Report on the technical functioning of central SIS II 2017-2018

October 2019

Protection level: PUBLIC

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 its communication infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.

eulisa.europa.eu

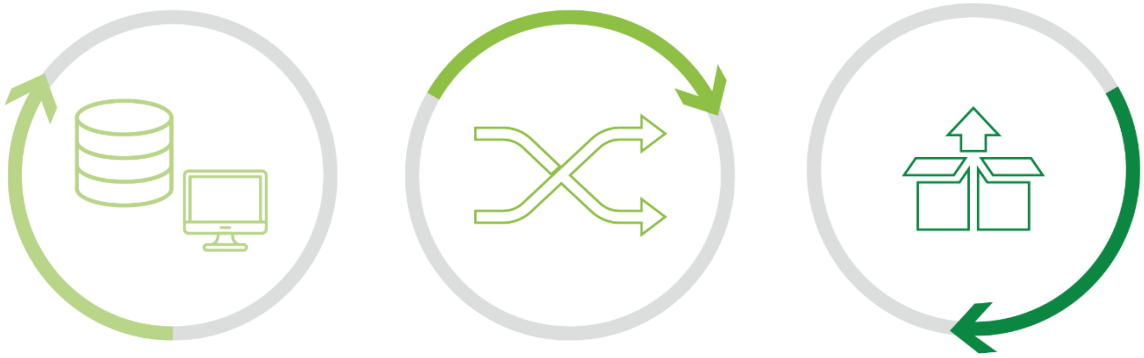
ISBN 978-92-95208-88-9
ISSN 2443-8294
doi: 10.2857/725446
Catalogue number: EL-AE-19-001-EN-N

Contents

Executive summary

Schengen Information System II (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 in law enforcement and judicial cooperation throughout Europe. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) guarantees the effective and uninterrupted operational management of its critical infrastructure.

Use of SIS II is constantly growing; in 2018, Member States reported an average of almost **16.8 million searches[1] per day in SIS II**, whereas in 2017 there were 14.1 million on average a day.



MONITORING

eu-LISA ensures that central SIS II and its infrastructure are **monitored 24/7**, as is the operational status of the exchange between central SIS II and the national copies (the bridge).

Central SIS II **had very high availability** during the reporting period.

On average, in 2017 and 2018, **11% of the total searches** performed in SIS II were performed against the central system.

CHANGE MANAGEMENT

Developments and changes are discussed and formalised within the Change Management Group, thus ensuring **agreement and coordination with Member States**. Once agreed, the changes are implemented in production as per the annual release plan.

The Change Management Group met regularly in 2017 and 2018, in particular **to discuss and agree** on the technical solution to align SIS II with the latest **ICAO specifications** for Machine-Readable Travel Document (MRTD).

TEST/RELEASE

During the reporting period, several **test campaigns** were conducted to validate the releases, while ensuring the integrity of central SIS II.

In 2017 and 2018, the following **releases were deployed** in SIS II: in July 2017, functional Release 8.2.0, including the **NIST checker** as part of the Automated Fingerprint Identification System (AFIS); in November 2017, technical Release 8.3.0; in March 2018, Release 9.0.0 for the **deployment of SIS II AFIS**; and, in July 2018, technical Release 9.1.0.

SIS II AFIS phase 1 **entered into operation on 5 March 2018**. Close cooperation with the Member States and the European Commission was instrumental in successfully delivering this complex and interdependent project. By the end of 2018, 11 Member States[2] were performing fingerprint searches in SIS II.

[1] Searches can be performed against the national copies of central SIS II.
[2] Germany, Greece, Hungary, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Poland, Portugal and Slovenia.

1. Introduction

Schengen Information System II — SIS II — provides extensive support for operational cooperation between national competent authorities, such as border guards, police, and judicial, customs and immigration authorities. Currently, SIS II is used by 26 EU Member States and 4 Schengen Associated Countries[3], and it is consulted by Europol and Eurojust[4]. 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 in law enforcement and judicial cooperation throughout Europe. The system enables competent authorities to enter and consult data on persons sought for arrest or subject to surveillance or checks, persons who may not have the right to enter or stay in the EU or who are sought to assist with a judicial procedure, missing persons — in particular children — and objects that may have been stolen, misappropriated or lost.

After more than 6 years in operation[5], statistics provided by the Member States[6] clearly show a significant increase in use of the system. In 2018, Member States performed on average more than 16.8 million searches[7] per day in SIS II, whereas the equivalent figures were 14.1 million per day in 2017 and almost 6 million per day in 2014.

Access to SIS II data is limited to national competent authorities such as national border control, police, customs, judicial, immigration and visa-issuing authorities and vehicle registration services. On a yearly basis, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) publishes in the *Official Journal of the European Union* an updated list of Member State competent authorities having access to the system[8].

SIS II

In 2018, Member States performed on average more than 16.8 million searches per day in SIS II

In terms of governance, several stakeholders — the European Commission[9], the Member States and eu-LISA — have responsibilities when it comes to SIS II. eu-LISA is responsible for the operational management of central SIS II, and the Management Board together with the SIS II Advisory Group[10] support the Agency in this respect.

Close cooperation with the Member States and the European Commission has been instrumental in ensuring the operational management and proper evolution of central SIS II, and the Advisory Group plays an important role in this context. Inter alia, the Advisory Group discusses the availability of the central system and of the national copies; approves release plans; discusses and plans change requests and future developments; adopts training plans; validates the annual statistics; and advises on operational questions. In addition, Member States also participate in a number of regular fora — specific to SIS II or covering all systems — such as the Automated Fingerprint Identification System (AFIS) Project Management Forum (PMF), the Security Officers Network (SON), the National Contact Points (NCPs) for training and the Change Management Group (CMG).

[3] In September 2019, the Member States of the EU connected to SIS II were Austria, Belgium, Bulgaria, Croatia, Czechia, 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 were Iceland, Liechtenstein, Norway and Switzerland.
[4] As per Articles 41 and 42 of the SIS II Decision
[5] SIS entered into operation in 1995, whereas the second generation of the system (SIS II) was brought into operation on 9 April 2013.
[6] By the term 'Member States' the current document refers to the Member States of the EU and the Associated Countries, which are bound under Union law by the legislative instruments governing SIS II.
[7] Includes all searches in SIS II, those against Central SIS II and those against national copies.
[8] OJ C 222, 2.7.2019.
[9] The Commission chairs the SISVIS Committee, which regularly brings together representatives of the Member States with the aim of harmonising operational procedures, supporting the effective application of the rules and optimising the use of SIS II. eu-LISA regularly reports and contributes to the committee meetings.
[10] The group meets regularly, four times a year.

This report, which is the third report on the technical functioning of *c*entral SIS II and its communication infrastructure[11], covers the period from 1 January 2017 until 31 December 2018. The report, as part of eu-LISA's legal reporting obligations[12] for SIS II, aims to increase both transparency and visibility. It encompasses activities performed to ensure the operational management of central SIS II, including its security, together with the statistics collected annually.

1.1 Legal developments

During the reporting period, the most important legal developments affecting SIS II were the entry into force on 7 April 2017 of the regulation on systematic checks at the external borders and the entry into force on 28 December 2018 of the new enhanced SIS legal basis.

In spring 2017, Regulation (EU) 2017/458[13] on the reinforcement of checks entered into force. The regulation 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). Consequently, SIS II, being one of the databases in which these systematic checks were to be carried out, witnessed a significant increase in use.

The political negotiations on the new SIS package were finalised in the first semester of 2018. Thereafter, the new SIS regulations[14] were published in the *Official Journal of the European Union* and entered into force on 28 December 2018. eu-LISA has been supporting the European Commission and the Member States with technical expertise in the relevant SIS expert meetings and subgroups. In particular, efforts focused on drafting the necessary delegated and implementing acts and defining the requirements stemming from the revised SIS legal basis. That work was carried out in tandem with the SIS recast project set up by eu-LISA.

The new SIS legal basis entered into force in December 2018, strengthening SIS's ability to fight terrorism and cross-border crime

The implementation of the new legal basis will be carried out gradually[15] in the period 2019-2021. By 28 December 2019, the European Border and Coast Guard Agency (EBCGA/Frontex) teams shall have access to SIS and Europol shall have extended access. Within 2 years, all Member States shall be connected to AFIS and be able to perform biometric searches. By the end of the 3-year implementation period, the European Commission shall adopt a decision setting the date when all the remaining changes envisaged in the recast should be implemented.

The recast represents a major enhancement of the system, in particular strengthening the ability of SIS to fight terrorism and cross-border crime, improving border and migration management and ensuring effective information exchange between Member States, while increasing the security of European citizens. The main changes encompass new categories of data (i.e. DNA) and new categories of alerts (i.e. preventive alerts for children, alerts on return decisions and unknown persons), and will provide access to new users such as the EBCGA and greater access to Europol and Eurojust.

[11] Previous issues are available here: https://www.eulisa.europa.eu/our-publications/reports
[12] Pursuant to Article 50(4) of the SIS II Regulation and Article 66(4) of the SIS II Decision. If not otherwise specified, in this report SIS II Regulation refers to Regulation (EC) No 1987/2006 (OJ L381, 28.12.2006) and SIS II Decision refers to Council Decision 2007/533/JHA (OJ L 205, 7.8.2007).
[13] OJ L 74, 18.3.2017.
[14] Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006; Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU. OJ L 312, 7.12.2018.
[15] As per Article 66 of Regulation (EU) 2018/1861 and the parallel provision in Article 79 of Regulation (EU) 2018/1862.

In June 2019, outside the reporting period for this report but impacting SIS in the coming years, the interoperability regulations[16] entered into force. These create a new architecture for the EU large-scale IT systems in order to streamline and increase the effectiveness of identity checks and ensure seamless access for law enforcement authorities. To make better use of the existing IT systems, while respecting all the original system safeguards, the interoperability legal basis envisages putting in place four new components, namely the European Search Portal (ESP), the shared Biometric Matching System (sBMS), the Common Identity Repository (CIR) and the Multiple Identity Detector (MID). In addition, a central repository for reporting and statistics (CRRS) is to be established. All these components, with the exception of the CIR, once developed, will be connected to the SIS central system.

2. Operational management of central SIS II

eu-LISA is responsible for the operational management of central SIS II, ensuring uninterrupted 24/7 access to the system and allowing the continuous exchange of data between the 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.

During the reporting period, maintenance in working order (MWO) has been provided by different contractors. The first MWO framework contract, LISA/2014/RP/02[17], expired in March 2018[18] and the new MWO framework contract, LISA/2017/RP/01, was signed on 1 June 2018[19]. Following the transition period between June and September 2018, on 14 September 2018 the new MWO contractor took over MWO of the Schengen Information System. In the context of MWO, eu-LISA is responsible for the operational management of Central SIS II and is directly accountable for the performance of the system. The contractor provides MWO.

The new SIS II MWO framework contract was signed on 1 June 2018 for 4 years with the possibility of an extension for 2 years

The evolutionary maintenance of the first MWO contract included, since summer 2016, the development and implementation of the state-of-the-art biometric functionality AFIS, the first phase of which successfully entered into operation on 5 March 2018.

The new MWO contract was awarded by eu-LISA following a restricted procurement procedure the first phase of which was launched in February 2017[20]. The new MWO was signed for 4 years, with the possibility of an extension for an additional 2 years. By the end of 2018, the majority of the work packages were active, including corrective maintenance, adaptive maintenance, evolutionary maintenance, support for Member States' testing, technical assistance and training.

From October 2018, the SIS MWO contractor started using SM9 (Service Manager 9, an incident manager tool), with the aim of making the exchange of information between the eu-LISA users and MWO users easier. Similar integration projects had already been implemented for the other systems managed by the Agency, and thus the incident management tools used were harmonised in line with eu-LISA's implementation of IT service management (ITSM) standards and processes.

[16] Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, and Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA. OJ L 135, 22.5.2019.
[17] Signed by the consortium Atos, Accenture and HP.
[18] The period between March and June was covered by the standard implementation clause.
[19] The new contract was signed by Sopra Steria Benelux.
[20] More information is available at http://ted.europa.eu/udl?uri=TED:NOTICE:60835-2017:TEXT:EN:HTML

2.1 Technical infrastructure of central SIS II

In the context of maintenance activities, the Agency regularly carries out volumetric monitoring and analysis of central SIS II to avoid degradation of the services. On a yearly basis, eu-LISA consults the Member States on volumetrics, to ensure that the central system will cope with increasing business needs and use for both alerts and storage of binaries, as well as searches against the central system. By the end of 2018, over 82.2 million alerts were stored in the SIS II central system[21], which had registered an increase of over 5.5 million alerts per year both in 2016 and in 2017. Currently, the central database is sized to store 100 million alerts.

As indicated in Article 4(1)(b) of the SIS II legal basis, Member States may have a national copy, complete or partial, of the SIS II database. Twenty-five Member States have a national copy; Denmark, Finland, Liechtenstein, Norway and Slovenia do not, so they search central SIS II. In addition, there is a group of Member States that have a national copy but have subscribed to use the services of the central system for certain types of searches.

Following a study in 2016 and an analysis of the capacity of the central system to dynamically cope with the changing load profiles, the solution arrived at was to replace the current search engine with a new one. In April 2017, the Agency implemented a short-term action upgrading the infrastructure [22]. Thanks to this enhancement, the system is able to sustain at least twice the search load for which it was initially designed, and therefore to handle up to 2.6 million searches per day without any issues with the current search distribution. A project to increase the capacity of central SIS II, encompassing replacing the search engine and a capacity upgrade to 130 million, alerts is planned to start in Q2 2019. The aim is to improve central system availability within the current set-up, while reducing downtime for the switchover. In the long-term, eu-LISA will work to redesign the system in an active-active mode. A request for a feasibility study to be performed by the MWO contractor was launched in Q1 2019.

At the beginning of 2017, a project to replace the outdated central system simulator (CSSIM) kicked off. The new CSSIM was intended to support the Member States in testing and training at their premises. The Member States received the beta version of the simulator on 1 December 2017. In February 2018, the final version of the CSSIM was successfully delivered. The CSSIM is based on the SIS central system application version 8.2.0 (without AFIS). At the same time, extensive training activities were organised in January and February 2018 in order to familiarise Member States with the simulator.

In February 2018, the final version of the central SIS simulator was delivered to support Member States in testing and training

During the reporting period, the integration project to connect Croatia to SIS II was successfully completed. In line with Council Decision 2017/733[23], as of 2 May 2017 alerts covered by the SIS Decision and the SIS Regulation, as well as supplementary information and additional data connected to those alerts, were made available to Croatia. Since 27 June 2017, Croatia has been able to enter alerts and perform searches against SIS II.

In addition, in May 2018 activities started for the integration of Ireland. Ireland is expected to be technically ready to connect to SIS by the beginning of 2020.

On 28 December 2018, the new legal basis for SIS entered into force. As mentioned above, the timeline for implementation is clearly indicated in Article 66 of Regulation 2018/1861 and the parallel provision, Article 78, in Regulation 2018/1862.

[21] As per the annual statistics published by eu-LISA: https://www.eulisa.europa.eu/our-publications/reports
[22] The central processing units on the search nodes were doubled.
[23] OJ L 108, 26.4.2017.

2.2 AFIS for SIS

In June 2016, following the Commission communication COM(2016) 205 final[24], which mandated eu-LISA to develop and implement an AFIS functionality for SIS II, the Agency[25] launched the AFIS project phase 1. Equipping SIS II with biometric matching capabilities would allow a person to be identified based on fingerprints stored in the system, thus strengthening border management and internal security in the Schengen area.

eu-LISA adopted a two-step approach to the AFIS project phase 1: (1) all necessary preparatory works, including the design of the AFIS solution, were planned for 2016; (2) implementation took place in 2017 and entry into operation was planned for Q1 2018. From the beginning of the project, the stringent timeline in addition to the complexity and interdependency of the project were considered important risks to be constantly monitored. Multiple mitigation actions were put in place, such as ensuring leverage of the in-house knowledge already acquired in similar projects[26] and adopting a phased approach to guarantee faster delivery. Monthly PMF[27] meetings were held in order to streamline coordination and communication, in particular with Member States.

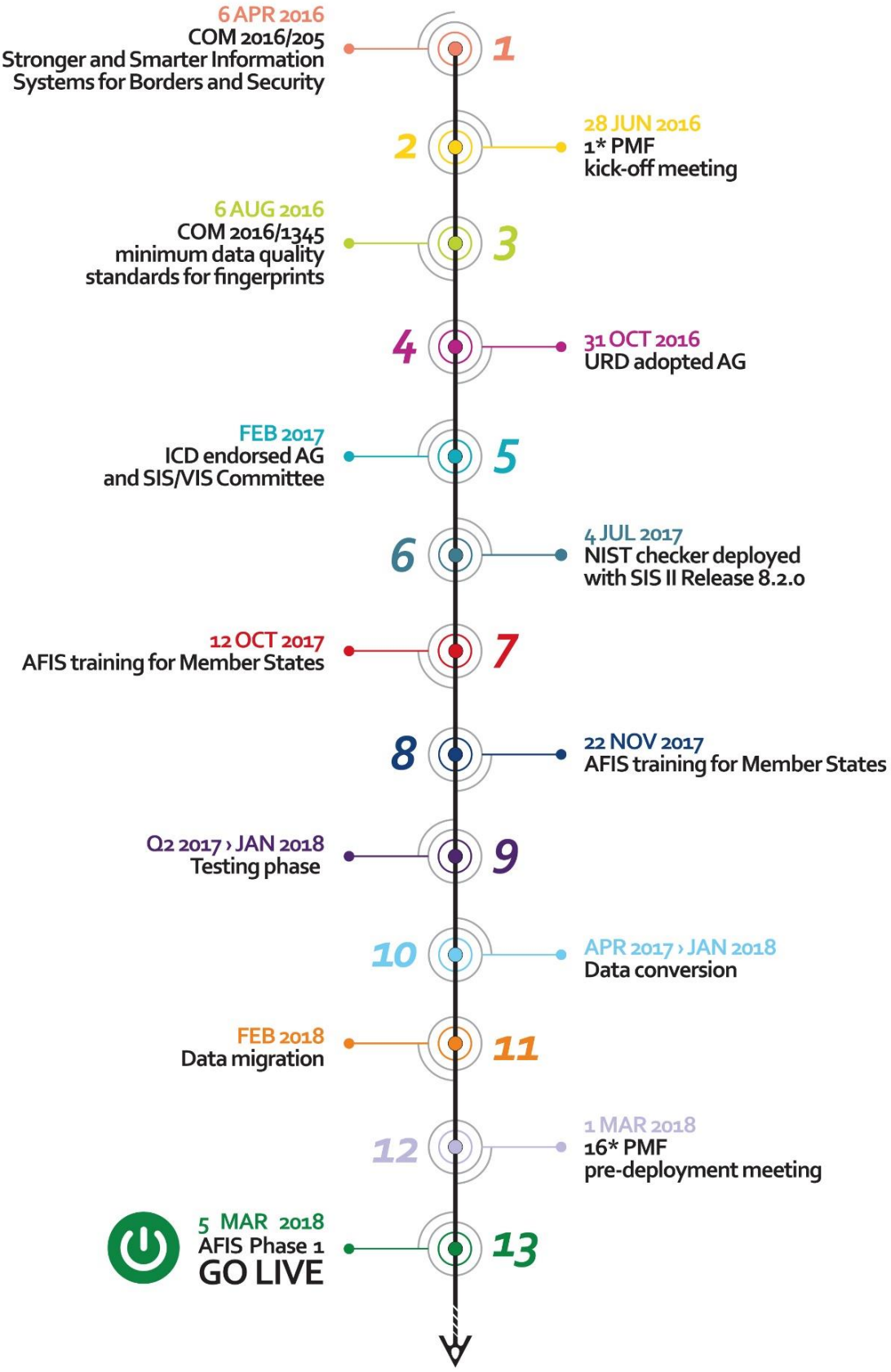
Equipping SIS II with biometric matching capabilities allows a person to be identified based on fingerprints stored in the system, thus strengthening border management and internal security in Schengen

At the PMF meetings, functional, technical, quality, performance and volumetric requirements for phase 1 were discussed and consolidated. The reference for quality was the European Commission decision[28] on minimum data quality standards for fingerprint records within SIS II. At the Advisory Group meeting of 31 October 2016, the User Requirements Document (URD) was adopted. By February 2017, the detailed analysis and design phase was completed with the endorsement — by the Advisory Group and the SISVIS Committee — of the SIS II AFIS Interface Control Document (ICD)[29]. SIS II Release 8.2.0, deployed in July 2017, included the NIST checker. This was the first element of the delivery of AFIS at central system level. From its implementation, Member States began receiving notifications on the compliance of their fingerprint NIST containers based on defined specifications; the central system rejects NIST files that are not compliant. By the end of 2017, the build phase for the central system infrastructure and application was completed.

During the build phase, the national systems and central system were set up according to the specifications. Several test campaigns were run. eu-LISA made available to the participating Member States[30] a new pre-production environment to perform integration tests to validate the implementation at national level. The integration tests were passed in Q3-Q4 2017. Validation of the new functionalities of the central system was achieved with through provisional system acceptance testing in January 2018. Furthermore, the new basis for the central system was thoroughly tested, with end-to-end testing in all environments.

Prior to entry into operation, conversion of the fingerprints in SIS II was carried out, being completed at the end of January 2018. Member States[31] had to ensure that fingerprint records were in the right format, meaning that they had to convert (update/adapt) their NIST files in SIS II to the new standard defined for AFIS.

[24] Communication from the Commission to the European Parliament and the Council — 'Stronger and Smarter Information Systems for Borders and Security', COM(2016) 205 final, 6.4.2016.
[25] AFIS was not part of the activities planned for 2016 and further budget was needed to ensure its development. eu-LISA made a proposal to review and amend the Agency's Working Programme, a proposal that was adopted by the Management Board.
[26] In particular in the implementation of the Biometric Matching System for the Visa Information System.
[27] The PMF is composed of eu-LISA SIS II AFIS project team members, national project managers from all the SIS II Member States and representatives of the European Commission. The forum has been meeting on a monthly basis (face-to-face or by web conference) since its establishment and reports directly to the SIS II Advisory Group.
[28] Commission Implementing Decision (EU) 2016/1345 on minimum data quality standards for fingerprint records within the SIS II; OJ L 231, 6.8.2016.
[29] The ICD provides Member States with the technical specifications needed to implement the XML schemas used to interact with the SIS central system.
[30] Austria, Germany, Latvia, Liechtenstein, Luxembourg, the Netherlands, Poland, Portugal, Slovenia and Switzerland.
[31] Germany developed conversion software and shared it with the SIS community.



Following the conversion period, data from the correctly formatted NIST files were migrated[32] into the SIS II AFIS database[33].

SIS II AFIS phase 1 was successfully delivered and entered into operation on 5 March 2018, with SIS II Release 9.0.0. Thanks to the close cooperation of all the stakeholders, and intense efforts to prepare for deployment, the go-live went smoothly. AFIS phase 1 final system acceptance was successfully passed on 5 July 2018. It must be emphasised that, given the complexity of the project, significant efforts were invested in planning and coordination. The project was eventually implemented without substantially deviating from the agreed initial planning.

By the end of 2018, Germany, Greece, Hungary, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Poland, Portugal and Slovenia were performing fingerprint searches in SIS II

Before the go-live, Bulgaria and Malta joined for the testing phase. After the entry into operation of AFIS, Germany and Latvia started using the new fingerprint search capability on a daily basis. The other countries that passed the integration tests followed gradually (Malta, Portugal, the Netherlands and Slovenia). In addition, other countries started testing (Czechia and Norway). By the end of 2018, 11 Member States[34] were performing fingerprint searches in SIS II. Under the SIS recast, from the end of 2020 all Member States have to be able to carry out fingerprint searches in SIS.

To ensure the proper functioning of SIS II AFIS, at the beginning of 2018 the Agency initiated the required upgrade to the SIS II network. SIS II turnkey access points (TAPs) at national level had to be upgraded to a higher bandwidth to accommodate AFIS functionality needs as well as future SIS II operational needs. During the first phase, started in Q1 2018 and finalised in Q1 2019, the primary TAPs of six Member States[35] will be upgraded. During the second phase, the rest of the sites will be upgraded (starting in November 2019).

Following the conclusion of phase 1, preparations for SIS II AFIS phase 2 started. The first PMF meeting for phase 2 was held in November 2018, where the first discussions in relation to different use cases and the new SIS recast biometric requirements took place.

2.3 Monitoring and operational activities

Central SIS II monitoring is carried out at the operational site in Strasbourg by the eu-LISA Service Desk, operational 24 hours a day, 7 days a week. The system and its infrastructure are continuously monitored, as is the operational status of the exchange between Central SIS II and the national copies (the bridge). Any unavailability leading to a business impact is immediately reported and escalated on a 24/7 basis.

The eu-LISA Service Desk is the entry point for users' reports of incidents as well as for requests for information or technical advice and support. Any request or incident is registered with a central incident management tool (SM9) for follow-up. During the reporting period, 1,465 interactions related to SIS, including incidents and requests for information, were registered[36]. The critical interactions represented on average 3% of the total, in line with past reporting periods. eu-LISA has implemented ITSM processes to ensure quality of service and to cope better with incidents and service requests. This is a continuous exercise to ensure efficient and cost-effective management of the systems operated by continuously monitoring and developing operational processes.

To ensure effective backup of all functionalities of the SIS II central system in the event of failure of the system and full redundancy, as laid down in Article 4(3) of the SIS II legal instruments, the central system has two data centres. The SIS II central unit (CU) is located in Strasbourg, France, whereas the SIS II backup CU (BCU) is

[34] Germany, Greece, Hungary, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Poland, Portugal and Slovenia.
[35] Austria, Germany, the Netherlands, Poland, Portugal and Switzerland.
[36] There were 1,257 interactions during the period 2015-2016.

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 means that the data contained in the CU and BCU must remain synchronised at all times.

Central SIS II provides functionalities for ensuring synchronisation and consistency of national copies, using data consistency checks (DCCs), as well as for the restoration of data, should this be necessary. Each month, the DCC monthly campaigns support Member States to achieve technical compliance. Checks are performed on all alerts and links, and any discrepancies found are automatically repaired by the mechanism itself. In the reporting period, 1,121 DCCs were run, including monthly campaigns, partial DCCs and those requested by a Member State. The majority of monthly DCC campaigns found zero discrepancies in alerts. The results of the DCCs are regularly analysed at Advisory Group meetings in order to share and discuss practices with Member States. In the light of continuing efforts to reach zero discrepancies, a dedicated workshop was held in February 2017.

To ensure synchronisation and consistency of national copies, in the reporting period 1,121 data consistency checks were run for Member States having a national copy

In spring 2018, the revised Operator Manual entered into force after its adoption by the SIS II Advisory Group. The updates related to maintenance and escalation procedures.

Following the established practice, the Agency carries out an annual customer satisfaction survey covering the performance of the Service Desk, incident and problem management, operational communication, technical assistance and support for national activities, as well as release management. In the last 2 years, the participation of the SIS community was very high, with 90% of the Member States participating in the survey. The overall satisfaction rate, taking into account the 'satisfied' and the 'very satisfied' replies, was also very positive, showing an upward trend, from 94.8% in 2017 to 96% in 2018. The results of the survey were presented and analysed during the Advisory Group meetings. Following analysis, changes were implemented in areas requiring improvement.

2.4 Performance and availability

Central SIS II was designed and optimised for a specific level of use, including with regard to search distribution, traffic rate, maximum load and volume. This context should be taken into account when measuring performance and availability[37] indicators for the system.

In 2017, almost 23.3 million create/update/delete (CUD) transactions were performed. The level was stable in comparison with the previous year. In 2018, the CUD operations performed were over 25.3 million, an increase of 11% on 2017. During the reporting period, the majority of the transactions — 99.5% in 2017 and 98.2% in 2018 — were performed in less than 3 minutes, in line with the design requirements of the system.

In 2017, Member States reported having performed more than 5.1 billion searches in SIS II, of which 11% (over 561 million) were performed against the central system. In 2018, Member States reported more than 6.1 billion searches, of which 11% (more than 687 million) were performed against the central system.

As in the previous reporting period, SLA1 searches made up the majority of searches performed at central level. Over 58% of the searches performed at central level in 2017 were SLA1 searches, whereas SLA2 searches made

[37] The system's availability is defined in Section 7 ('Availability') of the 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%.' To measure the SIS central system availability and response time, two key performance indicators were adopted by the Agency's Management Board in March 2017.

up 41%. In 2018, SLA1 searches were 59% of all searches performed in Central SIS II, whereas SLA2 searches made up 40%.

SIS II was highly available in the reporting period: in 2017, central SIS II overall availability, including the associated connectivity network, was over 99.82%; in 2018, the overall availability was over 99.75%

In 2017, 99.93% of all searches against central SIS II received a reply within the agreed time for the type of search. Taking into account only SLA1 searches, 99.92% of them were answered in 3 seconds or less. In 2018, 99.98% of all searches performed against SIS II were answered within the agreed time for the type of search, and considering SLA1 searches only this goes up to 99.99%.

Central SIS II was highly available in 2017 and 2018, confirming the trend seen in previous reporting periods. Availability is calculated against the critical SIS II functionalities, such as searching the central system or properly processing and broadcasting alerts received from Member States. Unavailability is defined as when all Member States cannot use the critical functionalities, and it includes outages due to planned and unplanned maintenance.

In 2017, central SIS II's overall availability[38], including the associated connectivity network, was over 99.82%. The system was not available for 15 hours and 37 minutes of outages. In 2018, availability was over 99.75%, with the outage time amounting to 21 hours and 39 minutes in total.

2.5 Change management and releases

Developments and changes related to central SIS II are discussed and formalised within the CMG[39], thus ensuring the agreement and coordination necessary for implementation at national level. Once agreed, the changes are implemented in production following the multi-annual SIS road map and the annual release plan, presented at the beginning of the year to the Member States. Following the established practice, the Agency presents to the Advisory Group at the beginning of each year a release plan for the given year comprising two releases, one major and one minor release, with some flexibility for implementing small modifications such as updating code tables. The release plan might require changes depending on operational needs throughout the year.

The number of change requests logged in the reporting period decreased compared with previous reporting periods, indicating that Central SIS II has reached a certain level of maturity. During the reporting period, eu-LISA logged 27 new change requests in relation to SIS II. Requests included changes to data quality reports and statistical refinements; updates to code tables; message-orientated middleware qualification; refinements to SIS II implementation (transferred to the SIS recast project); and a request related to SIS II compliance with the new International Civil Aviation Organization (ICAO) 2015 enhanced specifications for machine-readable travel documents (MRTD). This last, being a particularly complex change, required intensive efforts from all stakeholders to reach a satisfactory agreement and a viable technical solution. In practice, the SIS II transliteration tables needed to be aligned with the latest ICAO specifications.

In February 2018, Member States reported a business issue[40] related to the ICAO transliteration. The work of the SIS II CMG focused on this matter from February 2018 until February 2019, when a technical solution was defined and an agreement reached on implementation in 2019.

[38] The availability target for Central SIS II, as per the legal basis, is set at 99.9%.
[39] 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 process applies equally to all systems under eu-LISA's responsibility, in a uniform manner.
[40] The checks performed using SIS II at borders were particularly affected by lack of alignment due to different sets of transliteration rules. Passports issued from 2016 were in line with the enhanced ICAO standards, whereas the SIS II transliteration tables were not.

In addition to the several meetings organised to deal with ICAO transliteration, the CMG met several times during the reporting period by webinar and face to face to discuss data quality, identity management for alerts on persons, and release management. In total, 13 meetings were held during the reporting period.

The functional Release 8.2.0, initially planned for June, was eventually implemented on 4 July 2017. Release 8.2.0 included, in particular, improvements to the DCC functionality, the introduction of the EU laissez-passer as a type of document, the implementation of a NIST checker as part of the AFIS project, a new check to detect the file type for attachments to alerts (aiming to further improve data quality), and an update to code tables. The release was deployed with a switchover to the BCU on 4 July and a switchback to the CU on 10 July.

Following the established practice, the Agency presents to the Advisory Group at the beginning of each year a release plan for the given year comprising two releases, one major and one minor

An unplanned release, Release 8.2.1, was deployed after the implementation of Release 8.2.0 to fix a bug [41]. After deployment of Release 8.2.0, the DCC functionality was not working as expected, and thus a new version of the application was deployed to ensure a stable service. The release was implemented in both the CU and the BCU, with a switchover to the BCU on 2 August 2017 and a switchback to the CU on 3 August.

Release 8.3.0 was deployed in the CU between 21 and 23 November. The release deployed corrective and adaptive items at application and system infrastructure levels to SIS II, as well minor functional changes (e.g. to code tables, two new categories of firearm and a new error code). A switchover and switchback were carried out.

The implementation of AFIS was part of Release 9.0.0, deployed on 5 March 2018. In addition to AFIS, Release 9.0.0 covered a new business rule [42], improvements to the performance of the NIST checker and corrective items. The deployment strategy was a standard one, including data migration, with a switchover to the BCU on 5 March and a switchback to the CU on 7 March. Furthermore, as part of a ramp-up approach, two Member States took part in a gradual entry into operation [43] to ensure the proper functioning of the newly implemented AFIS biometric search functionality. The business benefits of Release 9.0.0 were, among others, providing Member States with a biometric search capability and increasing the throughput for the updating of NIST files. The standard two-phase approach was used to update the central system, with the CU site active and the BCU site on standby.

The technical Release 9.1.0, including adaptive, corrective and evolutionary measures, was deployed on 10 July 2018. The release implemented some bug fixes in relation to identified corrective items, improvements and functional changes (implementing a change request with regard to reports on expired alerts). The release was deployed with a switchover to the BCU on 10 July and a switchback to the CU on 12 July.

In total there were 13 switches to the BCU during the reporting period, due to releases as well as unplanned maintenance. This is always a transparent procedure for Member States [44].

2.6 Testing activities

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 carried out as part of corrective,

[41] The bug affected mainly Belgium, right after its incident on 24 July.
[42] To deny creation of alerts with EU Member State or Associated Country nationalities as the main identity, in accordance with Article 24 of the SIS Regulation.
[43] Two Member States (Portugal and Germany) deployed the new release one by one, and after that the other Member States followed in group.
[44] A switch operation (switchover or switchback) produces a downtime window of around 30 minutes.

adaptive and evolutionary maintenance do not adversely affect the system and its performance. All evolutions are thoroughly tested to ensure the integrity of SIS II and the absence of regression once deployed.

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

For each release, test campaigns are conducted to validate the changes while ensuring the integrity of central SIS II and the absence of regression

Extensive tests, both functional and non-functional, were conducted prior to a release being deployed in 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 the 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 will be impacted as little as possible.

For the releases deployed in SIS II during the reporting period, successful tests were carried out in the first half of 2017 for Release 8.2.0; in the second half of 2017 for Release 8.3.0; in the first half of 2018 for Release 9.0.0; and in the second half of 2018 for Release 9.1.0.

AFIS integration

In Q3-Q4 2017, nine pilot Member States — Austria, Germany, Latvia, Liechtenstein, Luxembourg, the Netherlands, Poland, Portugal and Switzerland — started tests to validate that SIS II could handle fingerprints as part of the alert management process and that the related fingerprints could be searched. In 2018, Greece, Hungary, Italy, Malta, Slovenia and Spain also successfully passed those sets of tests.

Test campaigns with Member States

Tests are also executed to support new Member States and agencies integrating SIS II into or substantially changing their national systems. eu-LISA coordinates and plans these tests, as well as determining the test requirements. Member States assist eu-LISA in the overall performance of all tasks related to test execution. The results of tests 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 main test campaigns performed in the reporting period were as follows:

- Bulgaria conducted a compliance test campaign to validate the update to the N.SIS hardware infrastructure in 2017.
- Croatia performed an entry into operations rehearsal test on the procedure for going live in Q1-Q2 2017.
- In 2017, Estonia conducted compliance, performance and SIRENE test campaigns to validate the move of the N.SIS to a new data centre. In 2018, it carried out compliance and performance test campaigns to validate the N.SIS Java upgrade.
- France conducted compliance and performance test campaigns in 2018 to validate the upgrade to the Steria Interconnect Box and Oracle Database.
- Greece carried out connectivity, robustness and performance test campaigns in 2017 to validate the replacement of the main site hardware and the activation of a backup site.
- Iceland conducted performance tests in 2017 to validate the migration of N.SIS to a new platform.
- Ireland began conducting a test campaign to validate its integration into SIS II in 2018 and was to continue in 2019.

- The Netherlands conducted a CRUD, DCC test campaign to validate the patch update to the N.SIS message-orientated middleware in 2018.
- Portugal conducted compliance and performance test campaigns in 2018 and was to continue in 2019 to validate the update to the N.SIS database.
- Slovakia conducted a performance test campaign in 2017 to validate the N.SIS database 2 upgrade.
- Slovenia conducted a compliance test campaign in 2017 to validate linking operations.
- Spain conducted a connectivity test campaign in 2017 to validate a change to the message-oriented middleware.
- Switzerland conducted a connectivity test campaign in 2018 to validate a patch update to the N.SIS message-orientated middleware.

2.6 Data quality and reporting

Member States are responsible for ensuring that the data they enter into SIS II are accurate, up to date and entered lawfully under Article 49 of the SIS II Decision and Article 34 of the SIS II Regulation. Data quality is a key element to ensure and maintain the efficiency of SIS II. Efforts to support Member States in improving data quality continued throughout the reporting period.

Since the summer of 2016, monthly reports on data quality have been produced based on a set of identified criteria. Since April 2017, enhanced reports have been provided focusing on alerts on person. These reports allow Member States to perform checks on their data and if necessary to correct the data stored in SIS II, as they provide an overview of the data that do not match the rules set out in the requirements (the criteria). Thus, the reports are a tool for monitoring the quality of the data and also for developing a national approach to data quality.

Since 2016, the criteria have been regularly updated, revised and/or adjusted at the request of Member States. Requirements have been discussed and collected during meetings of the CMG, as well as in dedicated workshops. Data quality workshops with the participation of Member States were held in February, March and October 2017 and in June 2018.

With the new eu-LISA Regulation, the Agency became responsible for reinforcing data quality by introducing a central data quality monitoring tool

The important topic of data quality generated widespread discussion among political and technical stakeholders, resulting in clear legislative developments. The extensive discussions on how to improve the data quality of large-scale IT systems, and related legislative proposals and negotiations, shaped the Agency's new mandate on data quality. The new eu-LISA Regulation[45], which entered into force at the end of 2018, tasks the Agency with ensuring data quality without prejudice to Member States' responsibilities[46]. In addition, the new SIS legal basis moves in the same direction, indicating that eu-LISA is responsible for reinforcing data quality by introducing a central data quality monitoring tool[47]. The tool, envisaged as a central repository, will serve also for reporting and statistics.

In terms of statistics, eu-LISA regularly provides the Member States and the European Commission with a set of daily and monthly statistics on the business use of SIS II and AFIS. Currently, these statistics are provided using a secure dedicated environment with controlled access. Moreover, following a request from the Commission in spring 2017 and a subsequent agreement with the Member States, eu-LISA has started proving SIS II statistics on an annual basis to support the Commission in monitoring the fulfilment of the visa

[45] OJ L 295, 21.11.2018.
[46] Article 1(7)(a) and Article 12 of Regulation (EU) 2018/1726.
[47] Recital 14, Articles 15(4) and Article 60(2) of Regulation (EU) 2018/1861 and the parallel provisions in Regulation (EU) 2018/1862.

liberalisation benchmarks[48] in the context of the visa suspension mechanism. In addition, the Agency provided statistics on an ad hoc basis during the reporting period, in particular to support the Commission in its task of implementing the SIS II legal framework.

In July 2017, the data amnesty exercise was deemed to be concluded, as there were no more non-compliant alerts[49] in the system. Therefore, since then no further statistics have been generated in this respect.

On an annual basis, the Agency collects statistics from Member States as per Article 50(3) of the SIS II Regulation and Article 66(3) of the SIS II Decision. The data collected and statistics available at a central level are compiled in the SIS II annual statistics report submitted to the EU institutions and published on the Agency's website[50].

2.8 Training activities

Training activities represent part of the Agency's responsibilities towards the SIS community[51]. eu-LISA is responsible for providing training on the technical use of the system to national SIS II operators, SIRENE staff and Schengen evaluators. In addition to being a legal requirement, the training programme for national IT operators and technical SIS II experts facilitates the operational management of the system because it supports technical maintenance; facilitates communication through the single point of contact (SPoC/Service Desk); and helps to ensure data consistency, synchronisation and data quality. Furthermore, training in SIS II is part of the integration project scheme for connecting new Member States to the system, thus supporting newcomers in developing and operating their national systems.

29 training activities were provided to the SIS community in 2017 and 24 in 2018, including face-to-face training and webinars

Once a year in autumn, a questionnaire is sent to NCPs to collect information on all training needs. The NCPs meet to discuss and agree on an analysis, which is then translated into training activities for the following year. The annual training plan is presented to the Advisory Group at the beginning of each year. During the year, changes and additions to the plan — following requests from the various stakeholders — are accommodated depending on the availability of resources. In the first semester of 2018, the Management Board adopted the updated training strategy.

In September 2017, a new training framework named Development Training Programme for IT Operators (DTPITO) was launched; it is a three-level programme (entry, intermediate, advanced). In 2017, eu-LISA delivered 29 training activities focusing on SIS II. The majority of these activities were managed by the Agency and a few by the Agency in cooperation with CEPOL and the European Commission. Activities included the first full DTPITO cycle; two training sessions on AFIS; five webinars on technical topics[52]; eight webinars on preparation of Schengen evaluations for SIS/SIRENE; and two sessions for the integration of newcomers (Croatia and Ireland).

Similarly in 2018, the Agency delivered 24 training activities, including four face-to-face sessions on the SIS II central simulator; the full DTPITO cycle; five webinars on preparation of Schengen evaluations for SIS/SIRENE; one session to support Ireland's integration; two webinars on technical topics; and two sessions on AFIS. During

[48] Visa liberalisation regimes can be suspended if certain criteria are met, including significant increases in rates of refusal of entry to the Schengen area for citizens of a country or in the number of serious criminal offences committed by citizens of that country. The European Commission is required to monitor these criteria and report on them annually.
[49] Regular statistics were provided for monitoring alerts migrated from SIS1+, which required intervention in order to comply with SIS II legal requirements.
[50] Annual statistics are 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. The report in which they are published can be found at http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx
[51] As per Article 3 of the new eu-LISA Regulation and the parallel provision in the old regulation.
[52] DCCs, national copies, switch operations (switchover or switchback).

the 2018 NCP meeting, a new methodology was agreed for the SIS training programme 2019. The new methodology entails a shift from the DTPITO-based programme to a profile-based approach. This new approach will be used for SIS training activities in 2019, and for training activities in relation to the other systems thereafter.

Cooperation with the Justice and Home Affairs agencies continued, in particular with CEPOL and Europol. Horizontal activities such as the train-the-trainers course and a training session in the context of the EU policy cycle for the Empact facilitation of illegal immigration priority[53] are organised regularly, once a year.

In 2017, eu-LISA launched the Learning Management System platform, and since then it has been growing significantly. The purposes of the platform are multiple: supporting training activities, providing opportunities for independent study (by functioning as a library of e-learning materials), information sharing and acting as a cooperative space for the NCP community.

In relation to the Schengen evaluation mechanism, in addition to the webinars, eu-LISA supported the European Commission and the Member States by participating as an observer in all SIS/SIRENE evaluation missions organised during the reporting period[54]. Being responsible for the operational management of central SIS II, the Agency has built up unique technical expertise that is particularly relevant in this context.

3. Communication infrastructure

According to Article 4(1)(c) of the SIS II legal instruments, one of the three elements comprising SIS II is a communication infrastructure between the central system (CS-SIS) and the national interfaces (NI-SIS). The communication infrastructure 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 SIS II communication infrastructure is a community under the European private secure network named Trans European Services for Telematics between Administrations — New Generation (TESTA-ng). TESTA-ng was initially implemented by the European Commission's Directorate-General for Informatics.

The services covered by the TESTA-ng network include the provision of a Core Management Team, responsible for the overall vision, design and security of TESTA-ng and the leadership, communication and management of the service delivery team; a dedicated centralised Support and Operations Centre (SOC), responsible for ensuring the operational management by the provider and the quality of the network on a 24/7 basis; consultancy services; connectivity; network; and 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.

During the reporting period, the tasks regarding the communication infrastructure (including operational management and security) were divided[55] between eu-LISA and the European Commission as defined in the Memorandum

Implementation of the budget, acquisition and renewal, and contractual matters relating to the communication infrastructure between the SIS II central system and national interfaces are now entrusted to the Agency

[53] Eurodac and SIS II: the role of large-scale IT systems in combating facilitation of illegal immigration.
[54] In line with Regulation (EU) No 1053/2013, the Commission has invited eu-LISA to participate as an observer in SIS/SIRENE evaluations since 2015. During the reporting period, eu-LISA experts supported 13 evaluation missions (eight in 2017 and five in 2018).
[55] The Agency was responsible for supervision, security and coordination of relations between the Member States and the network provider for the communication infrastructure of SIS II. In addition, eu-LISA was also in charge of the security measures in respect of the exchange of supplementary information through the communication infrastructure of SIS II. The Commission was 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 was also responsible for adopting the security measures, including a security plan, in relation to the communication infrastructure.

of Understanding concluded in June 2014. Meanwhile, at the end of 2018 the new eu-LISA Regulation entered into force, bringing about substantial changes in the management of the communication infrastructure. According to Article 11(1) of the new eu-LISA Regulation, the Agency must carry out all tasks related to the communication infrastructure of the systems conferred on it by the Union legal acts governing the systems, with the exception of those systems that make use of the EuroDomain. Therefore, tasks related to the implementation of the budget, acquisition and renewal, and contractual matters relating to the communication infrastructure between the SIS II central system and national interfaces are now entrusted to the Agency.

Furthermore, Article 11(4) states that tasks related to the delivery, setting up, maintenance and monitoring of the communication infrastructure may be entrusted to external private sector entities or bodies[56] in accordance with Regulation 2018/1046. The Agency implemented all necessary security measures in accordance with Articles 3 and 5 of the new regulation in order to prevent external private sector entities or bodies — including network providers — having access, by any means, to any operational data stored in the SIS II system or transferred through the communication infrastructure or to the SIS II-related SIRENE exchange.

3.1 Technical functioning of the communication infrastructure

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

The confidentiality of SIS II communications over the sTESTA/TESTA-ng network, in particular between the central system and national systems, is ensured by a secondary encryption layer made up of dedicated encryption devices. These are fully managed by eu-LISA to ensure that third parties cannot gain access to clear-text data.

In September 2017, the TESTA-ng roll out was completed at central level, concluding the complex and long SIS II network migration from the old sTESTA to the TESTA-ng

The SIS II-related SIRENE exchange service operates within the SIS II communication infrastructure and provides simple mail transport protocol (SMTP) relay functionality in a hub-and-spoke topology to SIRENE national systems for the purposes of supporting the SIS II-related SIRENE information exchange.

The SIS II communication infrastructure is permanently monitored to ensure continuous service availability; strict contractual performance service level requirements have been established. During the reporting period, there were no incidents with a critical impact[57] on the functioning of the overall SIS II community. There were in total two incidents affecting overall service availability with a less than critical impact, caused by hardware and software malfunctioning. These incidents caused in total 1 hour and 5 minutes of unavailability of the central system. Following the established practice, the incidents were analysed to identify the root cause and appropriate measures were implemented to prevent recurrence.

Between February 2017 and September 2017, the TESTA-ng roll out took place at central level. The rollout consisted in two main activities: the migration of the multiprotocol label switching (MPLS) network connecting NS-SIS and CS-SIS, and the migration of the point-to-point connection between Strasbourg and Sankt Johann im Pongau used by SIS II for database synchronisation. This activity concluded the complex and long migration

[56] All private sector entities or bodies must be bound by the security measures referred to in paragraph 3 and are to have no access, by any means, to any operational data stored in the systems or transferred through the communication infrastructure or to the SIS II-related SIRENE exchange.
[57] A critical impact is considered to have occurred when the service is not available for more than 8 hours and the entire community is affected.

of the network from the old sTESTA communication infrastructure to the new TESTA-ng[58]. The migration resulted in higher throughput for SIS II, allowing an increase in SIS II transaction capacity.

4. Security

The overall security framework for SIS II and its communication infrastructure provides assurance that, at central level, the system protects the information stored and it functions as required. The security measures applicable to CS-SIS, as per the legal provisions, are defined in the SIS II security plan and SIS II security policy, both adopted by eu-LISA's Management Board in March 2013. Currently, eu-LISA is in the process of revising the SISII security plan, in particular to include AFIS. The adoption of the new SIS II security plan is expected by Q4 2019.

The measures described in the security policy[59] define the principles of least privileges, security by default, defence in depth and segregation of duties. The SIS II security plan sets out measures for controlling access to data processing facilities; access to SIS II hardware and software; removable media containing data and any other important assets; storage of data; passwords; and communication through the communication infrastructure. The security controls are chosen based on a risk assessment done using the E-BIOS methodology.

In terms of physical security, the SIS II central system is protected by 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[60]. In the event of a disaster situation, operations can be switched to the backup site in Austria, where a permanent eu-LISA staff presence is ensured. All persons having logical or physical access to the production systems (central or backup sites) hold a valid personnel security clearance[61]. 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.

All activities carried out within SIS II are strictly controlled, monitored and logged. All communication with Member States is protected by multiple layers of encryption and by network security controls with several layers of firewalls and integrity checks. 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 incidents that may compromise SIS II operations and data.

In terms of security audits and assessments, the Agency's security policy requires that all Agency information systems are subject to regular security assessments and vulnerability and penetration testing. This in order to provide security assurance and to verify that the implementation, integration and configuration are compliant with defined security requirements. CS-SIS undergoes technical vulnerability tests and baseline security self-assessments on a regular basis.

The Security Unit was involved in several SIS II projects during the reporting period. Following the study completed in 2015 on a central user repository (CUR) for SIS II, the CUR was implemented in March 2018 as part

[58] Member States were migrated between November 2016 and September 2017.
[59] The measures to be provided for in the security policy, according to Article 16(1) of the SIS II Decision, include restrictions on 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.
[60] The security guard service is outsourced to an external company and it is supervised and monitored by internal security staff.
[61] Confidentiality and secrecy agreements are concluded with staff and contractors required to work with Central SIS II.

of the SIS AFIS. Thanks to that, all accounts are now provisioned and managed in a centralised way for all SIS II core and AFIS components (operating systems, applications, databases, network elements, etc.).

In the context of the implementation of the common shared infrastructure, the Security Unit is in the process of updating the security capabilities for all core business systems, including SIS II. This comprises the implementation of a new monitoring tool, Security Information Event Management, following the signature of the relevant contract in 2018, as well as a new public key infrastructure.

In 2018, the Security Unit participated in the evaluation of the call for tender for the new MWO for SIS II. Furthermore, the Security Unit was involved in the handover from the previous contractor to the new MWO contractor, to validate the security position of the new contractor (i.e. that this was aligned with the eu-LISA security requirements as defined in the Agency's security policies and rules). In this respect, multiple audits were performed at the MWO contractor's premises and sites to validate the operational effectiveness of the controls defined in the framework contract security plan, the Agency's security rules and industry security best practices.

The first end-to-end business continuity and disaster recovery exercise on SIS II was executed in October 2018 with the participation of several Member States

In November 2018, the European Data Protection Supervisor (EDPS) carried out an inspection of central SIS II with the support of the Security Unit. The inspection included checks to follow up on the recommendations from the previous SIS II inspection (carried out in 2015); an assessment of elements of information security management (e.g. the security incident management procedure, with a focus on personal data breaches); the personal data retention period; system acquisition; and the security of central SIS II and its communication infrastructure.

During the reporting period, the SON met regularly, twice a year[62].

Business continuity and disaster recovery exercise

In the second half of 2017, eu-LISA started preparations for the first business continuity and disaster recovery exercise for SIS II. The exercise was conceived as a technical end-to-end cyber-exercise aimed at testing the security, business continuity and disaster recovery capabilities of SIS II at central and national levels. In addition, the exercise was intended to improve the coordination and communication between the participating entities, providing an opportunity to identify gaps in resources, processes and procedures and, based on the outcomes, make recommendations for improvement.

The exercise involved several stakeholders: eu-LISA, nine Member States[63] as participants, seven Member States as observers[64], the European Union Agency for Cybersecurity providing support and the European Commission. The preparation lasted 1 year, and the exercise was executed at the end of October 2018 on the SIS pre-production environment (PPE). The PPE was connected with the participating Member States' test environments, which technically performed the exercise. Following the exercise, during the evaluation phase, a report with a set of recommendations was drafted. The report was first presented to the SIS II AG and later adopted by the Management Board, in spring 2019.

5. Data protection

[62] The forum was established by eu-LISA's Management Board in 2014 with the aim of facilitating more effective information exchange among Member State experts.
[63] Austria, France, Germany, Greece, Iceland, Latvia, the Netherlands, Portugal and Slovenia.
[64] Denmark, Hungary, Italy, Malta, Spain, Sweden and the United Kingdom.

At both central and national levels, the SIS II technical solution complies with strict data protection requirements. The EDPS, in close cooperation with eu-LISA's Data Protection Officer (DPO), monitors the implementation of data protection provisions, in particular concerning the processing of personal data by Central SIS II.

As mentioned above, in November 2018 the EDPS inspected Central SIS II. Following the established practice, the DPO coordinated the inspection and acted as a liaison between the Agency and the EDPS during the entire exercise (from the preparation phase through the on-site visit and the post-visit document requests and comments to the draft report).

During the reporting period, the DPO was involved in several projects of general scope, including data quality and change management matters, in particular in relation to the ICAO specifications. The EDPS was consulted on a regular basis.

In October 2018, the EDPS inspection on central SIS II was carried out in cooperation with the Security unit and DPO

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

6. Exchange of supplementary information between Member States

As mentioned above, on a yearly basis eu-LISA collects statistical data from the Member States. The number of hits achieved and the number of forms exchanged among Member States are some of the data collected. This section presents data on forms and hits reported by Member States for the reporting period.

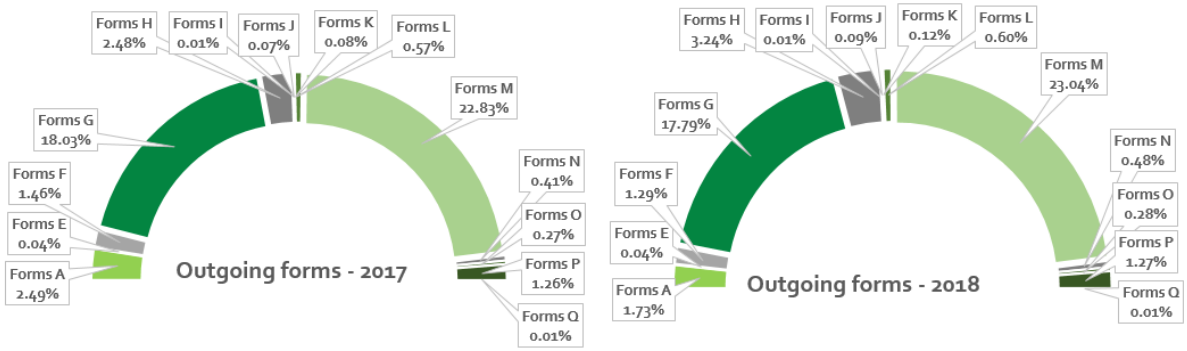
6.1 Exchange of forms

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 are to exchange supplementary information related to an alert that is required to implement certain provisions. The exchange of supplementary information is done using specific forms, and it may be on a bilateral or a multilateral basis. 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.

In 2017, there were in total 2,211,610 forms[65] exchanged bilaterally or multilaterally between Member States. In 2018, 2,132,760 forms were exchanged. The figures below provide a breakdown of outgoing[66] forms — the forms sent by all SIRENE Bureaux — for the reporting period. A further breakdown of the data is available in Table 1 in the annex.

[65] 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); however, 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.

[66] Some Member States reported having separately sent historical A and M forms to Croatia for the initial load prior to its connection to SIS II in May 2017, as per Council Decision 2017/733. Those forms are not counted in the statistics provided.



The exchange of supplementary information through SIS II has a crucial role, as it contributes to effective law enforcement cooperation and border management in Europe. Looking at the figures for the past 4 years, almost 3,900 forms (both outgoing and incoming forms) were exchanged on average each day among SIRENE Bureaux in Europe in 2014, whereas in 2018 the equivalent figure had increased to 5,900 per day.

6.2 Hits

A 'hit' occurs in SIS II when a user conducts a search and the search reveals a foreign alert (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).

In 2017, Member States reported 243,818 hits on foreign alerts; the figure had increased to 267,239 in 2018.The figures below provide a breakdown of hits on foreign alerts for the reporting period. A further breakdown of the data is available in Tables 2 and 3 in the annex.

The hits on foreign alerts reported by Member States in 2018 showed an increase of over 10% compared with the 2017 data. These have been steadily increasing in the past few years. Looking at the figures for the past 4 years, there were 353 hits per day achieved in 2014, in 2018 the equivalent figure had increased to 732 hits per day. This is an increase of over 100% in 4 years.

Conclusion and looking forward

SIS II, being at the heart of Schengen, is Europe's most widely used information-sharing system for internal security and border management. eu-LISA guarantees the effective and uninterrupted operational management of its critical infrastructure, agile project management for the timely evolution of the SIS central system and appropriate 24/7 operational monitoring support.

During the reporting period, central SIS II has been performing well, in line with the legal requirements, and no critical incidents were reported. Its use is constantly growing, as evidenced by:

- the 16% increase in data stored in the database from 2017 to 2018;
- the increase in searches reported by Member States from 10.6 million searches per day in 2016 to 16.8 million searches per day in 2018;
- the increase in hits achieved by Member States from 550 hits per day in 2016 to 732 hits per day in 2018.

Fruitful cooperation with all stakeholders involved, in particular the Member States and the European Commission, has been instrumental in ensuring effective operational management. An important milestone accomplished during the reporting period, on 5 March 2018, was the entry into operation at central level and in 10 Member States of AFIS. This development, enabling end-users to search SIS II on the basis of fingerprint data, has further increased the internal security of the Schengen area.

Looking to the future, eu-LISA remains strongly committed to keeping the SIS II central system in operation on a 24/7 basis while assuring its operational maintenance and development as per the legal requirements. Major enhancements to SIS II will continue in the coming years. In particular, the implementation in phases of the new legal basis has already started, with the aim of maximising the effectiveness and efficiency of SIS II, focusing on end-users and extending the access of EU agencies. Moreover, interoperability will be implemented, ensuring enhanced use in a smarter way of EU large-scale IT systems, including SIS II. This will allow, among other things, increased effectiveness of identity checks and easier access to the systems for relevant national authorities.

Annex

Table 1: SIRENE forms

	2017		2018	
	Outgoing	Incoming	Outgoing	Incoming
Forms A	29,594	633,103	20,449	596,066
Forms E	528	461	466	565
Forms F	17,372	17,309	15,240	14,620
Forms G	214,636	203,490	209,661	210,488
Forms H	29,521	32,519	38,239	41,364
Forms I	133	130	124	123
Forms J	888	985	1,107	1,196
Forms K	935	964	1,403	1,432
Forms L	6,747	10,339	7,102	10,470
Forms M	271,864	692,939	271,586	642,883
Forms N	4,859	4,975	5,602	5,645
Forms O	3,226	3,178	3,278	3,245
Forms P	14,947	15,661	15,020	15,068
Forms Q	102	205	106	212
Total forms	**595,352**	**1,616,258**	**589,383**	**1,543,377**

Table 2: SIS II hits

	2017		2018	
	hits abroad on own alerts	hits on foreign alerts	hits abroad on own alerts	hits on foreign alerts
Article 26 SIS II Dec	11,356	11,703	11,321	12,564
Article 24 SIS II Reg	30,540	38,070	39,518	47,740
Article 32 SIS II Dec	7,841	8,650	8,259	9,658
Article 34 SIS II Dec	43,800	57,706	46,652	54,744
Article 36 SIS II Dec	78,643	79,923	87,238	89,763
Article 38 SIS II Dec	41,672	47,766	47,487	52,770
Total hits	**213,852**	**243,818**	**240,475**	**267,239**

Table 3: Breakdown of hits under Article 38 of the SIS II Decision[67]

	2017		2018	
	hits abroad on own alerts	hits on foreign alerts	hits abroad on own alerts	hits on foreign alerts
Vehicles, trailers, car.	12,006	13,101	14,954	15,554
Boats	26	21	10	8
Aircraft	1	2	7	0
Industrial equipment	101	138	108	171
Boat engines	48	71	54	58
Containers	4	7	4	6
Firearms	208	185	237	199
Blank docs	1,655	1,610	1,236	1,216
Vehicle registration c.	1,126	1,256	945	1,221
Number plates	2,170	2,753	2,197	2,524
Issued docs	23,449	28,216	27,681	31,714
Banknotes	32	67	20	56
Securities & MoP	40	42	34	43
Total article 38 SIS II	**41,672**	**47,766**	**47,487**	**52,770**

[67] 'Vehicle, trailers, car.' stands for 'vehicles, trailers, caravans'; 'vehicles registration c.' stands for 'vehicles registration certificates'; 'securities & MoP' stands for 'securities and means of payment'.

EL-AE-19-001-EN-N

ISBN: 978-92-95208-88-9
ISSN: 2443-8294
doi: 10.2857/725446