Technical reports on the functioning of VIS

as per Article 50(3) of the VIS Regulation and Article 17(3) of the VIS Decision

May 2018

This report has been produced pursuant to Article 50(3) of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 as well as to Article 17(3) of Council Decision 2008/633/JHA of 23 June 2008 with the purpose of providing information on the technical function of VIS, including the security thereof, as well as the need and use made by Member States of Article 4(2) of the of Council Decision 2008/633/JHA.

This report is public. Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.
eulisa.europa.eu

Table of Contents

Executive summary

The Visa Information System (VIS) serves as the technology solution facilitating the visa-acquiring procedure and supporting Member States' authorities to check rapidly and effectively the necessary information about third-country nationals who need a visa to travel to the EU, as well as make decisions on visa applications. Since 1 December 2012, the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) has been the sole authority in charge of the operational management of VIS, including monitoring of the system, application of management services, implementation of corrective and evolutionary maintenance, legal reporting obligations and training of information technology operators.

Several business-critical projects were implemented during the reporting period considered, for example:

- In January 2016, VIS Mail 2 Consultation Mechanism entered into operation and consequently the Schengen Consultation Network (VISION) was discontinued.
- At the end of February 2016, VIS was deployed in the last region and the worldwide rollout was therefore completed.
- In May 2017, following 2 years of intensive efforts, heavy testing and a data migration procedure, the VISA Code Plus project was implemented as part of the VIS 3.0 release.
- In September 2017, the complex migration from the Secure Trans European Services for Telematics between Administrations (s-TESTA) to the new generation (TESTA-ng) was completed.

The overall technical performance of VIS during the reporting period was very satisfactory, and no significant performance issues were registered. The Biometric Matching System's (BMS's) capacity and performance were also adequate for the use made by Member States. Capacity increases were carried out to align the system with the business requests coming in particular from the consular posts and the borders. By the end of the reporting period on 30 September 2017, the VIS database stored over 49 million visa applications and almost 42 million fingerprint sets.

Based on the data provided by the Member States, the significant increase in the usage of VIS is clearly visible, in particular usage at consular posts and at the borders. The peak for the consular usage was reached in May 2017, with almost 2 million visa applications registered, whereas at the borders the peak was registered in July 2017, with over 4.6 million border checks (first-line checks) reported.

Monitoring activities showed that the peak usage was up to 40,000 operations/hour at the end of 2015, and it increased to 139,000 operations/hour by July 2017.

All in all, the overall VIS operations performed from the entry into operation until the end of 2015 were almost 287 million. On the other hand, in 2017 alone the overall VIS operations were almost 269 million.

Yearly operations and created visa applications
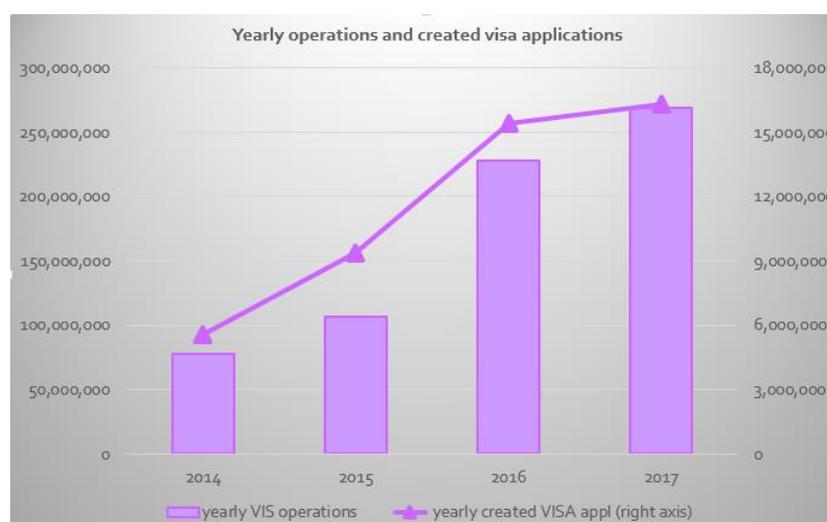
In the coming years, VIS will significantly evolve because of the recently adopted Entry/Exit Regulation, the interoperability proposals currently under negotiation and the expected revision of the VIS legal instruments.

Report pursuant to Article 50(3) of the VIS Regulation

The Visa Information System is an important element of the EU Common Visa Policy, an essential part of the Schengen *acquis*. The system started operations in October 2011, and on 1 December 2012 eu-LISA took over its operational management from the European Commission, in line with the VIS legal framework[1].

Since end of 2011, VIS has served as the technology solution facilitating the visa-acquiring procedure and helping Member States'[2] authorities to check rapidly and effectively the necessary information about third-country nationals who need a visa to travel to the EU, as well as make decisions on visa applications. In particular, VIS aims to improve the implementation of the Common Visa Policy, consular cooperation and consultation between central visa authorities by supporting the exchange of data between Member States.

The system has been implemented in order to facilitate the visa application procedure, to prevent 'visa shopping', to support the fight against fraud and to facilitate checks at external border-crossing points and within the territory of the Member States. In addition, VIS assists 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. Moreover, the system supports the processing of asylum applications and contributes to the prevention of threats to the internal security of Member States.

In terms of policy developments, during 2015 and 2016 the European Commission performed the first ever evaluation[3] of VIS as per Article 50(4) of the VIS Regulation, with the final report presented in autumn 2016. In addition, in the framework of a wider reform of the EU Common Visa Policy[4] initiated in March 2018, the European Commission planned to present the revision of the VIS legal framework in May 2018. The revision of the VIS legal framework foresees to include, among other changes, specific interoperability measures as well as to tackle some of the recommendations highlighted by the evaluation report.

Throughout the reporting period considered here, eu-LISA actively participated in a number of fora and workshops to support the European Commission in carrying out the overall evaluation of VIS as well as in providing input on technical aspects of possible changes and new requirements. In particular, the Agency contributed technical expertise to legal negotiations and supported the execution of impact assessments.

Being responsible for the operational management of Central VIS, the Agency has demonstrated its knowledge and expertise over the past few years. As from the beginning of 2017, the Agency is supporting the European Commission and the Member States in the context of the Schengen Evaluation Mechanism[5], in particular in the area of the Common Visa Policy (including VIS).

In performing the operational management of VIS, the Agency has been steered by the Management Board (MB) and the VIS Advisory Group (VIS AG)[6], which have played an important strategic role. In particular, as per

---

[1] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System, OJ L213, 15.6.2004; Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (hereinafter VIS Regulation), OJ L218, 13.8.2008.

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

[3] COM (2016) 655 final, Brussels, 14.10.2016.

[4] 'Adapting the common visa policy to new challenges', COM (2018) 251 final, Brussels, 14.3.2018.

[5] In line with Regulation (EU) No 1053/2013, the European Commission has invited eu-LISA to participate as an observer in the Common Visa Policy (including VIS) evaluations. In 2017, eu-LISA experts supported three evaluation missions (Denmark, Iceland and Spain), including on-site visits to consular posts.

[6] Both fora are composed of representatives of Member States and the European Commission.

Article 19(1) of the eu-LISA Regulation, the role of the VIS AG is to provide the MB with expertise related to VIS, especially in the context of the preparation of the programming documents and the annual activity report.

The VIS AG met regularly during the reporting period[7], and has been instrumental in overseeing the development and implementation of a number of business-critical projects such as the entry into operations of VIS Mail 2 and Visa Code Plus and the migration from Trans European Services for Telematics between Administrations (s-TESTA) to the new generation (TESTA-ng). Moreover, the AG actively contributed to the discussion on technical matters such as further evolution of the system, business requirements, enhancement of service level agreement definitions and data quality.

1. Legal basis and scope of the report

According to Article 50(3) of the VIS Regulation, every 2 years the Management Authority shall submit to the European Parliament, the Council and the European Commission a report on the technical functioning of VIS including the security thereof. Member States shall provide the Management Authority with the information necessary to draft the abovementioned report as per Article 50(6).

This report was drafted thanks to the Member States' contributions[8] as well as eu-LISA qualitative information on the technical functioning of Central VIS, on the communication infrastructure and on the security of the system.

This report is the third one of this type. The previous ones were submitted to the EU institutions in March 2014[9] and July 2016[10].

The reporting period covered in this report goes from 1 October 2015 to 30 September 2017.

2. VIS operational worldwide

VIS was progressively deployed, region by region, in the order defined by the European Commission on the basis of three criteria defined by Article 48(4) of the VIS Regulation:

- the risk of irregular immigration;
- the threats to the internal security of the Schengen states;
- the feasibility of collecting biometrics from all locations in the region.

The rollout was successfully completed during the reporting period according to the schedule agreed by the Permanent Representatives Committee (Coreper). By the end of February 2016, VIS connected all consular posts in non-EU countries and all external border-crossing points of the Member States.

During the period covered by this report, the last set of regions were connected:

- region 19[11] on 12 October 2015;
- region 20[12] on 2 November 2015;

---

[7] During the reporting period, the VIS AG was convened nine times: in October and November 2015; February, May, October and November 2016; and February, May and October 2017.
[8] For the template, see Annex VI. The last contribution was received on 23 April 2018.
[9] https://www.eulisa.europa.eu/Publications/Reports/eulisa_Report%20VIS%20en.pdf
[10] https://www.eulisa.europa.eu/Publications/Reports/VIS%20Reports%20on%20the%20technical%20functioning%202015.pdf
[11] Region 19 was composed of China, Japan, Mongolia, North Korea, South Korea and Taiwan.
[12] Region 20 was composed of Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan and Sri-Lanka.

- regions 21-23[13] on 20 November 2015;
- external border-crossing points region on 29 February 2016.

Following the consolidated practice, eu-LISA supported Member States during the deployments, in particular with web conferences, to assure coordination, constant communication and monitoring. All deployments went smoothly without major issues, and the system was able to cope well with the increased traffic generated by the additional regions connected.

3. Operational management of VIS

As per Article 1(2) of Council Decision 2004/512/EC establishing VIS, the system consists of the Central VIS (CS-VIS), a national interface (NI-VIS) in each Member State connected to VIS and the communication infrastructure. The national interface provides the connection to the relevant central national authority of the respective Member State. The complete end-to-end solution includes the national systems providing the interface to the end-users.

Each Member State is responsible for implementing, operating and managing its own national system, while the operational management of CS-VIS and certain aspects of the communication infrastructure are under eu-LISA's responsibility. The Central VIS includes the Biometric Matching System (BMS), an Automated Fingerprint Identification System (AFIS) subsystem responsible for biometric operations entering into play depending on the specific VIS operation requested.

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

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

Data contained in the CU and BCU are kept synchronised at all times, guaranteeing business continuity. The average time for a switchover is approximately 30 minutes.

eu-LISA is responsible for the operational management of the Central VIS, ensuring uninterrupted access to the system 24 hours a day, 7 days a week 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, external technical support has been guaranteed by two different consortiums. The VIS Maintenance in Working Order and Evolutionary Maintenance (MWO) Framework Contract signed in August 2012[14] expired in August 2016, so a procurement procedure was launched in September 2015. The restricted call for tender for the establishment of the new MWO framework contract for VIS was published on 1 September 2015[15] and evaluation of the offers was carried out in spring 2016 with the support of volunteer

---

[13] Region 21 was composed of Andorra, the Holy See, Monaco and San Marino; region 22 of Ireland and the UK; and region 23 of Schengen Member States (Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and Switzerland).
[14] It was with a consortium composed of Accenture NV/SA, Hewlett-Packard Belgium BVBA/SPRL and Morpho SA.
[15] More information on the procedure is available at: http://www.eulisa.europa.eu/Procurement/Pages/ClosedTenders.aspx

Member States. The new MWO contract was eventually signed on 26 May 2016 with the consortium to which it was awarded[16].

A totally new concept for the interaction and management of the MWO contractor was put in place. The contract laid down, in particular, stricter rules, improved and more detailed systematic reporting, enhanced cross-cutting and planning. This new framework was then used as the basis for all future MWO framework contracts for the other systems too.

The new MWO contract covers the operations as well as corrective, adaptive and evolutionary maintenance of the Central VIS, including the BMS system and all associated services. The initial duration of the new framework contract is 4 years, with the possibility of one extension for a maximum period of 2 more years.

3.1 VIS: technical functioning and upgrades

The overall technical performance of VIS during the reporting period was very satisfactory, and no significant performance issues were registered. The BMS's capacity and performance were also adequate for the use made by Member States. Processing times for both consular posts and border posts[17] were in line with the VIS service level agreement, i.e. the system supports the business within seconds.

At the beginning of the reporting period, the end of 2015, VIS processing capacity was up to a maximum of 300 000 messages/hour, while monitoring activities showed that the peak usage was up to 40 000 operations/hour. The peak usage increased steadily throughout the reporting period:

- up to 51 000 operations/hour registered in Q1 2016;
- up to 88 000 operations/hour by November-December 2016;
- up to 139 000 operations/hour at peak time by July 2017.

At the beginning of 2016, the worldwide rollout of VIS was achieved and the technical performance of the system was upgraded with the release in August 2016, which brought VIS's processing capacity up to 450 000 messages/hour.

In autumn 2015, at the beginning of the reporting period, the VIS database's storage capacity was 40 million records and there were slightly more than 17.5 million visa applications stored and 13.7 million fingerprint sets stored. As per the VIS upgrade project, in August 2016 the VIS database's capacity was enhanced to 60 million visa applications. By the end of the reporting period on 30 September 2017, the VIS database stored over 49 million visa applications and almost 42 million fingerprint sets.

Release VIS 2.2/BMS 2.1.1 was deployed in production[18] between 17 and 20 November 2015. This release included VIS Mail consultation changes, an insertion of an O-FTE warning mechanism, and corrective items and patches. The VIS-BMS logging correlation, aimed at improving the logging for end-to-end troubleshooting and monitoring purposes, was also deployed. However, on 11 May 2016, a technical release, VIS 2.2.2, was needed to fix the service correlation between data from VIS and BMS databases, initially deployed in November. The main objectives[19] were to improve the VIS-BMS troubleshooting and the monitoring functionality at CS level. The release was transparent for national systems.

---

[16] Bridge3, composed of Accenture NV/SA, Atos Belgium NV/SA and Morpho SAS.
[17] The measurement of the system performance, in particular for the border post activity, is based on two checks: first-line check (verification) and second-line check (identification).
[18] The deployment was carried out in conjunction with a switch over to the BCU on 9 November 2015 and a switch back to the CU on 30 November.
[19] The release contained the changes related to the additional logging information in VIS databases and applications, VIS-BMS end-to-end troubleshooting through increased transaction logging information and the possibility of correlating VIS and BMS transactions as well as the start and end timestamps for the communication with the BMS.

In May 2016, a webinar entitled 'VIS Search Functions'[20] dedicated to ELISE, the VIS alphanumeric search engine, also took place.

In Q2 2016, eu-LISA launched a VIS-BMS active-active architecture study. The main goal of the study was to assess how availability and reliability could be improved through the implementation of dynamic allocation of the incoming data load. Moreover, the study investigated better system performance and more flexibility on the Agency's side with maintenance activities[21], using up-to-date technologies. In the framework of the study, several workshops took place, and directions for solutions were presented involving either architectural or non-architectural changes.

VIS evolution phase 3 — consisting in a capacity increase of the VIS database to 60 million records and enhancing the processing capacity to 450 000 transactions/hour — was rolled out in production at the end of August 2016, together with the Q3 2016 corrective release[22]. Final system acceptance was completed by 18 November 2016.

As part of the Visa Code Plus project, VIS 3.0 entered into operation on 13 May 2017. See more in the dedicated section 3.3.2.

Following the finalisation of the relevant study, in autumn 2017 the VIS database increase project was launched. The VIS database capacity increase is planned in two steps: the first one to increase capacity to 85 million records (planned to be implemented from Q2 2017 until the end of 2018 and deployed in production in Q3 2018) and a second step to increase capacity to 100 million records (deployment in production planned for Q3 2019). The project also includes the upgrade of the capacity of the VIS search engine and of the processing power, as well as regular qualification test campaigns (functional/performance).

A technical release, VIS 3.1 and BMS 2.4, was deployed on 8 November 2017. It included no functional changes but only corrective items.

3.2   Biometric Matching System (BMS)

The main objectives on BMS during the reporting period were to increase its capacity and performance in order to sustain the load resulting from the complete worldwide rollout, by renewing the whole system, as well as to ensure proper corrective maintenance of the system. In autumn 2015, the BMS had a capacity storage of 24 million records.

In order to support the increased capacity of the BMS, a new backup and an archive solution were needed. The different project phases were successfully completed (building, installation, configuration and test campaign). The backup and the archive solution for BMS Production, PreProduction and Playground were successfully released on 20 November 2015.

The BMS upgrade provided for the upscale of the BMS 2.1 production environment from a maximum of 24 million to 60 million fingerprint template records[23] (150 % increase), as well as the upscale of the pre-production environment to 40 % of the transactional and database capacity of BMS 2.2 (this being a prerequisite for the BMS 2.2 qualification process). In terms of throughput capacity, the production environment was not changed; the same throughput was maintained on a larger database without affecting the performance.

The upscale concerned only the increase of the biometric database size and throughput on deploying additional storage capacity — additional hardware components and software licences — into the existing BMS

---

[20] It was well received by the Member States, with 29 participants and a satisfaction rate of 4.37 out of 5.
[21] To investigate options to reduce how long it took to deploy releases.
[22] The deployment was carried out in conjunction with a switch over to the BCU on 18 August and a switch back to the CU on 25 August.
[23] This would support the creation of visa applications with biometrics till Q1 2019, as per the available capacity projections.

infrastructure, so no changes in functional or technology requirements compared with those existing for BMS 2.1 were made. No involvement of the Member States was required.

The BMS 2.2 entered into operation on the production environment on 26 April 2016[24]. The deployment went smoothly without any major technical issues, and Final System Acceptance was successfully completed on 28 August 2016. Meantime, the upscale of the pre-production environment was also completed on 27 May 2016.

Following a request by the Advisory Group, eu-LISA organised several training activities to support Member States with the new BMS. Technical workshops dedicated to 'BMS Accuracy' were organised in November 2015 and in March 2016. Moreover on 24 May 2016, a workshop on 'Biometric Performance, Quality Management and Evolutions for BMS' took place in Paris[25].

In the context of the reinforcement of the VIS-BMS testing capabilities, eu-LISA started a project in spring 2017 focusing on full alignment at the infrastructure and application levels to improve the internal product qualification at eu-LISA. The scope of the project encompasses the upscale of BMS pre-production to 100 % of the production size as well as the creation of an artificial test database of 600 000 fingerprint records for the qualification of future upgrades.

eu-LISA conducted an impact analysis and a wide-market analysis in order to investigate possible options for replacing the fingerprint acquisition toolkit, the end-to-end user quality software used by Member States. The aim was to find the best available biometric quality tool that could be offered to Member States in the long run[26].

The VIS User Software Kit tool currently in use was initially offered to Member States by the European Commission in 2008 as a local solution to be incorporated in VIS in order to support the proper data capture process. The tool provides immediate feedback on low-quality or incorrect data and avoids the transfer of data that would be rejected by the BMS. It has several benefits for promoting the standardisation of the fingerprint acquisition toolkit, among them optimising the implementation lead time; reduction of costs for implementation, licensing and support; and reduced resources required for end-to-end biometric quality computation, enabling the best possible biometric performance[27].

3.3   Projects

3.3.1   VIS Mail 2

Since the entry into operations of VIS, VIS Mail phase 1 Consultation Mechanism had been in operation in parallel with the Schengen Consultation Network (VISION). During the period covered by this report, preparations for the entry into operation of VIS Mail phase 2 and discontinuation of VISION were completed. VIS Mail phase 2 entered into operation on 20 January 2016, in line with the provisions agreed in the Visa/VISION Working Party meeting in May 2015, and subsequently endorsed by the SISVIS Committee — VIS Formation in July 2015[28].

In September 2015, a global test campaign (functional and non-functional) started, and it was successfully concluded on 14 December 2015. The VIS mail infrastructure operational management handover from the s-TESTA Security Operation Centre to eu-LISA was done as part of the TESTA-ng migration project and it was

---

[24] This followed a VIS-BMS switch over to the BCU on 18 April and a VIS-BMS switch back to the CU on 26 April.
[25] It drew 21 participants, and the satisfaction rate was 4.2 out of 5.
[26] The kit is used to ensure a consistent approach in the validation of biometric data quality before its insertion into the BMS.
[27] This would improve overall quality management across Member States and allow consistent data quality management, from acquisition to matching.
[28] In accordance with Article 46 of the VIS Regulation.

finalised on 10 October 2015. From that month onwards, the Agency has been responsible for the operational management of the VIS Mail infrastructure, and providing the VIS Mail business statistics.

A transitional period from 20 November 2015 was deemed necessary to ensure that, for those visa applications lodged before 20 November and therefore not present in VIS, notifications of visa issuance would still be sent relying on VISION. The transition period was completed on 20 January 2016, when VIS Mail 2 successfully entered into operation[29]. From that date, VIS Mail started managing all new consultation requests and notifications. After 2 months of semi-operational mode, in order to be able to cover the pending consultation replies, the old mechanism, VISION, was discontinued.

Following the entry into operation of VIS Mail 2, an informal group known as InfoVIS Task Force was created[30] in order to follow up on the different aspects of VIS Mail. In particular, the mandate of the task force is to investigate further improvements to the efficiency of various business procedures supported by the VIS Mail communication mechanism, to closely monitor its business usage and to analyse the business aspects of the future integration of the VIS Mail workflows into VIS.

3.3.2   Visa Code Plus

The Visa Code Plus project managed changes stemming from the Visa Code, the Member States or eu-LISA, in addition to changes related to the future integration of Croatia. In particular, the project ensured the full compliance of VIS with the legal basis and that the critical businesses supported by VIS Mail, such as the consultation, the ex post notification and other procedures, would be better managed. In addition to a number of modifications, the project also included a modern centralised management of the Member States' List of Authorities.

Heavy, extensive and intensive testing phases, both at central system level and at national level, were carried out throughout 2016 and at the beginning of 2017:

- Central Domain Simulator (CDSIM) tests;
- non-contractual tests (April-May 2016);
- pre-compliance tests (October-November 2016) with all Member States;
- formal compliance tests (January/April 2017), carried out in 3 Member States' waves;
- Provisional System Acceptance Test (PSAT), in which six volunteer Member States — Greece, Croatia, Poland, Sweden, Slovenia and Slovakia — tested and validated the new product;
- VIS Mail tests.

The involvement of Member States in the test phases was an important cornerstone in ensuring the systems' (CS and NS) stability once the release was rolled out.

The entry into operation, planned for 22 April 2017, was eventually moved to 13 May 2017, at the request of one Member State. After more than 2 years of intensive efforts, heavy testing and, for the first time, a data migration procedure, the deployment[31] went smoothly and VIS 3.0 successfully entered into operation with no deviation from the agreed plan. The Final System Acceptance period lasted for 4 months, until September 2017, without any blocking or major issue reported by the Member States.

The project has a considerable impact, as it required adaptation of all national systems, which had to be fully compliant with the new data model. This release was the most complex for VIS since its entry into operation. Because of the business-critical nature of the project, the possible high impact on the security of the Schengen

---

[29] In line with COM Decision C(2015) 7463.
[30] The VIS Advisory Group decided on 31 May 2016 to establish the task force.
[31] The deployment was carried out in conjunction with a switch over to the BCU on 13 May and a switch back to the CU on 16 May.

Area, there was no room for any mistake. During deployment, VIS was not available for any type of users: no border, no consular and no law enforcement access to VIS was possible.

Despite the complexity, the project was successfully delivered. Success factors were enhanced communication with all stakeholders involved, effective collaboration, end-to-end project management (monthly Project Management Forum meetings and regular reporting) and extensive testing campaigns including procedure and business testing.

In addition, a key aspect of the project was related to the data migration activities[32]. These activities were tested in the corresponding test environment; during the migration of the production data, no issues were encountered and the estimates were proven to be accurate.

Following the entry into operation of VIS 3.0, there was a need to update the VIS Operational Manual. The revised version was endorsed by the VIS Advisory Group in November 2016.

3.3.3   Integration of Croatia

At national level, as early as 2014 Croatia launched the public procurement tender for building the visa system in accordance with requirements and standards for C-VIS. The contract was signed at the beginning of 2015 and development started immediately after that. Several test campaigns were conducted at the central level and successfully completed: in May 2016, the informal compliance test; in November 2016, the pre-formal compliance test; in January 2017, the formal compliance test; and, in April 2017, the PSAT for the Visa Code Plus project.

Croatia's integration was, from a central perspective, part of the Visa Code Plus project, which ensured that the central system was properly configured to integrate Croatia as a new user. As mentioned above, Croatia was involved in the necessary tests carried out as part of the project, and proved its readiness at both the functional and performance levels for version 2.0 of the Interface Control Document (ICD).

In the framework of the VIS Newcomer Training Programme for Croatia, three study visits were carried out: in April 2015, a delegation from eu-LISA paid a first field visited to the Ministry of Foreign Affairs in Zagreb; in March 2016, a Croatian delegation visited the eu-LISA's operations site and data centre in Strasbourg; and, in September 2016, a second visit to Zagreb was organised for an eu-LISA delegation. In 2016, in total, 22 trainees from Croatia attended the VIS newcomer training.

3.3.4   Integration of Europol

From beginning of 2017, close cooperation on the technical side started with Europol[33] with the aim of establishing a connection with the VIS central system. It is to be mentioned that, since 2011, at central level the VIS application layer has been ready and fully supports Europol's functionality. eu-LISA provided Europol with up-to-date VIS documentation and also granted access to the VIS Central Domain simulator.

Europol for its part developed and tested their VIS application against the VIS simulator.

The cooperation will continue, among other tasks, with the creation of network connectivity and further tests throughout 2018 and 2019. The current plan is for the connection to be operational in Q1 2019. As is its practice for a new user, eu-LISA will organise the VIS Newcomer Training Programme for Europol, encompassing reciprocal visits and sharing of knowledge.

---

[32] Data migration and data transformation were attempted for the first time.
[33] As per Article 7 of the VIS Decision, Europol shall have access to VIS data within the framework of its tasks. However, at the time of writing this report, Europol was not yet connected to VIS.

3.4   National systems

Each Member State has its own national system that includes the interface used by the end-users allowing the connection to CS-VIS. Implementation, operation and maintenance of the national systems are solely the responsibility of Member States. In the process of collecting data for this report, Member States were invited to provide information on their NI-VIS in terms of technical functioning, updates and issues encountered, if any, during the reporting period. Very limited and fragmented information was provided by Member States in this respect.

In general, Member States praised the performance and functioning of CS-VIS, considering it satisfactory. The system has been running smoothly with an effective searching system, and its performance and behaviour have been as expected.

According to Article 28(2) of the VIS Regulation, each Member State shall designate a national authority that shall provide for access by the competent authorities referred to in Article 6(1) and (2) to the VIS Regulation and connect that national authority to the national interface. The list of national authorities pursuant to Article 28(2) of the VIS Regulation as reported by the Member States is available in Annex III.

Furthermore, each Member State shall designate the competent authorities[34], the duly authorised staff of which shall have access to enter, amend, delete or consult data in VIS as per Article 6 of the VIS Regulation. The number of end-users per authority as reported by Member States is available in Annex IV. By September 2017, the approximate total number of end-users using VIS pursuant to the VIS Regulation was more than 458 000[35].

3.4.1   Schengen candidate countries

Council Decision 2017/1908 of 12 October 2017[36] allows Romania and Bulgaria to have access to consult, in a read-only mode, the VIS data without the right to enter, amend or delete any data in VIS, at the latest by the entry into operation of the Entry/Exit System (EES)[37]. Bulgaria's and Romania's passive access to VIS[38] is a precondition for the application of the EES to those Member States.

A precondition for granting passive access to Bulgaria and Romania is that both national Visa Information Systems are compliant with protocol ICD 3.0 (Visa Code Plus). The national systems will be compliance tested and validated in VIS test environments prior to connecting in the C-VIS production environment.

Romania was involved in all the test activities related to the Visa Code Plus project and proved its compliance with ICD 3.0. In the framework of gaining the passive access, Romania will have to perform the same tests again once the central system is ready to allow the implementation.

Currently, the Bulgarian national system is compliant with an older version of the ICD, so developments of additional functionalities in accordance with ICD 3.0 are needed. According to eu-LISA's draft action plan, Bulgaria will have to pass the following tests: tests with the CD simulator; pre-compliance tests; and formal

---

[34] The list of the authorities, specifying for what purpose each authority may process data in VIS, is regularly published by the Commission. A consolidated list was published in OJ C187, 26.5.2016.

[35] The number is just an indication, as the collection of data from Member States was particularly fragmented. As in the report published in July 2016, no data were received from Germany. Therefore, to make the total calculation, Germany's input for the first report (March 2014) was used.

[36] 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.

[37] Regulation (EU) 2017/2226, OJ L 327, 9.12.2017.

[38] This is to help their national visa application procedures to prevent fraud and any abuse of Schengen visas by verifying their validity and authenticity against the data stored in VIS, to facilitate — with regard to third country nationals holding a Schengen visa — checks at border-crossing points at external borders and within the territory of the Member States, to facilitate the determination of the Member State responsible for applications for international protection, to facilitate the examination of such applications, and to increase the level of internal security in the territory of the Member States by facilitating the fight against serious crime and terrorism. The access for the consultation and use of VIS data should also assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, or stay in, the territory of the Member States concerned.

compliance tests. The positive results of the abovementioned tests will guarantee that the version used by the national system of Bulgaria is compatible with protocol ICD 3.0.

With a view to facilitating the future integration of Romania and Bulgaria, eu-LISA put in place a VIS Newcomer Training Programme for both countries. The first field visits to Bucharest and Sofia took place in September 2017.

During the reporting period, no major developments were recorded as far as Cyprus was concerned. Nevertheless, Cyprus's national VIS successfully carried out connectivity tests in the context of the migration from s-TESTA to TESTA-ng, between March and April 2017.

3.5   Monitoring and training activities

Central VIS monitoring is carried out at the operational centre in Strasbourg thanks to the eu-LISA Service Desk, operational 24 hours a day, 7 days a week. The monitoring system is continuously analysed and assessed for business impact. The business activity is represented by a status overview screen — VIS Business Dashboard — giving the current status of the traffic for each Member State connected to VIS.

The eu-LISA Service Desk is the entry point for users' reports of incidents as well as requests for information or technical advice and support. Any request or incident is registered in a central incident management tool[39] for follow-up. During the reporting period, 801 user requests related to VIS, including incidents and requests for information, were registered. Following IT best practice, eu-LISA has implemented IT Service Management (ITSM) processes to ensure quality of service and to cope better with incidents and service requests. This is a continuous exercise to ensure efficient and cost-effective management of VIS by continuously monitoring and developing operational processes.

The VIS-BMS central system was available to a great extent during the reporting period.

In 2015, the availability was 99.96 % of the time. The VIS-BMS central system was unavailable (only complete unavailability was considered) as a result of incidents for 3 hours and 32 minutes in the whole year[40]. The availability was calculated by the eu-LISA's Service Desk taking into account SM7, incident and s-TESTA reports.

In 2016, the system was available for 99.48 % of the time. From 2016, the methodology for calculating the availability was slightly modified compared with previous years, so that the unavailability[41] of VIS also included the outages due to maintenance. In 2017, the overall availability was 99.92 %, i.e. the VIS-BMS central system was not available for 6 hours and 57 minutes[42] in the whole year.

Once a year, the Agency carries out a customer satisfaction survey covering the performance of the Service Desk, incidents and problem management, operational communication and technical assistance, as well as support to national activities. In the last 3 years, the increasing participation of the VIS community was satisfactory: 61 % of VIS Member States participated in the survey in 2015, 73 % in 2016 and 77 % in 2017. The overall satisfaction rate[43] of the community also showed an upward trend from 80 % in 2015 to 94 % in 2017. As is standard practice, the results of the survey are analysed and discussed with the VIS Advisory Group. Following the analysis, changes are applied in the areas requiring improvements.

---

[39] Since 7 March 2016, the Agency's Service Desk has upgraded the incident management tool in use from Service Manager 7 (SM7) to SM9. Member States performed several test campaigns (connectivity tests started in December 2015 and functional tests in January 2016), and dedicated hands-on training sessions were organised as well. In addition, in October 2017, at the conclusion of the integration project, the VIS MWO contractor also started using SM9, with the aim of easing the exchange of information between the eu-LISA users and MWO users (similar integration projects for the other systems managed by the Agency will follow).
[40] The unavailability time due to maintenance was not taken into account.
[41] Unavailability time for incidents was 4 hours and 15 minutes.
[42] Including 2 hours and 57 minutes due to incidents.
[43] Considering the 'Very satisfied' and the 'Satisfied' replies.

During the reporting period, continuous efforts to increase the quality of the data stored in VIS have been made by eu-LISA together with the Member States. In particular, the Agency put in place a closer monitoring system to support Member States in enhancing the quality of data in the fields required by Article 9[44] of the VIS Regulation. Regular discussions and best practice exchanges are carried out in the Advisory Group meetings, and support is provided when needed. Given the criticality of the topic, training activities on VIS Data Quality for Member States' end-users were organised in November 2016 and in September 2017[45].

As per its mandate, the Agency provides training activities on VIS for national IT operators and technical VIS experts. In 2016, 27 % of the training initiatives organised by the Agency were dedicated to VIS and 12 % to horizontal topics[46] (common to the three systems). In 2017, the activities for VIS represented 17 % of the total training activities carried out by the Agency. The class 'Technical training on VIS — train the trainers' was organised once a year, in October 2015, March 2016 and September 2017. In 2017, the new training framework 'Development Training Programme for IT Operators (DTPITO)' was launched with a three-step programme going from Entry through Intermediate to Advanced Level. The first part[47], 'VIS: Operational training — Entry level', was delivered in October 2017. In addition to that, through regular analysis of Member States' training demands and needs, the Agency plans and implements ad hoc initiatives[48].

3.6   In the future

VIS and BMS upgrade programmes will continue, and planning is already advanced. A two-phase VIS database increase project is already in the pipeline: phase 1, an increase of the database to 85 million visa applications, followed by phase 2, an increase to 100 million. Parallel capacity increases are also planned for the BMS, to 85 million. These upgrades are required for the system to operate and reach its intended operational levels, to sustain the traffic as per the progressive worldwide rollout.

In addition, a study is being carried out for the fine-tuning of VIS throughput, aligning it with business needs. Several other projects are also already started or planned: among others, a reinforcement of the VIS-BMS testing infrastructure to be progressively carried out; enhancement of reporting and monitoring capabilities; development of a data warehouse; and implementation of changes requested by Member States such as search profiles or increased performance (managed through the change management process).

In terms of future developments, VIS was considered in the broader process of reflection on the interoperability of information systems, started in spring 2016 and driven by the European Commission. This process led to the interoperability proposals[49] to make EU IT systems in the area of security, border and migration management work together in a smarter and more efficient way.

The EES[50], scheduled to be operational as of 2020, is conceived to be fully interoperable with VIS. There will be interdependencies between the two systems, with elements of data exchange and synchronisation. The interoperability[51] between VIS and EES will promote the efficiency and rapidity of border checks. Ultimately, the planned connection between the EES and VIS central systems will reduce duplication of personal data in accordance with the 'privacy by design' approach. In particular, the EES will enhance the functioning of VIS by

---

[44] Article 9 fields are considered compulsory by the VIS legal basis; absence of information will affect the consultation process. All stakeholders were interested in ensuring that the consultation mechanism would not be hampered by missing data in the central VIS, and therefore a monitoring activity by eu-LISA to support Member States in this activity was agreed, in line with the Agency's mandate to provide statistics meant for monitoring and evaluating the system.

[45] Member States actively participated in the training activities: there were 33 participants in 2016 and 20 in the following year. Good satisfaction rates were registered: 4.3 out of 5 in 2016 and 4.5 out of in 2017.

[46] Horizontal training activities delivered in 2016 included Train the trainers — SIS II, VIS, Eurodac IT operators; Webinar on eu-LISA mandate; and Webinar on Change management at eu-LISA.

[47] The conclusion of the first VIS DTPITO cycle is expected in 2018.

[48] For example the ones on data quality and BMS accuracy already mentioned.

[49] COM(2017) 793 final and COM(2017) 794 final, Strasbourg, 12.12.2017.

[50] Regulation (EU) 2017/2226 of 30 November 2017, OJ L327, 9.12.2017.

[51] As per Article 8 of the EES Regulation.

providing more reliable information on third country nationals' compliance with the rules of authorised stay in the territory of Member States, and will help to establish the bona fide status of visa holders who have already visited the Schengen area.

4. Communication infrastructure

According to Article 1(2) of Council Decision 2004/512/EC[52] and parallel provision in Article 2 of the Annex of European Commission Decision[53] of 17 June 2008, one of the three elements comprising VIS shall be a communication infrastructure between the central system (CS-VIS) 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 CS-VIS. The abovementioned communication infrastructure is provided via a European private secure network named Trans European Services for Telematics between Administrations — new generation (TESTA-ng).

The scope of services covered by the TESTA-ng network includes:

- a dedicated centralised Security Operations Centre (SOC) responsible for ensuring the operational management by the provider and the quality of the network on a 24/7 basis;
- consultancy services;
- connectivity;
- network;
- security.

These services relate to the provision, set-up and operation of a dedicated centralised management, monitoring and support infrastructure. Additional services cover the provision of monitoring tools, reporting and SOC staffing.

According to Article 7 of the eu-LISA Regulation, tasks regarding the communication infrastructure (including operational management and security) are divided between eu-LISA and the European Commission. In order to ensure coherence between the exercising of their respective responsibilities, operational working arrangements were established between eu-LISA and the European Commission and are reflected in the Memorandum of Understanding (MoU) concluded in June 2014. As specified in Article 19 of the MoU, the Agency is responsible for the supervision, security and coordination of relations between the Member States and the network provider, and for the communication infrastructure for VIS.

On the other hand, the European Commission is responsible for all other tasks relating to the communication infrastructure, in particular tasks relating to the implementation of the budget, acquisition and renewal and contractual matters.

4.1   Technical functioning of the communication infrastructure

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 star topology with resilience. The central unit (CU in Strasbourg) and backup central unit (BCU in Sankt Johann im Pongau) contain the systems to which each national network connects. The central unit and backup central unit are interconnected by a dedicated point-

---

[52] Council Decision of 8 June 2004 establishing the Visa Information System, OJ L 213, 15.06.2004.
[53] 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, 23.07.2008.

to-point connection.

The VIS network[54] 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 three incidents with critical impact on the functioning of the overall VIS community and two incidents affecting the connectivity of more than one site, caused by issues with the underlying network infrastructure and by software malfunctioning. Each one of these incidents was analysed to identify root causes, and appropriate measures were implemented to prevent recurrence of the incident.

4.2   Communication infrastructure migration

During the reporting period, the preparation of the TESTA-ng network was completed and permission to migrate the VIS communication infrastructure to it was granted. The migration started in February 2017 and was completed in September 2017. As part of the migration, the capacity of the whole network was increased to be able to cover expected increase in VIS business traffic.

To facilitate this complex activity, particular attention has been paid to communication with stakeholders. Dedicated webinars for all stakeholders were regularly organised, and frequent individual sessions were arranged in line with the migration procedure. In addition, to facilitate this activity, a dedicated interest group was created, in a secure environment with controlled access, to share relevant documentation.

5. Security

As far as the VIS central system is concerned, eu-LISA ensures the operational effectiveness of the security controls and the continuous improvement of the security strategy in line with the requirements set by the VIS Regulation and relevant European Commission Decisions in terms of data protection and information security. Security is a core element of all activities undertaken at eu-LISA, because of the applicable stringent legal framework, but also as the Agency is growing into a centre of excellence in the provision of IT services, emphasising assurance of system and data security in all activities.

During the reporting period, the Agency's security function continued to maintain and develop security measures concerning both physical and system security, in order to facilitate the fulfilment of the Agency's mandate. As a core element of its Information Security Management Framework, the Agency operates and continuously evolves 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 throughout the reporting period to provide assurance that the appropriate security controls for the IT systems under eu-LISA management have been properly implemented and managed.

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, in accordance with the relevant security principles and standards set by the European Commission and good practices set by the ISO27001 standard. Security requirements are embedded

---

[54] 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 Commission Decision 2009/377/EC Annex. 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.

in all development projects, changes and maintenance activities. The Security Unit is part of the change advisory board and takes part in any VIS development project from the requirement phase.

During the reporting period, the VIS central system went through numerous important upgrades embedding new technologies and components (e.g. capacity increase, VIS Mail 2, Visa Code Plus). Because those projects were critical, revisions of the Security Risk Assessment, the Security Plan and the Business Continuity Plan of the Central VIS were necessary. After a thorough review process involving all relevant stakeholders, such as the Security Officer Network (SON), the European Commission and the VIS Advisory Group, the updated VIS Security Plan and VIS Business Continuity Plan were adopted by the Management Board in November 2016.

In September 2015, the European Data Protection Supervisor (EDPS) carried out an inspection of the Central VIS with a focus on operational management, internal communication infrastructure and security. The final inspection report issued a positive opinion on the eu-LISA processes in place. Nevertheless, the report provided a set of recommendations. The recommendations were assessed and, as per standard practice, they will be addressed in order to further enhance the level of trust in the management of the VIS central 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. It should be recalled that the central VIS system is an isolated, controlled and secure environment.

In 2016, the framework contract for the Maintenance in Working Order of the Central VIS was handed over to a new consortium. The eu-LISA Security Unit took an important role in this transition, establishing for the first time a contractor security framework for a multi-annual contract. This led to the establishment of a more robust security control framework in relation to development and maintenance activities carried out by external service providers[55].

Throughout 2017, eu-LISA and eight Member States[56] planned, prepared and executed the first ever VIS business continuity exercise. The end-to-end business continuity exercise aimed to test the security, the business continuity and the disaster recovery capabilities of VIS. The intensive preparations for the VIS exercise started at the beginning of 2017 and were followed by the performance of the VIS exercise on 24-25 October 2017.

The exercise was carried out combining the VIS central system[57] and the VIS national systems (on a voluntary basis). The exercise consisted in rehearsing the existing processes and technical procedures, as well as in further improving the overall coordination and readiness of the VIS community in case of disaster. Both the preparation and execution phases saw the contribution of several eu-LISA teams[58], which facilitated smooth preparation and execution.

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. The SON meeting at the beginning of November 2017 was organised in conjunction with the Europol Security Committee in Tallinn, under the auspices of the Estonian Presidency of the Council of European Union.

Member States were invited to provide their own assessment of the security measures and an audit of their national implementation of the NI-VIS during the reporting period. Based on the very limited amount of

---

[55] This new contractor security framework was then used as the basis for all future MWO framework contracts.
[56] Estonia, Finland, Germany, Greece, the Netherlands, Portugal, Slovenia and Sweden.
[57] The exercise was performed on the pre-production environment in order to avoid disruptions to the ongoing operations.
[58] The Security Unit led the exercise. Other teams involved were Test, Network Infrastructure, System Infrastructure, the Data Protection Officer (DPO) and Applications Support.

information received, it appeared that eight Member States went through an audit during the reporting period whereas four Member States reported that no audit was carried out. In addition, two Member States reported having had a Schengen evaluation in the field of the Common Visa Policy (including VIS).

No security incidents or relevant security issues in connection with the Central VIS were reported by Member States.

6. Data protection

The protection of personal data related to individuals processed by 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 CS-VIS and data subjects' rights, as per the legal provision, are ensured by the Member States.

During the reporting period, the DPO was consulted on the implementation of a number of projects, for example the creation of new test databases[59], VIS Mail 2, Visa Code Plus and the BMS retention policy. In future, regular involvement is also expected because carrying out a Data Protection Impact Assessment will be mandatory for any new projects involving personal data[60].

The eu-LISA's DPO represents the Agency at the meetings[61] of the Supervision Coordination Group of VIS reporting on the current state of CS-VIS, future developments, data quality issues and security incidents at CS-VIS level or reported by Member States. The group, composed of the National Data Protection Authorities and the EDPS, monitors data protection legal compliance at both Member State and central system levels.

7. Usage of VIS

By the end of September 2017, at the end of the reporting period, VIS was storing almost 48 million registered visa applications and almost 41 million fingerprint sets. Taking into consideration the values at the beginning of the reporting period (October 2015), this represent an increase of 178 % for the visa applications and an increase of 206 % for the fingerprint sets.

The major increase in the usage of the system has to be put in perspective, keeping in mind that the system entered into operation in October 2011 and had a progressive rollout. The rollout was completed eventually in February 2016, with two of the biggest regions in terms of issuing visas — China and Russia — being rolled out in autumn 2015.

---

[59] New test databases using the data of the CS-VIS that may result in an improvement in the performance and data quality of the system.
[60] As per the new legal provisions on data protection: the General Data Protection Regulation 679/2016 and the proposed Regulation repealing Regulation 45/2001 (currently under negotiation).
[61] Usually two meetings per year.

Yearly operations and created visa applications

The overall VIS operations performed from entry into operation until the end of 2015 were almost 287 million. On the other hand, just in 2016 the overall VIS operations were almost 228 million and in 2017 they increased to almost 269 million.

The usage of the system substantially differs from Member State to Member State. While the extent of the consular network and historical ties determine — among others — the workload of the consular posts, both the number of third country nationals crossing the external borders as well as the length of the external borders have an important impact on the usage of the system for border control purposes. This is clearly visible in the graph below.

Registered visa applications and operations at borders
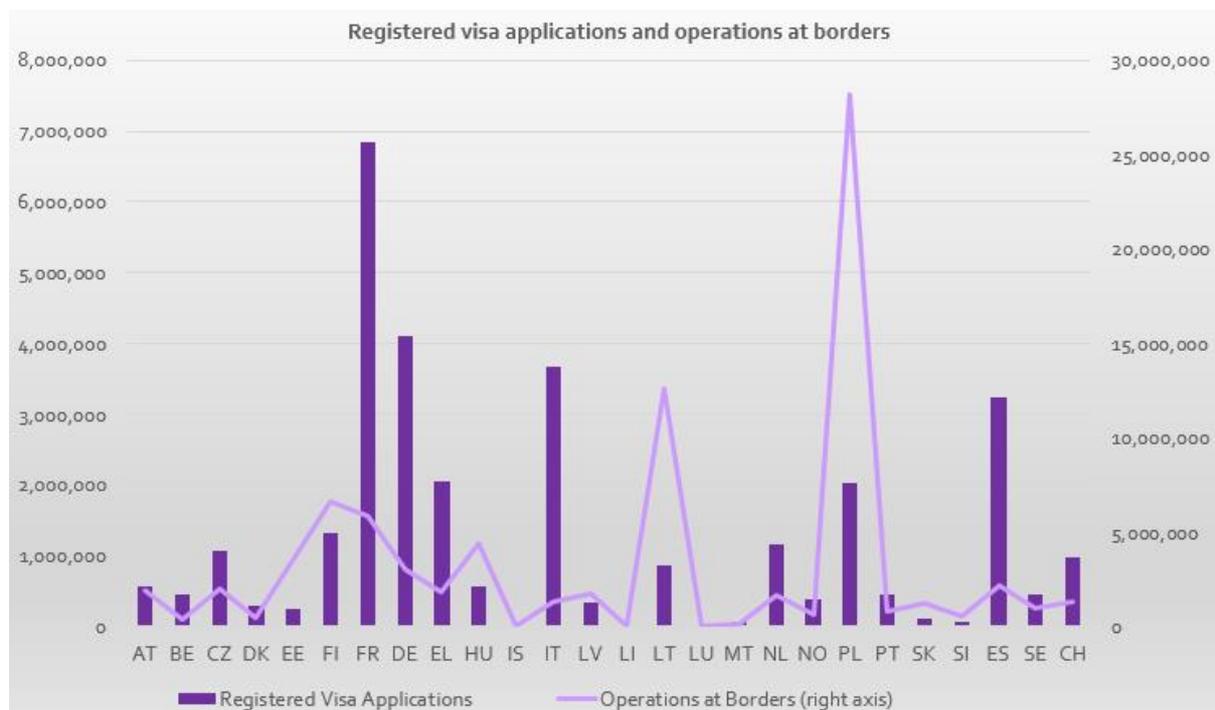
As per the data provided by Member States[62], in terms of registered visa applications from October 2015 till end of September 2017 the five biggest VIS users were France with 22 % of the applications registered, Germany with 13 %, Italy with 12 %, Spain with 10 % and Greece with 7 %.

On the other hand, looking at the figures collected in terms of activities performed at the borders — visa verifications border and identifications border — the biggest users were Poland with 34 % of the total operations considered, Lithuania with 15 % of the operations reported, followed by Finland with 8 %, France with 7 % and Hungary with 5 %.

Currently, the five most active VIS regions in terms of requesting visas are Russia, East Asia, North Africa, Eastern neighbouring countries and The Gulf region.

7.1   Activities at the consular posts

According to the data provided by the Member States, in the reporting period over 31 million registered visa applications were processed resulting in almost 29 million visas issued, and in over 2 million refused visas.

The number of visa applications processed in September 2017 represents an increase of 37 % compared with the volume reported for October 2015, at the beginning of the reporting period. The peak usage for consular activity is definitely in the summer season; May, June and July were the months with the highest activity.

In May 2017, VIS registered almost 2 million visa applications. This representing the peak for the reporting period, as well as the highest level ever registered for this operation.

Distribution of registered applications per Member State
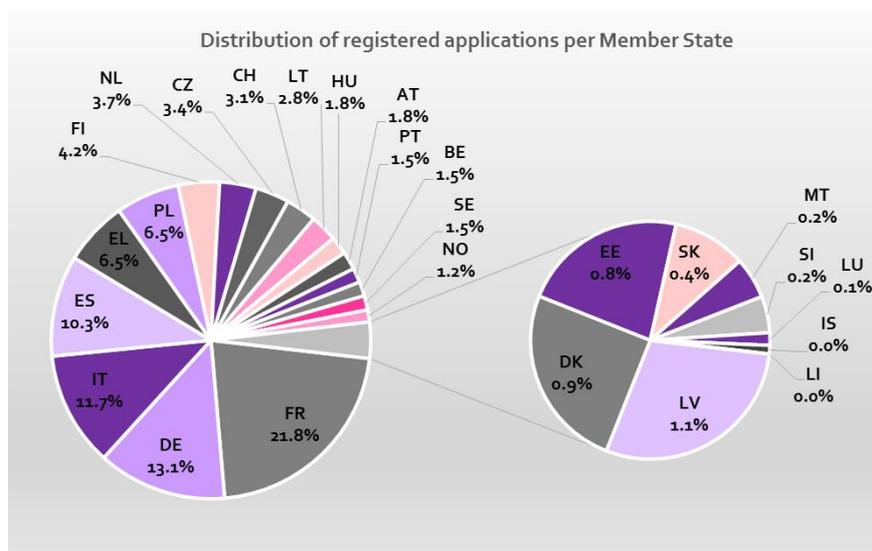
According to the data provided by Member States, the majority of the applications (89 %) included fingerprints. Out of the 11 % of applications without fingerprints, the majority (86 %) lacked them for legal reasons. A visa application can be submitted and stored in VIS without fingerprints for two different reasons according to the Article 13(7) of the Visa Code:

- the applicant is exempt from the fingerprinting requirement for legal reasons;
- it was physically impossible for the applicant to provide fingerprints.

[62] See table in Annex I, 'Data reported by Member States on the usage of VIS pursuant to the VIS Regulation'.

7.2   Activities at the border-crossing points

Over 83 million checks at the external borders of the EU were recorded by VIS during the reporting period, considering both first- and second-line checks (visa verification border operations and identification border operations), according to the data provided by the Member States.

Activities at the border-crossing points per month

As is clearly visible in the graph above, the majority of checks were first-line checks. The first-line checks reported by Member States during the reporting period were over 82 million, whereas the second-line checks reported were over 1 million.

Similarly to what was highlighted for the consular activities, for the border posts an increase in activity is also noticeable during the summer months compared with the rest of the year. Taking into account only the first-line checks (verification), the peaks were reached in July 2016, with over 4.3 million checks, and in July 2017, with over 4.6 million checks.

Comparing the average of 2.4 million monthly operations in 2016 (only 9 months were considered) and the average of almost 3.9 million operations in 2017, the major increase in usage is clearly visible. It is due certainly to the completed worldwide rollout, as well as to the growing number of visas stored in the database.

As already mentioned above, the usage of the system differs a lot among the Member States.

The graph below depicts the usage of the 26 Member States connected to VIS as far as first-line and second-line checks reported are concerned. The number of third country nationals crossing the external borders and moreover the length of the external borders have a significant impact on the usage of VIS at the external border-crossing points.

Activities at the border-crossing points per Member State

The standard first-line checks should be performed using the visa sticker number and, since 11 October 2014, the fingerprints of the visa holder in combination, as per the provisions of Article 18(2) of the VIS Regulation. Checks with fingerprints can be performed with one, two or four fingerprints.

In the VIS Advisory Group, eu-LISA regularly presents and analyses statistics in particular in relation to the usage of VIS at the external borders of the EU. The aim is to increase VIS usage[63] at the external borders, which will result in strengthening the internal security of the EU.

7.3   Activities for asylum purposes

The usage of VIS in relation to asylum activities was very fragmented during the reporting period. Eight Member States — the Czech Republic, Estonia, Greece, Iceland, Liechtenstein, Slovenia, Slovakia and Spain — did not provide any data on the three asylum indicators used in this report.

Searches and identifications for asylum purposes are performed in line with Articles 21 and 22 of the VIS Regulation. Data on Asylum Searches were provided by 18 Member States; data on Identifications For Asylum were provided by 11 Member States; and data on Hits/Successful Identifications For Asylum were provided by 6 Member States.

Taking into account the data reported, the usage of VIS for asylum purposes saw a decrease during the reporting period, as clearly shown in the graph below. The effects of the important migration crisis witnessed in 2015 were still visible at the end of 2015. In October 2015, more than 177,000 searches for asylum purposes and over 138,000 identifications for asylum purposes were registered, representing the peak for the reporting period.

By the end of the reporting period in September 2017, the searches for asylum purposes dropped by 63 % and the identifications for asylum purposes by 87 % compared with data available for October 2015.

---

[63] In supporting Member States in implementing their legal obligations.

Usage of VIS for asylum activites
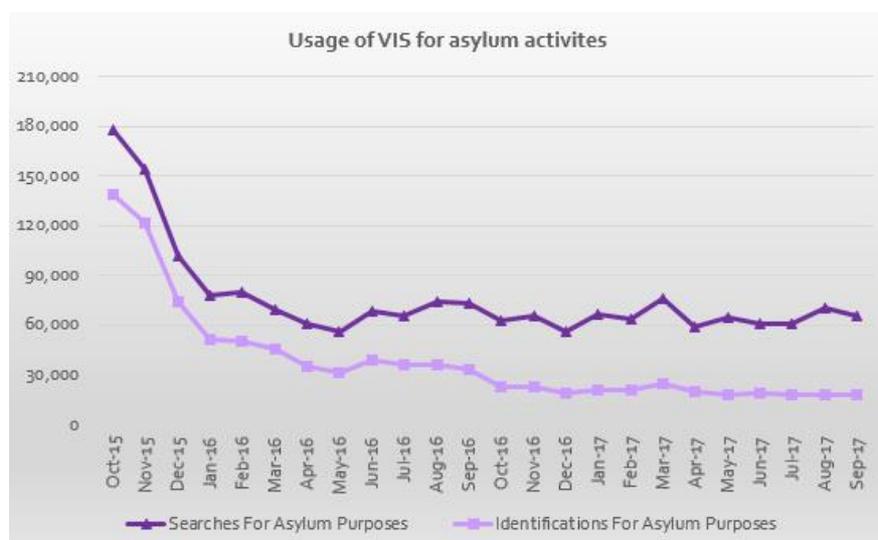
During the reporting period, Germany was the biggest user for the operations related to asylum purposes, accounting for 42 % of the searches, 43 % of the identifications and 35 % of the *Hits/Successful Identifications For Asylum.* Other big users were Sweden (27 % of the searches and 23 % of the identifications) and the Netherlands (14 % of the searches and 11 % of the identifications). Belgium, in contrast, reported having performed 5 % of the total searches for asylum purposes, 8 % of the total identifications and 44 % of the total *Hits/Successful Identifications For Asylum*.

The upward trend in *Hits/Successful Identifications For Asylum* is to be noted. Even though the operation was used by a very limited number of countries (only six countries reported data), it saw a significant increase of 67 % between October 2015 and September 2017.

7.4   Activities within the territory

During the reporting period, almost 2.5 million checks were performed using VIS in the territory of the Member States as per Articles 19 and 20 of the VIS Regulation. The majority of the checks, as per the graph below, were identifications, second-line checks.

Usage of VIS for activites within the territory
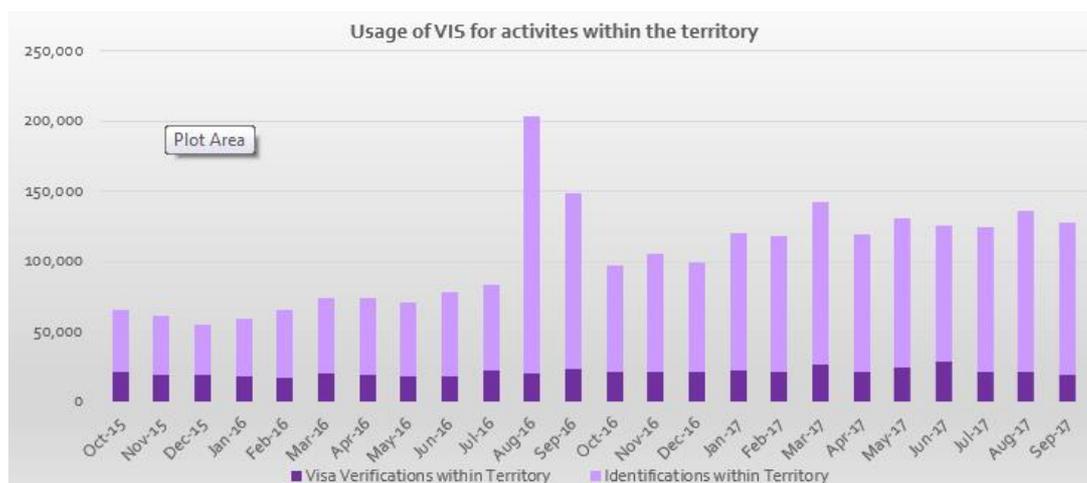
Austria, Iceland, Luxembourg, Malta, Norway, Spain and Sweden did not report any data for visa verification within the territory. Poland reported 69 % of the total visa verification operations, followed by Switzerland with 11 % and Germany with 8 %.

On the other hand, in terms of identifications within the territory, the biggest users were Austria, performing 36 % of the total operations, followed by Slovenia and France, with 14 % each, and Slovakia, with 11 % of the total operations reported.

eu-LISA   **PUBLIC**

Report pursuant to Article 17(3) of the VIS Decision

Council Decision 2008/633/JHA[64] (hereafter referred to as the VIS Decision), determining the conditions under which Member States' designated authorities and Europol may obtain access to VIS, produced effect as from 1 September 2013.

1. Legal basis and scope of the report

In accordance with Article 17(3) of the VIS Decision, every 2 years the Management Authority shall submit a report to the European Parliament, the Council and the European Commission on the technical functioning of VIS pursuant to the abovementioned Decision. The report shall include information in particular on the need and use made of Article 4(2).

This report is the second one of this type; the previous one was submitted to the EU institutions in July 2016[65].

This report covers the period from 1 October 2015 to 30 September 2017. Member States were requested to contribute to the reporting exercise with quantitative and qualitative information[66], as per Article 17(5) of the VIS Decision.

As per the VIS Decision, Europol should have access to VIS data within the framework of its tasks. However, Europol was not yet connected to VIS in the period covered by this report.

2. Operational management of VIS

The VIS central system has been supporting in a satisfactory way the Member States that granted access to designated authorities pursuant to the VIS Decision for the prevention, detection and investigation of terrorist offences and other serious criminal offences.

No issues have been reported by Member States in this respect.

At central level, there is no distinction between the operational management of VIS and its technical functioning pursuant to the VIS Regulation and pursuant to the VIS Decision. As a result, for information related to the technical functioning of VIS, see the sections above in this document.

3. Member States' reported usage

As per Article 3(3) of the VIS Decision, each Member State shall designate the central access point(s) through which the access pursuant to the Decision is done.

---

[64] OJ L218, 13.8.2008.
[65] https://www.eulisa.europa.eu/Publications/Reports/VIS%20Reports%20on%20the%20technical%20functioning%202015.pdf
[66] For the template, see Annex VII. The last contribution was received on 23 April 2018.

Annex V, 'Number of access points and end-users per Member State pursuant to VIS Decision', in this document shows the number of designated access points[67] and end-users reported by the Member States in the framework of this reporting exercise.

The numbers of access point(s) and end-users reported to eu-LISA vary considerably between the Member States[68]. In the framework of this exercise, the total number of access points reported by all Member States is 3 867. The estimated number of VIS end-users pursuant to the Decision is over 7 300.

Eight Member States reported having used VIS during the reporting period for the prevention, detection and investigation of terrorist offences and other serious criminal offences as allowed by the VIS Decision.

By the end of September 2017, almost 28 000 searches by law enforcement authorities in accordance with the VIS Decision were performed by Finland, France, Germany, Greece, Hungary, the Netherlands, Spain and Switzerland. Over 46 % of all the searches were executed by France, followed by Germany, with 19 %, and Switzerland, with 18 % of the total.

3.1 Usage of Article 4(2) of the VIS Decision

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) shall 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 shall take place without undue delay after the processing of the request. According to the data reported, during the reporting period 785 urgent searches pursuant to Article 4(2) were performed, 91 % by Spain and 9 % by Germany.

The ex post verification declared that all of the cases were urgent.

---

[67] Pursuant to Article 3(4) of the VIS Decision, the Declarations concerning Member States' designated authorities and central access point(s) for access to VIS data for consultation in accordance with Article 3(2) and 3(3) of VIS Decision shall be published in the Official Journal of the EU. The list was published in JO C236, 14.08.2013.
[68] The numbers of access point(s) and end-users is just an indication, as the collection of data from Member States in this respect was particularly fragmented.

Conclusion

Throughout the 24 months covered by the reports, the Central VIS was available to a great extent and it has been consistently performing well, proving to be a robust and reliable system. The Central VIS has met the expectations of Member States, effectively supporting the increased business demand following the finalisation of the rollout in the last sets of regions.

A number of business-critical projects of significant scale — VIS Mail 2, VISA Code Plus, migration from s-TESTA to TESTA-ng — were successfully delivered during the reporting period, to further support the Member States in the implementation of the Common Visa Policy and border management.

Based on the data provided by the Member States, the significant increase in the usage of VIS is clearly visible, in particular as far as the usage at the consular posts and at the borders is concerned. The peak for the consular usage was reached in May 2017, with almost 2 million visa applications registered, while at the borders the peak was registered in July 2017, with over 4.6 million border checks (first-line checks) reported.

According to the data available at central level, the overall VIS operations were almost 228 million in 2016 and increased to almost 269 million in 2017. The substantial increase in the usage is evident, considering that, from the entry into operation in 2011 until the end of 2015, the overall operations were almost 287 million.

Looking into the future, VIS will evolve as a result of various initiatives, in particular the interoperability legislative proposals under negotiation, the EES Regulation adopted at the end of 2017 and the forthcoming revision of the VIS legal basis.

Annexes

I.   Data reported by Member States on the usage of VIS pursuant to the VIS Regulation[69]

	Registered Applications	Registered Applications with Fingerprints	Registered Applications without Fingerprints	Registered Applications without Fingerprints – legal	Registered Applications without Fingerprints – factual	Issued Visas	Refused Visas	Refused Visas per Applicant	Refused Visas – fingerprints could not be provided factually	Visa Verifications Border	Visa Verifications within Territory	Identifications Border	Identifications within Territory	Searches Asylum	Identifications Asylum	Successful Identifications Asylum
Oct-15	880,496	794,238	85,311	71,367	5,495	813,199	69,320	1,389	817	2,357,617	21,210	67,308	44,261	177,573	138,496	2,930
Nov-15	989,739	879,852	109,049	76,110	24,021	892,725	78,401	1,536	1,006	2,364,093	18,915	46,578	42,639	153,586	121,725	2,562
Dec-15	893,805	797,526	95,189	80,110	8,426	812,790	69,043	1,722	704	2,784,925	19,220	36,971	35,391	101,463	74,100	2,473
Total 2015	2,764,040	2,471,616	289,549	227,587	37,942	2,518,714	216,764	4,647	2,527	7,506,635	59,345	150,857	122,291	432,622	334,321	7,965
Jan-16	746,887	681,566	64,406	51,962	5,746	670,865	60,351	1,358	892	2,509,849	17,877	32,200	41,242	77,772	51,123	2,535
Feb-16	907,080	824,669	80,717	61,443	9,988	791,110	71,321	1,287	925	2,264,046	16,955	28,547	48,808	79,689	50,192	2,445
Mar-16	1,163,141	1,057,506	103,668	82,136	8,405	1,063,951	81,066	1,527	1,053	2,775,219	19,720	33,970	54,297	69,435	45,689	2,706
Apr-16	1,395,024	1,252,782	139,995	118,188	10,108	1,292,852	81,465	1,445	864	2,938,055	19,225	31,554	54,386	60,731	35,228	2,244
May-16	1,644,877	1,440,168	202,047	174,560	12,812	1,521,089	91,466	1,875	860	3,246,047	17,694	32,905	53,080	55,712	31,057	1,927
Jun-16	1,833,045	1,576,402	253,542	222,627	14,633	1,710,343	94,224	2,194	995	3,411,667	17,739	32,569	60,855	68,434	38,848	2,402
Jul-16	1,650,096	1,434,100	213,169	188,462	13,084	1,542,851	86,646	1,953	850	4,303,296	22,314	39,653	61,253	65,761	35,950	2,209
Aug-16	1,600,744	1,422,614	175,656	153,057	10,127	1,482,849	100,353	2,734	828	4,164,954	20,064	37,109	183,798	74,315	36,605	2,648
Sep-16	1,244,530	1,139,280	103,455	86,858	8,100	1,142,372	85,478	2,138	739	3,731,467	22,959	43,598	125,586	73,427	32,982	2,839
Oct-16	1,075,200	976,998	96,332	79,083	8,542	968,380	88,805	2,132	842	3,615,803	20,977	40,731	75,963	62,901	23,203	2,266
Nov-16	1,141,496	1,027,032	112,819	94,538	8,999	1,022,885	99,363	2,224	779	3,316,290	21,433	44,659	84,148	65,752	23,268	2,092
Dec-16	1,019,562	898,210	119,840	101,604	9,236	915,350	92,681	2,445	842	3,534,537	21,227	48,303	77,749	55,852	18,792	1,754
Total 2016	15,421,682	13,731,327	1,665,646	1,414,518	119,780	14,124,897	1,033,219	23,312	10,469	39,811,230	238,184	445,798	921,165	809,781	422,937	28,067
Jan-17	901,899	814,324	86,502	72,641	6,305	801,953	85,981	2,009	754	3,198,599	22,441	48,421	97,361	66,133	21,237	2,252
Feb-17	996,696	900,230	94,886	78,464	7,512	888,238	93,860	2,012	704	2,818,607	20,815	47,786	97,171	63,637	21,077	1,757
Mar-17	1,486,265	1,334,355	149,669	128,091	10,739	1,354,041	111,575	2,441	1,168	3,656,431	26,397	54,958	115,804	76,101	24,499	2,138
Apr-17	1,523,371	1,341,238	179,866	159,425	11,208	1,408,123	95,692	1,789	879	3,843,177	21,186	49,621	97,710	59,143	19,630	1,698
May-17	1,919,476	1,644,008	272,276	243,637	15,056	1,771,286	121,251	3,043	1,072	4,192,605	24,368	54,947	106,884	64,371	17,849	1,786
Jun-17	1,862,693	1,585,346	274,224	249,259	14,147	1,731,834	105,453	2,691	1,046	4,204,977	29,053	49,335	96,470	60,412	19,279	4,092
Jul-17	1,701,980	1,453,008	246,301	221,358	12,843	1,567,745	113,484	2,591	1,135	4,623,636	20,663	51,537	103,849	61,315	18,070	4,058
Aug-17	1,571,257	1,382,306	186,454	168,256	10,831	1,431,770	119,143	3,126	1,087	4,429,733	20,774	53,706	115,413	69,929	18,181	4,455
Sep-17	1,210,347	1,100,464	108,174	95,840	7,321	1,091,056	102,667	2,683	1,725	3,991,830	19,371	47,359	108,365	65,647	17,862	4,881
Total 2017	13,173,984	11,555,279	1,598,352	1,416,971	95,962	12,046,046	949,106	22,385	9,570	34,959,595	205,068	457,670	939,027	586,688	177,684	27,117
Grand total	31,359,706	27,758,222	3,553,547	3,059,076	253,684	28,689,657	2,199,089	50,344	22,566	82,277,460	502,597	1,054,325	1,982,483	1,829,091	934,942	63,149

[69] Only 11 Member States reported data in relation to the 'Refused Visas per Applicant'.

II. **Data reported by Member States on the usage of VIS pursuant to 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-15	21	0	400
Nov-15	30	0	358
Dec-15	15	0	574
Total 2015	**66**	**0**	**1,332**
Jan-16	35	0	486
Feb-16	60	0	724
Mar-16	2	0	508
Apr-16	37	0	445
May-16	28	0	656
Jun-16	18	0	687
Jul-16	26	0	699
Aug-16	147	0	695
Sep-16	69	0	778
Oct-16	28	0	587
Nov-16	21	0	902
Dec-16	37	0	1,258
Total 2016	**508**	**0**	**8,425**
Jan-17	10	0	1,373
Feb-17	5	0	1,698
Mar-17	54	0	2,167
Apr-17	18	0	1,896
May-17	14	0	1,946
Jun-17	18	0	1,864
Jul-17	10	0	1,564
Aug-17	82	0	2,860
Sep-17	0	0	2,648
Total 2017	**211**	**0**	**18,016**
Grand total	**785**	**0**	**27,773**

III. List of national authorities per Member State pursuant to Article 28(2) of the VIS Regulation

Austria	Bundesministerium für Inneres
Belgium	FPS of Interior — DVZOE Brussels
Czech Republic	Directorate of Alien Police Service
Denmark	Ministry of Immigration and Integration
Estonia	Ministry of the Interior
Finland	Visa National Authority, Helsinki, Ministry for Foreign Affairs
France	Ministry of the Interior
Germany	Federal Office of Administration
Greece	Ministry of Foreign Affairs
Hungary	Office of Immigration and Nationality
Iceland	Directorate of Immigration
Italy	DGIT — Ufficio VI — Ministry of Foreign Affairs and International Cooperation
Latvia	OCMA Migration Division
Liechtenstein	Ausländer- und Passamt
Lithuania	Ministry of the Interior
Luxembourg	Ministry of Foreign and European Affairs — Bureau des Passeports/Visas/Légalisations
Malta	Central Visa Unit MFA — Central VISA Unit 11
Netherlands	Minister of Foreign Affairs
Norway	Directorate of Immigration
Poland	Central Technical Authority — Commander in Chief of the Police
Portugal	Ministry of Foreign Affairs, Consular Department
Slovakia	Ministry of Foreign Affairs
Slovenia	Ministry of Foreign Affairs, Consular Department
Spain	Directorate-General of Consular and Immigration Affairs — Ministry of Foreign Affairs and Cooperation
Sweden	Swedish Migration Agency in Norrköping
Switzerland	FDJP, SEM, Central National Authority

IV.   Number of end-users per Member State pursuant to the VIS Regulation

Austria	VISA CP — Ministry of European and International Affairs: 857 end-users VISA Border — Ministry of the Interior: 245 end-users VISA CNA — Ministry of the Interior: 10 end-users VISA Territory Check — Ministry of the Interior: 28 483 end-users Asylum Authority — Ministry of the Interior: 327 end-users National Supervisor: 6 end-users
Belgium	Asylum Authority: 181 end-users Border Post: 797 end-users Consular Post: 806 end-users Territory Check Authority: 181 end-users Visa National Authority: 413 end-users
Czech Republic	Directorate of Alien Police Service: 200 end-users Police of the Czech Republic — Section for residency issues: 700 end-users Ministry of Foreign Affairs: 550 end-users Department for Asylum and Migration Policy: 150 end-users
Denmark	Ministry of Immigration and Integration: 332 end-users Ministry of Foreign Affairs: 475 end-users Border control and other police: 25 021 end-users
Estonia	Ministry of the Interior: 6 end-users Ministry of Foreign Affairs: 98 end-users Police and Border Guard Board: 612 end-users
Finland	Ministry for Foreign Affairs: 550 end-users Finnish Border Guard: 1 880 end-users Customs: 1 070 end-users Police: 1 340 end-users Finnish Immigration Service: 180 end-users
France	Ministry of Foreign Affairs: consular posts Ministry of the Interior: border police authorities, immigration authorities, directorate of asylum Ministry of Finances: customs services The total number of end-users is about 80 000
Germany	Not provided
Greece	Ministry of Foreign Affairs: 561 end-users Aliens' Directorate of the Hellenic Police, Ministry of Citizens' Protection and Public Order: 3 513 end-users Hellenic Data Protection Authority: 3 end-users
Hungary	Office of Immigration and Nationality: 221 end-users Police: 3 415 end-users
Iceland	Directorate of Immigration: 4 end-users Icelandic Embassy in Moscow: 4 end-users Icelandic Embassy in Beijing: 6 end-users Police of the Greater Reykjavík Area: 3 end-users Police of Akureyri: 3 end-users District commissioner of Seyðisfjörður: 3 end-users Keflavík Area Border Police: 3 end-users
Italy	Ministry of Foreign Affairs and International Cooperation: 180 end-users Ministry of Home Affairs: 285 end-users
Latvia	Ministry for Foreign Affairs: 106 end-users State Border Guard: 611 end-users
Liechtenstein	Ausländer- und Passamt: 15 end-users Landespolizei: 20 end-users Datenschutzstelle: 1 end-user

Lithuania	Ministry of Foreign Affairs: 148 end-users State Border Protection Service, Ministry of the Interior: 1 950 end-users Department of Migration, Ministry of the Interior: 22 end-users
Luxembourg	Central Authority: 28 end-users Embassies: 105 end-users Frontiers: 37 end-users Asylum: 21 end-users Identification Territory: 1 end-user
Malta	Consular Posts: 119 end-users Immigration Police/Security: 81 end-users
Netherlands	Minister for Foreign Affairs: 200 end-users Royal Military Constabulary: 4 235 end-users Police: 150 end-users Immigration and Naturalisation Service 200 end-users Minister for Immigration and Asylum 200 end-users
Norway	Directorate of Immigration: 187 end-users Ministry of Foreign Affairs: 450 end-users National Police Directorate (Border Guard and Immigration): 1 263 end-users Immigration Appeals Board: 5 end-users
Poland	Government Protection Bureau (CPA): 2 end-users Police: 98 737 end-users Border Guard: 10 100 end-users Military Counterintelligence Service (CPA): 3 end-users Consulates and Ministry of Foreign Affairs: 519 end-users Office for Foreigners: 79 end-users
Portugal	450 end-users
Slovakia	Consular posts: 317 end-users Border post: 119 end-users Territory check: 176 end-users
Slovenia	Visa National Authority — Ministry of Foreign Affairs, Consular Department: 4 end-users Consular Post — Ministry of Foreign Affairs: 73 end-users Border Post — Ministry of the Interior, Police, State border and aliens sections: 2 108 end-users Territory Check Authority — Ministry of the Interior, General police directorate: 5 778 end-users
Spain	Directorate-General of Consular and Immigration Affairs — Ministry of Foreign Affairs and Cooperation: 690 end-users General Aliens and Borders Department — Ministry of the Interior: 1 589 end-users General Aliens and Borders Department — Ministry of the Interior: 4 573 end-users Directorate-General of Consular and Immigration Affairs — Ministry of Foreign Affairs and Cooperation: 9 end-users
Sweden	Migration Agency: 5 972 end-users Police: 10 400 end-users Embassies of Sweden: 6 64 end-users
Switzerland	Embassies: 1 171 end-users Border guards services: 2 092 end-users Federal Office for Migration: 763 end-users Migration offices of the cantons: 1 403 end-users

V.   Number of access points and end-users per Member State pursuant to the VIS Decision

Member State	Access point(s)	End-user(s)
Austria	1	16
Belgium	39	0
Czech Republic	250	1,700
Denmark	1	50
Estonia		
Finland	4	5,000
France	12	200
Germany	18	
Greece		
Hungary	1	41
Iceland	1	1
Italy		
Latvia	4	22
Liechtenstein	1	1
Lithuania	8	44
Luxembourg	11	41
Malta	1	22
Netherlands	1	11
Norway	2	
Poland	11	74
Portugal		
Slovakia		
Slovenia	3,500	54
Spain		42
Sweden		
Swizerland	1	24

VI. Template for Member States to submit the required information pursuant to the VIS Regulation

Report 3: Report on the technical functioning of the VIS and the security thereof pursuant to Article 50(3) of the Regulation (EC) No 767/2008	
Member State	\<Member State\>
Report generated at	\<timestamp\> [VIS into operation + 21 months, Frequency + 24 months]
Year:	\<Year(date)\>
Time period from	\<date\> to \<date\> [VIS into operation + 12 months + 9 months (separately), every 12 months thereafter]
Management of the System	
General Description of MS	
Central National Authority	\<Name\> [Article 28(2)]
End-Users[1]	\<Authority Name + Total Number of End-users in each\>…
Monitoring and Reporting	\<Description of Procedures\>
Description of audits, if any	\<Description of audits by the National Supervisor and findings\>
Technical Functioning of the System	
CS-VIS and BMS	\<Description of experiences and findings\>
NI-VIS	\<Description of technical functionality, updates, encountered issues, if any\>
VIS Mail	\<Description of functionalities, encountered issues, if any\>
Security of the System	
MS Security Measures	\<Description of audits, if any, any incidents or problems encountered\>
Workload and Performance[2]	
CS-VIS and BMS, NI-VIS	\<Description of the Performance\> + the following Statistics, if available

2 x 12 months data separately [Note exception with 1st report 12 + 9]	Registered Applications	Registered Applications with Fingerprints	Registered Applications without Fingerprints	Registered Applications without Fingerprints – legal	Registered Applications without Fingerprints – factual	Issued Visas	Refused Visas	Refused Visas per Applicant[3]	Refused Visas – fingerprints could not be provided factually	Visa Verifications Border	Visa Verifications within Territory	Identifications Border	Identifications within Territory	Searches Asylum	Identifications Asylum	Successful Identifications Asylum
January	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
February	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
March	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
April	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
May	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
June	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
July	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
August	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
September	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
October	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
November	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
December	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>	\<Total\>
Total	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**	**\<Total\>**

Reference for collection of data	C.C.R. 3.2.3	C.C.R. 3.2.3	C.C.R. 3.2.3	C.C.R. 3.2.3	C.C.R. 3.2.3	C.C.R. 3.2.2	C.C.R. 3.2.1	C.C.R. 3.2.14	C.C.R. 3.2.18	Retrieve VerificationBorder + AuthenticateByFingerprint VerificationBorder	Retrieve VerificationTerritory + AuthenticateByFingerprint VerificationTerritory	Search Identification Border + Retrieve Identification Border + SearchByFingerprint Identification Border	Search IdentificationTerritory + Retrieve IdentificationTerritory + SearchByFingerprint IdentificationTerritory	Search AsylumResponsibility/ AsylumExamination + Retrieve AsylumResponsibility/AsylumExamination + SearchByFingerprint AsylumResponsibility/AsylumExamination	SearchByFingerprint AsylumResponsibility/AsylumExamination	\<Positive Results of the Previous\>

VII. Template for Member States to submit the required information pursuant to the VIS Decision

Report No 4: Report on the technical functioning of the VIS pursuant to Article 17(3) of the Council Decision 2008/633/JHA				
Member State/Europol	<Member State/Europol>			
Report generated at	<timestamp> [VIS into operation + 21 months, Frequency + 24 months]			
Year:	<Year(date)>			
Time period from	<date> to <date> [VIS into operation + 12 months + 9 months (separately), every 12 months thereafter]			
Management of the System [pursuant to VIS Decision]				
General Description of MS				
Central National Authority	<Name> [Article 28(2) VIS Regulation]			
End-Users[1]	<Total Number of End-users>…			
Number of Access Points	<Total Number of Access Points>			
Monitoring and Reporting	<Description of Procedures>			
Description of audits, if any	<Description of audits by the National Supervisor and findings>			
Activities Performed on behalf of another MS	<Description and number of activities referred to in Article 6 of the VIS Decision>			
Technical Functioning of the System				
CS-VIS	<Description of experiences and findings> [Only pursuant to VIS Decision]			
NI-VIS	<Description of technical functionality, updates, encountered issues, if any> [as above]			
Use of Article 4(2)	<Description of situations and results of ex-post verifications>			
Workload and Performance				
CS-VIS and BMS, NI-VIS	<Description of the Performance> + the following Statistics [2] [From designated authorities viewpoint]			
2 x 12 months data separately [Note exception with 1st report 12 + 9 months]	**Use of Article 4(2)**		**Number of All Searches**	**Other Remarks**
	Number of Urgent Cases	**Number of 4(2) where ex-post no urgency**		
January	<Total>	<Total>	<Total>	<Description>
February	<Total>	<Total>	<Total>	
March	<Total>	<Total>	<Total>	
April	<Total>	<Total>	<Total>	
May	<Total>	<Total>	<Total>	
June	<Total>	<Total>	<Total>	
July	<Total>	<Total>	<Total>	
August	<Total>	<Total>	<Total>	
September	<Total>	<Total>	<Total>	
October	<Total>	<Total>	<Total>	
November	<Total>	<Total>	<Total>	
December	<Total>	<Total>	<Total>	
Total	**<Total>**	**<Total>**	**<Total>**	