

Report on the technical functioning of central SIS II 2021-2022

December 2023



European Union Agency for the Operational Management of Large-Scale IT
Systems in the Area of Freedom, Security and Justice

www.eulisa.europa.eu

Contents

Executive summary	3
1. Introduction.....	5
2. Operational management of central SIS II.....	7
2.1. Technical infrastructure of central SIS II.....	7
2.2. SIS Recast.....	9
2.3. Implementation of AFIS for SIS II.....	10
2.4. Deployment of releases and testing activities.....	11
2.5. Monitoring and operational activities	12
2.6. Performance of the central SIS II	14
2.7. Training.....	14
2.8. Communication infrastructure	15
2.9. Security.....	16
2.10. Data protection.....	17
3. SIRENE forms exchanged and hits reported	19
3.1. SIRENE forms exchanged	19
3.2. Hits reported	21
Conclusions	23

EXECUTIVE SUMMARY

DATA DELETED



Following the UK withdrawal from the EU, all UK alerts were deleted

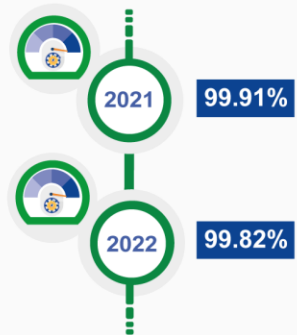
SIS Recast limits the possibilities to enter these alerts, making stored alerts obsolete

NEW USERS

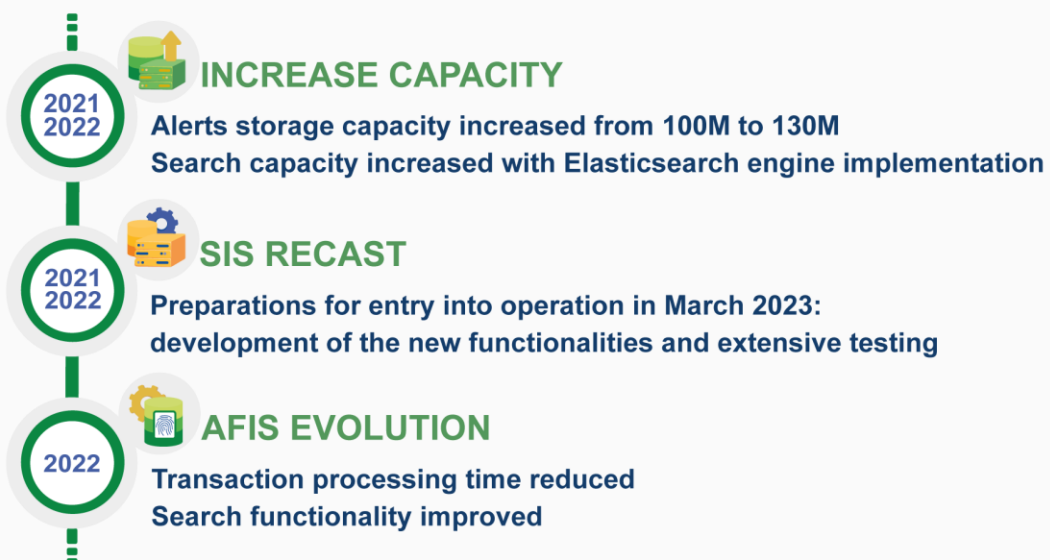
SIS II CENTRAL SYSTEM



AVAILABILITY



EVOLUTIONS



1

INTRODUCTION



1. Introduction

The Schengen Information System (SIS II)¹ is **the EU's largest and most widely used information-sharing system**, constituting a cornerstone of the Schengen acquis. SIS II facilitates the free movement of people within the Schengen area by offering 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 II **facilitates operational cooperation** between national competent authorities, including border guards, police, SIRENE Bureaux, and judicial, customs and immigration authorities. The system enables those competent authorities to enter and consult data on persons or objects, and take specific action where required. A list of the competent authorities authorised to search the system directly and a list of SIRENE Bureaux are published annually in the Official Journal of the European Union².

The UK was disconnected from SIS II as of 1 January 2021, while Ireland gained access to the system on 15 March 2021.

By the end of the reporting period (31 December 2022), **SIS II was used by 30 Member States³, Europol and Eurojust**. By the end of December 2022, Cyprus's integration into SIS II was in progress (completed in July 2023) as was the case for Frontex.

eu-LISA (the Agency) is responsible for the operational management of the SIS II central

system⁴, guaranteeing its effective uninterrupted access and functioning 24/7. The eu-LISA Management Board, together with the SIS II Advisory Group, support the Agency in this respect. eu-LISA shares responsibility for SIS II governance together with the European Commission, the Member States and several stakeholders. The Commission is responsible for the correct implementation of the SIS II legal framework and any legislative initiatives linked to the system.

The SIS II 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 implementation of timelines and dependencies. The SIS II Advisory Group also reports on the availability of the central SIS II and national systems, approves release plans, discusses and plans developments, assesses training activities and adopts the annual statistics report.

In addition, several dedicated and ad hoc fora support the work of the Agency, including the Recast Project Management Forum (Recast PMF), the Automated Fingerprint Identification System (AFIS), the Project Management Forum (AFIS PMF), the Security Officers Network and the National Contact Points for training.

This report, which is the fifth report on the technical functioning of the central SIS II and its communication infrastructure, covers the period **from 1 January 2021 until 31 December 2022**. The report, as part of eu-LISA's SIS II legal reporting obligations, aims to increase both transparency and visibility of system usage, maintenance and any developments. It encompasses all activities that contribute to the operational management of the central SIS II, including security, together with an overview of statistics collected annually.

¹ SIS II was the 'second generation' Schengen Information System (SIS), operational from 9 April 2013 until 6 March 2023. On 7 March 2023, SIS Recast entered into operation and SIS II is since then called SIS. This report refers to the 'second generation' Schengen Information System (SIS II) as SIS Recast entered into operation after the reporting period of this report.

² The latest list was published in OJ C 85, 7.03.2023. Since August 2023, eu-LISA maintains a continuously updated list of authorities on its website, containing changes sent by Member States between the annual publications in the OJ, as per the SIS Recast regulation.

³ All EU Member States (except Cyprus) and the Schengen Associated countries (Iceland, Liechtenstein, Norway and Switzerland).

⁴ eu-LISA is responsible for the SIS II central system (CS-SIS), while the Member States are responsible for their national systems (N.SIS).

2

OPERATIONAL MANAGEMENT OF CENTRAL SIS II



2. Operational management of central SIS II

SIS II facilitates the exchange of information on persons and objects between European national law enforcement and judicial authorities. 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 includes management services, supervision and the implementation of appropriate corrective, adaptive and evolutionary maintenance. During the reporting period, an external contractor⁵ provided maintenance and technical support to eu-LISA under the maintenance-in-working-order (MWO) framework contract, delivering continuous and reliable operational management of SIS II and ensuring the optimal performance of the system.

2.1. Technical infrastructure of central SIS II

SIS II usage has steadily grown over the years, demonstrating the importance of proper maintenance and evolution of the system.

As a result of the COVID-19 pandemic, SIS II usage experienced a sharp drop, but the current reporting period has shown a good recovery. **In 2021, SIS II was accessed almost 7 billion times**, an 89% increase from 2020 when the SIS II was searched 3.7 billion times. **In 2022, 12.7 billion accesses** were recorded, accounting for an increase of 82% compared to 2021.⁶

The number of alerts issued by Member States and stored in the SIS II central system grew steadily over the years, reaching a total of 93.4 million by the end of 2020. However, during the reporting period, the total number of alerts stored experienced a decrease. This was due to the deletion of UK data in 2021 as a result of the United Kingdom's withdrawal from the EU. Following changes in legislation, securities and non-cash means of payment alerts were deleted in 2022. Consequently, by the end of **2021** there were a total of **89.9 million alerts in SIS II** and by the end of **2022**, the figure had gone down to **86.5 million**.

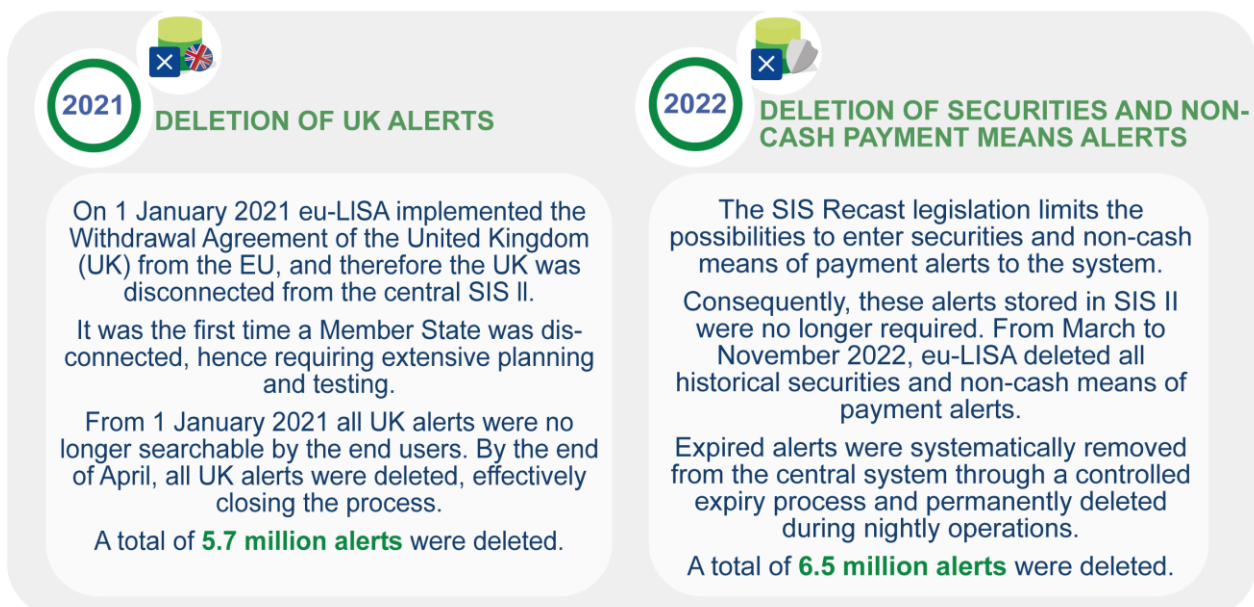


Figure 1: Deletion of alerts from central SIS II, 2021-2022

⁵ Sopra Steria Benelux SA/NV.

⁶ For more information, see the 2021 and 2022 annual statistical reports published on the eu-LISA website: <https://www.eulisa.europa.eu/our-publications/reports>.

In May 2018, the **integration of Ireland** into the SIS II central system began. Following extensive preparations that were finalised in 2020, the process of entry into operation started in January 2021 and was successfully completed on 15 March 2021. In May, Ireland conducted its first data consistency check, and also connected to the SIS Automated Fingerprint Identification System (AFIS), which it began to use on 28 July.

The Agency worked on **several projects** in order to upgrade and ensure the proper maintenance of the system, including for the preparations for the entry into operation of SIS Recast (see [section 2.2](#) for details).

In April 2019, the Agency launched the **SIS Increase Capacity project**, which introduced new technical, hardware and software components and also ensured that the system could handle a higher volume of alerts. More precisely, the project included:

SIS II was effectively managed in line with the Service Level Agreement, meeting set targets and undergoing various improvements.

- an upgrade of WebLogic application software and JDK 8⁷ – completed prior to the reporting period;
- increasing SIS II central system alerts' storage capacity to 130 million – completed in the fourth quarter of 2021 with the entry into operation (EiO) of Release 20_R1 (*further information on releases can be found in [section 2.4](#)*);
- implementation of the Elasticsearch search engine, which was expected to deliver a tenfold increase in terms of search capacity and significantly reduce system unavailability during the switch between the central unit (CU) and the backup central unit (BCU). This was delivered under the Release 20_R1 and was completed in November 2022 with the migration of all Member States to the new search engine;
- database migration to new Oracle version v19 – postponed to 2024 under Release 24_R1.

Due to business reasons, it was necessary to **increase the size of files** in binary format that can be attached to SIS transactions (e.g fingerprint files or scanned documents). The current size of files could not cope with increased quality of the fingerprints, the new types of fingerprints introduced by the SIS AFIS Phase II evolution (see *more details in [section 2.3](#)*) and the increased size of scanned documents. In May 2021, the impact study that explored the possibilities for increasing the size of files was finalised. Following this, as a first step, a project was launched to optimise the storage of binary files among the various database schemata of SIS II. This project ended in March 2023 after gaining more than 8 Terabytes in space.

Various other projects carried out during the reporting period include replacing network equipment with more powerful and more maintainable devices, improving SIS test tools such as the National Systems Simulator (NSSIM), moving the SIS II backup service to eu-LISA's Common Service Infrastructure (CSI), upgrading AFIS Oracle Database to v19, replacing Disk Storage by deploying new more powerful hard disks, etc.

Apart from the above, a project to **interconnect SIS II with ETIAS and interoperability components** started in 2022. The relevant contracts were signed and throughout 2022 the project underwent the design and analysis phase.

⁷ Java Platform, Standard Edition 8 Development Kit (JDK 8).

2.2. SIS Recast

To further enhance the effectiveness and efficiency of the Schengen Information System and to better tackle increasingly complex security challenges, major changes were foreseen for SIS II. On 28 December 2018, three new regulations on the establishment, operation and use of SIS, i.e. **the SIS Recast regulations**⁸, entered into force. The implementation of these has been carried out gradually since 2019 and throughout the reporting period. As a result of the joint efforts of eu-LISA, the Member States and the Commission, **the renewed SIS entered into operation on 7 March 2023**, with a delay of approximately 1 year compared to the initial plan.

The renewed system represents a **major enhancement**, with the main changes providing for new categories of data and alerts, and wider access to SIS alerts at national and European level (see [Figure 2](#) below for more details).

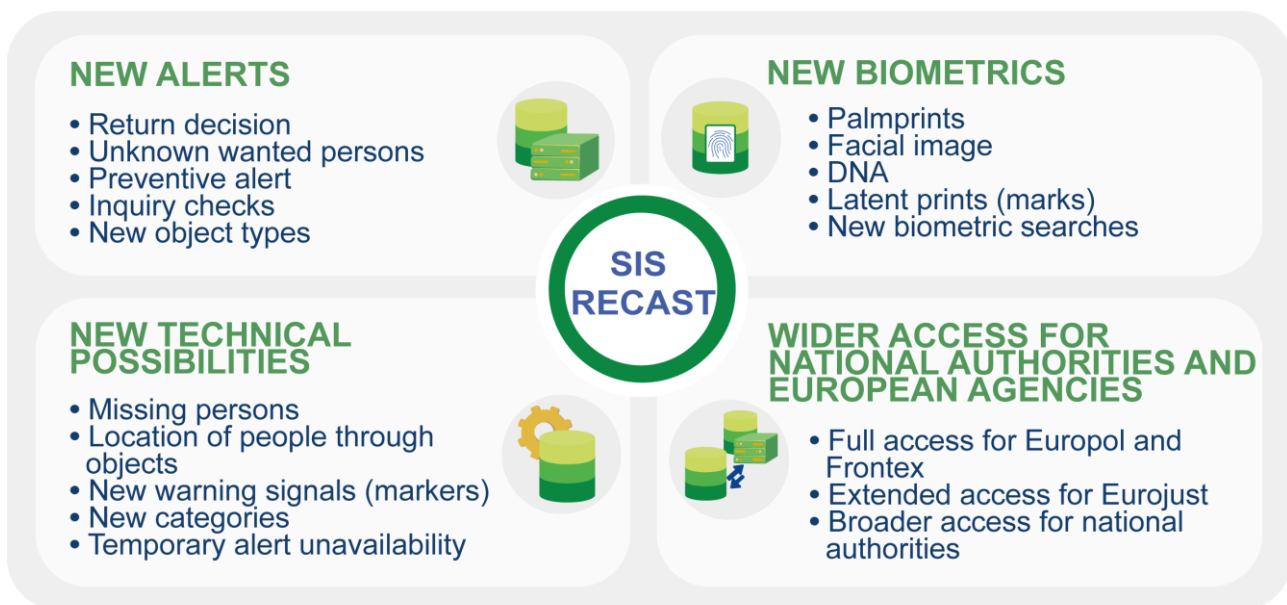


Figure 2: Changes introduced by SIS Recast

eu-LISA has been playing a crucial role in the implementation of the new regulations, being responsible for the communications infrastructure, the development of central SIS and the coordination of test campaigns with Member States and the EU agencies. Throughout the reporting period, **eu-LISA discussed the progress of Recast with stakeholders regularly**, including the SIS-SIRENE Committee, SIS II AG, the SIS II Expert Group and the Commission. By way of example, meetings with various stakeholders were held monthly, 39 SIS Recast and SIS AFIS Project Management Forum meetings were organised, and 30 test workshops with the Member States were carried out.

During the reporting period, **development of the new functionalities and extensive testing** needed for proper implementation were carried out. In addition, several review cycles of the interface control document (ICD) and of the detailed technical specifications (DTS) took place.

Testing involved the functioning and synchronisation of both central and national systems, and the exchange of SIRENE forms. Testing activities took place between July 2021 and January 2023. To support the Member States, major functional and non-functional improvements were delivered in SIS Central System Simulator (CSSIM)⁹, keeping up with Recast developments.

⁸ Regulation (EU) 2018/1860, OJ L 312, 7.12.2018, p. 1; Regulation (EU) 2018/1861, OJ L 312, 7.12.2018, p. 14; Regulation (EU) 2018/1862, OJ L 312, 7.12.2018, p. 56.

⁹ SIS CSSIM allows SIS users to execute the national system infrastructure tests without the SIS central system participation and is intended to support Member States in testing and training at their premises.

In 2021, the Commission worked on revising the **SIRENE Manual**, an implementing act that sets out the procedures for the exchange of supplementary information between SIRENE Bureaux related to SIS alerts. In July 2021, the SIS-SIRENE Police and Borders Committee gave a positive opinion on the new SIRENE manuals¹⁰, and on 18 November 2021 the manuals were adopted.

eu-LISA is responsible for the **Data Exchange Between SIRENE Bureaux (DEBS) documentation**, a set of technical specifications defining how SIRENE Bureaux exchange information. Throughout the reporting period, the Agency prepared and released several updates of the documentation to ensure its alignment with the new functionalities stemming from the SIS Recast.

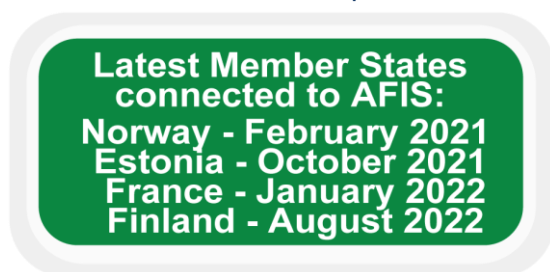
The initial **entry into operation** date for the SIS Recast was in December 2021. However, it was postponed several times, due to various challenges. These included, for example, hardware delivery difficulties as a result of the COVID-19 pandemic, the complexity of SIS II evolution projects, and Member States facing issues at national level with procurement, development and testing activities.

During the reporting period, **eu-LISA worked closely with the Member States to monitor the situation, mitigate the delays and replan activities**. By January 2023, all Member States had declared their technical readiness for the Recast, hence completing the legal requirements for the start of operation. The Commission Implementing Decision setting the date of entry into operation of the new system was published on 31 January 2023, and the new SIS entered into operation on 7 March 2023.

2.3. Implementation of AFIS for SIS II

In March 2018, eu-LISA implemented the **Automated Fingerprint Identification System (AFIS)**, for SIS II, introducing a biometric search capability at central level, allowing the identification of persons of interest solely based on their fingerprints.

All Member States were required to enable SIS-AFIS searches at national level by the end of December 2020. This was achieved by 25 Member States. The remaining Member States connected to AFIS during the current reporting period.



Although connected to the system, Estonia and Poland needed more time for national end users to start implementing the new functionality, which was achieved by the end of 2023. Ireland connected to AFIS shortly after gaining access to SIS II in 2021.

As more Member States enabled the fingerprint search functionality, the **usage of AFIS continued to increase**: from 38 860 searches in January 2021 to 281 753 in December 2022.

In 2019, eu-LISA launched the **SIS II AFIS Phase 2 project**. The project combined performance improvements with the new biometric functionalities stemming from the SIS Recast Regulations, including extension of search capabilities with dactyloscopic data on palm prints and latent prints (impressions on a surface). Good progress was made on this project during the reporting period:

- users were enabled to perform searches with only one fingerprint – completed in November 2021 under release 20_R1; and
- the AFIS architecture was redesigned to upgrade it and add hardware in order to process transactions more quickly – completed in June 2022 under Release 21_R1.

However, the largest AFIS functionality improvements came with Release 21_R2, i.e. with SIS Recast in March 2023.

¹⁰ The SIRENE Manual - Borders and return and the SIRENE Manual – Police.

2.4. Deployment of releases and testing activities

The deployment of releases allows the Agency to update the IT systems with the latest functionalities and patches, as part of the planned evolutions and projects. These activities are performed in such a way as to minimise the impact on the systems' operational activities, especially performance and availability. When needed, releases are associated with the switch of all operations from the central unit (CU) to the backup central unit (BCU) (switchover). The switch back to the CU is performed as soon as release activities are completed. This allows SIS II to be kept in operation from the BCU, without any degradation of performance and availability levels and simultaneously carrying out maintenance/releases on the CU¹¹.

During the reporting period, eu-LISA **deployed three releases**, which introduced new functionalities and technical changes. In addition, all releases included maintenance of the system as a whole, keeping its core components up to date and fixing identified issues.

- **Release 20_R1:** The Elasticsearch search engine was implemented (see [section 2.1 for details](#)) and AFIS functionality was improved (see [section 2.3 for details](#)). The alert management (CRUD – create, update, and delete) and central system searches were decoupled, removing their dependency on each other (for example, when performing maintenance), in order to minimise system downtime on searches. These changes enhanced search capabilities and system availability. The planned EiO for this release was in September 2020, but the actual deployment was completed in November 2021. The full benefits of the search engine were acquired in November 2022 with the migration of all Member States to Elasticsearch.
- **Release 21_R1:** AFIS architecture was redesigned (see [section 2.3 for details](#)). There were improvements to the speed of data consistency checks (DCC)¹² (see [section 2.5 for details](#)). The EiO was initially planned for July 2021, but eventually completed in June 2022.
- **Release 21_R2:** New SIS and AFIS features were implemented in order to align with the SIS Recast regulations (see [section 2.2 for details](#)). The initial EiO was planned for December 2021, but was actually in March 2023.

In addition, the Agency worked on **Releases 22_R1** and **23_R1**. Release 22_R1 will include the upgrade of the AFIS Database to Oracle v19, and Release 23_R1 contains an upgrade of the Elasticsearch package and fixes of a few minor defects that were introduced with SIS Recast. The two releases will enter in operation in December 2023.

eu-LISA supports and coordinates the Member States in a variety of **testing activities**. All releases, including during the reporting period, were deployed after successfully completing different types of tests (e.g. compliance and acceptance tests), ensuring the seamless implementation of the central system and national systems and guaranteeing optimal functionality and performance. In addition, the Agency facilitates the Member States' own testing activities whenever they need to validate their national system's implementation against the SIS II central system (e.g. when they have deployed changes to their systems). eu-LISA provides the necessary testing environments and, if needed, additional support to the Member States for these activities.

During the second half of 2021, the Agency concluded a contract with an external test support provider to better manage the increasing volume and complexity of testing. eu-LISA also defined the interoperability test approach in order to address the complex intertwined quality assurance procedures of system interoperability testing.

¹¹ The central unit (CU) is located in Strasbourg (France), whereas the backup central unit (BCU) is located in Sankt Johann im Pongau (Austria).

¹² DCCs are used by the Member States to maintain their national copies in line with the central system database as mandated by the SIS regulation. More information on DCC is available in section 2.5.

2.5. Monitoring and operational activities

Central SIS II monitoring is operational 24/7 and carried out at the operational site in Strasbourg by eu-LISA first level support. The operational status of the exchange between central SIS II and the national copies (the bridge)¹³ is continuously monitored. Any unavailability leading to a business impact is immediately reported and escalated, following the procedures described in the SIS Operator Manual.

eu-LISA first level support is the entry point for users' reports of incidents, as well as for requests for information or technical advice and support. All requests and incidents are registered in a centralised incident management tool (SM9) for follow-up. The relevant assistance is provided based on the initial analysis, and the impact, urgency and priority are defined accordingly.

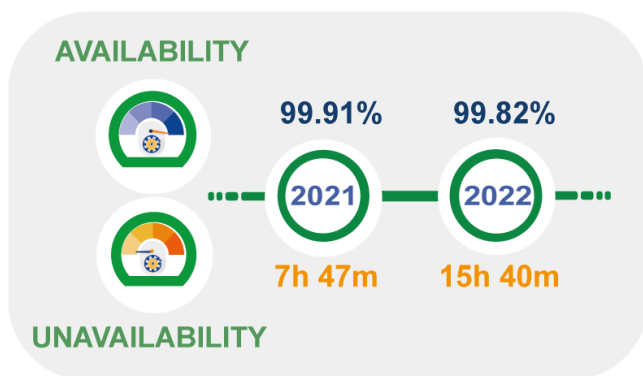


Figure 3: Availability of central SIS II, 2021-2022

As in previous years, **central SIS II was highly available** during the reporting period (see Figure 3). Availability is calculated based on critical SIS II functionalities, such as searching the central system by all Member States or properly processing and broadcasting alerts received from the Member States. Unavailability¹⁴ is defined as when Member States cannot use the critical functionalities, and it includes outages due to planned and unplanned maintenance.

In 2021, first level support handled 1,127 service requests and 1,288 incidents in relation to SIS II. In 2022, the number of

service requests was 1,089 and the number of incidents 1,528. The most significant incidents during the reporting period are the following:

- on 13 April 2021, the central system and AFIS were fully unavailable for all the Member States for around 1.5 hours due to an Oracle issue;
- on 13 February 2022, a malfunctioning cryptographic box in one Member State blocked messages on the SIS-SIRENE Mail¹⁵ for 22 hours, affecting several Member States on 14 and 15 February. No data loss was experienced and the messages were kept in the mail queue either on the central or the Member State side;
- on 15 March 2022, the SIS II central system was fully unavailable for 2 hours due to the failure of network devices;
- in May 2022, six instances of memory leak problems which led to partial and full outages were recorded; on 16 and 21 May, full unavailability of the central system was experienced by all the Member States for almost 1.5 hours each time;
- on 30 June 2022, an incident occurred just after the deployment of a new release (21_R1), making the system partially unavailable for almost 30.5 hours. Over the following days, eu-LISA worked closely with the Commission, the Presidency of the EU Council, and the Chair of the SIS II Advisory Group to stabilise the system and focus on the availability of the search functionality. By 5 July, SIS II configuration and operations were completely restored. During the incident, there was a severe degradation of the services, impacting mainly the CUD (create, update, delete) functionalities. Search queries remained available with reduced performance.

¹³ A communication infrastructure between central SIS II and national SIS II providing an encrypted virtual network.

¹⁴ Full unavailability occurs when central SIS II is not available for any of the Member States, whereas partial unavailability occurs when the central system is accessible for at least one Member State and they are able to use the search functionality and to receive notifications, broadcasts and to create, update and delete alerts.

¹⁵ SIRENE Mail is an information exchange mechanism for consultation between national SIRENE Bureaux with regard to supplementary information related to SIS II alerts.

- In October 2022, two incidents related to AFIS were recorded. On 4 October, AFIS CUD and search functionalities were unavailable for 1 hour due to power outage; on 31 October the biometric service halted due to which biometric transactions were not processed by AFIS for 8.5 hours.

The proper functioning of the SIS requires running regular **data consistency checks (DCCs)**. DCC is a procedure for updating national databases to ensure the national copies are fully synchronised with the central system (e.g. after the temporary disconnection of a national system). The DCC procedure only applies to Member States with national copy.

Each month, DCC campaigns are carried out to help Member States achieve technical compliance. Checks are performed on all alerts and links, and any discrepancies found are automatically repaired by the mechanism itself. Cases in which numerous discrepancies are found are mostly the result of incidents (for example as a consequence of a given Member State losing connectivity with the central system). The results of the DCCs are regularly analysed at Advisory Group meetings.

Owing to the active involvement of the Member States, the performance of DCCs continued to improve during the reporting period. The share of **DCC campaigns completed without discrepancies** was 21.6% in 2021 and 29.6% in 2022.

At the same time, the Agency worked on **the evolution of DCCs**, with a view to compressing the duration of these checks. With deploying Release 21_R1 in June 2022, the capacity to run up to two simultaneous DCCs on a daily basis¹⁶ was reached and the queues for high priority DCCs were maximised.

During the reporting period, eu-LISA also **updated the SIS Operator Manual**. The Operator Manual is the reference document used by eu-LISA first and second level support, the national SIS Single Point of Contacts and Europol, Eurojust and Frontex. It ensures a harmonised way of working between eu-LISA and stakeholders by providing a basic level of common working language, thereby ensuring communication between SIS stakeholders and a bi-laterally developed Escalation Procedure in case of incidents. The updated version, adopted in November 2022 by the SIS II Advisory Group, reflected new regulations and obligations, complemented the escalation procedure and included new technical features and general enhancements from lessons learnt.

Every year, the Agency carries out a **Custom Satisfaction Survey**, inviting the Member States to evaluate the support provided by eu-LISA in terms of first and second level support response, incident and problem management, operational communication, technical assistance, support for national activities and release management.

The **overall satisfaction rate was very positive** during the reporting period (see Figure 4). As a follow-up, for both years, eu-LISA prepared an action plan with measures to remedy the relevant areas for improvement.

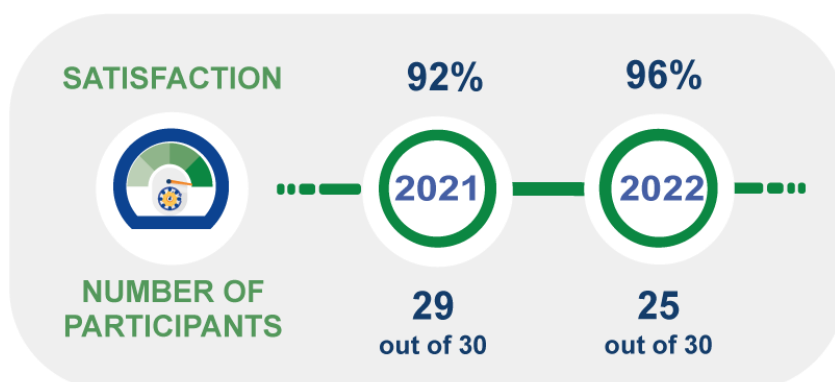


Figure 4: Share of Member States satisfied or very satisfied with eu-LISA support and number of participants in the survey, 2021-2022

¹⁶ Following the entry into operation of the renewed SIS in March 2023, up to four parallel DCCs can be run on a daily basis.

2.6. Performance of the central SIS II

Central SIS II was designed and optimised for a specific level of use. Therefore, indicators like **search distribution, traffic rate, maximum load and volume** are used to measure its performance and availability.

SIS II database capacity was increased from 100 million to 130 million alerts in 2021. By the end of the reporting period, 86.5 million alerts were **stored** in the central system.

In 2021, SIS II was **searched**¹⁷ almost 7 billion times. The vast majority of the searches were performed on national copies, as has been the case previously, while 5% (over 356 million) were performed in the central system. In 2022, the Member States performed 12.7 billion searches, of which 4% (over 544 million) were performed in the central system.

In 2021, 99.95% of all central SIS II alphanumerical **searches received a reply within the agreed time** for the type of search (less or equal to 3 seconds), compared to 99.90% in 2022. Similar performance levels were also achieved regarding AFIS searches, with 98.48% (less or equal to 11s) of searches falling within the Service Level Agreement (SLA) in 2021, and 97.87% (11s) in 2022.

In 2021, 16.4 million **create/update/delete (CUD) transactions** were performed, which was similar to 2020. In 2022, the number of CUD transactions increased by 17.1% and reached 19.2 million. The majority of the transactions (99% in 2021 and 96% in 2020) were performed in less than 3 minutes, in line with the design requirements of the system. AFIS CUD transactions have a longer SLA compared to alphanumerical CUD transactions. In 2021, 99.9% and in 2022, 98.7% of AFIS CUD transactions were performed in less than 10 minutes.

2.7. Training

eu-LISA is responsible for providing training on the technical use of the system to national SIS II operators, SIRENE staff and Schengen evaluators¹⁸. The training programme for national IT operators and technical SIS II experts facilitates the operational management of the system and supports technical maintenance, facilitates communication through the single point of contact (SPoC/Service Desk), and helps to ensure data consistency, synchronisation and quality. In order to support new users of the system, whether Member States or Agencies, training is provided as part of the integration project that connects and supports newcomers in developing and operating their national systems/interface.

During the reporting period, eu-LISA made **significant progress in further developing the training portfolio, its implementation modalities and collaboration with stakeholders**. This benefits the users of all systems managed by eu-LISA, including the SIS community.

The Agency's Annual Training Cycle includes a regular training needs analysis exercise and there are regular exchanges with the National Contact Points (NCP) network for training, and with other stakeholders like the European Commission and the Justice and Home Affairs (JHA) agencies. In 2021, in addition to an annual NCP meeting that took place in October, an interim NCP meeting was held in June reinforcing cooperation and further exchange on training needs with the Member States' representatives. In November 2022, a hybrid NCP meeting was held at the eu-LISA headquarters, following two online meetings held earlier in the year.

In the last couple of years, **the eu-LISA Learning Management System (LMS) was revamped** following feedback gathered from stakeholders and an external evaluation. The platform underwent a technical upgrade and outdated materials were archived.

¹⁷ In 2021 and 2022, around two thirds of the searches were automatically processed searches, e.g. searches carried out by automatic number plate recognition system (ANPR) or other types of automated bulk searches without human intervention.

¹⁸ In accordance with Article 3 of the eu-LISA Regulation.

The quality of the training delivered was further enhanced by **adopting a clear profile-based approach**, whereby an *‘Essential Course for all Core Business Systems’* is delivered as a pre-requisite to dedicated training courses for different groups/profiles.

During the reporting period, SIS training activities covered SIS II training needs as well as SIS Recast training needs. **The SIS training portfolio** consisted of **13 activities in 2021** and **15 activities in 2022**. The activities included awareness sessions and courses on SIS Recast, a technical profile course for SIS and SIRENE, and training aimed at SIS newcomers (Frontex and Cyprus) and Schengen evaluations. In 2022, the SIS portfolio was enriched with training initiatives on new SIS functionalities and new SIS AFIS.

Close cooperation continued with other JHA agencies. Joint courses were developed together with CEPOL, and eu-LISA also contributed to training provided by Frontex and CEPOL.

Participation in the SIS portfolio training activities:

- 796 trainees in 2021
- 856 trainees in 2022

During the reporting period, the majority of activities were delivered online in various formats (webinars, courses and training programmes).

A face-to-face two-day training course *‘The new SIS AFIS for SIRENE profile’* was provided in June 2022, which was a great success in terms of participation and feedback.

The **satisfaction rate** among training activity attendees continued to be very high: **91% in 2021** and **92% in 2022**.

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

The confidentiality of SIS II 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 to ensure that third parties cannot gain access to clear-text data.

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, the overall average **availability was 99.9996% in 2021** and **99.9984% in 2022**. Only a few incidents were recorded, of which **none had a critical impact**¹⁹.

In 2021, the SIS II communication infrastructure was **upgraded to accommodate the increased bandwidth requirements** stemming from the revised SIS legislation. Before the upgrade, the

¹⁹ 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.

system supported a throughput of 10 Mbps for each Member State or agency connecting to SIS II; the connection has now been upgraded to 100 Mbps. The SIS second encryption layer was renewed as well, also enabling more secure encryption protocols so as to prevent third parties from gaining access to SIS II data.

2.9. Security

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

The SIS II central system is **protected around the clock in physical terms** as a critical infrastructure, as per legal requirements. This includes multi-layer perimeter fencing and physical access controls, all integrated in a global security environment.

Communication with Member States is protected by multiple layers of encryption and by a network of security controls, comprising several layers of firewalls and integrity checks. The central SIS II 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, cleared to perform system administration activities based on established roles and responsibilities.

The central SIS II, including the AFIS component, follows the security measures set out in the **SIS security plan**, which contains controlled measures following a risk assessment. The current security plan in place was adopted by eu-LISA's Management Board in March 2021.

The SIS II central system falls under the **security policy framework of eu-LISA**. This 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. Under this common framework, the Agency continuously monitored and managed the residual security risks during the reporting period to provide assurance that the appropriate security controls were effective, properly implemented and managed. This included, for example, an assessment review of the status of eu-LISA's information security management system (ISMS).

Security evolved in 2021-2022 by:

- **improving the security policy framework;**
- **evolving the security risk management approach;**
- **consolidating the development of the technical security architecture.**

In terms of **information security**, eu-LISA improved the security of the systems in

various ways. There were a number of projects, including ones implementing the Security Information and Event Management System (SIEM) and the new Public Key Infrastructure.

The systems operated by eu-LISA, SIS II included, must undergo audits and inspections by different stakeholders. Following the **2022 inspection by the European Data Protection Supervisor (EDPS)** of central SIS II, the Security unit – in close collaboration with the Data Protection office – implemented the recommendations identified during the reporting period.

The Agency also regularly **collaborated with the Commission's Internal Audit Service (IAS)**, which ran an IT Security audit on the large-scale IT systems within eu-LISA's remit.

In addition, as per consolidated practice, eu-LISA ran **business continuity exercises** aimed at measuring the effectiveness of the Agency security posture. In 2022, the Agency conducted the SIS II Security Exercise 2022, focusing on the central system (including business continuity elements and other horizontal business areas).

2.10. Data protection

The SIS II 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 eu-LISA Data Protection Officer (DPO), monitors the implementation of data protection provisions, in particular concerning the processing of personal data by central SIS II.

During the reporting period, efforts were made to implement recommendations received from the EDPS on central SIS II in relation to an audit performed prior to the reporting period. The recommendations were transposed into an action plan, which was implemented throughout the reporting period. In November 2021, EDPS provided additional feedback that was taken into account by the Agency in order to continue implementing the EDPS's recommendations.

In October 2022, the **EDPS carried out a new audit on SIS II**. The initial draft minutes of this inspection were received in November 2022, and were internally reviewed and returned to EDPS in December 2022. Once the final report is received, the DPO monitors the implementation of all the recommendations, organising quarterly follow-ups.

As per standard practice, the **DPO was consulted regularly** during the reporting period on several general projects and, in particular, on specific projects related to preparing for the SIS Recast. Several data protection impact assessments were carried out to embed 'data protection by design and by default' into the design of the new system, including specific one-time data processing activities such as the data migration process.

During the reporting period, the **SIS II Supervision Coordination Group (SCG SIS II)**, which brings together representatives from Member States' national data protection authorities and from the EDPS, met twice a year as usual, and eu-LISA's DPO was regularly invited to attend the meetings. The objective of this group is to improve cooperation between the national supervisory authorities and to coordinate the supervision of central SIS II and the national systems, contributing to the exchange of relevant information and the implementation of common practices. The SCG SIS II also 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.

3

SIRENE FORMS EXCHANGED AND HITS REPORTED



3. SIRENE forms exchanged and hits reported

eu-LISA collects statistical data from the Member States every year, including data on the exchange of supplementary information between Member States (SIRENE forms) and on hits reported. This section presents data on SIRENE forms and hits reported for the reporting period.

3.1. SIRENE forms exchanged

SIS II contains information that can identify a person or an object and the necessary action to be taken (alert data). **Member States are legally required to exchange supplementary information**, i.e. to consult each other about the circumstances and follow up on the specific case. In every Member State connected to the system, there is a **SIRENE Bureau**, a single point of contact that is fully operational 24/7, which is responsible for coordinating and verifying the quality of the data entered in SIS II and facilitating the necessary information exchange with other Member States. The SIRENE Bureaux are at the very heart of SIS operations and play a key role in effective and efficient law enforcement cooperation and border management in Europe.

The different SIRENE Bureaux exchange information in a structured way using specific **forms**. The exchange can be bilateral or multilateral. During the reporting period, there were 14 different SIRENE forms in use, the most frequently used ones being:

- the *A Form*: supplementary information pursuant to Article 26 of the SIS II Decision²⁰, for European arrest warrants or for extradition requests;
- the *G Form*: matching an alert (hit);
- the *H Form*: procedures cannot be followed;
- the *M Form*: miscellaneous information.

The full list of SIRENE forms is available in the SIRENE Manual²¹.

In 2021, a total of 1,878,997 forms were exchanged between the Member States. Of those, 534,725 were outgoing and 1,344,272 were incoming forms. The number of forms exchanged increased slightly **in 2022, with a total of 1,921,011 forms** exchanged between the Member States (569,421 outgoing and 1,351,590 incoming forms).

Table 1 and **Figure 5** below provide a breakdown of outgoing and incoming forms for the reporting period.

²⁰ Council Decision 2007/533/JHA, OJ L 205 7.8.2007, p. 63.

²¹ Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second-generation Schengen Information System (SIS II), OJ L 231, 07.09.2017, p. 1.

FORMS EXCHANGED, 2021-2022

FORMS	2021		2022	
	OUTGOING	INCOMING	OUTGOING	INCOMING
FORM A	20,784	539,788	17,322	495,472
FORM E	3,355	5,339	240	287
FORM F	11,918	11,868	11,165	11,194
FORM G	176,661	175,807	202,606	206,621
FORM H	38,144	40,077	50,684	53,345
FORM I	68	99	38	44
FORM J	777	822	758	821
FORM K	6,628	6,678	13,989	13,809
FORM L	6,405	7,584	6,756	10,306
FORM M	245,140	530,855	236,965	530,290
FORM N	6,069	6,130	8,835	8,813
FORM O	4,299	4,321	4,224	4,287
FORM P	14,396	14,828	15,778	16,231
FORM Q	81	76	61	70
TOTAL	534,725	1,344,272	569,421	1,351,590

Table 1: Number of outgoing and incoming forms by form type, 2021-2022

OUTGOING FORMS EXCHANGED, 2021 - 2022, IN THOUSANDS

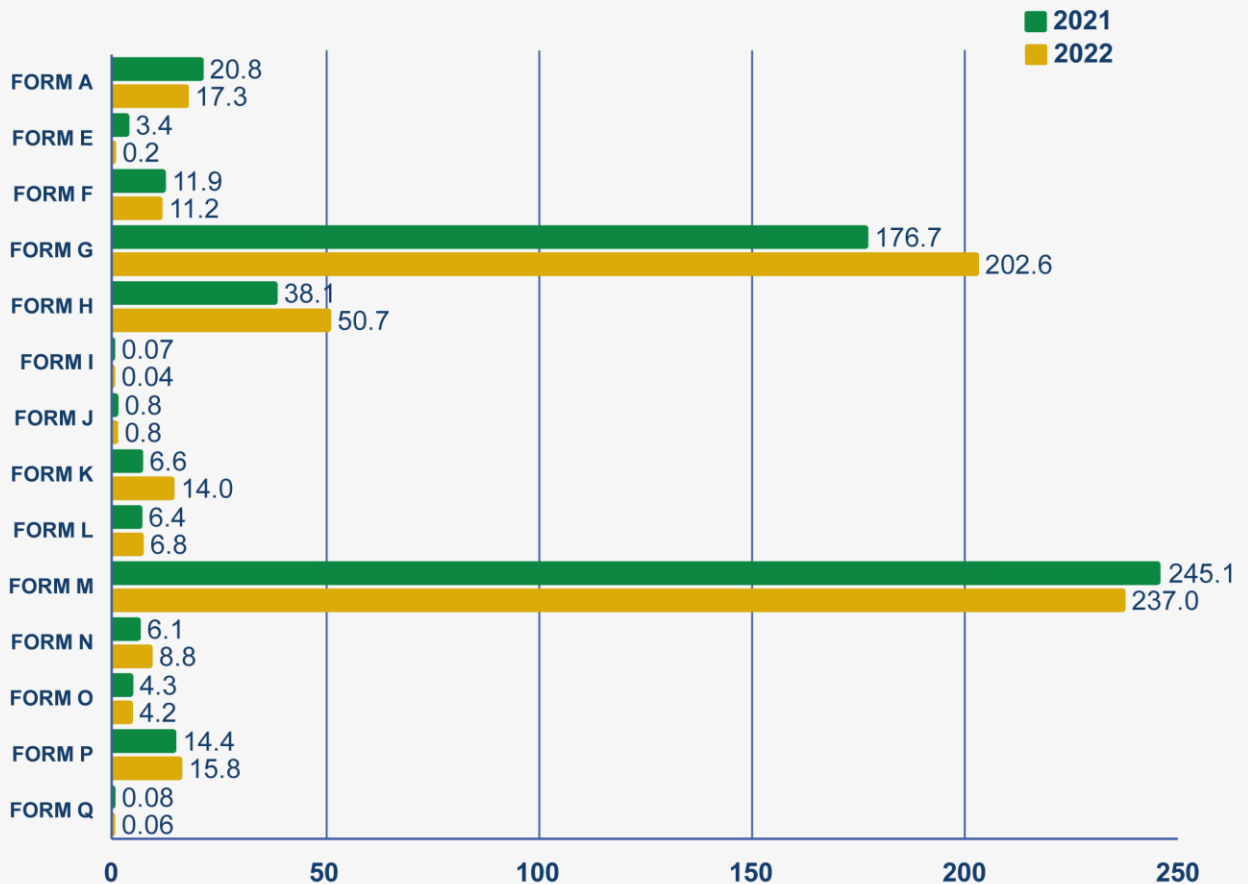


Figure 5: Outgoing forms by form type, 2021-2022

3.2. Hits reported

A **hit** occurs when a user conducts a search in SIS II and the search reveals a foreign alert (i.e. the alert in SIS II matches the searched data). A distinction is made between hits achieved on alerts issued by other countries (hits on foreign alerts) and hits achieved in other countries on alerts issued by the reporting country (hits abroad on own alerts).

The Member States reported a **total of 222,967 hits on foreign alerts in 2021** and **263,452 in 2022**. Compared to 2020, the number of hits increased by 6.6% in 2021 and 26% in 2022, confirming a recovery from the decrease in usage during the COVID-19 pandemic.

Figure 6 below provides a breakdown of hits on foreign alerts for the reporting period.

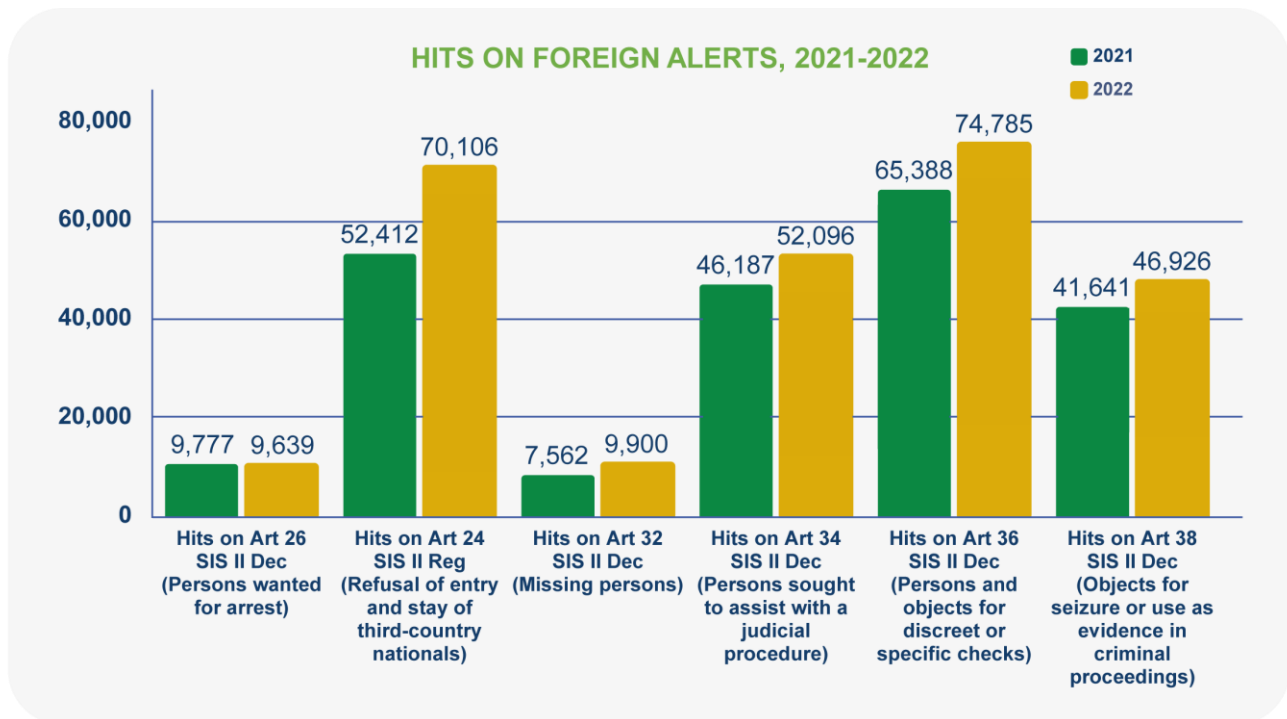


Figure 6: Hits on foreign alerts, 2021-2022

CONCLUSIONS

Conclusions

SIS II, being at the heart of Schengen, is Europe's most widely used information-sharing system, playing a crucial role in the area of freedom, justice and security in Europe. eu-LISA ensures the effective and uninterrupted operational management of its critical infrastructure, including agile project management for the timely evolution of the central system and appropriate 24/7 operational monitoring support.

SIS II use made a good recovery from the low usage experienced during the COVID-19 pandemic period, with 12.7 billion searches in 2022. The data stored in the system decreased slightly, due to the deletion of UK data in 2021 following the United Kingdom's withdrawal from the European Union, and the deletion of securities and non-cash means of payment alerts in 2022 as a result of changes in legislation. By the end of 2022, 86.5 million alerts were stored in SIS II.

New Member States were connected to either SIS II or AFIS during the reporting period, increasing the usage of the system. Ireland was connected to SIS II and AFIS as a new user in 2021, while Estonia, Finland, France and Norway connected to AFIS in 2021 and 2022.

During the reporting period, central SIS II performed very well and in line with the legal requirements. The Agency deployed several releases and finalised various projects, which introduced new functionalities and ensured that the system remains operational, secure and efficient. Tremendous efforts were made by the Agency, the Member States, the Commission, the JHA Agencies and the wider SIS community to be ready to implement the new Schengen Information System (SIS recast), which eventually entered into operation in March 2023.

To better support the user community and to facilitate the implementation of the upcoming new system, significant efforts were made to further develop the SIS training portfolio. The Agency also carried out continuous security and data protection activities throughout the reporting period, ensuring adherence to the core principles of security, confidentiality, integrity and availability. The recommendations made by the EDPS are also being implemented.

Looking to the future, eu-LISA remains strongly committed to keeping the SIS central system operational around the clock, whilst ensuring the system's operational maintenance and further development as per the legal requirements.



Publications Office
of the European Union

Manuscript completed in November 2023.

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.

ISBN 978-92-95227-67-5 ISSN 2443-8294 doi:10.2857/02574 Catalogue number: EL-AE-23-001-EN-N

© European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), 2023

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of elements that are not owned by eu-LISA, permission may need to be sought directly from the respective rightsholders.

The image on the cover and the flag icons in the executive summary have been retrieved from and licensed by Adobestock – www.adobestock.com.

www.eulisa.europa.eu