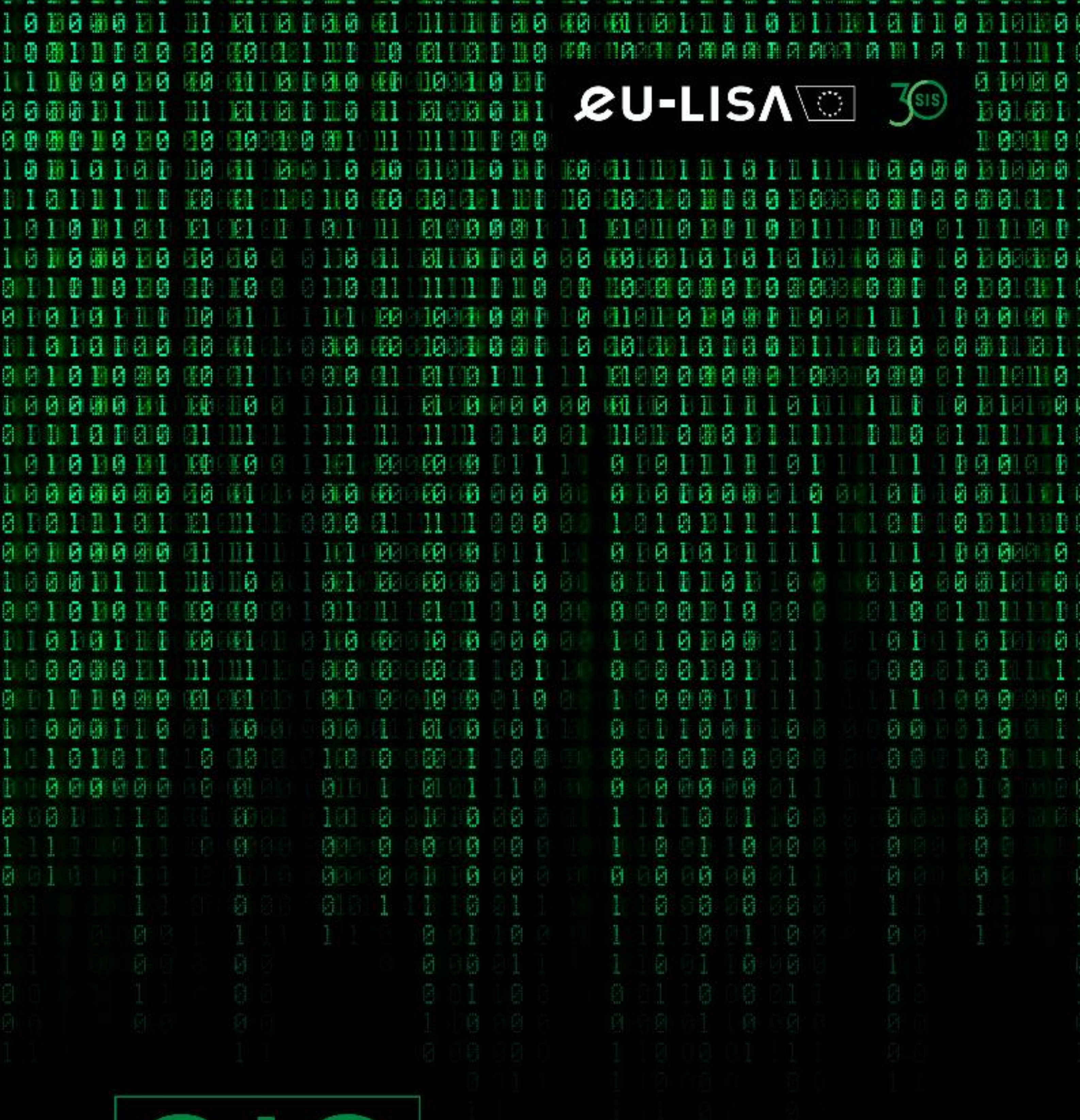


SIS 2023 - 2024

TECHNICAL REPORT

Contents

3 **Executive Summary**

4 **1. Introduction**

6 **2. Operational management of central SIS**

7 2.1. Entry into operation of SIS Recast

9 2.2. SIS biometric system evolution

10 2.3. Integration projects

11 2.4. Further evolution of Central SIS – projects

13 2.5. Deployment of releases and testing activities

14 2.6. Monitoring and operational activities

16 2.7. Performance of the central SIS

16 2.8. Training activities

17 2.9. Communication infrastructure

18 2.10. Security

19 2.11. Data protection

20 **3. SIRENE forms exchanged and hits handled**

21 3.1. SIRENE forms exchanged

23 3.2. Hits handled

24 **Conclusion**

26 **Annex**

EXECUTIVE SUMMARY

EVOLUTIONS

RECAST
EiO MARCH 2023

NEW ALERTS

WIDER ACCESS

NEW FUNCTIONALITIES

NEW BIOMETRICS

AFIS EVOLUTION

INTEGRATION PROJECTS

CYPRUS
JULY 2023

FRONTEX
JUNE 2024

AVAILABILITY

99.67%
2023

99.78%
2024

MOST RELEVANT PROJECTS

SIS4ETIAS

SIS4VIS

SIS4IO

INFORMATION ALERT

SIS FACIAL RECOGNITION

SIS CORE TO ORACLE EXADATA

SIS INCREASE CAPACITY

1 INTRODUCTION

1. Introduction

Serving as a key component of the Schengen *acquis*, the Schengen Information System (SIS) is **the EU's most widely used information-sharing system** for internal security, border management and migration. SIS, which entered into operation in 1995, compensates for the abolition of internal border controls in the Schengen area, allowing for the free movement of people within the area by providing essential support for managing Schengen's external borders, ensuring a high level of internal security and contributing to law enforcement and judicial cooperation across Europe.

SIS facilitates operational cooperation between national competent authorities, including border guards, police, SIRENE Bureaux, as well as judicial, customs and immigration authorities. The system enables these competent authorities to enter data on persons of interest or objects, use it for consultation purposes, and to take specific action where required. eu-LISA publishes an updated list of the competent authorities having access to the system, as well as of SIRENE Bureaux[1], in the Official Journal of the EU on a yearly basis.

By the end of the reporting period (31 December 2024), SIS was in use by **31 countries[2], as well as by Europol, Eurojust and Frontex**. During the reporting period, both Cyprus and Frontex were also granted access to the system.

eu-LISA (the Agency) is responsible for the operational management of central SIS and for guaranteeing its effective **uninterrupted access and functioning 24/7**. The eu-LISA Management Board, together with the SIS Advisory Group (AG), support the Agency in this respect. eu-LISA shares responsibility for SIS governance together with the European Commission, Member States and several other stakeholders. The Commission is responsible for the correct implementation of the SIS legal framework and for any legislative initiatives linked to the system.

The SIS Advisory Group comprises representatives from each Member State, a representative of the Commission and appointed observers from Europol, Eurojust and Frontex. This regular forum decides on changes to be endorsed and on the implementation of timelines, taking into account both constraints and dependencies. The SIS Advisory Group also reports on the availability of the central SIS and national systems, approves release plans, discusses and maps out developments, assesses training activities, and issues an annual statistics report.

In addition to the SIS Advisory Group, several dedicated and *ad hoc* fora support the work of the Agency in relation to SIS. These include the SIS Interoperability Project Management Forum (SIS IO PMF), SIS Recast PMF[3], and more broadly the Security Officers' Network, the Biometric Working Group and the National Contact Points for training.

This report, as part of eu-LISA's legal reporting obligations[4], covers the period from **1 January 2023 to 31 December 2024**. As the sixth in a series of reports on the technical operation of the central SIS and its communication infrastructure, the report aims to enhance transparency and visibility of system usage, maintenance and ongoing developments. It reviews all activities related to the operational management of the central SIS, including security, together with a yearly statistical report in particular the number of SIRENE forms exchanged and the hits reported by the Member States.

[1] OJ C/2024/3875 and 3876 of 05.07.2024.

[2] The 31 countries using the SIS are all EU Member States and the Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland).

[3] Discontinued with the launch of the SIS Recast.

[4] As per Article 60(7) Regulation (EU) 2018/1861 and Article 74(8) Regulation (EU) 2018/1862.

2

OPERATIONAL MANAGEMENT OF CENTRAL SIS

2. Operational management of central SIS

SIS enables the sharing of information about individuals of interest as well as objects, such as identity documents or vehicles, for example, between law enforcement authorities and judicial bodies across Europe. Responsibility for the operation of the central SIS lies with eu-LISA, which ensures 24/7 uninterrupted access to the system and enables continuous data exchanges between national authorities, in full compliance with the relevant legal framework. Operational management is carried out largely through management services, supervision and the implementation of appropriate corrective, adaptive and evolutionary maintenance.

Under the maintenance-in-working-order (SIS MWO) the SIS framework contract, an external contractor oversaw maintenance and technical support for eu-LISA during the reporting period. However, the former SIS MWO contract expired during the reporting period. To develop synergies and increase economies of scale, eu-LISA established new framework contracts of a transversal nature covering adaptive and corrective maintenance, development and further evolution for several systems (including SIS). The process of transferring SIS knowledge and responsibility from the previous contractor to its successors was completed in autumn 2024, with the final pending transfer being concluded at the end of April 2025.

Usage of the Schengen Information System has steadily increased over the years reaching over 15 billion searches in 2024, reflecting the system's high relevance in meeting the operational needs of competent authorities. This growth is also attributable in part to the most recent implementation of the Recast, which broadened the scope of the system and at the same time expanded the authorities having access. Given this context, proper maintenance and timely evolution of the system are of primordial importance.

2.1. Entry into operation of SIS Recast

During the reporting period, SIS underwent the last stage of its most significant and comprehensive update since 2013. This update, titled SIS Recast, introduced new categories of data and alerts, extended the scope of some alerts, as well as expanded access to SIS alerts at both the national and European levels. The updated system became operational on 7 March 2023 with the Release 21_R2, when its name was changed from SIS II to SIS.

The updated system introduces a range of new features, including alerts for return decisions, unknown wanted persons and preventive measures, as well as enhanced enquiry checks and new object types. Additionally, the biometrics capabilities have been expanded to include palmprints, facial images[5], DNA and latent prints, thereby allowing for more advanced searches. The technical possibilities have also been expanded to include additional tools for protecting missing persons, tracking individuals through objects, and utilising new warning signals and categories. Furthermore, the SIS Recast has led to increased access for national authorities and European agencies, with Europol and Frontex now having full access, Eurojust having extended access, and national authorities benefiting from broader access overall.

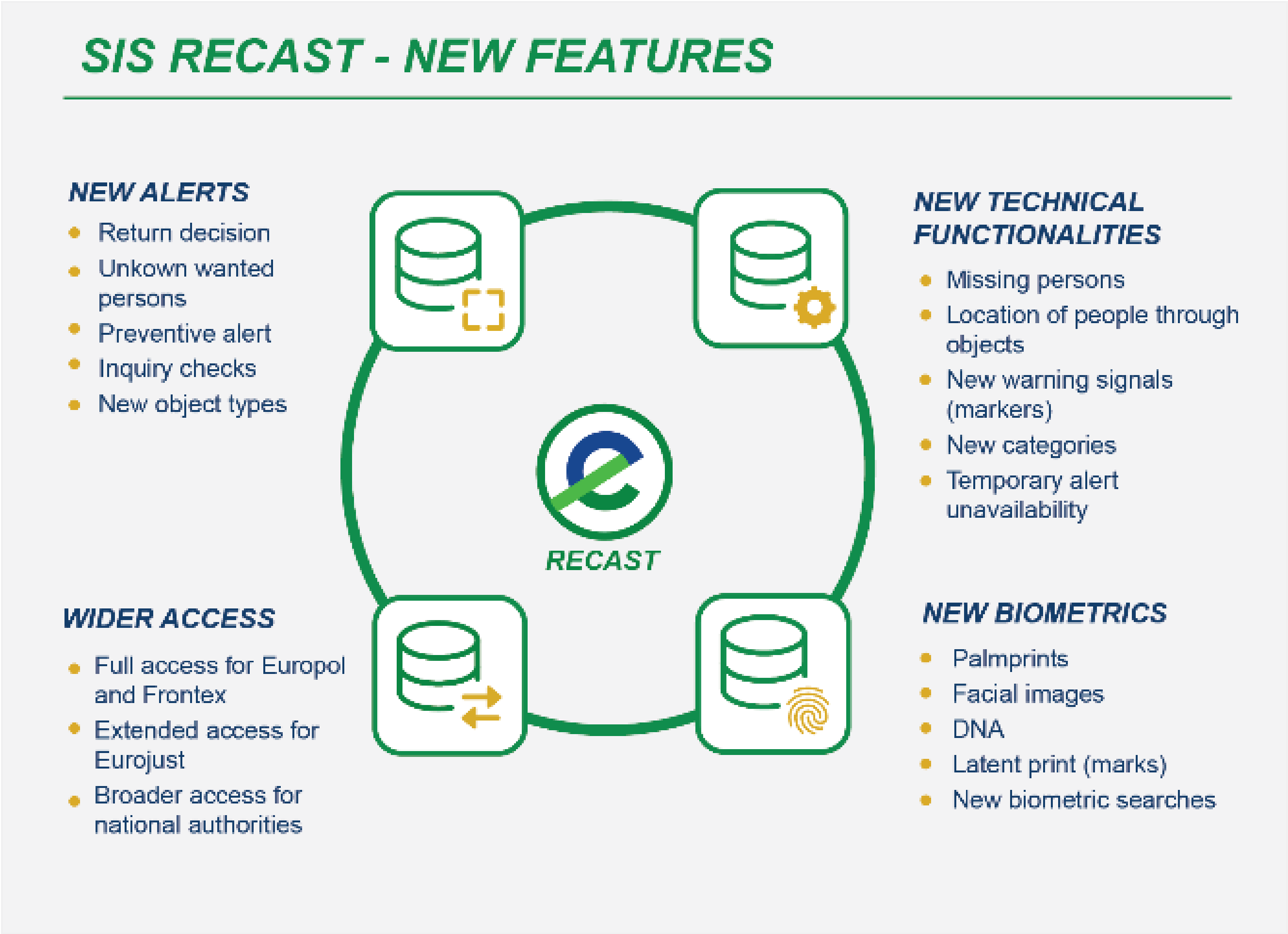
eu-LISA played a fundamental role in the implementation of the new regulations, developing the central SIS, and coordinating test campaigns with both Member States and EU agencies.

In order to ensure the successful implementation of SIS Recast, eu-LISA maintained regular communication with stakeholders on its progress, including via the SIS Recast PMF, the SIS AG, the SIS-SIRENE Committee, the Heads of SIRENE and SPoC, the Working Party on JHA Information Exchange (IXIM) and the SIS and SIRENE Expert Group.

[5] Facial images are stored but are not currently being used for identification.

The development of new functionalities and extensive testing required for proper implementation were being carried out up until January 2023. Major functional and non-functional improvements were delivered in the SIS Central System Simulator (CSSIM) in conjunction with SIS Recast developments.

The entry into operation of SIS Recast was implemented with a delay of approximately 1 year compared to the initial plan. Contractual and testing issues were encountered by some stakeholders as the entry into operation had to be performed following the big bang approach. By January 2023, all Member States and eu-LISA notified the Commission on their technical readiness[6], allowing the Commission to set the date for the entry into operation. The entry into operation of Recast required considerable efforts. To support all stakeholders involved, three internal rehearsals were performed, in addition to one conducted with Member States, focusing on migration and fallback.



SIS RECAST - NEW FEATURES

NEW ALERTS

- Return decision
- Unkown wanted persons
- Preventive alert
- Inquiry checks
- New object types

NEW TECHNICAL FUNCTIONALITIES

- Missing persons
- Location of people through objects
- New warning signals (markers)
- New categories
- Temporary alert unavailability

WIDER ACCESS

- Full access for Europol and Frontex
- Extended access for Eurojust
- Broader access for national authorities

NEW BIOMETRICS

- Palmprints
- Facial images
- DNA
- Latent print (marks)
- New biometric searches

Technical readiness was declared on 20 January 2023. On 30 January, the Commission adopted the Commission Implementing Decision (EU) 2023/201[7] setting **7 March 2023 as the date on which operations for the SIS Recast would commence**, in line with the decisions taken by eu-LISA Management Board[8] and the Council.

[6] As per Article 79(2) of Regulation (EU) 2018/1862 and Article 66(2) of Regulation (EU) 2018/1861.
[7] OJ L 27, 31.01.2023.
[8] On 16 and 17 November 2022, the eu-LISA Management Board decided that SIS Recast entry into operation should happen no later than 7 March 2023, and confirmed to convey it to the Justice and Home Affairs Council.

To support the release activities, a control room was set up in Strasbourg at the operation site. eu-LISA staff, representatives of Member States, together with the Commission and the experts from the contractor, worked throughout the day. The detailed plan for attaining same by 7 March was adhered to; activities began at 07:00 CET with the switchover to BCU (resulting in a downtime of 5 hours and 40 minutes) and concluded at 22:00.

The entry into operation consisted of **the following main stages**:

- Stopping and **consuming all SIS and SIRENE traffic** except for alphanumeric searches;
- **Upgrading to SIS Recast,** resulting in downtime for users;
- Observation period where the service was granted to three Member States for limited operations;
- The **gradual rollout of the service to all Member States**

Alert management operations[9] were not available from 10:00 to 15:40 during the release day, whereas alphanumeric search functionalities remained available throughout the operation, except for an approximate wait time of 5 minutes during the technical process of switching from CU to BCU.

At 19:42, once the observation period ended successfully, the new SIS was progressively rolled out to all Member States. Entry into operation activities continued over a few days, with the switch back from BCU to CU executed on 14 March at 23:00, resulting in 3 hours and 14 minutes of downtime for alert management operations.

Entry into operation consisted of a very large set of interdependent and synchronised activities taking place simultaneously at the central level and the national level. All stakeholders recognised the added value of the rehearsals, which allowed them to build confidence, reduce risks and potential issues, and at the same time, gain an enhanced understanding of the procedure, steps and dependencies.

2.2. SIS biometric system evolution

Since 2018, SIS has been equipped with biometric search capabilities through the Automated Fingerprint Identification System (AFIS), which enables the identification of individuals using fingerprints. This advancement has made SIS a key component of the Schengen framework, playing an important role in managing the EU's external borders while also facilitating cooperation in law enforcement and judicial matters across the Union.

AFIS 2 was a sizeable and integral part of SIS Recast (Release 21_R2). In addition to fingerprints, a broader range of biometric data can now be stored in the system such as palmprints, latent prints, facial images and DNA records.

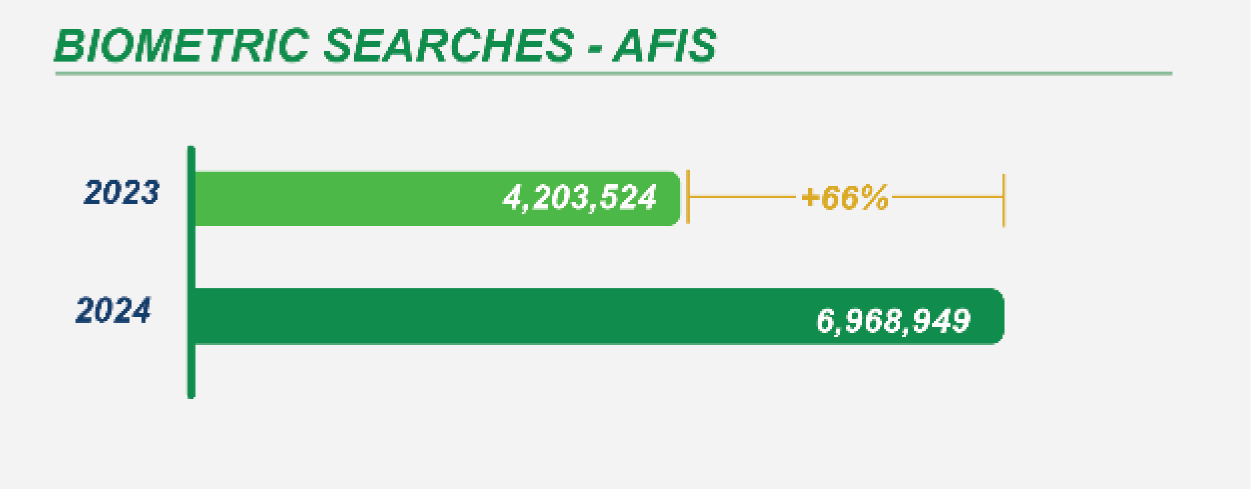
New biometric search functionalities were added as well for latent prints, allowing searching with prints from crime scenes. Since the Recast, there has been increased usage of biometric searches[10].

In the second half of 2024, a survey was conducted among the Member States to learn about the impact of EES entry into operation on the usage of SIS AFIS, as the latter will be used during the EES process. An analysis of the replies is ongoing so as to assess whether the current AFIS functionality will be able to handle the business demands once the EES is live or if a capacity increase will be required.

[9] Create, update and delete alerts.
[10] *SIS – Annual Statistics Report 2024* available at **https://eulisa.europa.eu/our-publications/reports**.

Preparations for the migration of SIS AFIS functionalities to the shared biometric matching service (sBMS) was worked on throughout the reporting period. sBMS is an interoperability component that would allow matching of an individual's biometric data across different systems. The sBMS will be supported by the multiple-identity detector (MID) which will create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for *bona fide* travellers and combatting identity fraud.

Once SIS will be connected to sBMS, the dedicated SIS-AFIS will be discontinued. This enhancement, part of the SIS4IO project, is currently due to be delivered in Q2 2027.



2.3. Integration projects

In July 2023, eu-LISA and Cyprus successfully completed **integration, allowing Cyprus to connect to SIS**. Testing activities were performed from 2 May to 8 June. On the central system side, integration was achieved by means of a configuration change which enabled the Cyprus's connection, and other Member States had visibility on this. Similarly to other integration projects, eu-LISA held a dry-run exercise with Cyprus before the data upload.

From 13 June to 24 July, the Cyprus SIRENE Bureau gathered historical SIRENE forms from other Member States, and SIS production data was uploaded to the Cyprus N.SIS. As per the Council Decision (EU)2023/870[11] of 25 April 2023, from 25 July 2023, the provisions of the Schengen *acquis* relating to SIS applied in the Republic of Cyprus. On that same day, the Cypriot national authorities issued their first SIS alerts and gained the ability to search in SIS.

In July 2023, **Cyprus** and by June 2024, **Frontex** successfully integrated with SIS, enhancing **EU border management and migration support capabilities.**

Concurrently, the Agency collaborated with **Frontex** in developing the necessary technical components for their SIS connection. The project to establish the technical interface allowing Frontex Standing Corps officers to search SIS

[11] OJ L 113, 28.04.2023.

when teams are deployed at the external EU borders was launched in 2021, and Frontex was connected to the system in June 2024. Following this connection, Frontex began conducting searches in Italy in June 2024, and subsequently in Cyprus in December.

Frontex opted for a step-by-step approach in the development and finalisation of the web application to be used by its teams, allowing them to use the pilot/first version while still working towards the full implementation/deployment of the application. In the first phase, the application is used by a limited number of Standing Corps to perform manual alphanumerical searches for second-line checks. In case of a hit, further communication is the responsibility of the host Member State, as Frontex does not have access to the channel of communication with the SIRENE Bureaux.

The integration of Frontex with SIS has significantly enhanced their capabilities, enabling return and migration management support teams to access and search SIS data. This, in turn, facilitates the effective execution of tasks related to border checks, surveillance and returns, ultimately strengthening the management of the European Union's external borders.

2.4. Further evolution of Central SIS – projects

During the reporting period, the Agency worked on several projects with the aim of updating SIS, including the completion of the SIS Recast (see **section 2.2** for details), integrating it with interoperability (IO) components, and improving its maintenance. Following the successful launch of the SIS Recast in March 2023, eu-LISA focused on defining the overall architecture and functionalities of several upcoming evolutions to ensure continuous system improvements. Below are the most relevant projects.

The **SIS Increase Capacity project** introduced new hardware (new versions of technical components) and software in order to be able to handle more alerts and larger attachments. Business needs necessitated increasing the size limit for files that could be attached to SIS alerts, such as fingerprint files or scanned documents. The previous file size limit, for example, could not accommodate the improved quality of fingerprints needed due to advancements in fingerprint identification technology and the evolution of AFIS[12].

In March 2023, over 8 TB of **additional storage** were added to the database, allowing the system to handle up to 130 million alerts. The project was completed in July 2023 with the end of the final testing period.

The **SIS Interconnection with Interoperability** project was launched in January 2022 to align SIS with the requirements set by the Interoperability legal framework and was continuously worked on throughout the reporting period. The project aims to implement interoperability interfaces for biometric/alphanumeric searches across JHA systems and implementing SIS interconnection with other systems.

Close coordination with Member States has been achieved mainly due to the SIS IO Project Management Forum (PMF), a new forum which was established in the second half of 2023 and which was convened for the first time in November 2023. The PMF met 12 times during the reporting period in order to validate user requirements and ICD[13] changes with Member States, to present eu-LISA projects impacting the central SIS, to discuss dependencies and constrains at central and national level, and to share success stories and challenges among Member States.

SIS4IO: By the end of 2024, the SIS interconnection with IO project continued to advance, with a mature requirements package and business use cases under review. In October 2024, a first draft SIS-IO ICD covering yellow and red link notifications was shared with the SIS community. In addition, a separate SIS ICD outlining the query format for SIS through ESP[14] was in preparation. At the time of

[12] Automated Fingerprint Identification System.
[13] Interface Control Document.
[14] European Search Portal.

writing this report, the SIS connection with interoperability components (ESP, sBMS[15], MID[16] and CRRS[17]) was planned for Q2 2027, considering dependencies with other SIS projects and the revised interoperability roadmap.

SIS4ETIAS: SIS connection with ETIAS aimed at enabling automated searches and more streamlined services to system end-users progressed during the reporting period. In particular, the design and functionality testing of the required interconnection module with ETIAS was completed, together with the relevant data protection impact assessment (DPIA). The SIS-IO ICD shared in October 2024 also covered this connection. In addition to that, a full package of SIS ICD/DTS[18] was shared in December. The build phase for the test environment for both hardware and software was successfully completed in 2024.

SIS4rVIS: The project focuses on the integration between SIS and the Revised VIS. By the end of 2024, the SIS4rVIS was undergoing requirement analysis and high-level design finalisation.

In first half of 2024, eu-LISA organised three DEBS[19] workshops with Member States. The aim was to design and update SIRENE forms as per SIS Recast, as well as to facilitate the communication of interoperability notifications to SIRENE Bureaux, similar to the new U SIRENE form to be used for ETIAS.

The **information alert on third-country nationals in the interest of the Union[20]** is a new specific type of known person alert that will be able to be added by Member States upon a proposal by Europol. Since information on third-country nationals is frequently provided by third countries or international organisations only to Europol, Europol will propose the creation of such an alert to Member States. The creation of the alert will be at the discretion and responsibility of the Member State. The issuing Member State will keep the responsibility and data ownership of the alert. By the time of writing this report, the high-level design phase for this new type of alert was completed. The estimated entry into operation was planned for the second quarter of 2026, considering the priorities of the 2025 SIS roadmap (completion first of a corrective release, a business continuity release and the completion of the common tests with ETIAS).

During the reporting period, the **DCC[21] Evolution project** intended to improve data consistency checks continued. The implementation of technical enhancements, such as improvements to broadcast handling, were foreseen as part of 24_R1. The latter, initially planned for implementation during the reporting period, was eventually postponed and its entry into operation is now foreseen for the end of 2025.

Following a one and half year project, all network switches were replaced with newer models and those with long-term support. The project aimed at replacing the end of service-life backend switches and also introducing a homogenous LAN switches platform in all sites (CU and BCU) for all SIS environments (production and pre-production). Implementation included several test phases (unit tests, non-regression tests and low-level infrastructure tests). The migration was successfully completed by December 2023, and was followed by the physical decommissioning of the old appliances.

In addition to the projects mentioned above, **other ongoing and future projects are being worked on and considered**, including:

[15] Shared Biometric Matching Service.
[16] Multiple-Identity Detector.
[17] Central repository for reporting and statistics.
[18] Detail Technical Specifications.
[19] Data Exchange Between SIRENE Bureaux.
[20] Introduced by Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union.
[21] Data Consistency Checks.

Move of SIS Core database to Oracle Exadata: with the aim to modernise the SIS infrastructure, increase its maintainability, improve performance, standardise hardware while generate economies of scale. Testing is ongoing at the central level. Entry into operation is planned with 24_R1 release.

SIS Increase capacity: in addition of increasing the size of the binaries up to 20 MB a redesign of the CUD architecture for a more efficient solution is planned to improve performance,. enabling management of the additional traffic foreseen from interoperability with the other JHA systems. As a first step, a CUD performance study was commissioned. requirement analysis and the high-level design phase for this planned increase are currently ongoing.

SIS Facial Image Recognition: discussions have begun, and the project will be implemented once the legal provisions have been finalised. Similar to the implementation of the AFIS, the first step is for the Commission to present a report to the European Parliament and the Council on the availability, reliability and readiness of the technology as per the provision in the SIS Regulations[22].

The planning of SIS evolutions, i.e. further development and integration with other systems, was revised several times during the reporting period due to numerous constrains and dependencies in relation to the **interoperability roadmap**. At the time of writing, in March 2025, the revised interoperability roadmap has endorsed by the JHA Council.

2.5. Deployment of releases and testing activities

eu-LISA updates SIS with the latest patches and functionalities by means of deploying releases. Rigorous and extensive testing campaigns are carried out before each release minimising the impact on the operational activities of the systems, all the while ensuring steady progress of planned evolutions and projects. During the reporting period, eu-LISA supported the Member States in a variety of testing activities, ensuring that SIS was functioning properly, as required by the SIS legal framework.

The deployment of releases is usually carried out through a switchover and switchback procedure. First, all operations from the central unit (CU) are switched over to the backup central unit (BCU). Once release activities are completed, operations are switched back to the CU. This allows SIS to be kept in operation from the BCU, without any deterioration in performance and availability levels and simultaneously carrying out maintenance/releases on the CU.

During the reporting period, **the following releases were deployed**, introducing new functionalities and technical changes:

21_R2 **Release 21_R2 (Recast)**: SIS and AFIS features were implemented to align with the Recast regulations. The release also addressed technical issues, ensuring core components were up to date in terms of maintaining system stability. 21_R2 was deployed on 7 March 2023.

22_R1 **Release 22_R1**: the objective of this technical release was to upgrade the AFIS Oracle database and implement the Data Guard Broker. This release, initially planned for spring 2023, was combined with release 23_R1 and deployed on 10 January 2024.

23_R1 **Release 23_R1**: this release contained fixes for SIS Recast defects and an upgrade of Elasticsearch to a newer version. Initially planned for October 2023, 23_R1 was eventually deployed on 10 January 2024, together with release 22_R1.

[22] As per Article 33(4) Regulation (EU) 2018/1861 and Article 43(4) Regulation (EU) 2018/1862.

Work on Releases 23_R1 and 24_R1 was also ongoing during the reporting period. 23_R1 is a corrective release and entry into operation is planned for mid-2025. On the other hand, 24_R1 foresees the SIS core database upgrade to Exadata and improvements for DCC broadcast handling, initially planned for 2024, is expected to enter into operation at the end of 2025.

eu-LISA assists and coordinates various **testing activities with Member States and EU Agencies**. Every system release during the reporting period was implemented only after completing several test phases – such as compliance and acceptance testing – in order to ensure the smooth integration of national and central systems, as well as to maintain high standards of functionality and performance.

Additionally, the Agency supports Member States in conducting their own system validation efforts, particularly when updates to their national systems require verification against the SIS central system. To facilitate this, eu-LISA offers dedicated testing environments and provides further assistance when necessary. During the reporting period, national testing was performed by Cyprus, Austria, Estonia, Switzerland, Iceland, Ireland, Sweden, the Netherlands, Malta, Norway and Czechia (full new system), in addition to Frontex.

Overall, eu-LISA committed to improving coordination through enhanced communication and the introduction of a live testing calendar and updated dashboards. This initiative was driven by the identification of testing environment availability and overlapping schedules as key challenges by the Member States.

In 2023 and 2024, several workshops were organised[23] with the participation of Member States, focusing on data quality (DQ). The **DQ mechanism**, aimed at improving the accuracy of the data stored in SIS, provides regular DQ reports to the Member States. During these workshops, DQ reports were reviewed, and improvements with regard to aligning the reports to the new legal framework and existing standards were discussed. By the end of the reporting period, some DQ reports had already been updated, and a new flagging mechanism had been implemented.

2.6. Monitoring and operational activities

Central SIS monitoring is conducted around the clock at the operational centre in Strasbourg by the **eu-LISA First level support team**. This service serves as the primary point of contact for users to report incidents, as well as for inquiries and requests related to technical support or information. Eu-LISA ensures a single point of contact through the First level support team, enabling users to submit incident reports and request various services. The operational status of the connection between the central SIS and the national copies is continuously monitored. Any disruptions that could affect business operations are promptly reported and escalated in accordance with the procedures outlined in the SIS Operator Manual.

During the reporting period, the **central SIS maintained a high degree of availability**. Critical SIS functionalities, such as allowing all Member States to search the central system or ensuring the proper processing and broadcasting of alerts from the Member States, are used to calculate availability. Unavailability occurs when Member States are unable to access these critical functionalities, which may result from both planned maintenance and/or unplanned or incident maintenance outages. Unavailability is partial when it affects only some of the Member States, and full when it affects all Member States.

In 2023, the performance of SIS and AFIS remained within the requisite service level targets, with **availability at 99.67 %** and response time at 99.99 %,. Switchover/switchback from CU to BCU was operated four times, including for the SIS Recast implementation.

[23] In September and November 2023; in April, September and November 2024.

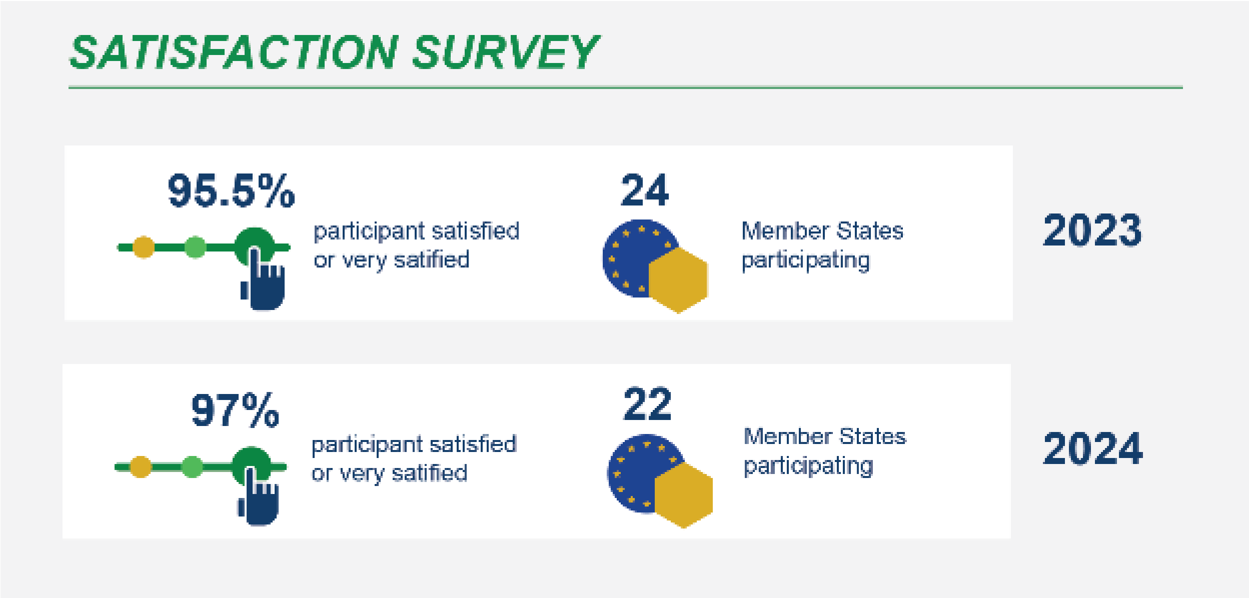
In 2024, SIS and AFIS remained again within the requisite service level targets – this time **availability of 99.78 %** and a response time of 100 %. Switchover/switchback from CU to BCU was carried out seven times due to maintenance for the 22_R1 and 23_R1 releases, electrical maintenance, security patching and support for incident fixing.

Central SIS includes a **data consistency check (DCC)** feature that ensures the synchronisation and consistency of national copies and restores data. Monthly DCC campaigns assist Member States in achieving technical compliance. The system checks all alerts and links, automatically fixing any discrepancies it finds. Most cases in which repeated discrepancies occur are due to incidents in which a Member State's connection to the central system is disrupted.

These regular DCC campaigns ensure that each national copy is checked at least once a month. Analysis on the DCC results is regularly presented at AG meetings. During the reporting period, the DCC mechanism was reviewed so as to align with the SIS Recast, as well as to contribute to improving it by means of more detailed reporting for Member States.

eu-LISA conducts an annual Customer Satisfaction Survey asking Member States in order to assess the support eu-LISA offers. This evaluation covers eu-LISA First level support team performance, incident and problem management, operational communication, technical assistance and support for national activities and release management.

During the reporting period, the satisfaction of the SIS community was very high, with 97 % of stakeholders reporting having been either **very satisfied or satisfied** in 2023, and 95.5 % in 2024. The participation rate showed a decreasing trend compared to the past, with 24 Member States contributing to the survey in 2023, which decreased to 22 in 2024. Feedback provided was analysed, and actions for improvement were planned.



SATISFACTION SURVEY

95.5% participant satisfied or very satified

24 Member States participating

2023

97% participant satisfied or very satified

22 Member States participating

2024

The **SIS Operator Manual was updated** in 2023 and 2024. This manual serves as the reference document for eu-LISA's first- and second-level support teams, national SIS Single Points of Contact, and organisations such as Europol, Eurojust and Frontex. It ensures harmonised operations between eu-LISA and its stakeholders by providing a common working language and communication framework. Additionally, it outlines a bilaterally developed Escalation Procedure for incident management. The updates in 2023 reflected Cyprus' integration, the updated DCC process, updates in the Eopm message templates, and alignment with the EDPS recommendation regarding avoiding usage of production data for testing and training purposes. In addition, the manual was updated in 2024 to include a new chapter expanding on security-related practices as per interoperability requirements.

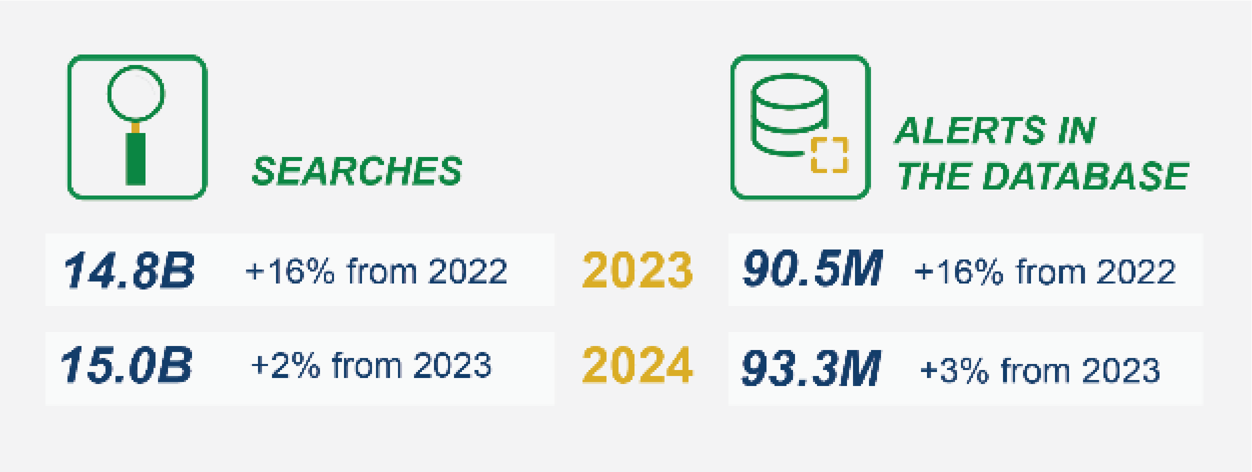
2.7. Performance of the central SIS

Central SIS was designed and optimised for a particular usage level. In order to gauge its performance and availability, metrics such as search distribution, traffic rate, maximum load and volume are employed.

More than 8 TB of space were added in March 2023, allowing for a capacity of 130 million alerts. The number of alerts issued by Member States and stored in the SIS central system grew steadily over the years, reaching a total of 90.5 million alerts at the end of 2023. In 2024, the total number of alerts reached 93.3 million; a 3 % increase from the same period in 2023[24].

In 2023, SIS was searched 14.76 billion times; a 16 % increase from 2022. A significant majority of the searches were automatic searches, for example via automatic number plate recognition systems (ANPR). Over 4 million of the total number searches performed were biometric in nature.

The majority of Member States have a national copy, hence they mainly use their copy for alphanumeric searches. However, Denmark, Finland, Liechtenstein, Norway and Slovenia do not have a national copy, therefore they search SIS via the central system. On the other hand, biometric searches can be performed only against the central system, in the SIS-AFIS. In 2023, 6 % of the total searches (908 million) performed in SIS were performed against the central system.



SEARCHES			ALERTS IN THE DATABASE	
14.8B	+16% from 2022	2023	90.5M	+16% from 2022
15.0B	+2% from 2023	2024	93.3M	+3% from 2023

In 2024, **Member States performed 15.01 billion searches**, a 2 % increase from 2023. The number of biometric searches on the other hand reached 6.9 million, i.e.an increase of 66 % compared to 2023. The number of searches performed against the central system was over 1 billion.

2.8. Training activities

Throughout the reporting period, eu-LISA made significant advancements in terms of expanding its training portfolio, refining its implementation methods, and enhancing collaboration with stakeholders. These improvements benefit all users of systems managed by eu-LISA, including the SIS community.

eu-LISA delivers training on the technical use of the system to national SIS operators, SIRENE staff and Schengen evaluators[25]. The training programme for national IT operators and technical SIS experts enhances operational management and provides support for technical maintenance. It also improves communication through the single point of contact (SPoC/Service Desk) and ensures data consistency, synchronisation and quality. To assist new users such as Member States or Agencies, eu-LISA provided training as part of the integration project. This project connects and supports newcomers in developing and operating their national (or Agency) systems and interfaces.

[24] For more details, see SIS annual statistics available at **https://eulisa.europa.eu/our-publications/reports**.
[25] In accordance with Article 3 of the eu-LISA Regulation (EU) 2018/1726.

In 2023, eu-LISA delivered a comprehensive training program, comprising 41 activities for managed and future systems, combining 8 face-to-face courses and 33 online training activities. These included 11 specialised sessions focused on **SIS, SIRENE and Schengen Evaluators for SIS/SIRENE**.

Building on this momentum, eu-LISA's 2024 training portfolio featured 29 activities, with a significant shift towards online delivery, accounting for 90 % of all sessions. The online offerings included 20 webinars, four online courses (with two updates), and two online modules, while three activities took place in person. Notably, the SIS training portfolio consisted of 11 activities in 2024.

The year 2024 saw a record-breaking number of participants engage with eu-LISA's training, with over 4 100 individuals taking part, including over 1 700 new enrolments in previously launched online training available on the eu-LISA Learning Management System (LMS). Participant satisfaction with SIS training activities remained high, with an 87 % satisfaction rate, demonstrating the effectiveness of eu-LISA's training initiatives.

During the reporting period, close cooperation with other JHA Agencies continued. Joint courses were developed together with CEPOL, and eu-LISA also contributed to training provided by Frontex and CEPOL.

The eu-LISA Learning Management System (LMS), the Agency's online learning platform, supports its extended e-learning offer, catering for diverse learning styles with a dynamic package design that stimulates active learning, including interactive audio-visual elements, self-assessment and knowledge checks. It has been revamped in recent years following feedback from stakeholders and external evaluation with a technical upgrade and archived outdated materials.

The training quality was further improved by implementing a clear, profile-based strategy. This involved delivering an "Essential Course for All Core Business Systems" as a mandatory prerequisite before offering specialised training courses tailored to various groups and profiles. Several LMS courses were added during the reporting period, raising awareness on the SIS Recast including an updated "SIS and SIRENE Essentials 2.0" course in September 2023 and "The New SIS for SIRENE Profile" course added in June 2024.

2.9. Communication infrastructure

The communication infrastructure provides an encrypted virtual network dedicated to the exchange of data between central and national systems, as well as between the authorities responsible for the exchange of supplementary information (SIRENE Bureaux).

The SIS communication infrastructure is a community under the European private secure network named Trans European Services for Telematics between Administrations – New Generation (TESTA-ng).

The architecture of the SIS communication infrastructure can be described as a star topology with resilience. The CU and the BCU contain the central SIS systems to which each national SIS system connects. The CU and BCU are connected by a dedicated point-to-point connection.

The confidentiality of SIS communications over the 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 so as to ensure that third parties cannot gain access to clear-text data.

The SIS-related SIRENE exchange service operates within the SIS 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-related SIRENE information exchange.

The SIS communication infrastructure is permanently monitored to ensure continuous service availability and strict contractual performance service level requirements have been established. During the reporting period, the **overall average availability was 99.9998 %** in 2023, and **99.9961 %** in 2024.

In 2023 and 2024, the SIS communication infrastructure was enhanced by eliminating single points of failure in the service provider's nodes, thereby preventing major incidents. Additionally, in order to ensure business continuity, a refresh programme was carried out so as to renew end-of-life equipment across the communication infrastructure. Lastly, the successful signing and implementation of new contract agreements with the TESTA-ng provider proved to be an important milestone, as the consistent operation of the current communication infrastructure was thereby achieved.

2.10. Security

SECURITY EVOLVED BY:

Implemented EDPS recommendations with the DPO

Conduct comprehensive security and business continuity exercises

Enhanced risk management and residual security monitoring

The SIS security framework relies on the core principles of security, confidentiality, integrity and availability. At a central level, the SIS infrastructure and the communication network ensures the system protects the information transmitted and stored.

The SIS central system is protected in physical terms 24/7 like a critical infrastructure, as per legal requirements, including multi-layer perimeter fencing and physical access controls – all of which are integrated in a global security environment.

Communications with the Member States are protected by multiple layers of encryption and by a network of security controls. The central SIS is physically isolated from external networks, systems and the internet. In the event of technical failure, operations can be promptly switched over to the backup site in Austria. Access to both systems is only granted to duly authorised staff who are cleared to perform system administration activities based on established roles and responsibilities.

The central SIS, including the AFIS component, follows the security measures set out in the **SIS Security Plan and the SIS Business Continuity Plan** which contains controlled measures following a risk assessment. The current plans were adopted by eu-LISA's Management Board in December 2024 as an update to previous planning.

The SIS central system falls under the Security Policy and Business Continuity framework of eu-LISA. The latter requires that all eu-LISA systems undergo technical vulnerability tests on a regular basis, and must provide assurance that the implementation, integration and configuration of controls are compliant with the security requirements. In light of this common framework, the Agency maintained continuous monitoring and management of residual security risks during the reporting period to provide assurance that the appropriate security controls were effective, properly implemented and managed.

In terms of information security, eu-LISA carried out several activities aimed at improving the security posture of the system and carrying out constant security assessments.

The systems operated by eu-LISA, hence SIS included, are subject to audit and inspection from different stakeholders. Following the 2023 inspection of the European Data Protection Supervisor (EDPS) of central SIS, during the reporting period the Security Unit, in close collaboration with the Data Protection Office, implemented the recommendations identified.

In addition to that, as per consolidated practice, eu-LISA ran **business continuity exercises** aimed at measuring the effectiveness of the Agency security posture. In 2024, the Agency conducted the Security and Business Continuity Exercise, focusing on the central systems, including aspects pertaining to SIS.

2.11. Data protection

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

During the reporting period, efforts were made to implement recommendations on central SIS received from the EDPS in relation to audit performed in 2018 on SIS II and VIS. In 2023, as an outcome of the quarterly internal follow-ups, eu-LISA considered all **EDPS recommendations** of this audit completed.

Following the reception of the draft report of the SIS II, VIS and Eurodac audit carried out in October 2022, an internal revision at staff level and an informal consultation with the three Advisory Groups (SIS, VIS, Eurodac) were carried out in May 2023. Subsequently, in accordance with Article 19(1)(hh) of eu-LISA Regulation[26], the matter was referred to the Management Board for consultation and comment. The formally adopted comments were sent to the EDPS on 26 June 2023.

The final report of the EDPS received in September 2023 contained 37 recommendations. Additionally, in the same report the EDPS officially ratified and confirmed the closure of the recommendations stemming from previous 2018 audit on SIS II (and also on VIS).

A new inspection was carried out by EDPS on the SIS Recast in December 2023 which aimed at verifying on-the-spot compliance with the Regulation (EU) 2018/1725, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862.

The SIS audit, conducted in December 2023, culminated in a final report which eu-LISA received in September 2024, containing 22 recommendations (one of which the Agency had closed by the end of 2024). The Management Board adopted its final comments on the draft report in June 2024 which was formally adopted on 31 July 2024. The comments were subsequently submitted to the EDPS on 2 August 2024 within the stipulated deadline.

In 2023, the SIS coordinated supervision passed to the Coordinated Supervision Committee (CSC), within the framework of the European Data Protection Board (EDPB). The groups and committee, composed by representatives of the National Data Protection Authorities along with the EDPS, requested updated information regarding the three EU Large-Scale IT Systems on operational matters.

At the meetings that were held during the reporting period, members were informed, either orally or in writing, about the latest developments and issues related to the system that may impact the processing of personal data. Members expressed interest variously in how the systems were performing, related incidents and the quality of the data.

[26] Regulation (EU) 2018/1726.

3

SIRENE FORMS EXCHANGED AND HITS HANDLED

3. SIRENE forms exchanged and hits handled

On an annual basis[27], eu-LISA collects statistical data from the Member States, including data on the exchange of supplementary information between Member States (SIRENE forms) and on hits handled. In this section, data on SIRENE forms and hits handled for the reporting period (2023-2024) is presented.

In March 2023, the reinforced SIS entered into operation following the implementation of the SIS Recast project. There were several changes between the SIS II (in operation until 6 March 2023) and the new SIS (in operation as from 7 March), including extended access rights, additional categories of alerts stored, and also categories of data with changed or expanded scope. Against this backdrop, any comparison with the data sets from the previous few years should be considered in context.

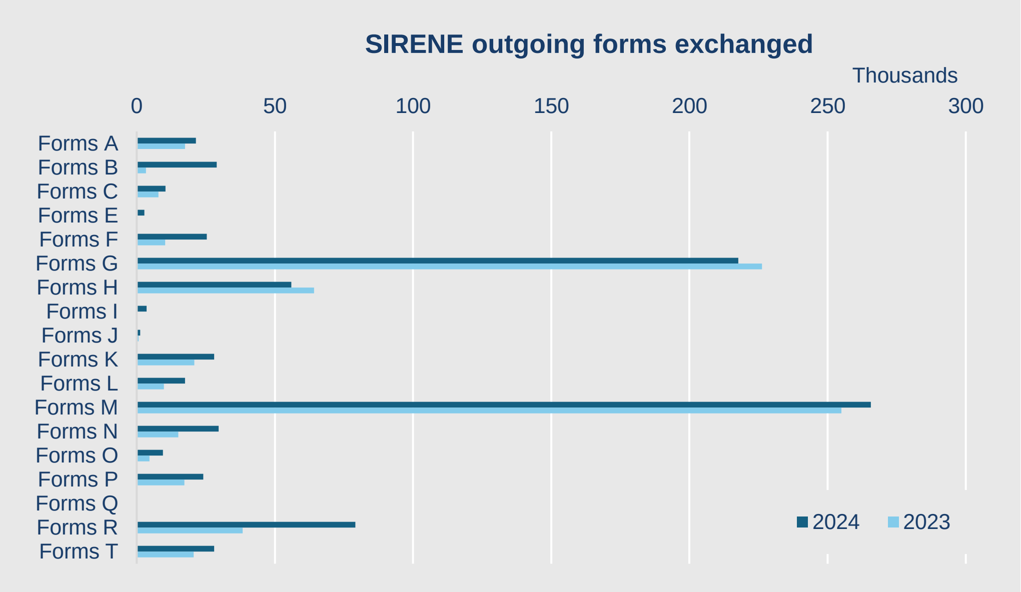
3.1. SIRENE forms exchanged

In addition to the data contained in SIS alerts stored in the SIS database, Member States exchange supplementary information, which consists of information related to alerts but not forming part of it. The supplementary information is exchanged through a single network of national offices called SIRENE Bureaux, using specific SIRENE forms.

SIRENE forms are standardised templates used by SIRENE Bureaux and Europol to exchange supplementary information in a structured way. The SIRENE forms are designed according to the technical specifications maintained by eu-LISA in the document Data Exchange Between SIRENE Bureaux (DEBS).

In 2023, a total of 2 257 236 forms were exchanged between the Member States. Of those, 711 696 were outgoing and 1 545 540 were incoming. The number of forms exchanged increased in 2024, with a total of 2 691 800 forms exchanged between the Member States (848 722 outgoing and 1 843 078 incoming). Table I in the Annex provides a breakdown of outgoing and incoming forms for the reporting period.

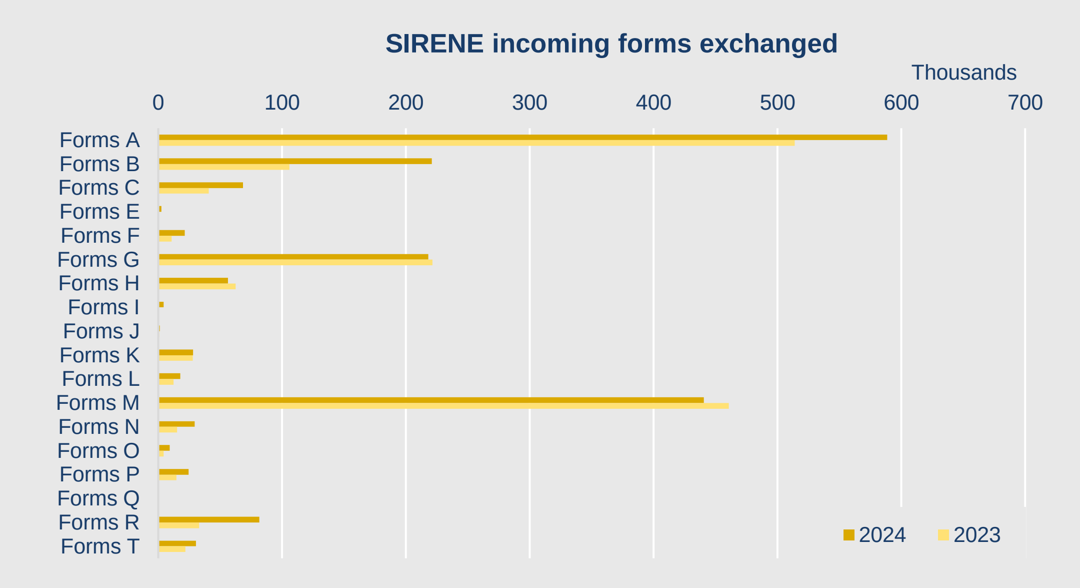
As shown in the graph below, the SIRENE outgoing forms most used in both 2023 and 2024 were form G and form M.



[27] Pursuant to Article 16 Regulation (EU) 2018/1860, Article 60(3) Regulation (EU) 2018/1861 and Article 74(3) Regulation (EU) 2018/1862.

The following SIRENE forms are used to exchange supplementary information:

- **A form** (European arrest warrant or extradition request) for supplementary information related to alerts on persons wanted for arrest for surrender or extradition purposes;
- **B form** for supplementary information related to alerts on persons or objects for discreet checks, inquiry checks or specific checks and, from the date indicated in Article 60(3). In the future, this will cover also information alerts on third-country nationals entered in SIS in the interest of the Union ("information alerts");
- **C form** for supplementary information related to alerts on missing persons or vulnerable persons who need to be prevented from travelling;
- **E form** for supplementary information related to incompatible multiple alerts;
- **F form** for supplementary information related to flagging or unavailability of alerts;
- **G form** for supplementary information related to a hit (action has been taken);
- **H form** for supplementary information related to a hit (action could not be taken);
- **I form** for supplementary information when SIS data is to be used for other purposes;
- **J form** for supplementary information related to SIS data that is legally or factually inaccurate;
- **K form** for supplementary information related to data subjects rights;
- **L form** for supplementary information on a person's identity;
- **M form** for miscellaneous supplementary information if no procedure is laid down requiring the use of a more specific form;
- **N form** for initiating and conducting consultations on alerts on return or alerts for refusal of entry and stay;
- **O form** for supplementary information related to the decision on the residence permit or long-stay visa in the context of a consultation procedure;
- **P form** for supplementary information to be supplied by the issuing Member State when an object needs to be recovered;
- **Q form** for supplementary information related to misused identity;
- **R form** for supplementary information related to a hit on an alert on return;
- **T form** for supplementary information related to the surrender or extradition of a person subject to an alert for arrest.



An additional SIRENE form, the U form will be used in the future when the SIS and ETIAS will be connected, for supplementary information related to automated notifications generated by the ETIAS central system.

SIRENE forms B, C, R and T were introduced following the implementation of the SIS Recast, hence those were not in use until 6 March 2023.

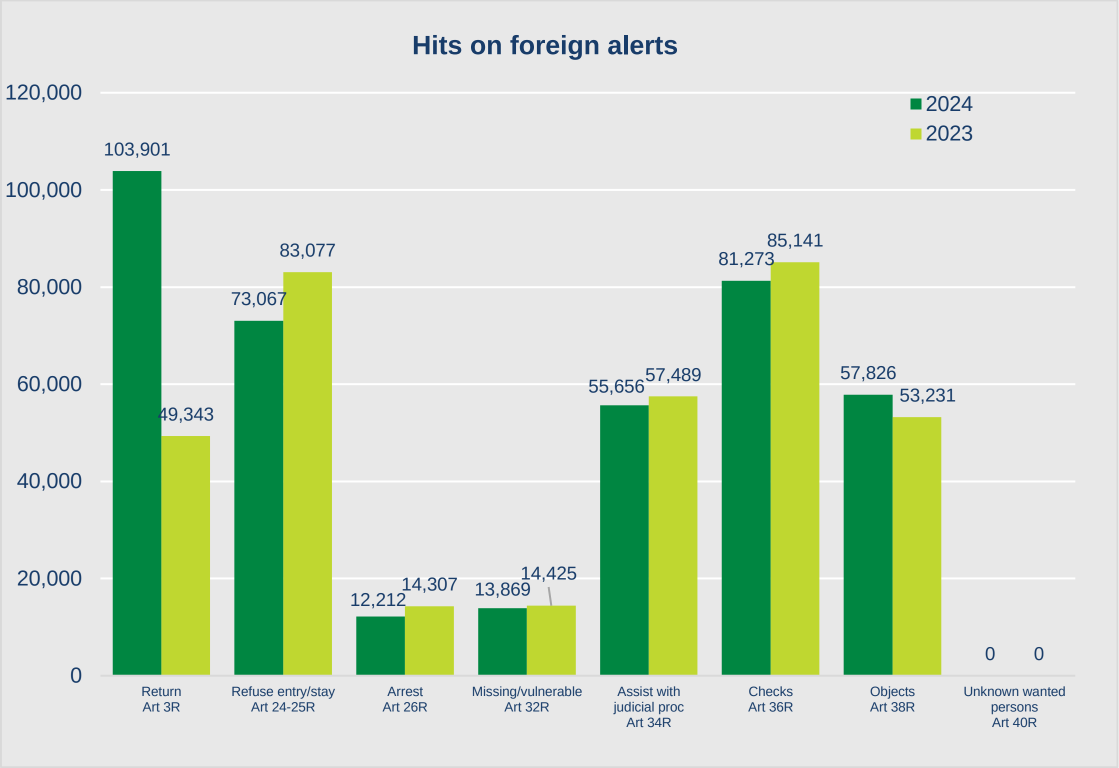
As shown in the graph above, the SIRENE incoming forms most used in both 2023 and 2024 were form A and form M.

3.2. Hits handled

A hit occurs when a user conducts a search in SIS and the search reveals a foreign alert (i.e. when the alert in SIS matches the data being searched). As per Article 3(8) of the Regulation (EU) 2018/1861 and parallel provision in Article 3(7) Regulation (EU) 2018/1862, a “hit” means any match which has been confirmed by the end-user; or the competent authority in accordance with national procedures (where the match concerned was based on the comparison of biometric data); and further actions are requested.

The Member States reported a total of 357 013 hits on foreign alerts in 2023, and 397 804 in 2024, showing an increase of 11 %. Novelties from SIS Recast are represented by the hits on alerts on third-country national subject to a return decision (Article 3 of Regulation (EU) 2018/1860), and the hits on alerts on unknown wanted persons for identification (Article 40 of Regulation (EU) 2018/1862). No hits were reported for the latter.

A breakdown of hits on foreign alerts is provided in Table II in the Annex and on the graph below.



CONCLUSION

Conclusion

Following the last SIS evaluation performed in 2016, the Commission tabled legislative proposals to reinforce SIS, highlighting the operational success and relevance of the system, and emphasising opportunities for improving efficiencies at the same time. The proposals adopted in 2018 aimed to rebuild the SIS with additional functionalities, expanded scope and extended accesses so as to better support competent authorities in dealing with the ever-changing security landscape.

The journey of the SIS upgrade culminated with the entry into operation of the SIS Recast in March 2023, representing a major achievement for the entire SIS community and, more broadly, for the Schengen internal security community. This challenging feat was accomplished thanks to the dedication, commitment and resilience of the Member States, eu-LISA, the Commission and the experts who implemented it.

The renewed SIS, currently being set up by the EU, constitutes the foundation of one of the most advanced border management system in the world. Together with the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS), SIS will form part of the interoperability (IO) architecture. Plans to integrate SIS with IO are already underway, in line with the revised interoperability roadmap as endorsed by the JHA Council in March 2025.

From the operational side, with 1.7 million searches performed on average per hour in 2024 – including 800 AFIS searches – SIS continues to be the most widely used information sharing system for security and border management. Looking ahead, eu-LISA remains strongly committed to ensuring that the SIS central system remains operational around the clock, thereby guaranteeing its availability and performance as per the high standards set down by relevant legal requirements.

ANNEX

Annex

Table I – Breakdown of SIRENE forms exchanged per type of form

SIRENE forms	Outgoing forms		Incoming forms	
	2024	2023	2024	2023
Forms A	21,453	17,443	588,646	513,899
Forms B	28,975	3,354	220,939	105,867
Forms C	10,363	7,856	68,512	40,645
Forms E	2,806	179	2,395	182
Forms F	25,310	10,309	21,250	10,851
Forms G	217,698	226,247	218,129	221,445
Forms H	55,934	64,212	56,364	62,430
Forms I	3,560	28	4,405	27
Forms J	1,205	621	1,242	634
Forms K	28,001	20,863	28,033	27,880
Forms L	17,444	9,818	17,791	12,272
Forms M	265,666	254,925	440,429	460,673
Forms N	29,586	15,099	29,247	15,056
Forms O	9,464	4,578	9,151	4,298
Forms P	24,056	17,214	24,556	14,519
Forms Q	55	63	78	80
Forms R	79,081	38,288	81,583	32,950
Forms T	28,065	20,599	30,328	21,832
Total	**848,722**	**711,696**	**1,843,078**	**1,545,540**

Table II – Breakdown of hits on foreign alerts

Hits on foreign alerts	2024	2023
Hits on alerts on third country nationals subject to a return decision, Article 3 of Regulation (EU) 2018/1860	103,901	49,343
Hits on alerts on third country nationals to be refused entry and stay into the territory of the Member States, Articles 24 and 25 of Regulation (EU) 2018/1861	73,067	83,077
Hits on alerts on persons for arrest and surrender or extradition, Article 26 of Regulation (EU) 2018/1862	12,212	14,307
Hits on alerts on missing persons, vulnerable persons at risk (adult & child), Article 32 (1) of Regulation (EU) 2018/1862	13,869	14,425
Hits on alerts on persons to assist with a judicial procedure, Article 34 of Regulation (EU) 2018/1862	55,656	57,489
Hits on alerts on persons and objects for discreet, inquiry and specific check and for national security, Article 36 (3) and (4) of Regulation (EU) 2018/1862	81,273	85,141
Hits on alerts on objects for seizure and use as evidence in criminal proceedings, Article 38 of Regulation (EU) 2018/1862	57,826	53,231
Hits on alerts on unknown wanted persons for identification, Article 40 of Regulation (EU) 2018/1862	0	0
Total	**397,804**	**357,013**

Manuscript completed in June 2025.

Neither eu-LISA nor any person acting on behalf of eu-LISA is responsible for the use that might be made of the following information.

PDF ISBN 978-92-95237-01-8 ISSN 2443-8294 doi:10.2857/3086040

Catalogue number: EL-01-25-005-EN-N

Cover image - Christian Horz / stock.adobe.com