



Council of the
European Union

Brussels, 3 September 2020
(OR. en)

10389/20

VISA 96
COMIX 360

NOTE

From: General Secretariat of the Council

To: Visa Working Party/Mixed Committee (EU-Iceland/Norway and
Switzerland/Liechtenstein)

Subject: Report on the technical functioning of the Visa Information System (VIS)

Delegations will find attached the 2020 report from eu-LISA regarding the technical functioning of the Visa Information System (VIS).

Report on the technical functioning of the Visa Information System (VIS) August 2020

Protection level: **PUBLIC**

This document has been produced in application of Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Council Decision 2008/633/JHA to provide information on the technical functioning of the VIS, including the security thereof. The report also describes the use made by Member States of Article 4(2) of Council Decision 2008/633/JHA. This document is public. Reproduction is authorised, other than for commercial purposes, provided that the source is acknowledged.

eulisa.europa.eu

ISBN 978-92-95217-65-2

ISSN 2467-3099

doi:10.2857/66661

Catalogue number: EL-AM-20-001-EN-N

© European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), 2020

Contents

Executive summary	5
1. Introduction	6
2. Operational management of the VIS	7
2.1 VIS-BMS evolutions and releases	7
2.2 Projects and activities	10
2.3 Integration projects	12
2.4 Quality of service	13
3. The communication infrastructure and its functioning	15
4. Security	16
5. Data protection	17
6. Usage of the VIS: trends and figures	18
6.1 Usage per activity reported by Member States	19
6.2 Reported usage of Article 4(2) of the VIS Decision	21
Conclusions	23
Annexes	24
1. Data reported by Member States on usage of the VIS pursuant to the VIS Regulation	24
2. Reported usage of Article 4(2) of the VIS Decision	25

Executive summary

Operational Management



- VIS capacity increase to 100 million records
- First step of BMS virtualisation
- Upgrade of the VIS ELISE search engine

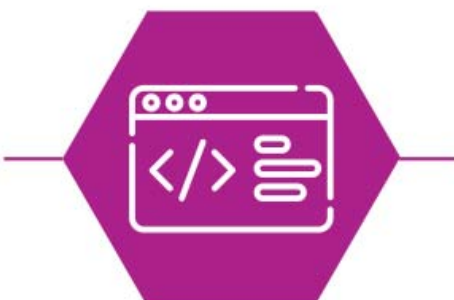


- The VIS-BMS central system was stable
- In 2018 the availability was 99.87%
- In 2019 the availability was 99.91%

Availability

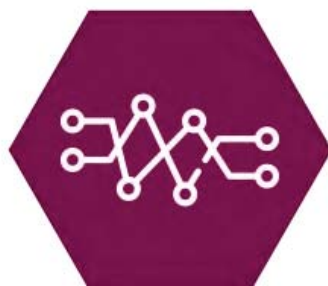
Integration Projects

- RO and BG passive access
- Europol access



Projects

- Tuning VIS-BMS throughput
- New end-to-end testing tool



VIS-EES Interoperability

- Updated VIS ICD
- Feasibility study on VIS network upgrade
- Second encryption layer pilot initiated



Usage Trends

- 25 million alphanumeric searches in 2019
- 7 million biometric searches in 2019
- 43 million border operations in 2019
- 1.87 second processing time for border FP verification

1. Introduction

The Visa Information System (VIS) started operating in October 2011, and since February 2016 it has been operational worldwide¹. Since 1 December 2012, eu-LISA (the 'Agency') has been in charge of the operational management and the further development of the central system.

The VIS is at the core of the Schengen area, connecting Member State² consulates in non-EU countries and all external border crossing points. It supports Member States' consular authorities in the **management of applications for short-stay visas to visit or to transit through the Schengen Area**. Thanks to its Biometric Matching System (BMS) – the subsystem responsible for biometric operations – the VIS allows Member State borders authorities to **identify and verify third-country nationals who travel to the EU**. Furthermore, the VIS supports the fight against fraud and facilitates checks within the territory of the Member States, assisting in the identification of any person who may not or may no longer fulfil the conditions for entry to, stay in or residence on the territory of the Member States. In addition, as ancillary objectives the VIS supports the asylum applications process and contributes to the prevention of threats to internal security³.

In managing data for borders, migration and security, the VIS is an integral part of the Justice and Home Affairs (JHA) interoperable IT architecture that is under development. In May 2018, the Commission proposed⁴ a **revision of the VIS legal framework** to better respond to changing security and migratory challenges and improve management of the EU's external borders. The main objective of the revision proposal is to have a stronger, more efficient and more secure common visa policy. The proposed changes to the VIS will enable more thorough background checks on visa applicants, closure of security information gaps through better information exchange and full interoperability with other EU-wide databases. The proposal also foresees the introduction of facial image search capability and the storage of more information such as long-stay visas and residence permits. As part of interoperability, **full interconnection between the VIS and the EES**⁵, with elements of data exchange and synchronisation, will be paramount. This will limit duplication of personal data in accordance with the 'privacy by design' approach.

As it is responsible for the operational management and further development of EU large-scale IT systems in the JHA area, the Agency is building up specialised technical expertise and has become a recognised player. The technical expertise is particular relevant in supporting the co-legislators during the whole legislative process. At the time of writing, these negotiations were still ongoing.

This report is published every 2 years and submitted to the EU institutions⁶ in line with Article 50(3) of Regulation (EC) No 767/2008⁷ and Article 17(3) of Council Decision 2008/633/JHA⁸. It details the technical functioning of the VIS central system, providing an overview of operational management activities during the reporting period (1 October 2017-30 September 2019). The report includes data provided by Member States on usage of the VIS⁹, and the requirement for and use made of Article 4(2) of the VIS Decision.

¹ Between October 2011 and February 2016, the VIS was deployed in phases in the Member States' consulates worldwide.

² Member States in the current document refers to the Member States of the EU and Schengen Associated Countries which are connected to the VIS, unless otherwise specified. Member States of the EU connected to the VIS are Belgium, Czechia, Denmark, Germany, Estonia, Greece, Spain, France, Italy, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Slovenia, Slovakia, Finland and Sweden. Schengen Associated Countries connected to the VIS are Iceland, Liechtenstein, Norway and Switzerland. The EU Member States of Romania, Bulgaria, Cyprus and Croatia are not yet connected to the VIS.

³ Since 1 September 2013, the VIS has also been accessible for consultation to Member States' designated authorities and to Europol as per Council Decision 2008/633/JHA, for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

⁴ COM(2018) 302 final, 16.5.2018.

⁵ Regulation (EU) 2017/2226, OJ L 327, 9.12.2017

⁶ Previous reports are available on eu-LISA website <https://www.eulisa.europa.eu/our-publications/reports>

⁷ OJ L 218, 13.8.2008, hereinafter 'VIS Regulation'.

⁸ OJ L 218, 13.8.2008, hereinafter 'VIS Decision'.

⁹ As per Article 50(6) of the VIS Regulation and Article 17(5) of the VIS Decision. The latest contribution was received from Hungary on 23 July 2020.

2. Operational management of the VIS

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

During the reporting period, the maintenance in working order (MWO) has been provided through the framework contract (FWC) signed in May 2016 with the successful consortium²⁰. The FWC has been signed for 4 years with the possibility of renewal for up to 24 months. The MWO covers the provision of services related to corrective, adaptive, preventive, perfective and evolutionary maintenance of the central VIS, the BMS and the VIS Mail System and devices shared between the VIS and SIS II, as well as associated services and technical support to the Member States. eu-LISA is responsible for the operational management of the central VIS and the BMS. On the other hand, the contractor provides the MWO and is responsible for the performance of the system, any dysfunction or degradation in the performance of services and for complementary maintenance needed to overcome and solve such dysfunctions or degradations.

Operational management of the central VIS system is done in strict coordination with the Member States and the Commission. Several fora²¹ exist in this respect, primarily eu-LISA's Management Board (MB) and the VIS Advisory Group (AG). The AG meets regularly four times a year, to discuss, inter alia, the availability and performance of the central system, approve proposed changes and release plans and also future developments.

The specific technical expertise developed by the Agency is also recognised and relevant in the Schengen Evaluation Mechanism. Since 2017, the Agency has been supporting the Commission and the Member States on a best efforts basis in the context of common visa policy evaluations²².

2.1 VIS-BMS evolutions and releases

As eu-LISA is in charge of the VIS central system's operational management it is also responsible for the continued technological and functional development of the system. Developments and changes are discussed and formalised within the change management process, ensuring agreement with Member States and thus coordinated implementation. Once agreed, the changes are implemented in line with the annual release plan, which is discussed at the beginning of each year with the Member States. A release plan for a given year comprises two releases, one major and one minor release, with some flexibility to accommodate operational needs throughout the year.

In autumn 2017, at the beginning of the reporting period, the VIS database's storage capacity was up to 60 million records. In terms of data stored, there were slightly more than 49 million visa applications and over 41 million fingerprint sets. In the light of the projections model used periodically for estimates of future usage, at that point in time, the capacity limit was going to be reached by the end of 2019. To align the system with business requirements, a central system capacity upgrade project was planned in two phases:



²⁰ Bridge³, composed of Accenture NV/SA, Atos Belgium NV/SA and Idemia Identity and Security France SAS.

²¹ For example: the Change Management Group, the National Contact Points for training (NCP network), the Security Officer network (SON).

²² In line with Regulation (EU) No 1053/2013, the Commission has invited eu-LISA to be an observer in common visa policy evaluations. During the reporting period, eu-LISA experts supported six evaluation missions in Member States' consulates worldwide.

- phase 1 VIS capacity increase to 85 million records
- phase 2 VIS capacity increase to 100 million records and phase 1 BMS increase to 85 million records

A **technical release** (R2-17) including corrective and adaptive items at application, database and system infrastructure level for both the VIS and the BMS was deployed in November 2017. Member States were asked to perform tests in Q3 2017. The first deployment attempt was not successful as it caused an issue with the BMS. The release was finally deployed a day later, once the issue had been solved. The deployment strategy adopted for the release was the standard one, with a switchover to BCU²³ on 9 November and switchback to CU on 14 November.

The first 2018 release – R1-18, including VIS version 3.2 and BMS version 2.5 – consisting of the **upgrade of the VIS ELISE search engine**, in addition to the deployment of corrective and adaptive items at application, database and system infrastructure levels on both VIS and BMS was planned for the spring. After a first deployment attempt at the beginning of April, which identified an issue with the BMS asynchronous transactions, the release was put on hold to allow investigations. The issues encountered were due to hardware failure in BCU and were not related to the release itself. R1-18 was eventually successfully deployed with a switchover to BCU on 18 May, and a switchback to CU on 29 May. Due to the release, the search functionality was unavailable for 7 hours (during the night of 18-19 May), this being the time needed to upload all records into the memory.



By mid-2018, considering the steep growth in visa activity, the increase of the VIS database capacity became critical. Release R2-18 included the increase of the **VIS database capacity to 85 million records** (VIS 3.3), the alignment with a new test environment (NTE) allowing partial virtualisation and the deployment of corrective and adaptive items at application level. During this release, a PSAT (soak test with Member States) was carried out. Two volunteer Member States – Germany and Poland – took part in the test, whereas the rest of Member States were simulated. Deployment and switchover to BCU were done on 20 August 2018 following an intensive month of preparation, while deployment and switchback to CU took place on 8 October with another intensive month of preparation. With VIS 3.3 a significant step was achieved. Beside the significant

increase in the capacity of the database, the first step for virtualisation of the VIS was implemented and the ELISE search engine licence was upgraded to deal with more than 60 million records.

The last release initially planned at the end of 2018 was postponed to the beginning of 2019 due to its technical complexity and very long deployment per site. Release R3-18 included evolutive, corrective and adaptive items at levels of application, database, system infrastructure and hardware. The main goals of the release were to implement the **BMS virtualisation** (production and pre-production environments) and the first phase of the transactional tuning/alignment between the VIS and the BMS (enabling better use of existing computational resources). The integration of the new users – Europol, Romania and Bulgaria – was eventually not included in the scope, due to the re-prioritisation exercise. The release came into operation on 11 March 2019 with a switchover to BCU and on 24 April with a switchback to CU. Important business benefits of R3-18 were the alignment of the architecture between the BMS and the new test environment, enabling alignment the transactional distribution of VIS-BMS with the Member States' use of the central system.

²³ BCU: Backup Central Unit; CU: Central Unit.

In the summer 2019, the second phase of the VIS database upgrade was finally implemented. Release R1-19 included the **VIS capacity increase to 100 million records**, and the deployment of corrective and adaptive items at application level on both the VIS and the BMS. R1-19 came into operation on 12 June with a switchover to BCU. Following the switchover, some incidents occurred in relation to the BMS virtualisation (released early in the year). Performance degradations were observed, thus the switchback was put on hold until the BMS was stable. Once root causes had been established and the BMS stabilised, the switchback was done following the activation of the release in BCU on 19 August. A thorough investigation was launched, and major efforts were made by the MWO contractor and the Agency. A patch for middleware components was deployed in September. The medium-term solution to the issue involved a reconfiguration of the middleware database and application which will be implemented with the 2020 releases. Due to this issue, no additional releases on the BMS were implemented in 2019. The planned BMS virtualisation step2, initially planned for end 2019, was eventually postponed to 2020.

Release R1-19 concluded the project initiated in May 2017 for the VIS upgrade (in two steps). The Final System Acceptance was completed on 3 October 2019 after 4 months of intensive monitoring of the system in production without there being any issues related to the upgrade.

The initial scope of release R2-19 included increasing the BMS database to 85 million records and other technical BMS upgrades. On the other hand, as mentioned above, due to the incident during the summer it was decided to reduce the scope of R2-19. The decision was based on business needs – the BMS will not need 85 million records in the short term – and furthermore it was considered preferable to extend the test campaigns to prevent a similar situation to the first phase of the BMS virtualisation. Release R2-19 finally included the deployment of corrective and adaptive items at application and database levels for the VIS and the **connection of Europol as a new user**. Deployment took place on 15 October with a switchover to BCU, and the deployment and switchback to CU occurred on 6 November.

The test team is fully involved in all release. The team attends release management meetings, reviews and provides input on different deliverables (e.g. release scope, test design descriptions, detailed test plans, test reports, lessons learned, release planning, environment planning, etc.) and liaises with the contractor during the tests. Prior to each deployment, depending on the type of the release, different kind of test campaigns⁴⁴ are carried out. The eu-LISA test team plays a central role by directly carrying out some test campaigns, supervising tests done by the contractor in close cooperation with the Agency and planning and coordinating the tests done by the Member States.

During the reporting period, intensive efforts continued to **increase the quality of the data** stored in the system. To support Member States in acquiring good quality fingerprints to be uploaded to the system, eu-LISA has already conducted impact analysis and wide-market research on replacing the **fingerprint acquisition software toolkit** in use⁴⁵. The project which focused only on the VIS was put on hold, as it was preferred – in line with the interoperability requirements – to have one tool that could be tailored and used across systems. Requirements for this were included in the call for tender for sBMS.



⁴⁴ System Solution Test (SST), Non-regression test (NRT), SOAK test, Factory Acceptance Test (FAT), resilience tests, Provisional System Acceptance Test (PSAT).
⁴⁵ The end-to-end user quality software currently in use provides immediate feedback on low-quality or incorrect data, avoiding the transfer of data that would be rejected by the BMS, ensuring a consistent approach in the validation of biometric data quality.

In line with its mandate, the Agency continued the **regular monitoring activity**, both for data in the fields required by Articles 9 and 10 of the VIS Regulation, but also for the presence or not of fingerprints and facial images. Thorough business analysis was regularly presented and discussed with the Member States at the AG meetings. Given the critical nature of the topic, dedicated training activities were also organised focusing on data quality and on best practices to be implemented at national level. The *VIS data quality* training course was organised in September 2018 and focused on use of the fields deriving from Articles 9 and 10 and on the relevant business rules.

To enhance best practice implementation and support the most recent developments, a series of webinars were organised during the reporting period on the following topics:

- *VIS ICD*²⁶ focusing on the purpose and structure of the ICD and on how the national systems communicate with the VIS central system;
- *VIS Search Functions* dedicated to the ELISE search engine; introducing available search profiles and how to use them effectively; providing an overview of the scoring and ranking mechanism of search results;
- *VIS Best Practices* to raise awareness on the most frequent deviations observed in VIS transactions and how mitigate them with processes at national level;
- *VIS business analytics* introducing data collection and consolidation principles for generating VIS business analysis reports.

In addition to the webinars, face-to-face training activities also continued during the reporting period. The first cycle of *VIS Development Training Programme for IT Operators* (VIS DTPITO) was completed in 2018; the second cycle started in 2018 and was completed the following year.

A total of 20% of the **training activities** delivered in 2018 were dedicated to the VIS, while this was 12% in 2019.

2.2 Projects and activities

In addition to the central system evolutions and releases mentioned above, several other activities, studies and projects were conducted on the VIS and BMS during the reporting period, not necessarily on the production environments. Below there is information about the main ones, while there were many others of lesser importance.



VIS refactoring for flexible transactional tuning: the project was initiated in the summer 2017, on the basis of the VIS-BMS active-active study in 2015 and 2016, providing the directions for a better and more flexible use of the systems with the main target being to reduce significantly the system being unavailable due to planned maintenance. While the system never suffered extended periods of unplanned unavailability, business stakeholders continue to feel that the duration of planned system maintenance continues to have too great an impact. After numerous optimisations to the deployment and switchover procedures over the years, it was clear that the objective could be reached only reconsidering the VIS's architecture. The

scope of the project, which was to validate a proof of concept for the active-active setup of the VIS-BMS technical stack, was complemented in 2018 by including the entire VIS business analysis. The aim was to build a new VIS custom application based on micro-services which could replace the incumbent one-piece Java application. With the introduction of the EES in the landscape of the systems to be developed and managed by eu-LISA and the EES's

²⁶ Interface Control Document.

future connection with the VIS, the expected outcomes of the project were challenged and only some of the source code will be valuable for the future micro-services based platform.

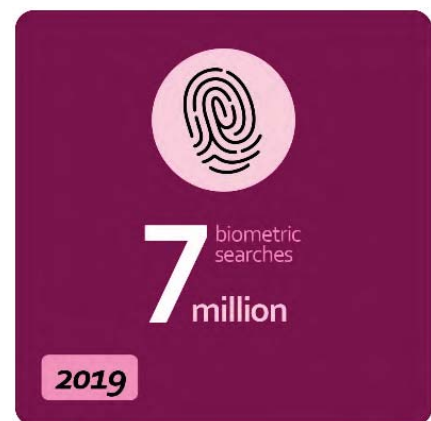
VIS-EES interoperability: the EES Regulation requires the establishment of interoperability between the EES and the VIS by providing a direct communication channel between the two central systems. Interoperability should enable direct consultations from the VIS to the EES and vice versa. The full implementation of VIS-EES interoperability is a complex and long-lasting project composed of several phases. The VIS will be affected from different angles: operational, performance requirements (network, infrastructure, volume/capacity), availability requirements, fingerprint quality, and search performance. Recent VIS-BMS developments have already been greatly influenced by the future interconnection between the VIS and the EES. A first project in this area focused on the requirements analysis and high-level design of the functional changes, which were described in an updated VIS ICD and in a new VIS-EES interoperability ICD²⁷. To achieve this, a series of Change Management Group meetings were held in Q2 2019 and attended by many Member States, in particular for the review phase. The VIS ICD was formally endorsed by the VIS formation of the SIS/VIS Committee in September 2019. A Project Management Forum (PMF) was set up to coordinate the implementation phase, i.e. to start the development and testing at national level²⁸.

Replacement of components:

- **VIS SAN²⁹ switches replacement:** as a link between the VIS database servers and the infrastructure hosting the data, the eight VIS SAN switches are crucial backend interconnection components. Moves to replace them before the end-of-support date were initiated at the beginning of 2019 and finalised in November that year.
- **VIS management firewalls replacement:** 16 VIS management firewalls were replaced during 2018 and 2019 to ensure a third-party vendor continued to provide support for them and to prevent lack of contractual coverage in the event of problems.

Migration of the VIS legacy Storage Area Network solution to the Common Shared Infrastructure (CSI): the VIS disk arrays (one in CU, one in BCU) hosting the VIS data (test data in pre-production and business data in production) were installed during the course of the development of the VIS. The end-of-support of those components was announced by the manufacturer in 2018 as the 31 December 2019. This triggered the project for their replacement. As per the Agency's strategy, the data and the database engines will be migrated to the CSI. The project is ongoing and is to be completed in the first half of 2020. A dedicated extension of the support was contracted beyond the end of 2019 to ensure business continuity and contractual coverage in the event of problems before the project was completed.

Assessment of the quality of facial images stored in VIS: the project on evaluation of technical support for the quality of facial images stored in VIS started in December 2018 and was concluded in November 2019. In order to prepare the technical background for the implementation of recent and upcoming legislation such as interoperability and VIS revision, eu-LISA conducted a technical assessment of the existing VIS facial images. Quality information from around 68 million facial images stored in the VIS database was extracted and the logs were assessed with the intention to understand both the overall quality and eventual problem areas. The general conclusion of the assessment was that the future



²⁷ This project only concerned the VIS; changes required to the BMS – including possible changes to the BMS interface to the VIS – will be addressed in a separate project.

²⁸ Since October 2019, the PMF has been meeting monthly via video conference to provide overview progress, coordinate the national teams in line with the central activities, identify potential roadblocks and report on the advancement of VIS and EES governance.

²⁹ Storage Area Network

migration of the VIS facial image database to the sBMS database is not likely to lead to a significant degradation of the global performance of the EES-BMS database. This will also depend on vendor technology used.

Tuning of VIS-BMS transactional throughput: in order to use the VIS-BMS computing resources efficiently, the Agency planned to improve the VIS-BMS front-end configuration to align the distribution of transactions with the actual usage of the Member States. In 2019, the analysis report on the tuning of VIS-BMS transactional throughput was delivered and accepted. In the meantime, however, it became clear that the introduction of the VIS-EES interconnection would have a significant impact on the VIS-BMS transaction usage and distribution. As a result, no implementation could be planned for the tuning of the transactional throughput. As soon as the EES final usage forecasts are released, the analysis will be updated accordingly, and implementation will be initiated.

SLA for test environments: during the summer 2018, following an incident which caused the unavailability of the test environment for almost 6 weeks, in-depth discussions started with Member States on the critical nature of non-production environments for business. At that point, non-production environments did not have an SLA in place nor dedicated resources allocated (best effort obligations from the contractor). On the other hand, those outages could have serious consequences on Member State activities, resulting in delays and extra costs of testing and related activities for national systems. The AG strongly recommended making sure that proper SLAs were in place for non-production environments to prevent those incidents, and proposed working together with the Agency to define them. A dedicated project was launched in order to make the VIS test infrastructure more resilient.



42.8 million
border checks

2019

End-to-end testing tool: eu-LISA's approach to testing and the existing tooling landscape have been in place since the VIS-BMS first started and has proved to be a success over the years. Looking ahead, the Agency aims to achieve shorter test cycles of higher quality and obtain a more industrialised tools landscape. In 2018, a project was launched to set up a non-proprietary²⁰ testing solution leveraging industry-standard test tools for the VIS and the BMS, including support for end-to-end testing to result in an easier, faster and higher quality test processes. The project aimed to expand the test strategy to a holistic approach, in which the combination of the VIS and the BMS would be considered as a single unit²¹ from the Member States' point of view. The test strategy was enhanced with end-to-end testing for

performance tests to guarantee that the VIS-BMS could deliver the response times agreed with the Member States as documented in the ICD. Furthermore, an integrated test management and automation tool was set up allowing the creation of new test cases in an intuitive manner. Implementation of the VIS-BMS end-to-end testing platform was concluded in Q1 2019.

2.3 Integration projects

Works to provide **access to the VIS to Bulgaria, Romania and Europol** progressed during the reporting period. As soon as the legal framework allows, integration projects with Croatia and Cyprus will start. The following is the situation from the policy/legislative side:

- Pursuant to Council Decision 2017/1908²², Bulgaria and Romania will have access to consult the VIS data in a read-only mode, without the right to enter, amend or delete it, at the latest by the time the EES has come

²⁰ Non-proprietary in this context means not developed and owned by the maintenance contractor (i.e. Bridge³).

²¹ The initial testing approach was very focused on testing VIS and BMS separately, with separate processes and tools.

²² Council Decision on the putting into effect of certain provisions of the Schengen *acquis* relating to the Visa Information System in the Republic of Bulgaria and Romania, OJ L 269, 19.10.2017.

into operation. Passive access to the VIS for Bulgaria and Romania is a precondition for the application of the EES to those Member States.

- On 22 October 2019, a communication from the Commission confirmed that Croatia had taken the measures needed to ensure that the necessary conditions for the application of all relevant parts of the Schengen acquis were met, thus paving the way for preparation of passive access to the VIS. No Council Decision had been adopted on this matter yet at the time of writing.
- Cyprus is yet to have its Schengen evaluation process concluded, therefore no progress was made on the technical connection to the central system during the reporting period.

Preparatory works for the integration of Bulgaria and Romania started in 2017 with a plan to implement passive access in 2018. However, following an eu-LISA Management Board decision to re-prioritise some activities, the project started in March 2019. It consisted of different phases encompassing, inter alia, compliance testing of Member States' national VIS systems against the VIS ICD 3.0 (Visa Code Plus), and being validated in the VIS test environments prior to their connection to the central VIS production environment. As part of this implementation, these Schengen candidate countries will have to successfully carry out pre-compliance and compliance tests, as well as a PSAT campaign. Passive access for Bulgaria and Romania is currently planned for Q3 2020.

A feasibility study was run to assess Europol access to the system for consultation purposes²³. A project to establish a connection between Europol and the VIS central system had already started at the beginning of 2017. In Q2/Q3 2019, Europol successfully carried out the following tests on the VIS: tests on the central domain simulator, pre-compliance tests (pre-CT), formal compliance tests (CT), List of Authority tests, non-contractual free testing and national system performance testing. Release R2-19 came into operation in autumn 2019 and included Europol as a new user. Europol's first activity in the VIS is expected in the course of 2020.

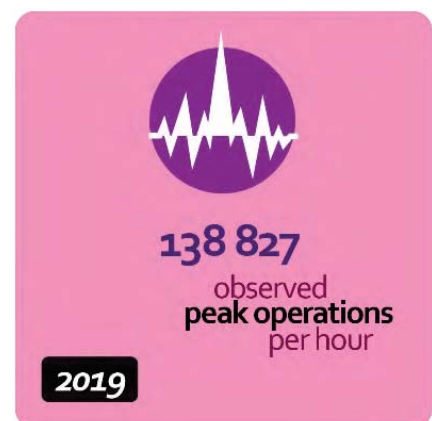
With a view to integrating Bulgaria and Romania, eu-LISA provided them with a dedicated VIS newcomers training programme. Field visits to Bucharest and Sofia took place in September 2017, and given that the projects gained pace again in 2019, a training session for all stakeholders was held at the operational site in Strasbourg in November 2019²⁴.

2.4 Quality of service

During the reporting period, the **VIS-BMS central system was stable and performed as expected** within the agreed service level agreement, in line with the legal requirements. **No major deviations** were found with regard to the central system performance. The BMS capacity and performance were adequate for Member States' usage.

The **availability** is calculated by the eu-LISA first-line support team taking into account SMg tickets²⁵, incidents and TESTA-NG reports, and the results were as follows:

- in 2017, the VIS-BMS central system was available 99.92% of the time; the total outages due to planned maintenance and unavailability due to incidents accounted for 6 hours and 57 minutes²⁶;
- in 2018, the VIS-BMS central system was available 99.87% of the



²³ As per Article 7 of the VIS Decision, Europol shall have access to VIS data within the framework of its tasks, for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

²⁴ Following the Management Board decision to de-prioritise activities, two planned courses for VIS newcomers planned in 2018 were postponed.

²⁵ Service Manager 9 (SMg) incident management tool in use.

²⁶ Including 2 hours and 57 minutes due to incidents.

time; total outages due to planned maintenance and unavailability due to incidents accounted for 11 hours and 38 minutes²⁷;

- in 2019, the VIS-BMS central system was available 99.91% of the time; outages due to planned maintenance accounted for 6 hours; in 2019, no full unavailability was registered due to incidents, on the other hand, the system was partially unavailable for over 22 hours²⁸.

To be able to maintain the requested **high level of performance** at central level, the VIS should be used in compliance with its design and contractual limits. There are service level targets for each business group – asylum, border, consular, law enforcement and territory – using VIS. In this framework:

- 99.24% of the operations were processed within the agreed SLA in 2017;
- 97.17% of the operations were processed within the agreed SLA in 2018;
- 97.79% of the operations were processed within the agreed SLA in 2019²⁹.

Looking more in details in terms of **average processing time** for some specific operations, the system is performing very well:

- the average processing time for *retrieval of a visa application by its number or visa-sticker number* was 0.24 seconds in 2019 and 0.32 seconds in 2018 – the SLA in this case is 30 seconds;
- the average processing time for *alphanumeric searches* was 0.78 seconds in 2019 and 0.89 seconds in 2018 – the SLA is set at 30 seconds;
- the average processing time for *fingerprint verification* (operation performed mainly at the borders) was 1.87 seconds in 2019 and 1.46 seconds in 2018 – the SLA is 3 seconds;
- the average processing time for *CUD operations* (create/update/delete), for example, for visa application and visa issuance, was 2.24 seconds in 2019 and 4.41 seconds in 2018 – the SLA for CUD is 30 minutes.

The eu-LISA first-level support team – operational 24 hours a day, 7 days a week – monitors the central system, and the traffic for each Member State connected to the VIS, carrying out analyses and assessing the business impact of any incident. The team is the entry point for users' reports of incidents or to request a service. During the reporting period³⁰ 3 625 tickets related to the VIS, including incidents³¹ were registered. Based on the initial analysis, impact, urgency and priority are defined, the relevant assistance is provided and functional and/or managerial escalation is triggered. Following IT best practice, eu-LISA has implemented IT service management (ITSM) processes³² to ensure

quality of service and to cope better with incidents and service requests. This is a continuous exercise to ensure efficient and cost-effective management of the VIS by continuously monitoring and developing operational processes.

From October 2017, the VIS MWO started using SMg to handle all kind of tickets (incidents, request, problems and changes). Allowing all tickets to be handled in one unique tool streamlined the communication and eventually improved the performance of the technical teams significantly. Prior to this, tickets were logged in two different tools³³. In mid-2018, the VIS operation manual was also updated. The new version included, in particular, revisions of some procedures and communication channels.



²⁷ Including 3 hours and 38 minutes due to incidents.

²⁸ See issues encountered with the BMS virtualisation mentioned above.

²⁹ This is KPI g.

³⁰ From 1 October 2017 to 30 September 2019.

³¹ From the total incidents during the 24-month of the reporting period, 0.5% incidents were classified as critical.

³² ITSM processes currently implemented include: Incident management, Request Fulfilment, Problem management, Change management, Test management, Release and Deployment management, Access management, Service Level management, Service Catalogue management, Configuration management. The Agency is finalizing the implementation of Availability management, Capacity management, Knowledge management and Continual Service Improvement.

³³ SMg for internal use and JIRA for communication with the contractors.

Every year, the Agency carries out a customer satisfaction survey covering the performance of eu-LISA's first-line support, incident and problem management, operational communication, technical assistance and support for national activities. The participation of the VIS community was stable in 2017 and 2018, but dropped from 80% in 2018 to 55% in 2019³⁴. Nevertheless, the satisfaction rate remained very high (over 91%). Improvements were deemed necessarily in particular for the test environment used by Member States (for the support model, governance and communication about the periods for maintenance). The results of the survey were analysed, lessons were learned and improvements were regularly applied.

3. The communication infrastructure and its functioning

In accordance with Article 1(2) of Council Decision 2004/512/EC³⁵ and the parallel provision in Article 2 of the Annex to Commission Decision 2008/602/EC³⁶, one of the three elements comprising the VIS is a communication infrastructure between the VIS central system and the national interfaces (NI-VIS). The infrastructure provides an encrypted, virtual, private network dedicated to VIS data, for communication among Member States and between Member States and the authority responsible for the operational management for the VIS central system. The abovementioned communication infrastructure is provided via a European private secure network named Trans European Services for Telematics between Administrations – new generation (TESTA-ng)³⁷.

The VIS network provides a secure wide area network for the exchange of data between central and national systems. The architecture of the network can be described as a dual star topology with resilience. The central unit (CU) and backup central unit (BCU) contain the systems to which each national network connects. The CU and BCU are interconnected by a dedicated point-to-point connection. The VIS network³⁸ is permanently monitored in order to ensure continuous service availability, while strict performance service level requirements have been established. During the reporting period covered in this report, there were no incident with critical impact on the functioning of the overall VIS community and no incidents affecting the connectivity of more than one site.

Pursuant to Article 7 of the eu-LISA Regulation, tasks regarding the communication infrastructure – including operational management and security – were divided between eu-LISA and the Commission until 30 June 2018. To ensure coherence of the responsibilities, operational working arrangements were established between eu-LISA and the Commission via a memorandum of understanding concluded in June 2014. As specified in Article 19, the Agency was responsible for the supervision, security and coordination of relations between the Member States and the network provider, and for the communication infrastructure for the VIS. On the other hand, the Commission was responsible for all other tasks relating to the communication infrastructure, in particular tasks relating to the implementation of the budget, acquisitions and renewal and contractual matters.

However, eu-LISA has been responsible for the VIS administrative tasks related to the communication infrastructure between the central VIS and



³⁴ Data was collected in the first quarter of 2020, and the COVID crisis might have affected the response rate.

³⁵ Council Decision of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004.

³⁶ Commission Decision of 17 June 2008 laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase, OJ L 194, 23.7.2008.

³⁷ The scope of services covered by the TESTA-ng network includes: a dedicated centralised Service Operations Centre (SOC) responsible for ensuring the operational management by the provider and the quality of the network on a 24/7 basis; consultancy services; secure connectivity; network services. These services relate to the provision, set-up and operation of a dedicated centralised management, monitoring and support infrastructure. Additional services cover the provision of monitoring tools, reporting and SOC staffing.

³⁸ The VIS Mail Relay service operated within the VIS network provides Simple Mail Transport Protocol (SMTP) relay functionality in a hub-and-spoke topology to national systems (NS-VIS) for the purposes of providing the VIS Mail consultation mechanism as stipulated in Article 2 of the Annex to Commission Decision 2009/377/EC. The VIS Mail SPoC (Single-Point-of-Contact) servers are two mailbox servers, one at the CU site and one at the BCU site, which host the VIS central SPoC mailbox. This allows NS SPoC mailboxes to send email messages to the central SPoC mailbox, and the central mailbox to send messages to the NS SPoC addresses.

national interfaces since 30 June 2018 pursuant to the VIS Regulation as amended by Article 61 of the EES Regulation. Management before that date was done by the Commission³⁹. Furthermore, Article 7 of the EES Regulation requires certain hardware and software components of the EES communication infrastructure to be shared with the VIS communication infrastructure. Logical separation of VIS data and EES data is to be ensured.

To accommodate the legal changes and in particular the new EES requirements, the Agency signed contracts with the TESTA-ng provider on 27 June 2019 to re-design and increase the capacity of the VIS communication infrastructure. A **feasibility study on the upgrade of the VIS communication infrastructure** to satisfy additional bandwidth needs for EES and ETIAS started in March 2019 and finalised in June. The upgrade will be achieved through a combination of line upgrades and replacement of the turnkey access points (TAPs) by new models at the sites where line upgrades alone would not be sufficient. A survey of the situation in the Member States was carried out during Q3 2019, including whether new equipment would be required for the line upgrades. By the end of the upgrade, the VIS communication infrastructure will have a capacity almost seven times higher than before and will be ready to support the entry into operation of the EES and ETIAS.

In 2018, a **second encryption layer⁴⁰ pilot on the VIS communication infrastructure** was initiated. The first part of the pilot was successfully conducted by implementing the solution for three Member States on the pre-production network. The second encryption layer of the VIS and the EES need to co-exist since they use the same communication infrastructure, while at the same time they need to adhere to the requirements of the legal provisions (i.e. logical separation of data). More clarity on the design of the EES second encryption layer is required before rolling out the VIS second encryption layer to all Member States to avoid the risk of additional cost and unavailability if both second encryption layer solutions are not designed in parallel. The project has thus been put on hold until more clarity on the EES side is available.

4. Security

eu-LISA ensures the operational effectiveness of the security controls at VIS central level, and the continuous improvement of the security strategy, in line with the requirements of the VIS Regulation and relevant Commission Decisions in terms of data protection and information security. Security is a core element of all activities undertaken at eu-LISA, due to the stringent legal framework. Furthermore, the Agency is growing into a centre of excellence in the provision of IT services, emphasising assurance of system and data security in all its activities.

In the context of the Agency's security monitoring and incident management processes, no critical security incidents occurred during the reporting period. The Agency's security unit continued to maintain and develop security measures concerning both physical and system security. As a core element of its Information Security Management Framework, the Agency operates and continuously develops its Information Security Management System (ISMS), in compliance with the relevant ISMS standards and ISO27001. Continuous monitoring and management of the residual risks took place to provide assurance that the appropriate security controls for the large-scale IT systems have been properly implemented and managed.

In accordance with the relevant security principles, standards and good practices mentioned, the VIS security and continuity risk management strategy covers all layers of the security spectrum: physical security, personnel security, network security, operating systems security, application security, business continuity and data security. Security requirements are embedded in all development projects, changes and maintenance activities. The eu-LISA's Security Unit is part of the VIS Operational Change Advisory Board, and takes part in any VIS development project from the initial phase to develop requirements.

³⁹ Pursuant to Article 26 of the VIS Regulation.

⁴⁰ While the SIS communication infrastructure has a second encryption layer to ensure that a third party cannot have access to clear-text data, the VIS communication infrastructure has no second encryption layer.



During the reporting period, the VIS central system went through numerous major upgrades embedding new technologies and components (e.g. capacity increase, new test environments, background databases, virtualisation). To reflect the security state of VIS-BMS after the latest evolutions, the **revision of the Security Risk Assessment, the Security Plan and the Business Continuity Plan** of the central VIS were deemed necessary. A thorough security assessment was initiated in Q3 2019 aimed at reviewing, with the support of the MWO contractor, the VIS-BMS Security Documentation.

After several months of preparation, eu-LISA and eight Member States⁴¹ together with ENISA and the Commission ran **the first VIS business continuity exercise** in October 2017. The end-to-end business continuity exercise aimed to test the security, business continuity and disaster recovery capabilities of the VIS. The exercise covered rehearsing the existing processes and technical procedures and further improving the overall coordination and readiness of the VIS community in the event of a disaster. The outcome of the exercise was mainly analysed with Member States at SON⁴² meetings. A list of improvement measures was drawn up and monitored continuously through the operation and secure management lifecycle of the system.

As part of the update of the VIS ICD due to the interconnection with the EES mentioned above, there was a thorough review of the interconnection security requirements.

In November 2018, the European Data Protection Supervisor (EDPS) carried out an inspection on the VIS central system focusing on operational management, internal communication infrastructure and security. The final **EDPS 2019** inspection report was received by eu-LISA in November 2019. The recommendations were analysed and, as per standard practice, they will be addressed in order to further enhance the level of trust in the management of the system. Overall, the inspection report noted no critical findings regarding the security of the central VIS, and no security incidents regarding any unauthorised access to VIS data. Note that the VIS central system is an isolated, controlled and secure environment.

Fruitful cooperation with Member States and other EU Agencies has been maintained in particular through the SON, where knowledge and best practices have been exchanged. The network meets twice a year, discussing developments in the threat landscape, latest trends in the security and business continuity fields, and ways ahead for the security community.

5. Data protection

Data protection is a key factor in the success of the VIS's operations and for the Member States using the system. The quality of the data, data security and regulatory compliance with the legal framework provide the conditions for the VIS to support Member States effectively in the visa procedure and in border checks, while upholding the rights and freedoms of third-country nationals applying for a Schengen Visa.



⁴¹ Estonia, Finland, Germany, Greece, Netherlands, Portugal, Slovenia and Sweden.

⁴² Security Officer Network.

The protection of personal data related to individuals processed by the VIS at central system level is monitored by the European Data Protection Supervisor (EDPS) in close cooperation with eu-LISA's Data Protection Officer (DPO). Quality of data stored in the VIS central system and the rights of data subjects, as per the legal provisions, are ensured by the Member States.

As mentioned above, at end 2018, the **EDPS carried out an inspection of the VIS central system** with the support of the Acting DPO and the Security Unit. The inspection also included checks to follow up on the recommendations from the previous VIS inspection – carried out in 2015 – and new checks on personal data breach procedures, personal data retention periods and system acquisition. The Acting DPO coordinated the inspection and acted as a liaison between the Agency and the EDPS during the entire exercise.

Throughout the reporting period, the DPO of eu-LISA was regularly consulted by the VIS Product Manager and the VIS Operational Change Advisory Board on a number of VIS-related projects involving personal data.

Accountability, a risk-based approach, transparency and managing data breaches are key aspects stemming from the EUI-DPR⁴³, which came into force on 11 December 2018. eu-LISA's DPO is committed to informing, raising awareness and advising on these new obligations, in particular, in regard to the operational management of the VIS central system and the developments required for interoperability with other large-scale IT systems.

The eu-LISA DPO represents the Agency at the twice-yearly meetings of the VIS Supervision Coordination Group, and reports on the current state of the VIS central system, future developments, data quality issues and security incidents at central system level or reported by Member States. This group, composed of the National Data Protection Authorities and the EDPS, monitors data protection legal compliance at both Member State and VIS central system levels.

6. Usage of the VIS: trends and figures

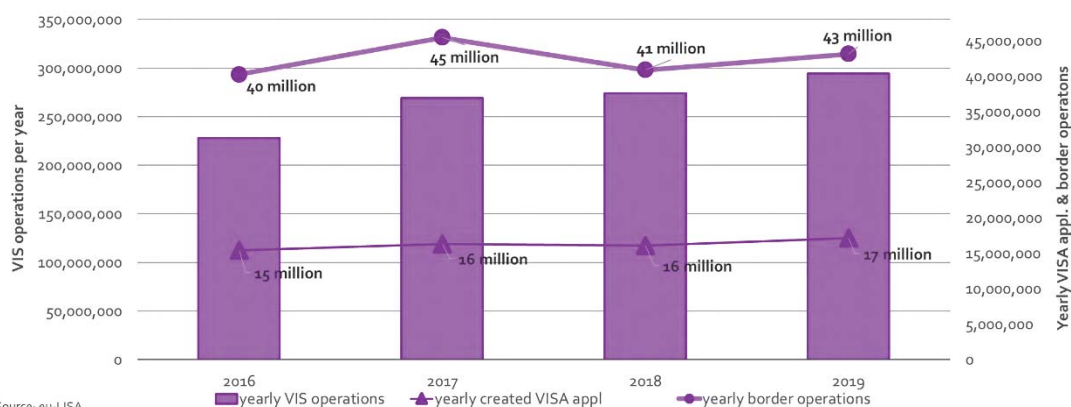
The VIS started operations in 2011 and was rolled out in phases worldwide with the two biggest regions in terms of issuing visas – China and Russia – rolled out in Q3/Q4 2015. Since completion of the rollout in February 2016, the system has been operational worldwide in all consulates of the Schengen countries.

Data from the VIS central system for the last 3 years (see Graph 1) show that:

- the total number VIS operations per year has been slowly increasing;
- the number of visa applications processed per year is quite stable;
- border operations fell in 2018 but rose slightly in 2019.

⁴³ Regulation (EU) 2018/1725 – GDPR for EU Institutions and Bodies (EUI-GDPR) – came into force on 11 December 2018.

Graph 1: VIS operations, visa applications and border operations, 2016-2019



Source: eu-LISA

The maximum number of operations per hour observed (peak/hour) was 123 393 operations in 2018 and 138 827 operations in 2019, which still represents only one-third of the total capacity. In fact, the VIS was tested with a maximum throughput of up to 450 000 operations per hour without performance deterioration.

The busiest month was July in both 2018 and 2019. This is in line with past usage and reflects the fact that over 53% of the visa applications registered in 2019 were for tourism reasons. In terms of searches, the VIS central system processed:

- 25 million alphanumeric searches in 2019 (2018: 23 million)
- 7 million biometric searches in 2019 (2018: 8 million)
- 17 million biometric authentications⁴⁴ in 2019 (2018: unchanged)

The highest demand for Schengen visas was registered by the Russian Federation. With over 4 million visa applications registered in 2019, growing from over 3.5 million in 2018, the Russian Federation continued to be the most active region worldwide. The second most active region was China with almost 3 million visa applications in 2019, up from 2.8 million in 2018.

As per Article 50(6) of the VIS Regulation and Article 17(5) of the VIS Decision, Member States have a legal obligation to provide data to eu-LISA to compile this report. The data collection has been a very long and complex exercise⁴⁵. An overview of the data is available in the annexes and there is a short analysis below.

6.1 Usage per activity reported by Member States

Usage of the system differs substantially between Member States. While the extent of the consular network and historical ties determine – amongst other things – the workload of the consular posts, both the number of third-country nationals crossing the external borders and the number of crossing points have a significant impact on usage of the system for border control purposes.

The breakdown of data sets collected from the Member States in relation to usage of the VIS pursuant to the VIS Regulation is available in Annex 1. Taking into account the data sets provided by the Member States (see Graph 2), analysis shows that during the reporting period:

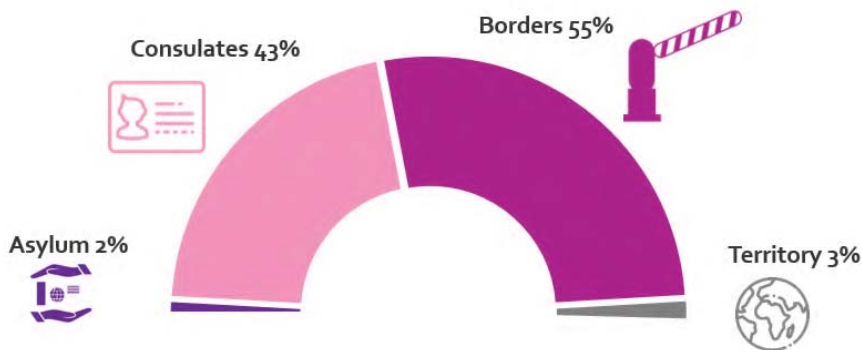
- 55% of the operations were carried out at the borders – ‘visa verifications border’ and ‘identifications border’;
- 43% of the operations were carried out at consular posts – ‘registered applications’, ‘issued visa’ and ‘refused visa’;

⁴⁴ Fingerprint verification mainly performed at the border posts.

⁴⁵ The last contribution was received from Hungary on 23 July 2020.

- 2% of the operations were carried out for asylum purposes⁴⁶ – ‘searches asylum’ and ‘identifications asylum’;
- 3% of the operations were carried out by the competent authorities within the territory⁴⁷ – ‘visa verifications within territory’ and ‘identifications within territory’.

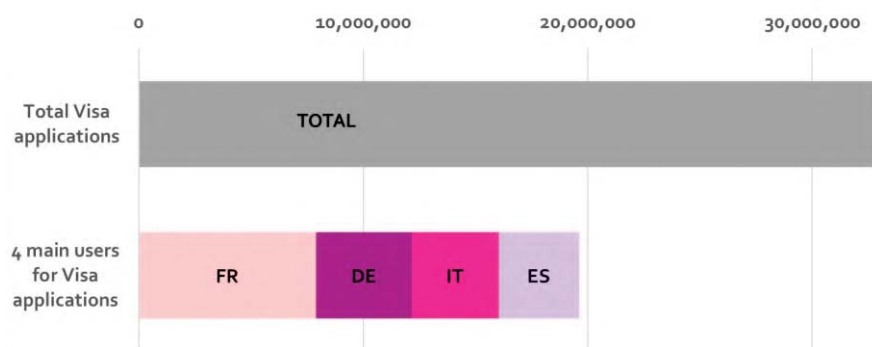
Graph 2: VIS usage per user group during the reporting period



Source: eu-LISA

From October 2017 until the end of September 2019, almost 33 million visa applications were handled via the VIS resulting in almost 29.5 million visas issued and over 3 million refusals. The peak was registered in July 2019 with almost 2 million applications handled within 1 month. Four Member States – France, Germany, Italy and Spain – handled 60% of all visa applications (see Graph 3).

Graph 3: Four main VIS users for visa applications during the reporting period



Source: eu-LISA.

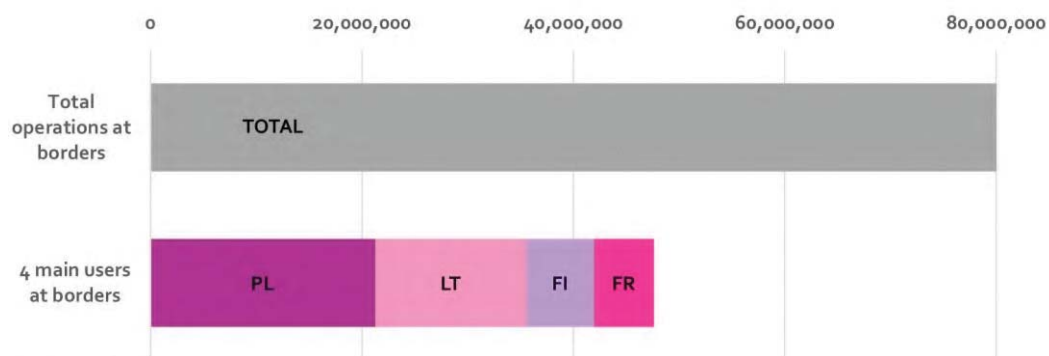
During the reporting period, over 84 million checks⁴⁸ at the external borders were carried out, the vast majority being first-line checks (the ‘visa verifications border’ operation). As shown in Graph 4, four Member States – Poland, Lithuania, Finland and France – accounted for 57% of all checks reported. As with visa application operations, the majority of border checks were carried out during the summer period. The peak was registered in August 2019 with almost 4.4 million first-line checks.

⁴⁶ As per Articles 21 and 22 of the VIS Regulation.

⁴⁷ As per Articles 19 and 20 of the VIS Regulation.

⁴⁸ As per the data collected, these were ‘visa verifications border’ (first-line checks) and ‘identifications border’ (second line checks).

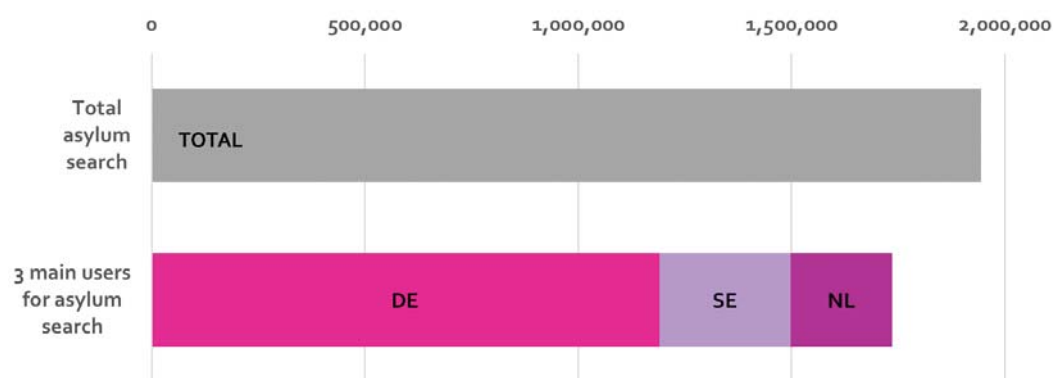
Graph 4: Four main users at borders as per the data during the reporting period



Source: eu-LISA.

The reporting of usage of the VIS for asylum purposes was very fragmented. Five Member States – Estonia, Greece, Slovenia, Slovakia and Spain – did not provide any data on the three asylum indicators used in this report. A total of 89% of the searches for asylum were performed by three Member States (see Graph 5).

Graph 5: Three main users for asylum searches during the reporting period



Source: eu-LISA.

6.2 Reported usage of Article 4(2) of the VIS Decision

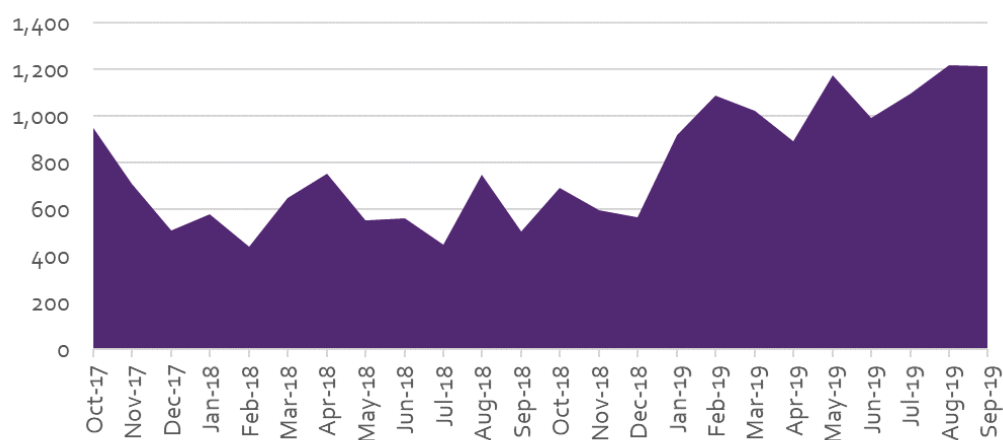
Pursuant to the VIS Decision, Member States' designated authorities and Europol have been able to access the VIS for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences since 1 September 2013. During the reporting period, only some Member States accessed the VIS for these purposes. Austria, Belgium, Estonia, France, Greece, Hungary, Iceland, Italy, Liechtenstein, Lithuania, Portugal, Norway and Sweden⁴⁹ did not report any activity in this respect. No activity was reported by Europol during the period either because, as described above, the VIS central system was made ready to connect Europol as a user by the end of the reporting period in autumn 2019.

⁴⁹ The Swedish Police started using the VIS in Q3 2019 with a limited number of searches. This type of usage is expected to increase in the future.

The collection of Member State data on usage of the VIS pursuant to the VIS Decision was very time-consuming and the data received was extremely fragmented. Thirteen Member States (Czechia⁵⁰, Denmark⁵¹, Finland⁵², Germany, Latvia, Luxembourg, Malta, Netherlands, Poland⁵³, Slovakia, Slovenia, Spain, and Switzerland) reported that they had used the VIS for law enforcement purposes during the reporting period. The level of usage varied considerably between those Member States.

Almost 19 000 searches were carried out in accordance with the VIS Decision by law enforcement authorities in eleven Member States in the reporting period. Over 34% of all searches were carried out by Germany, followed by Slovakia with 28% and Switzerland with 17%. As shown in Graph 6, usage was not regular during the reporting period. At the beginning of 2018, states using the VIS doubled compared to end 2017. Luxembourg, Slovenia and Slovakia started using the VIS pursuant to the VIS Decision in February 2018, Latvia in March, and Czechia in April.

Graph 6: VIS law enforcement searches reported



Source: eu-LISA

On average, there were 591 law enforcement searches per month in 2018; these increased to 1 069 on average per month in 2019⁵⁴.

In accordance with Article 4(2) of the VIS Decision, in an exceptional case of urgency, the central access point(s) may receive written, electronic or oral requests. In such cases, the central access point(s) are to process the request immediately and only verify *ex post* whether or not all the conditions of Article 5 are fulfilled, including whether or not an exceptional case of urgency existed. The *ex post* verification is to take place without undue delay after the request has been processed.

The data shows that 391 urgent cases pursuant to Article 4(2) were registered during the reporting period, 79% by Spain and 13% by Germany. Following *ex post* verification, 155 cases were deemed not urgent.

A breakdown of this data is available in Annex 2.

⁵⁰ Only the total searches were provided, as no tool has been yet implemented to analyse data from Article 4(2).

⁵¹ As activity for the whole period, one urgent case was reported. The Danish Security and Intelligence Service has not been able to provide the number of cases.

⁵² During the whole period, one urgent case and one case not considered urgent following *ex post* verification were reported.

⁵³ During the whole period, four urgent cases were reported.

⁵⁴ Until September 2019, i.e. for the last 9 months of the reporting period.

Conclusions

Throughout the reporting period, the availability of the VIS central system was very high and it consistently performed well, proving to be robust and reliable. Performance was very good in terms of the average processing time reported: in 2019 it was less than 0.8 seconds on average for alphanumeric searches (SLA is 30 seconds) and less than 2 seconds on average for fingerprint verification (SLA is 3 seconds). The VIS central system met the expectations of Member States and effectively supported the increased business demand.

Based on the data provided by the Member States, in the first 9 months of 2019, the VIS central system processed over 1.5 million visa applications on average per month and over 3.5 million first-line checks. Over the past 3 years, usage has been quite stable; however, peaks are visible in the summer months in line with the fact that most visa applications are for tourism purposes.

In terms of its evolutions, the VIS central system has been hugely affected by the development of the EES. This situation will continue for the next couple of years until there is full interconnection between the two central systems. The Agency is ready to implement the new VIS legal framework, once agreed and finalised, in close cooperation with the Member States. This will allow the VIS to fully integrate the future interoperable IT architecture for the JHA area.

Annexes

1. Data reported by Member States on usage of the VIS pursuant to the VIS Regulation⁵⁵

	Registered Applications	Registered Applications with Fingerprints	Registered Applications without Fingerprints	Registered Applications without legal Fingerprints –	Registered Applications without factual Fingerprints –	Issued Visas	Refused Visas	Refused Visas per Applicant	Refused Visas – fingerprints could not be provided factually	Visa Verifications Border	Visa Verifications within Territory	Searches Asylum	Identifications Asylum	Successful Identifications Asylum
Oct-17	1,098,557	1,021,554	76,942	64,892	7,542	969,057	112,953	13,553	8,288	3,524,096	18,407	51,071	119,487	1,296
Nov-17	1,129,749	1,039,670	90,030	77,811	7,199	992,694	156,248	13,145	9,078	3,243,671	21,837	49,938	118,651	7359
Dec-17	935,668	845,751	89,861	78,731	7,489	834,770	99,137	11,709	9,202	3,446,732	19,434	75,708	90,292	34,081
Total 2017	3,163,974	2,906,975	256,833	221,434	23,030	2,796,521	328,237	38,407	26,568	10,214,489	59,658	245,355	328,490	13,306
Jan-18	981,096	906,581	74,480	64,939	5,690	851,391	111,932	11,144	8,852	3,069,190	21,822	52,940	113,736	5,995
Feb-18	987,939	911,958	75,451	64,301	7,426	878,696	104,550	10,790	8,571	2,575,347	19,334	48,702	118,472	31,642
Mar-18	1,346,929	1,244,144	105,667	89,640	10,741	1,192,010	122,308	12,574	9,646	3,222,349	20,659	80,488	125,259	33,868
Apr-18	1,521,722	1,385,868	135,837	117,998	12,396	1,389,344	115,873	11,818	9,140	3,288,643	19,983	56,904	116,873	30,867
May-18	1,817,812	1,620,147	197,645	176,055	15,488	1,660,094	131,385	12,854	11,409	3,406,788	27,388	57,596	119,943	4,631
Jun-18	1,769,449	1,566,030	203,309	180,752	14,588	1,591,771	133,253	12,866	12,481	3,801,301	83,001	60,298	114,670	29,506
Jul-18	1,789,166	1,589,649	199,428	178,477	13,946	1,633,195	144,711	14,066	14,694	4,185,727	21,372	66,009	114,123	33,541
Aug-18	1,491,047	1,370,988	119,971	103,101	10,847	1,357,420	128,759	15,579	12,801	3,954,178	20,056	62,933	110,811	4,934
Sep-18	1,219,567	1,144,516	75,003	62,018	7,779	1,092,346	118,680	13,822	9,705	3,510,448	20,650	65,946	118,338	31,590
Oct-18	1,207,879	1,125,513	82,156	69,311	8,343	1,044,912	146,807	13,735	10,147	3,295,012	31,114	71,729	128,725	5,146
Nov-18	1,131,137	1,042,603	88,422	76,037	8,250	980,560	133,637	12,113	10,239	3,012,425	36,724	64,841	122,829	4,759
Dec-18	919,567	833,772	85,694	75,266	7,346	801,537	115,578	12,283	10,482	3,166,785	40,846	53,377	96,162	3,762
Total 2018	16,182,850	14,738,749	1,443,033	1,257,895	122,780	14,473,186	1,507,473	153,644	128,167	40,488,193	362,949	980,907	1,399,941	58,675
Jan-19	1,005,407	933,365	71,980	62,834	6,021	871,832	123,089	11,694	9,561	2,850,856	53,500	64,351	151,615	6,372
Feb-19	1,007,516	934,383	73,019	63,561	6,445	869,585	120,982	11,479	8,252	2,419,749	45,249	59,072	148,225	4,332
Mar-19	1,399,280	1,292,441	106,732	92,799	8,801	1,240,480	135,798	14,544	10,021	3,164,167	48,124	69,025	159,629	4,951
Apr-19	1,637,253	1,488,844	148,098	132,770	10,485	1,480,371	131,758	12,977	9,900	3,256,607	56,693	72,983	160,949	5,109
May-19	1,894,902	1,693,697	200,875	180,683	12,558	1,719,841	147,016	15,797	11,821	3,812,876	57,218	89,622	163,644	4,603
Jun-19	1,743,092	1,543,467	199,299	179,201	11,206	1,569,845	134,009	14,814	11,480	3,934,619	58,402	71,661	155,162	3,676
Jul-19	1,978,241	1,765,001	212,950	194,239	12,421	1,799,682	165,549	16,917	15,317	4,369,780	58,801	82,709	192,054	5,176
Aug-19	1,544,661	1,426,470	117,994	103,174	9,686	1,397,436	134,512	16,225	11,665	4,388,215	60,443	78,718	207,046	4,874
Sep-19	1,394,801	1,309,824	84,821	72,139	7,777	1,237,598	137,736	14,528	9,367	3,675,695	54,036	84,102	225,773	5,160
Total 2019	13,605,163	12,387,492	1,215,768	1,081,400	85,380	12,186,600	1,220,449	128,975	97,304	31,872,564	492,486	715,805	1,564,097	44,253
Grand total	32,951,987	30,033,216	2,915,634	2,560,799	231,190	29,446,397	3,066,289	321,026	252,119	82,575,246	915,043	1,523,509	3,292,468	116,234

⁵⁵ Data for 'refused visas per applicant' was reported by 10 Member States; whereas data for 'successful identifications asylum' was provided by 9 countries. Among them, Netherlands provided only the total without a breakdown per month.

2. Reported usage of Article 4(2) of the VIS Decision

	Use of Article 4(2)		Number of all searches
	Number of urgent cases	Number of 4(2) where ex-post no urgency	
Oct-17	3	0	948
Nov-17	5	0	709
Dec-17	0	0	508
Total 2017	8	0	2,165
Jan-18	2	0	578
Feb-18	3	5	439
Mar-18	6	4	650
Apr-18	4	3	755
May-18	1	5	554
Jun-18	0	4	562
Jul-18	8	11	448
Aug-18	2	7	749
Sep-18	4	13	505
Oct-18	44	29	693
Nov-18	34	4	597
Dec-18	79	1	568
Total 2018	187	86	7,098
Jan-19	73	3	919
Feb-19	95	4	1,090
Mar-19	4	21	1,022
Apr-19	3	13	893
May-19	1	5	1,174
Jun-19	8	2	994
Jul-19	4	10	1,096
Aug-19	4	9	1,219
Sep-19	4	2	1,216
Total 2019	196	69	9,623
Grand total	391	155	18,886

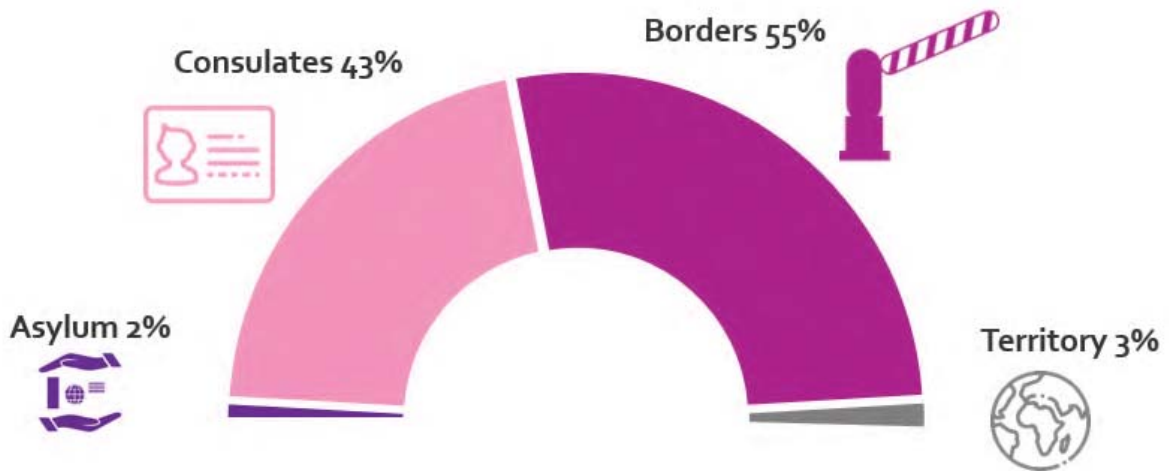
ISBN: 978-92-95217-65-2
ISSN: 2467-3099
doi: 10.2857/66661

VIS is at the core of the Schengen Area, connecting Member State consulates in non-EU countries and all external border crossing points. It supports Member States' consular authorities in the management of applications for short-stay visas to visit, or to transit through, the Schengen Area. Thanks to its Biometric Matching System (BMS) - the subsystem responsible for biometric operations - VIS allows Member State border authorities to perform identification and verification of third country nationals who travel to the EU.

The system first started operations in 2011 and, from February 2016, is deployed worldwide. eu-LISA took charge of the day-to-day management and further development of the central system on the 1st of December 2012. Operational management entails the application of management services, supervision, and the implementation of corrective, adaptive and evolutionary maintenance.

The report provides an overview of the activities carried out on the VIS central system from October 2017 to September 2019, and its usage based on data provided by the Member States. In September 2019 VIS was in use in 26 countries: 22 EU Member States and 4 Associated Schengen Countries (Iceland, Liechtenstein, Norway and Switzerland).

Graph 1: VIS usage per user group during the reporting period 2017-2019



Source: eu-LISA

ABOUT eu-LISA

eu-LISA is the European Union Agency which ensures the 24/7 operational management of the European Union's large-scale IT systems -as well as their respective communication infrastructure- in the area of freedom, security and justice. Apart from the systems currently under management (*Eurodac*, *SIS* and *VIS*), the Agency is also in the process of developing three new systems (*EES*, *ETIAS* and *ECRIS-TCN*), along with their interoperability components. For further information, please visit our website: www.eulisa.europa.eu



OPERATIONAL MANAGEMENT

- During the reporting period, VIS storage capacity increased from 60 million to 100 million records.
- The first phase of the BMS virtualization project was implemented.



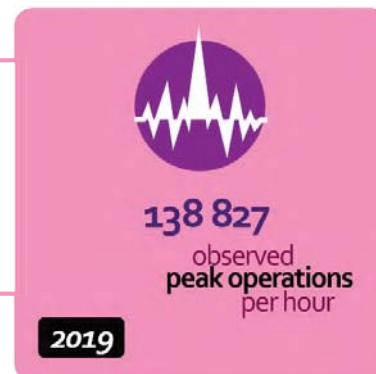
USAGE TRENDS

- The number of fingerprints stored rose from 41 million sets in autumn 2017 to 69 million two years later.
- In 2019, 25 million alphanumeric searches and 7 million biometric searches



SYSTEM OPERATIONS

- Operations per hour observed (peak/hour) were 123,393 in 2018 and 138,827 in 2019.
- The busiest months in terms of operations were July both in 2018 and 2019.



AVERAGE PROCESSING TIME IN 2019

- Less than 0.8 seconds on average for alphanumeric searches (SLA 30 seconds).
- Less than 2 seconds on average for fingerprint verification (SLA 3 seconds).
- For create/update/delete operations- 2.24 seconds (SLA 30 minutes).

