searches, where a hit[11] can be achieved when a search reveals an alert and further actions are requested. An alert consists of the data as described in Article 20 Regulation (EC) No 1987/2006 and Decision 2007/533/JHA. At the end of the reporting period (31 December 2014), the system contained almost 56 million[12] alerts, which makes it the largest database for public security in Europe. In 2014

[6] The first generation of the Schengen Information System became operational in 1995. Different evolutions were performed on the system through the years - the main ones being SIS 1+ and SISone4all – mainly to allow the connection of new countries joining the Schengen area.
[7] In SIS II an alert represents a set of data entered into the system that allows competent authorities to identify a person or an object with a view to taking specific action.
[8] OJ L286, 1.11.2011
[9] Together with the Regulation (EC) NO 1986/2006 regarding access to SIS II by the services in the MS responsible for issuing vehicle registration certificates, OJ L 381, 28.12.2006
[10] For the same owner of the alerts.
[11] As per the SIRENE Manual a hit occurs in SIS II when all the following criteria are met: i) a search is conducted by a user; ii) the search reveals a foreign alert in SIS II; iii) data concerning the alert in SIS II matches the search data; iv) further actions are requested as a result of the hit.
[12] On 31 December 2014, SIS II contained 55.97 million records.

the number of alerts increased by over 11% compared to the number of alerts available in the system on 31 December 2013, when there were over 50 million alerts. Since the entry into operation on 9 April 2013, when there were almost 47 million alerts, the increase was over 19%[13].

Access to SIS II data is limited to national border control, police, customs, judicial, immigration authorities and vehicle registration services. These authorities may only access the SIS II data that they need for the specific performance of their tasks. Europol[14] and Eurojust[15] have the right to access and directly search data in SIS II that is related to their mandates.

At the end of the reporting period, the Member States[16] of the EU connected to SIS II were Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. The United Kingdom successfully joined SIS II on 13 April 2015 following extensive technical preparations and tests performed by eu-LISA together with the Member States during the reporting period. Associated Countries connected to SIS II were Iceland, Norway, Switzerland and Liechtenstein.

A consolidated list of Member States` competent authorities specifying, for each authority, which data it may search and for what purposes, is published annually in the Official Journal[17] of the EU pursuant to Article 31(8) of the SIS II Regulation and Article 46(8) of the SIS II Decision.

1.1 Legal bases and scope of the report

In accordance with Article 50(4) of the SIS II Regulation and Article 66(4) of the SIS II Decision, the Management Authority (eu-LISA) hereby submits to the European Parliament and the Council 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 two years after SIS II is brought into operation.

The reporting period covered in the report is from entry into operations of SIS II on 9 April 2013 until 31 December 2014. The report was drafted with information available at central level (operational activities, change management, releases, test activities, availability and performance) together with statistical data provided by Member States in the framework of the annual statistics exercise.

This report, the first of its type for Central SIS II, should be read in conjunction with the published annual statistics and the list of competent authorities authorised to access and search the data contained in SIS II. The report aims to support the goals of enhanced transparency and visibility sought by the SIS II legislator compared with the previous reporting provisions.

1.2 Governance

eu-LISA's administrative and management structure stems from Article 11 of the Agency's establishing Regulation[18]. Member States' delegates together with representatives from the Commission sit in the

[13] For more details, see the SIS II statistics annually published by eu-LISA pursuant to Article 50(3) of SIS II Regulation and Article 66(3) of the SIS II Decision.
In June 2014, eu-LISA published "*SIS II – 2013 statistics*" available here http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx
In March 2015, eu-LISA published "*SIS II - 2014 statistics*" available here http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx
[14] As defined in Articles 41 and 43 of the SIS II Decision. Europol was connected to SIS II on 10 December 2014.
[15] As defined in Articles 42 and 43 of the SIS II Decision. Eurojust was connected to SIS II on 09 April 2013.
[16] The authorities of Ireland, Cyprus and Croatia are currently preparing for technical connection to SIS II.
[17] OJ C 278, 22.08.2014.

Management Board (MB) as well as in three Advisory Groups (AGs), one for each system managed by the Agency. As per Article 19(1) of eu-LISA Regulation, the role of SIS II AG is to provide the MB with expertise related to SIS II.

By the end of the reporting period, the SIS II AG had been convened ten times, for the first time in June 2012 by the Commission and for the following meetings in 2013 and 2014[19] by the Agency. The SIS II AG met regularly, providing relevant technical support and advice to the Agency's MB concerning a number of technical matters relating to operations, evolution and further development of Central SIS II. The SIS II AG has been instrumental in developing and overseeing the implementation of a number of business-critical processes such as the establishment of the Change Management Process as well as discussing technical matters such as data quality, Data Consistency Checks and the implementation of statistical reports.

Member States` experts are also the main drivers in several groups and fora supporting the work of the Agency and the Advisory Group to guide specific matters or to elaborate proposals impacting SIS II, for example the Change Management Group, the National Contact Points for Training (NCP), the Security Officers Network (SON) and the working group on statistics.

In terms of SIS II governance, the Commission retains responsibility for any legislative initiatives linked to the system as well as the implementation of the SIS II legal framework, assisted by a Committee[20] - SISVIS Committee bringing together representatives of the Member States.

2. Operational management of Central SIS II

eu-LISA has been responsible for the operational management of the Central SIS II since 8 May 2013 ensuring uninterrupted access to the system 24 hours a day, 7 days a week, to allow the continuous exchange of data between national authorities, in accordance with the legal provisions. The operational management is achieved, in a large part, 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 two different contractors due to the fact that the first Maintenance in Working Order (MWO) framework contract[21] expired on 31 July 2014 and was replaced by a second contract[22] signed on 13 March 2014. On 1 August 2014, following a hand-over phase of four months, the new MWO contractor took over the external support.

The new MWO contract was awarded by eu-LISA following a restricted procedure which was launched in December 2012 by DG HOME[23] and was completed by eu-LISA in December 2013. The MWO contract entered into force on 1 April 2014 with the activation of the first work package on acquisition of knowledge and the setting up of the environments. As of 1 August 2014 the majority of the work packages[24] of the MWO contract were activated including: corrective maintenance, adaptive maintenance, evolutionary maintenance, support

[18] Regulation (EU) No 1077/2011, OJ L286, 1.11.2011.
[19] Meetings were organised in April, May, June, September and November 2013 as well as in February, May, September and December 2014.
[20] A committee as per Article 51 of the SIS II Regulation and parallel provision in Article 67 of the SIS II Decision.
[21] The MWO framework contract expired in July 2014 was operated by HP and Steria.
[22] ATOS in consortium with Accenture and HP.
[23] The restricted procedure was launched before eu-LISA reached financial independence.
[24] A final work package, to be activated at the very end of the contract, covers the so-called 'reversibility' (i.e. hand-over to a new contractor).

to Member States testing, technical assistance and training. The initial duration of the contract is three years with the possibility of extension for one more year[25].

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

2.1 Description and functioning of the technical infrastructure of Central SIS II

The architecture of the SIS II is defined in common Articles 4 of the SIS II Decision and the SIS II Regulation. The Schengen Information System is composed of:

- a central system (Central SIS II);
- a national system (N.SIS II) in each of the Member States, consisting of the national data systems which communicate with Central SIS II;
- a communication infrastructure between CS-SIS (technical support function with the database) and NI-SIS (national interface) that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux[26].

The Central SIS II has a technical infrastructure which is composed of:

- a technical support function (CS-SIS) containing the database, that contains alerts sent to the CS-SIS by all countries connected to SIS II;
- a uniform national interface (NI-SIS), a uniform means used to exchange alerts within the Schengen architecture.

The Central SIS II communicates with national systems - the N.SIS II in each of the countries connected to SIS II - through a secure communication infrastructure, used to provide online services such as searches and creation/update/deletion (CUDs) of alerts.

Although the Central SIS II is the repository of all SIS II alerts, countries connected to SIS II have the possibility to have a national copy – a full or partial copy - of the Central SIS II database which they can use for carrying out automated searches in their territory. Member States without a national copy, and therefore querying only the central system, are Denmark, Finland, Liechtenstein, Norway and Slovenia.

Searches carried out in SIS II can be performed in the SIS II Central database or in the national copy that a Member State may have. However in both cases, the searches have to provide an equivalent result in line with Article 9(2) of the SIS II legal instruments. Countries having a national copy may also carry out searches in the Central SIS II, depending on which type of SIS II services they have subscribed to[27].

Alerts are created and managed by Member States. CUDs of alerts are sent by the N.SIS II to the Central SIS II.

---

[25] More information on the contract is available at the following link http://ted.europa.eu/udl?uri=TED:NOTICE:123203-2014:TEXT:EN:HTML For more information on eu-LISA resources devoted to SIS II, see corporate reports published annually by the Agency available at the following link http://www.eulisa.europa.eu/Publications/p_corporate/Pages/default.aspx.

[26] As per common Article 7(2) of SIS II legal instruments a SIRENE (Supplementary Information Request at the National Entries) Bureau is the designated authority, in each Member State, which shall ensure the exchange of all supplementary information.

[27] Member States with a national copy which have subscribed for certain type of queries to use the services of the central system are Austria, Czech Republic, Greece, Hungary, Iceland, Luxembourg, the Netherlands, Poland, Romania, Sweden and Slovakia.

After technical checks, the CS-SIS - within a maximum time of three minutes - broadcasts the alerts to all N.SIS II with a national copy or sends a notification to countries which do not have national copy.

The Central SIS II system provides functionalities for ensuring synchronisation and consistency of national copies as well as their restoration should this be necessary.

In order to maintain national copies consistent with CS each change of alert in CS is followed by a broadcast sent to all Member States having a national copy. Upon receipt of the broadcast[28] the Member States have to update their national copy with the broadcast content. Member States without national copy do not receive broadcasts except if they issued the CUD and this, to confirm that the operation has been successfully completed. The process "Data Consistency Check (DCC)" verifies that all broadcasts are applied correctly in each national copy and in case of discrepancies, the DCC process fixes them.

The central system also issues notifications in specific situation such as creation/modification of alerts on persons and flags[29], prior alert expiration and for deletion note[30].

The Central SISII architecture is supported by two data centres in different locations:

- the technical support function (Central Unit – CU) located in Strasbourg (France) for the technical supervision and administration of the CS-SIS;
- the back-up site located in Sankt Johann im Pongau (Austria) which ensures all the functionalities of the principal CS-SIS in the event of failure or planned maintenance of the system (Back-up Central Unit - BCU).

This allows redundancy through real time data copying between the two sites. During the reporting period, the switchover from the CU to the BCU occurred four times, always in conjunction with one of the releases[31]. The average time for a switchover is approximately 20 minutes, a bit longer if in conjunction with deployment/release activities.

For the purpose of maintaining the Central SIS II and the national systems' N.SIS II in operational conditions, there are also various technical environments at the technical support site including pre-production, testing, and "playground", used for training as well, available to all Member States.

2.2 Reporting and statistics

At the time of the entry into operations SIS II had only a limited statistics and reporting module embedded. Thanks to common efforts of the Commission, Member States and eu-LISA a working group was setup in summer 2013 to collect and define further requirements, and to submit proposals for the implementation of new statistical reports to the Advisory Group.

An impact assessment was carried out on the development and the contractor was consulted on the technical feasibility. Further to this a set of daily statistics was designed, built internally by eu-LISA and made available to Member States at the end of 2013. Work on this topic continued and will continue among others to address

[28] Broadcast are essential to keep national copies up to date as they notify the users with national copy that changes have been performed in the central database.
[29] A flag is a suspension of validity at the national level that may be added to alerts for arrest, alerts on missing persons and alerts for checks where a Member State considers that to give effect to an alert is incompatible with its national law, its international obligations or essential national interests. When the alert is flagged, the requested action on the basis of the alert shall not be taken on the territory of this Member State.
[30] The purpose of deletion note notification is to allow a user who could not create an alert due to a compatibility conflict with another alert, to receive a notification indicating that the conflict alert has been deleted. Having received this information the user may then retry the operation to create the alert.
[31] For more details, see the section on Change management and releases.

statistics reporting. Meanwhile, a number of enhanced reports were delivered to Member States from August 2014 onward on regular statistics.

At present a large number of statistics on the business usage of the system – for example data regarding the number of requests, valid and expired alerts, number of alerts on persons, number of alerts on vehicles – are periodically produced by the central system and made available to the stakeholders via a dedicated web platform. The central system can also produce pre-defined reports on demand, following a request from a Member State. These reports are only accessible to the requesting country.

Pursuant to Article 50(3) of SIS II Regulation and Article 66(3) of the SIS II Decision, eu-LISA annually collects statistics from Member States and together with data available at central level publishes[32] 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.

2.3 Monitoring and operational activities

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

- A 24/7/365 monitoring régime by the eu-LISA Service Desk is active and enables event-triggered incident 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[33] for each Member State[34] connected to SIS II;
- The operational status of the exchange between the central system and the national copies (also known as 'the bridge') is continuously monitored. Any system unavailability is reported and escalated on a 24/7/365 basis.

The eu-LISA Service Desk is the service entry point where a user reports an incident[35] or requests a service. Any request or incident is registered in a central incident management tool for follow-up. Based on the initial diagnosis[36] the relevant assistance is provided or functional and/or hierarchical escalation is triggered.

The Service Desk of eu-LISA is operative 24 hours a day, seven days a week.

The eu-LISA technical function is the specialist team that further analyses, investigates and resolves incidents. The eu-LISA technical function consists of Application Administrators, System Administrators and Network Administrators, together with Security Officers and other experts if necessary. The eu-LISA Service Desk recorded 1352 user requests (including incidents, requests for information, etc.) related to SIS II during the reporting period. The incident management process is under the supervision of the Incident Manager who orchestrates the involvement of incident support staff (first- and second-line), monitors the effectiveness of incident management and makes recommendations for improvement.

[32] See foot note 11 above.
[33] Queue for a country (as well as organisation) connected to SIS II is represented by the activity performed against the central system. The activities performed against the central system can vary a lot between countries. It depends on whether a country has a full or partial national copy as well as on which type of SIS II services the country has subscribed to.
[34] As well as organisations connected to the system.
[35] An incident is opened by the service desk following an exchange/interaction with Member States or following eu-LISA monitoring activities (abnormal observations).
[36] Impact, urgency and priority of the incident are defined at this first stage. All long the process, eu-LISA technical staff reviews the status and priority assessing the severity of the incident.

eu-LISA has defined and implemented IT Service Management (ITSM) processes following international standards[37] to assure quality of service and an incident management policy is in place.

Incident management is one of the activities carried out by the service desk together with operational tasks. Data Consistency Checks[38] (DCC) are part of the eu-LISA daily operational tasks. Each national copy is checked monthly for consistency with the central system. Any anomaly is reported for investigation. Over 500 DCCs were successfully performed since the entry into operations of SIS II. A DCC can be triggered by eu-LISA (part of the monthly planned campaigns) or by the relevant country in case of need.

Two technical workshops[39] on DCC were convened as a result of persisting high number of discrepancies[40] and so called "false positives" reported by some Member States during the monthly DCC campaign. The aim of the workshops[41], as mandated by the Advisory Group, was to undertake the necessary actions to achieve zero discrepancies. Additionally a note explaining the maintenance of national copies in terms of links[42] was presented together with an enhanced operations report[43] to be used. Thanks to all activities performed, the number of countries with high number of real discrepancies was significantly reduced by end of 2014. Activities and efforts in this respect will continue in the future.

An Operator Manual (OPM)[44] which describes and regulates all communication exchanges and procedures applied is in use by all Single Point of Contacts (SPoCs) at central level as well as at national level. Different communication channels (functional mailboxes, video/audio conference, dedicated platforms) between eu-LISA and the Member States are available and can be used depending on the scope and recipients of the messages.

In the second half of 2014, eu-LISA together with Member States and the Commission launched a process to update the OPM as well as the relevant escalation procedure. The aim of the exercise was to enhance the manual and the procedure making sure that they are in line with the needs of all stakeholders.

A workshop was organised in October 2014 with the participation of 19 Member States together with the Commission. Further to this the revised SIS II OPM together with the new escalation procedure were approved by the SIS II Advisory Group in March 2015 and have been applied since the beginning of April 2015.

The main enhancements of the revised OPM were the introduction of a SPoC communication architecture to highlight clearly the separation between "Operation" and "Business" related communication; description of the life cycle of a ticket allowing a common understanding of ticket-handling; clearly defined requirements for staff working in the SPoC[45].

In addition to that a few templates were also introduced i.e. bridge re-start templates[46] and DCC follow-up templates for a common understanding and a quicker handling of the tickets.

---

[37] eu-LISA follows Information Technology Infrastructure Library (ITILv3) best practices.
[38] Data Consistency Check is an exercise run to support Member States to achieve the technical compliance as requested by Article 9(2) of the SIS II Decision and parallel provision in Article 9(2) of the SIS II Regulation.
[39] In May and November 2014.
[40] The real discrepancies represent severe legal consequences as they could result in missed hits.
[41] The workshops run by eu-LISA together with the contractor supported Member States in better understanding the synchronization and data consistency check mechanism in SIS II.
[42] Links are slightly different from other entities and may cause a number of discrepancies, thus the need for a technical note.
[43] The new report identifies only real (actual) discrepancies and not false positives.
[44] The Operator Manual is the reference document in use by all SPoCs at central level as well as at national level in the frame of the operational environment communication. Aims of the Manual are: i) to describe defined and approved procedures; ii) to provide a basic level of common working language guaranteeing the communication between the SIS II stakeholders.
[45] Examples of requirements for staff working in the SPoC are: English identified as the working language and required a minimum level of B2; ability to assess the severity and urgency of incidents/interactions; access to national supervision tools including national networks.
[46] The SISII Bridge restart is needed for re-connection from CS to the Member States or vice-versa, in case of disconnection or maintenance.

2.4 Change management and releases

eu-LISA is tasked with managing the evolution of SIS II, technologically and functionally, in order to ensure that the system utilises state-of-the-art technologies and fulfils Member States` needs while safeguarding compliance with the legal instruments. All change requests[47] follow a defined Change Management Process (ChMP) in a uniform manner, equally applying to all systems under eu-LISA's responsibility.

eu-LISA has adopted a standardised change management process in order to guarantee the application of a common process in line with international standards for the applications used by Member States. The principles underlying the process aim to guarantee the stability of the system, ensuring that any change is supported by Member States and changes in the central system and the national systems are implemented in a coordinated manner.

The ChMP is carried out with the involvement of several stakeholders from the technical side, the business side but also the decision makers and thus posing additional complexity and challenges. Proper coordination is sought and required for successful implementation among the Member States` representatives from different levels, the Change Management Group, the Change Management Board, eu-LISA staff and the SISVIS Committee.

eu-LISA is responsible for discussing and formalising change requests related to the central system and ensuring agreement with Member States for all changes having an impact on national systems (impacting the ICD[48]). In case changes have an impact on SIS II legal instruments or ICD, eu-LISA has to inform the SISVIS Committee chaired by the Commission. The Commission, with the assistance of the Committee, takes the final decision on the change requests making use of the recommendations of the Agency.

During the testing period prior to the entry into operations of SIS II, several issues were reported by Member States, which were registered by the Commission for future assessment. A total of 43 change requests were registered and handed over to eu-LISA. Following the entry into operations of SIS II, eu-LISA analysed and produced detailed impact assessments[49] to plan for their implementation.

During the reporting period several SIS II releases were deployed:

- On 18 July 2013 release 7.1.6.3 was deployed; among other aspects, changes were related to the time standard used, compliance of notifications, broadcast in relation of the creation of binary and transliteration rules. eu-LISA deployed the new central system release with a Central Unit – Backup Central Unit (CU-BCU) switch-over and switch-back;
- On 4 December 2013, eu-LISA managed a Central SIS II technical release to allow for technical maintenance; eu-LISA deployed the central system release with a CU-BCU switch-over and switch-back;
- On 19 February 2014, SIS II Release 7.2.0 was deployed in the central system; among other aspects, changes were related to flags, binary broadcasts and multiple compatible alerts. eu-LISA deployed the central system release with a CU-BCU switch-over and switch-back;

[47] A change is any modification to the existing system or deliverable already approved by Member States, including the addition, removal, or replacement of any component of the system.
[48] The Interface Control Document (ICD) defines in detail the interface between the Central SIS II and each national system. The document gathers the technical specifications of the system-to-system interactions in terms of data items and messages passed, protocols used as well as timing and sequencing of events.
[49] The impact assessment covers technical, financial and legal implications of each change request.

- On 23 June 2014 SIS II Release 7.3.0 was installed in the central system; changes related to the abbreviated entry search tool (KenoKey support) and to standard queries. eu-LISA deployed the central system release with a CU-BCU switch-over and switch-back;
- On 15 October 2014 a set of updated SIS II code tables was implemented in the central system.

During the second semester of 2014, urgent technical changes related to recommendations in the context of counter-terrorism were endorsed by the SISVIS Committee and planning for implementation was initiated by eu-LISA in the very short term. The changes related to relevant codes tables, definition of new business rules and the check on compatibility of alerts. In practice, the changes allow the authorities having access to the system to trigger immediate actions towards the appropriate SIRENE Bureau as well as the display of the invalidated travel documents which should be seized..

Following the ChMP, these urgent changes were assessed, designed, tested and successfully implemented in the central system and at national level in the course of 2015, revealing great and coordinated efforts from all stakeholders involved.

Preparations started at the end of 2014 to accommodate a change request related to the incompatibility rules and the UK integration[50]. The change request – aimed at ensuring the overall coherence of SIS II due to the fact that the UK is taking part only in some of the provisions of the Schengen *acquis* - will be implemented in the course of 2015.

2.5 Test activities

2.5.1 Internal Testing

As for any major information system, the central system of SIS II has to undergo regular system maintenance to ensure its continuous smooth operation. It is the role of the eu-LISA internal test team to ensure that the corrective, adaptive and evolutionary maintenance does not adversely affect the system.

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

Extensive tests, both functional and non-functional, are conducted prior to a release being put into production. Functional testing is the type of testing done against the business requirements of the application and it verifies compliance with all business and use-cases of the system. Non-functional tests are done 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 guarantee that the impact on on-going business is as minor as possible.

[50] SIS II generates an automatic notification – following the compatibility rules as per the SIRENE Manual - if a Member State inserts an alert which is not compatible with an existing one. The system allows, however, the insertion of such alert as it is for the countries to solve the incompatibility bilaterally and withdraw the alert. Due to the fact that UK does not participate in the SIS II Regulation, it is necessary to ensure the overall coherence of SIS II and thus notify the UK about an incompatible Article 24 alert. This does not mean that the UK would see, would be able to search or act upon Article 24 alerts, but shall receive a notification to allow an early communication with the other issuing country to resolve the incompatibility issue before a second alert is inserted into SIS II on the same data subject.

2.5.2 Testing with Member States and Europol

eu-LISA, exercising its role as the Management Authority for SIS II, is also responsible for coordinating tests, determining test requirements and planning, covering integrating countries and new or substantially-changing national systems. Member States assist eu-LISA in the overall performance of all tasks related to test execution.

In 2014 the need was identified to codify the testing requirements for new countries integrating into SIS II or Member States significantly changing their national systems. eu-LISA supported the Commission in the preparation of an Implementing Decision on this matter. The Commission Implementing Decision was adopted on 16 March 2015[51].

The results of tests executed by countries and organisations connected to SIS II receive, after endorsement by the SIS II Advisory Group, the final endorsement of the SISVIS Committee.

The major test campaigns performed in the reporting period are listed below.

2.5.2.1 The United Kingdom

Between January and October 2014, eu-LISA and the test team from the UK Home Office, along with teams from all other existing users of the SIS II, conducted extensive test campaigns to ensure that the UK national SIS II system was compliant with the technical specifications governing the functioning of the SIS II. Further attention was given to the technical compliance of the implementation by the UK authorities of the SIRENE workflow system, allowing the exchange of supplementary information between Member States. These tests came to a positive end in the month of October 2014.

The UK successfully joined the SIS II and inserted its first alert on 13 April 2015, based on the related Council Implementing Decision[52].

2.5.2.3 Italy

Between January and April 2014, eu-LISA and the test team from the Italian Ministry of the Interior conducted extensive tests to ensure that the Italian national SIS, modified upon a request from the Italian Data Protection Authority, was compliant with the technical specifications governing the functioning of the SIS II. The test campaigns ended successfully in April 2014 and the modified Italian system was put into operation in the course of the second quarter of 2014.

2.5.2.4 Poland

Between April and August 2014, eu-LISA and the test team from the Polish Ministry of the Interior conducted extensive tests to ensure that the new Polish N.SIS, launched upon their own request and intended to significantly reduce searches in the central system, was compliant with the technical specifications governing the functioning of the SIS II. The test campaigns ended successfully in August 2014 and the new Polish N.SIS was put into operation in the course of the fourth quarter 2014.

2.5.2.5 Switzerland

[51] Commission Implementing Decision (EU) 2015/450 of 16 March 2015 laying down test requirements for Member States integrating into the second generation Schengen Information System (SIS II) or changing substantially their directly related national systems (notified under document C(2015) 1612), published on OJ L 74, 18.3.2015, p. 31.

[52] Council Implementing Decision (EU) 2015/215 of 10 February 2015 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of parts of the provisions of the Schengen acquis on the Schengen Information System for the United Kingdom of Great Britain and Northern Ireland, published on OJ L 36, 12.2.2015, p. 8.

In September and October 2014, eu-LISA and the test team from the Swiss Ministry of the Interior conducted extensive tests to ensure that changes associated with the maintenance of the national system envisaged by Switzerland, were compliant with the technical specifications governing the functioning of the SIS II. The test campaigns ended successfully for Switzerland in November 2014 and the updated system was put into operation at the time of drafting this report, in February 2015.

2.5.2.6 Europol

In September and October 2014, eu-LISA and the test team from Europol conducted extensive tests to ensure that the system used by Europol to perform searches in the SIS II concerning alerts issued in accordance with Articles 26, 36 and 38 of the SIS II Decision was compliant with the technical specifications governing the functioning of the SIS II. The test campaigns ended successfully in October 2014.

Europol performed its first search in the Central SIS II on 10 December 2014.

2.5.2.7 Croatia

Since September 2014 eu-LISA, has been in contact with various authorities of the Republic of Croatia in order to prepare their integration into SIS II. The main focus is on ensuring the proper functioning of both the SIS II central system and the national system, much like the integration process just finalised for the UK (see above 2.5.2.1).

This activity is currently in its inception stage and will see changes being brought to the central system in the second half of 2015 in order to prepare the central system for the arrival of a new country. Further to this activity, all necessary test plans, training maps and changes to the legal instruments will be developed and/or implemented in 2015.

2.5.3 SIRENE testing

The SIRENE tests aim at validating 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 the Central SIS II. Those tests address the functioning of the national SIRENE workflow system and the exchange of information between the SIRENE Bureaux[53] using this system, entering, modifying, flagging and deleting corresponding alerts in SIS II and attaching/detaching relevant additional information to SIS II alerts.

2.5.3.1 The United Kingdom

In June 2014, eu-LISA organised and executed with the assistance of experts from Member States, SIRENE tests in the UK. During those tests both the communication infrastructure as well as the SIRENE business process flow - encompassing the exchange of SIRENE forms and SIRENE specific actions towards SIS II - were successfully tested.

2.5.3.2 Finland

In parallel with the SIRENE tests run with the UK in June 2014, eu-LISA also coordinated and executed SIRENE tests with Finland and this to validate the new Finnish SIRENE workflow application. The tests were completed successfully.

2.5.3.3 Poland

[53] Through forms sent via the SIRENE Mail infrastructure according to the specifications provided for in the SIRENE Manual.

In March 2015, eu-LISA assisted by experts from Member States also executed SIS/SIRENE tests with Poland. The purpose of the SIS/SIRENE Functional Tests was 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.

2.6 Training activities

The mandate of eu-LISA in providing training in relation to SIS II is based on the eu-LISA Regulation, where training topics and target groups are specified in:

- Preamble, recital 11: the Agency should perform tasks relating to training on the technical use of SIS II[54];
- Article 3(b)[55]: 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

In addition of 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 SPoC, as well as ensuring data consistency and synchronisation.

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

2.6.1 2013 training activities

The first eu-LISA Training Strategy 2013-2016 was adopted by the Management Board in December 2013.

In 2013, training activities delivered by eu-LISA included classroom courses and webinars organised in cooperation with CEPOL[56], the Commission and Member States experts. Training modules focused on the entry into operations of SIS II, SIS II new functionalities, the SIRENE Manual, the architecture of the SIS II central system as well as the role and tasks of eu-LISA. A classroom course for the pre-launch of SIS II was organised in March 2013 in the UK, while a post-launch of SIS II classroom course was held in Italy in May 2013. In addition to that, webinars were organised in March for the pre-launch of SIS II, in May for the post-launch of SIS II, and in June for the SIRENE Bureaux.

eu-LISA participated in training for SIRENE officers organised by CEPOL, namely the Training for SIRENE Officers - Basic level held in September in Münster (Germany) and the Training for SIRENE Officers - Advanced level organised in October in Riga (Latvia).

In the framework of the Schengen evaluation missions, eu-LISA organised a series of webinars that were delivered to designated Schengen evaluators prior to the missions to the countries to be evaluated. At the end of 2013, a questionnaire on the training needs of the relevant national authorities for 2014 was sent to the Member States. Input received was used to develop and carry out the training activities in 2014, as indicated in the 2014 training plan.

[54] As well as of VIS and Eurodac and other large-scale IT systems (which might be entrusted to the Agency in the future).
[55] For the sake of completeness, it may be noted that Article 4(b) of the eu-LISA Regulation reads: The Agency shall perform tasks relating to training on the technical use of VIS. And Article 5(c): In relation to Eurodac, the Agency shall perform tasks relating to training on the technical use of Eurodac.
[56] The European Police College.

2.6.2 2014 training activities

In 2014, eu-LISA was engaged with the Member States joining SIS II. Training activities in this respect comprised:

- preparation and delivery of SIS II newcomer training for the UK (SIS II and SIRENE sessions),
- preparation of a newcomer training programme for Croatia (SIS II and SIRENE[57]).

Training programmes for newcomers are focused on architecture, business and technical aspects of SIS II and are delivered through various methods (e.g. e-learning, lectures, study visits, webinars).

Following identified operational needs, two ad hoc technical workshops on Data Consistency Checks were organised in Strasbourg (France) in May and November 2014. The objective of this activity was to achieve, together with the countries connected to the system, zero discrepancy between national copies and the Central SIS II database.

In 2014 for the first time, eu-LISA delivered three classroom courses on the technical use of large-scale IT systems[58]. The training on SIS II took place on 13-14 November in Strasbourg (France) and was attended by representatives of 21 Member States. The course was addressed to IT operators responsible for managing SIS II at national level and focused on the technical aspects of the system such as change management, communication tools and the Operator Manual. The classroom course had a train-the-trainer module to facilitate the transfer at national level of the obtained knowledge.

A total of 166 staff from 28 countries[59] followed SIS II training activities organised by eu-LISA in 2014. The average participants' satisfaction for the training activities organised in 2014 was 4.6[60] in a scale of 1 to 5.

Cooperation with CEPOL continued in 2014 and resulted, among other activities, in eu-LISA contributing to training for SIRENE officers organised by CEPOL. eu-LISA delivered modules on eu-LISA`s role and tasks; SIS II architecture; as well as a specific module on SIS II statistics. In 2014 two sessions were delivered: a Basic SIRENE course in February in Tampere (Finland) and an Advanced SIRENE course in September in Lyon (France).

In 2014 eu-LISA was also involved in the delivery of the CEPOL course on Schengen Evaluation with modules about the Agency`s role, a SIS II introduction and SIS II statistics. The training, organised in June 2014 in Slovakia, targeted future evaluators of Schengen Evaluation missions (police cooperation and SIS II/SIRENE). As in 2013, also in 2014 the designated Schengen evaluators had the possibility to follow a webinar organised by eu-LISA.

The majority of eu-LISA training materials and recorded training sessions are available on the eu-LISA training platform currently hosted on CEPOL's e-Net[61]. The platform is open to all registered SIS II IT operators, SIRENE officers and Schengen evaluation team members. Preparation activities for the establishment of an eu-LISA training platform, hosted together within its corporate infrastructure, started in 2014 and will be finalised in the course of 2015.

Finally, as a part of training-related activities, the National Contact Points for Training (NCP) were established in October 2014. The NCP is a formal eu-LISA network of nominated national representatives acting as training counterparts from the Member States. The NCP is actively contributing to the process of

[57] A module for VIS is also foreseen.
[58] One training session was organised for each of the IT systems operated by the Agency: SIS II, VIS and Eurodac.
[59] For repartition by Member States, see in the Annex, Graph I - Participation to 2014 SIS II training activities, breakdown per countries.
[60] For more information, see the Annex, Graph II – Satisfaction rate for 2014 SIS II training activities.
[61] E-Net is the CEPOL web platform dedicated to learning and training materials and activities.

establishment of training needs and is supporting eu-LISA in the development and updating of training courses, methodologies, training materials and tools in order to fully respond to the training needs of the Member States.

3. Communication infrastructure

3.1 General description of the management

According to Article 4(1)c of the SIS II Regulation and a parallel provision in Article 4(1)c of the SIS II Decision, one of the three elements comprising SIS II shall be a communication infrastructure between the central system (CS-SIS) and the national interfaces (NI-SIS) that 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 above-mentioned 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 Directorate General for Informatics (DIGIT).

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 24/7/365 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 Regulation, tasks regarding the communication infrastructure (including operational management and security) are divided between eu-LISA and the Commission. In order to ensure coherence between the exercise of their respective responsibilities, operational working arrangements were established between eu-LISA and the Commission and are reflected in a Memorandum of Understanding (MoU) concluded in June 2014.

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 for SIS II[62]. The Agency is also responsible for the security measures in respect to the exchange of supplementary information through the communication infrastructure of SIS II[63].

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.

[62] As well as for VIS and Eurodac.
[63] And for establishing the technical procedures necessary for the use of the communication infrastructure for Eurodac.

3.2 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.

Secrecy 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 completely 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 and as such it presented a certain risk to the availability of the service. Therefore an activity to mitigate this risk was started in 2014 consisting of deployment of a secondary encryption layer in the pre-production part of the communication infrastructure[64].

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 (see below section 6 of the report).

The SIS II Mail SPoC (Single-Point-of-Contact) Servers are 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 for the central 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 (09 April 2013 to 31 December 2014), there were no incidents with critical impact 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. Every one of these incidents was analysed to identify the root cause and appropriate measures were implemented to prevent reoccurrence of the incident.

Currently, there is an on-going project to migrate the current sTESTA network to the new TESTA-ng (New Generation) network. The migration 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 related to SIS II - from the old sTESTA network to the new TESTA-ng network. Thus the migration will be also implemented for the SIS II network.

4. Availability and performance

The central system has been designed and optimised for a specific usage, search distribution, load and maximum volume. The system has been designated to hold up to 100 million alerts with a certain average

[64] This will also support the agency in complying with the legal requirement on availability of the service.

traffic rate of CUD transactions per second. On 31 December 2014, the system contained 55.97 million alerts and in the entire reporting period the average load over 24 hours was well below the planned capacity. In terms of availability, some requirements are also mentioned in the description of the network availability[65].

During 2013, the overall availability of the SIS II central system including the associated connectivity network was over 99.99%, exceeding all the expectations for such a sensitive and critical large-scale IT system.

This availability is considered against critical SIS II functionalities, such as searching the system or properly processing and broadcasting the alerts received from the Member States. It does not take into account maintenance activities which were properly announced in advance.

During 2014, the availability of the SIS II central system and associated connectivity network measured in the same manner was slightly lower than in 2013 as a result of incidents[66] that were nonetheless properly managed in order to immediately restore service and minimise operational impact on the SIS II community.

From the entry into operations on 9 April 2013 until 31 December 2013, over 11 million CUD transactions were performed towards the Central SIS II. For the entire calendar year of 2014, the SIS II central system processed over 17 million CUD transactions. During both periods, the large majority of transactions were performed within three minutes, in line with the design requirements of the system[67].

It is possible to perform several types of searches against Central SIS II. 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, as per the design, can be expected. The most used types of search are first line searches known as category 1 and the back office searches known as category 2.

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. Category 1 searches represented respectively 72% of the total searches against the central system in 2013 and over 69% in 2014.

In 2013 as regards the response time, over 99.75% of category 1 searches were performed in one second or less; in total 99.99% of category 1 searchers were performed in three seconds or less. In 2014, very similar response times were reported[68].

Category 2 is the type of search that does not have the need to receive an answer immediately and deals with inexact information. This type of search represented 27% of the total searches against the central system in 2013 and over 29% in 2014. 99.73% of category 2 searches were performed in three seconds or less in 2013 and this proportion went up to 99.97% in 2014.

Taking into account all types of searches performed against the central system, 99.92% were performed in three seconds or less in 2013 and this went up to 99.98% in 2014. It is to be noted that during the reporting period, the majority of searches in SIS II were performed against national copies. In 2013 the searches performed against the Central SIS II represented 20% of the total searches performed in SIS II, in 2014 those were 18%.

Response times for searches performed against the central system registered during the reporting period are in line with demands and expectations.

[65] Commission Decision of 16 March 2007 laying down the network requirements for the Schengen Information System II (1st pillar) 2007/170/EC and parallel Decision (3rd pillar) 2007/171/EC. OJ L 79, 20.03.2007.
[66] The incidents were with less than critical impact, as described in the section above on the communication infrastructure.
[67] For more details, see in the Annex, table III Response time for CUD processed.
[68] For more details, see in the Annex, table IV Response time for central search.

5. Security and Data Protection

5.1 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.

The legal instruments governing SIS II, in particular Article 16(1) of the SIS II Regulation and the parallel Article 16(1) of the SIS II Decision, provide that the Management Authority in relation to Central SIS II (CS-SIS) and the Commission in relation to the communication infrastructure have to adopt the necessary security measures prescribed therein. 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 Agency has planned to review the SIS II Security plan and policy in the first quarter of 2015. The measures described by the Security Policy[69] implement the principles of least privileges, security by default, defence in depth and segregation of duties.

The SIS II central system is protected with a very strong set of physical controls including a 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.

Moreover, in case of need, operations can be switched to the back-up site in Austria where a permanent personnel presence of eu-LISA's staff is ensured. All persons having logical or physical access to the production systems (central or back-up sites) have a valid personnel security clearance at EU Secret level.

In terms of information security, operational and administrative access to the central and back-up systems is only 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 have been concluded with all persons to whom no European Union or Member State public service rules apply[70]. Staff and contractors required to work with the 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 towards Member States is protected with multiple layers of encryption and network security controls with several layers of firewalls and integrity checks. The CS-SIS is located in an isolated, controlled and secure environment, physically 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.

[69] The measures to be provided for in the security policy, according to the Article 16 (1) of the SIS II Decision include: access restrictions to data processing facilities, personnel security requirements, controls of 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.
[70] For example citizens from the Associated Countries: Norway, Iceland, Liechtenstein and Switzerland.

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 has undergone periodic technical vulnerability testing and baseline security self-assessments and will continue to be subject to an independent security assessment process in the first quarter of 2015.

In 2013 the Agency and the countries connected to the SIS II initiated an end-to-end security evaluation of the SIS II environment upon the initiative of the Commission. This initiative addressed the security at both the central and national levels and provided a set of recommendations for security improvements. This outcome has served as a basis for agreement among Schengen members on a set of minimum security standards to be met to increase the overall level of security of the SIS II environment. An ad hoc Cyber-security Working Group, led by eu-LISA, was also established in this respect.

eu-LISA, being responsible for the security of the SIS II central system, has become a recognised player in the coordination of the end-to-end security of SIS II together with Member States. In this respect, eu-LISA has supported the Commission with technical expertise, when requested, in the review of the new Schengen Evaluation Mechanism and will support, always when requested, the actual evaluations.

Finally, in order to increase the level of cooperation in the area of security operations, an informal network of security contact points, the Security Officers Network (SON), was established by eu-LISA's Management Board to facilitate more effective information exchange among Member States` experts. The first SON meeting was convened on 17-18 September 2014 at eu-LISA's HQ premises in Tallinn.

5.2 Data Protection

SIS II complies strictly with the requirements of the SIS II legal instruments in terms of data protection and with international best practice in information security. The protection of personal data related to individuals processed by the SIS II at central system level is monitored by the European Data Protection Supervisor (EDPS) in close cooperation with the eu-LISA Data Protection Officer.

In terms of the quality of data stored in the central system, although Member States as owners of the data are liable, eu-LISA is fully committed to providing monitoring capabilities and technical solutions to help Member States improve the quality of their data.

The topic on how the Agency could support Member States in improving the quality of data has been a recurrent theme in the Advisory Group`s agenda all through the reporting period. Based on practises established with SIS II's predecessor, Member States requested eu-LISA`s support on this matter. Discussions were ongoing at the time of drafting this report in order to agree on the support activities which eu-LISA will provide within the boundaries of the legal provisions.

On 25-26 February 2015, the EDPS inspection to the SISII took place pursuant to Article 47(2) of Regulation (EC) 45/2001, Article 45 SIS II Regulation and parallel provision in Article 61 SIS II Decision. Aims of the inspection were: the operational management of SISII – central system and its communication infrastructure; the security of the central SISII and its communication infrastructure.

eu-LISA's Data Protection Officer represents the Agency at the Supervision Coordination Group of SIS II, reporting about the current state of the central system and future evolutions. The group monitors legal compliance with all relevant aspects of the data protection acquis at national level as well as central system level.

6. Exchange of supplementary information between Member States

The alerts contain a set of data which is described in the SIS II legal instruments. In addition to that, according to the SIS II legal instruments, Member States exchange supplementary information related to the alerts as defined in Article 3(b) of the SIS II legal instruments.

The exchange of supplementary information is carried out via form exchange between the SIRENE Bureaux. Rules and procedures governing the bilateral and multilateral exchange of supplementary information are laid down in the SIRENE Manual[71].

In order to fulfil the legal reporting obligations as set in Article 50(3) of the SIS II Regulation and Article 66(3) of the SIS II Decision, eu-LISA annually collects statistics from Member States. This section presents part of this statistical data.

6.1 Exchange of forms

Fourteen different forms[72] are available to support the exchange of supplementary information between the Member States.

From 9 April until 31 December 2013, a total of 242,754 outgoing forms and 645,419 incoming forms were exchanged among all countries connected to SIS II. In 2014, for the entire calendar year, 366,561 outgoing forms and 1,052,843 incoming forms were reported to be exchanged.

Taking the average of forms exchanged in a 30-day period, in 2014 the outgoing forms increased on average of 10% and the incoming forms on average of 19%[73] compared to 2013 activities.

Figure 1 gives the breakdown of outgoing and incoming forms exchanged by all countries connected to SIS II during the reporting period covered by this report.

[71] OJ L44, 18.2.2015.

[72] 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 is 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.

[73] In 2013 for a 30-day period an average of 27,276 outgoing forms and 72,519 incoming forms were exchanged, whereas in 2014 for a period of 30-day on average 30,1280utgoing and 86,535 incoming forms were exchanged.

Form	2013*		2014	
	Outgoing	Incoming	Outgoing	Incoming
Forms A	18,638	314,885	22,090	534,806
Forms E	107	119	222	232
Forms F	7,316	6,612	11,467	10,985
Forms G	57,817	60,470	99,732	100,173
Forms H	8,300	9,405	14,505	16,505
Forms I	12	10	8	9
Forms J	351	349	472	604
Forms K	364	373	497	509
Forms L	4,219	5,075	5,322	7,099
Forms M	129,216	232,238	189,631	358,882
Forms N	3,526	3,501	5,277	5,364
Forms O	2,377	2,362	2,232	2,264
Forms P	10,446	9,814	15,005	15,146
Forms Q	65	206	101	265
Total	**242,754**	**645,419**	**366,561**	**1,052,843**

* For 2013 the reporting period was from 9 April to 31 December; whereas for 2014 a full calendar year was considered.

Figure 1: Total number of forms exchanged in the reporting period

For the sake of clarity, the SIRENE Bureaux can exchange forms bilaterally or multilaterally. In some cases a Bureau will only wish to inform one other Bureau of certain information, for example a hit on an alert. Alternatively, there are some forms which must go to all Bureaux, such as the creation of a new alert for arrest and the details of the case.

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.

6.2 Hits

A hit occurs in SIS II when a search is conducted by a user and the search reveals a foreign alert, i.e. the alert in SIS II matches the searched data. According to the legal provisions, further actions are requested as a result of the hit.

From 9 April until 31 December 2013, a total of 86,822 hits on foreign alerts were registered by all countries connected to SIS II. In 2014, for the entire calendar year, 127,935 hits on foreign alerts were reported by all Member States.

Taking the average of hits generated in a 30-day period, in 2014 the reported hits on foreign alerts – compare to data available for 2013 - increased on average of 7.8%[74].

Figure 2 presents the number of hits reported by all countries connected to the system in 2013 and in 2014. 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).

[74] In 2013 for a 30-day period there were on average 9,755 hits, whereas in 2014 there were on average 10,515 hits.

There is always a difference between the two sets of figures due to several factors, the major factor being that a Member State may ask to be informed of any hits on alerts for refusal of entry or stay that it has entered as described in Section 4.7 of the SIRENE Manual. Without this request the alert-issuing country may not be informed of a hit on such an alert.

Alert determining the hit		2013*		2014	
		hits on foreign alerts	hits abroad on own alerts	hits on foreign alerts	hits abroad on own alerts
Art 26 SIS II Dec[75]		5,777	6,121	8,774	9,071
Art 24 SIS II Reg[76]		22,702	12,440	25,888	20,104
Art 32 SIS II Dec[77]		2,667	2,519	3,961	3,794
Art 34 SIS II Dec[78]		18,068	14,113	31,255	25,343
Art 36 SIS II Dec[79]		14,169	13,424	23,942	23,222
Art 38 SIS II Dec[80]	vehicles, boats, aircraft, trailers, caravans, industrial equipment, boat engines, containers	10,985	12,197	14,422	13,113
	Firearms	105	89	180	387
	blank docs	979	1,075	1,247	1,584
	vehicle registration certificates	1,497	1,142	791	658
	number plates			2,337	2,220
	issued docs	9,863	6,525	12,852	11,346
	Banknotes	5	8	2,275	152
	securities and means of payment	5	3	11	14
Total hits		**86,822**	**69,656**	**127,935**	**111,008**

* For 2013 the reporting period was from 9 April to 31 December; whereas for 2014 a full calendar year was considered.

Figure 2: Total number of reported hits for the reporting period

7. Conclusion and forward looking

The SIS II entered into operation on 9 April 2013 and since then excellent levels of performance and availability have been maintained during 2013 and 2014. eu-LISA has adopted and implemented all security measures as per the legal provisions.

Since its establishment, the Agency has been closely working together with all stakeholders involved in the SIS II community in order to ensure high quality operational management of Central SIS II and it will continue to do so going forward.

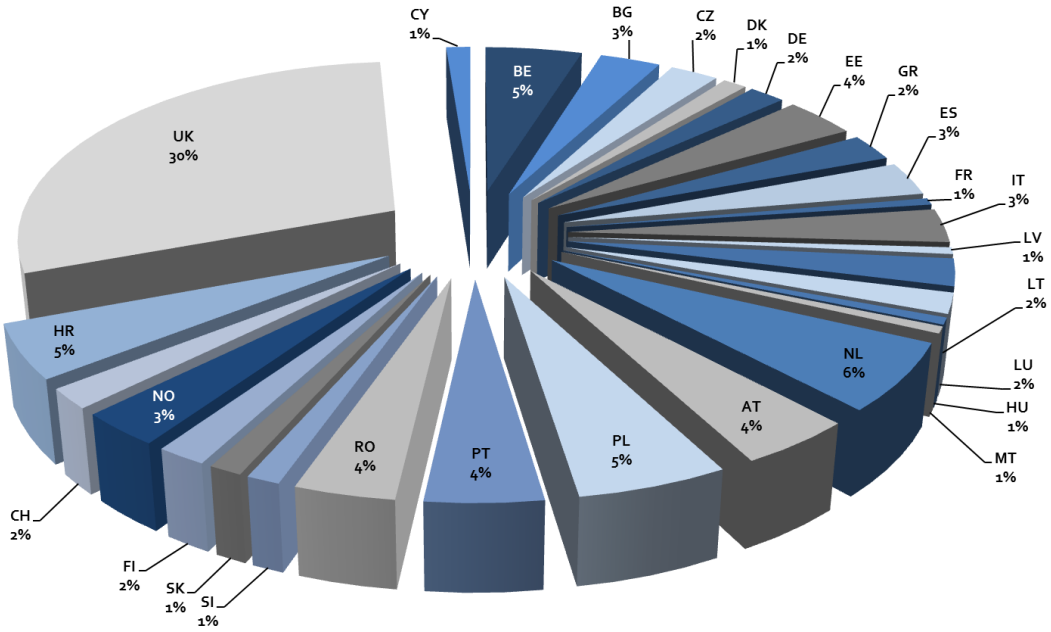
eu-LISA is strongly committed to maintaining full SIS II central system functionality 24 hours a day, seven days a week to serve the SIS II community, to endeavour to implement any changes requested by an evolution of the legal framework or the business context and to ensure continuous relevant test and release activities.

[75] Persons subject to arrest for surrender or extradition.
[76] Third country nationals to be refused entry into or stay within the Schengen Area.
[77] Missing persons (adults and minors).
[78] Persons to assist with a judicial procedure.
[79] Persons and objects for discreet or specific check; or for discreet or specific check for national security.
[80] Objects for seizure or to use as evidence in criminal proceedings.

A number of projects are ongoing or foreseen to support the technical improvements and evolutions of Central SIS II in the coming years. In case of changes, they will go through the Change Management Process already established. The SIS II central system can evolve also as a result of the integration of new Member States. Croatia's integration is already planned and work has started, as described in this report; some other Member States, such as Ireland and Cyprus that are not yet scheduled for integration. However, these integrations will not require major change to the central system.

Annex

Graph I – Participation to 2014 SIS II training activities, breakdown per countries



Graph II – Satisfaction rate for 2014 SIS II training activities

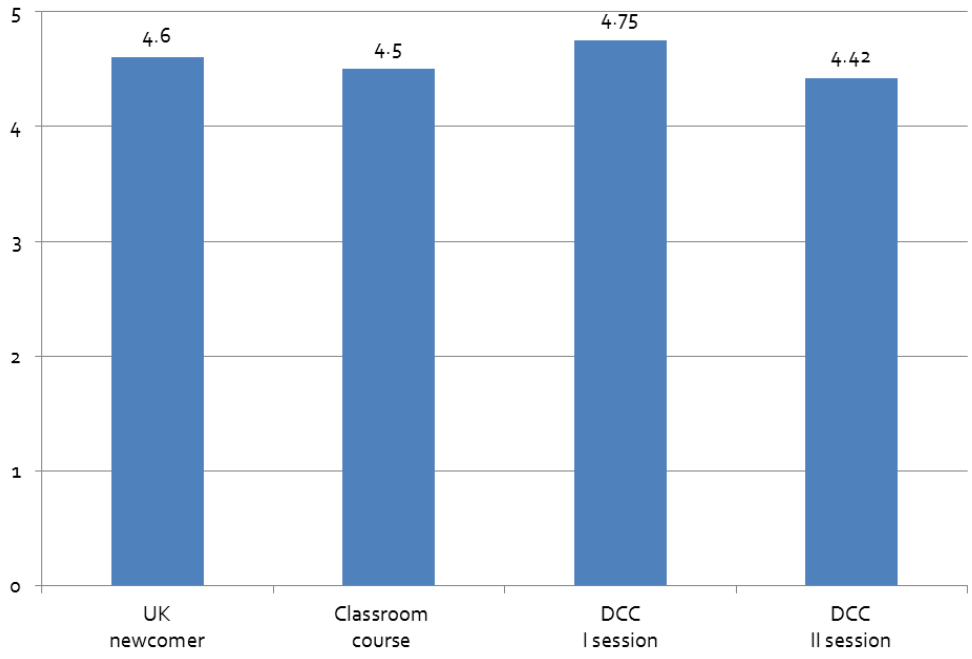


Table III – Response time for CUD processed

Reporting period	Broadcasts (CUD)processed	Broadcasts <3 min	Broadcast 3-5 min	Broadcast >5 min
from 9/04/2013 till 31/12/2013	over 11 million	99.7%	0.1%	0.2%
from 1/01/2014 till 31/12/2014	over 17 million	95.8%	0.4%	3.8%

Table IV – Response time for central search

2013	group1 responded<= 1s	group2 1s < responded<= 3s	group3 responded > 3s	Total Number of search
Category 1	99.75%	0.24%	0.01%	186 225 993
Category 2	99.60%	0.13%	0.27%	70 270 949
ALL TYPE	99.71%	0.21%	0.08%	258 907 214

2014	group1 responded<= 1s	group2 1s < responded<= 3s	group3 responded > 3s	Total Number of search
Category 1	99.71%	0.28%	0.01%	242 384 402
Category 2	99.92%	0.05%	0.04%	103 361 361
ALL TYPE	99.77%	0.21%	0.02%	349 468 503