EUROPEAN DATA
PROTECTION SUPERVISOR

Security Audit
VIS Central System

Summary Report

1 June 2012

1. INTRODUCTION

1.1 Visa information system

The Visa Information System (VIS) is a system for the exchange of data on short-stay visas among Member States[1]. It is established by 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 (VIS Regulation).

It has the purpose of improving the implementation of the common visa policy, consular cooperation and consultation between Central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto in order to facilitate the visa application procedure, to prevent ‘visa shopping’, to facilitate the fight against fraud and to facilitate checks at external border crossing points and within the territory of the Member States. The VIS should also assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States and facilitate the establishment of the criteria and mechanism for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national and contribute to the prevention of threats to the internal security of any of the Member State.

In specific cases, the national authorities and Europol may request access to data entered in the VIS for the purpose of preventing, detecting and investigating terrorist and criminal offences. The procedures for such consultations are established in Council Decision 2008/663/JHA. These consultations are carried out via central access points in the participating countries and by Europol.

Two main types of search are possible: verification and identification. Verification consists of a check, carried out by the separate Automated Fingerprint Identification System or Biometric Matching System (hereinafter AFIS or BMS) that the fingerprints scanned at the border crossing point correspond to those associated with the biometric record attached to the visa (fast check done in few seconds). Identification consists of comparing the fingerprints taken at the border crossing post with the contents of the entire database (duration up to several minutes).

The system will be implemented at all national consulates and official EU border crossing points within 3 years of the system going live.

The VIS consists of the Central VIS, a national interface in each Member State and a communication infrastructure between the Central VIS and the national interfaces. The VIS is connected to the national visa systems of all Member States via the national interfaces to enable competent authorities of the Member States to process data on visa applications and on all visas that are issued, refused, annulled, revoked or extended.

The Central VIS is composed of two systems: the VIS central database with alphanumerical searching capabilities and the BMS that compares new fingerprints against those in the database and returns hit/no hit response, along with matches.

[1] For the whole report, when referring to Member States, national consulates, national competent authorities, Member States competent authorities, national data protection authorities and other similar terms, it should be understood only in the context of the Member States included in the Schengen Agreement.

The Central VIS is composed by:

- A Central Unit (CU) in Strasbourg (France).
- A Back-up Central Unit (BCU). It is a system capable of ensuring all functionalities of the Central Unit in case of failure and it is located in Sankt Johann im Pongau (Austria).

The VIS continuously processes the information collected by Member States' consulates. For example, any information entered by local visa authorities will be available almost immediately in the VIS. Border authorities can then verify visa holders' identities at the border crossing points. The VIS operates 24/7, 365 days a year.

The Commission is in charge of the development of the central database, the national interfaces and the communication infrastructure between the Central VIS and the national interfaces. Each Member State is responsible for the development, management and operation of its national system.

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice will be the Management Authority in charge of the operational management of the system from 1 December 2012, as provided by Regulation 1077/2011. Until the Agency becomes operational, the Commission will be responsible of the tasks assigned to the Management Authority as provided for in Article 26 of Regulation 767/2008.

1.2 Competence of the European Data Protection Supervisor to perform the audit

The European Data Protection Supervisor, as established by Regulation 45/2001, monitors the activities of the EU institutions, offices, bodies and agencies in relation to the processing of personal data. The duties and powers referred to in Articles 46 and 47 of Regulation 45/2001 shall apply accordingly.

Article 42 of Regulation 767/2008 explicitly provides that the European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in compliance with applicable law and that the EDPS shall ensure that an audit of the personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years.

1.3 Scope of the security audit

The scope of this audit is limited to the evaluation of the security aspects associated to the personal data processing activities of the Management Authority of the VIS. Therefore, only the Central VIS was audited. Consequently, the audit involved infrastructure, personnel, organisation and technologies associated to the Central Unit (CU) and the Backup Central Unit (BCU).

The audit did not involve the network between the Central VIS and the Member States or the connection between the two premises of the Central VIS. National interfaces and client facilities used by Members States to gain access to the VIS were also beyond the scope of this audit.

The functionality of the VIS was not audited. As the users of the VIS are Member States´ competent authorities, the compliance of the VIS Application functionality and the data processing operations in place with applicable legislation should therefore be mainly evaluated in each Member State by each national data protection authority in the context of coordinated supervision.

At application level, only the records kept in the system of the data processing activities as provided for in Article 42 of Regulation 767/2008 were assessed. However, as the system had only been in production for one month, and limited to a region, at the time of the audit, there was not enough data to extrapolate reliable statistics.

The audit assessed whether the security measures implemented by VIS comply with the requirements defined by the legislation applicable to VIS (See Annex I for the main references). Therefore, this audit report is not intended to describe or assess the functionality of the VIS but to highlight the main findings impacting security that were detected.

1.4 Methodology of the security audit

The Methodology chosen to audit the VIS was a combination of a BSI Information Security (IS) Quick Audit (based on BSI Standards and IT-Grundschutz Catalogues) and a classic Penetration Test targeting specific parts of the systems.

In a BSI IS Quick Audit, the approach is subject-oriented rather than activity-driven. The audit areas cover all five IT-Grundschutz Layers (General Aspects, Infrastructure, IT-Systems, Networks, Applications) and are predefined in a publically available document ("mandatory audit areas for the IS Quick Audit"). In addition, other obligations established by Regulation 45/2001, Regulation 767/2008, Commission Decision 260/2010 and the other legislative instruments referred in **Error! Reference source not found.** were also taken into consideration by the audit team and have been checked through the five IT-Grundschutz layers.

The audit was divided in two phases. A first on-site visit was organised on 7 and 8 July 2011 and was limited to the Central Unit when the system was still in development. The second visit took place on 16, 17 and 18 November 2011 approximately one month after the system had entered into production (11 October 2011) and covered the two premises where the Central VIS is located (the Central Unit and the Backup Central Unit).

During the audit, the auditors have interviewed key staff members, have conducted vulnerability tests, have examined existing documentation and controls and have looked into IT assets and the organisation of security for the VIS.

In particular, the audit team carried out a vulnerability test during the second visit with the view to determine the major deficiencies in terms of software updates or parameterization of the configuration that can be found by automatic means for the servers and administrative workstations of the VIS. The test was carried out using the nmap tool[2] to find the servers present in a specific network segment and nessus tool[3] to indentify vulnerabilities, also some specific information scripts were run in selected servers while administrative workstations were assessed without the use of any specific tool. Although it was requested, the VIS persons responsible of security did not agreed to the execution of intrusion tests[4] during the audit.

[2] See http://nmap.org/ for further details

[3] See http://www.tenable.com/products/nessus for further details

[4] An intrusion test consists in once vulnerability has been detected, try to exploit it in order to gain access to the system or attack the system.

The audit team was composed of three representatives from the EDPS, one representative from the Bundesamt für Sicherheit in der Informationstechnik (BSI) from Germany and two representatives from the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) from France.

1.5 Contextual aspects of the security audit

The following aspects should be taken into consideration:

- The system had only been in operation for approximately one month when the audit took place. The handover of the system from the software providers to the team in charge of the operations had only finished officially in the two previous months but there were still some pending points. Therefore, at the moment of the audit, the operations team was still building up some of the procedures and expertise required for the operation and management of the VIS.
- The European Commission showed during the audit awareness of many of the issues discussed in this document. Not only that, the Security Officer conveyed to the auditors that the European Commission was already making genuine efforts to improve the situation in terms of security and that several actions were already taking place. To this effect, it is worth mentioning, that prior to the start of the operations of the VIS system on 11 October 2011, an audit with a third party company was carried out by the European Commission and this assessment revealed similar findings to what is presented in this document.
- According to Regulation 1077/2011 of the 25 December 2011, the operational management tasks associated to the VIS system should be handed over on 1 December 2012, to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
- The VIS had a number security measures in place, however, the audit team was not in a position to evaluate if such security measures were compliant or not with a previously adopted and documented Security Policy since such a Security Policy had not been established, as required in Commission Decision 260/2010. This fact, impacted significantly the execution of the audit since, as commented, it was not possible for the audit team to assess the level of confidence associated to security controls in place. Notwithstanding this, the audit team would like to stress that this does not necessarily mean that the system was insecure or the measures inadequate. It means that the audit team was not in a position to evaluate if the security measures in place were compliant or not with a Security Policy established or if the residual risk accepted by DG Home corresponded to the reality.

2. SUMMARY AND CONCLUSIONS

In compliance with the provisions of Regulation 767/2008, the EDPS has carried a security audit of the VIS Central VIS (including the Central Unit and the Backup Central Unit) in the premises of Strasbourg (France) and Sankt Johann im Pongau (Austria). This audit consisted in two visits (7, 8 July 2011 and 16, 17, 18 November 2011).

This audit assessed if the infrastructure, personnel, organisation and technologies complied with the security requirements provided in the applicable legislation and particularly in the Commission Decision 260/2010 on the Security Plan for the operation of the Visa Information System.

The Methodology chosen to audit the VIS was based on BSI IS Quick Audit (Information Security Quick Audit) according to the BSI audit guidelines and a vulnerability test targeting specific elements of the VIS.

The absence of a properly established Security Policy impacted the execution of the audit since it was not possible to assess the security measures in place with regard to a specific target. Consequently, the audit team based its findings and recommendations not in the compliance with an established Security Policy but only on the requirements provided for in the Commission Decision 260/2010 on the Security Plan for the operation of the Visa Information System and also on assessment of the Mandatory Areas defined in the BSI IS Methodology. As a summary, the main recommendations issued in this report concerned:

- Relevant aspects of security that should be taken into account and tackled as soon as possible. In particular, a Security Policy should be properly established by the Director General of DG Home according to Commission Decision 260/2010, the documentation of the system should be improved, the training needs of the operational staff should be assessed and planned, the Business Continuity Plan should be set adequately and the incident management mechanism should be improved.

- IT Systems (Servers and workstations). The vulnerability analysis and the inspection of the configuration of both the servers and workstations showed that in many cases, it is required to update and in some cases strengthen the configuration to restrict access to the minimum required. Also USB ports and CD/DVD media should be deactivated unless explicitly needed.

- Some specific physical measures should be improved. Among others, improve cabling order and labelling in operational rooms, remove unnecessary cardboard from data center rooms and have a consistent CCTV coverage.

- Concerning Network Infrastructure. The Firewall Policy should be better defined and some specific access rules reviewed.

- The Logs. It should be verified that all activities (including law enforcement ones) are recorded, the fields stored in the logs should be re-arranged according to applicable legislation and some specific queries and reports should be provided to ease the extraction of aggregated information about the activities in the system for future inspections.

The EDPS has not found in the course of the audit critical security weaknesses that would justify imposing a temporary ban on processing according to Article 47.1(f) of Regulation 45/2001. Notwithstanding this, several of the problems found (taking as reference mainly the requirements expressed in Article 22 of Regulation 45/2001, the Commission Decision 260/2010 and BSI Quick Audit

Reference) represent important risks for the security in the operations of the VIS and the EDPS requires a prompt correction.

Against this background, the EDPS requests the Commission to put in place an Implementation Plan to address all these recommendations and also to address the additional actions that could be needed to adapt the current system to the requirements of the Security Policy (once it is properly established).

The EDPS will follow up the execution of this Implementation Plan and requests that the associated activities and deliverables are duly reported. Two check-points have been established, one after 3 months of the issue of this report and another one before the end of 2012 (or one month before the handover of VIS to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice if it happens as planned on 1 December 2012).

Additionally, the EDPS, upon the assessment of the reporting done by the Commission, might require that a new security audit is carried out before the handover of the VIS to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

Finally, the EDPS announces its intention to make an additional inspection of the Central VIS with a broader scope (including security and also other compliance aspects not explicitly associated to security) to evaluate data processing activities, in principle, soon after the system is handed over to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.