Summary report on the EURODAC Audit

9 November 2007

1. Introduction

As the supervisory authority[1] of the Central Unit, and in compliance with Article 20(2) of the EURODAC regulation[2], the EDPS launched a comprehensive inspection, completed in March 2006, and decided to initiate an in-depth security audit. A summary of this in-depth security audit is presented here.

2. Scope of Audit

The EURODAC central system consists of a Central Unit, a Business Continuity System and terminal units at four different locations. Network communications between these premises are facilitated via the European Commission network (SNET) using VPN boxes to create secure channels. The scope of this audit was limited to the four sites of the central components. The audit did not involve the network between the Central Unit and the Member States nor SNET itself. Client facilities used by Members States to gain access to EURODAC were also beyond the scope of this audit.

Within this framework, the audit did apply to the EURODAC central infrastructure, personnel, organisation and technologies. It assessed whether the security measures implemented by EURODAC still comply with the requirements defined by the EURODAC Regulation and the corresponding security policy of the European Commission applied to EURODAC. It further assessed whether the security measures implemented by EURODAC comply with best current practices.

According to an Administrative Arrangement formalised between ENISA[3] and the EDPS, ENISA suggested a couple of national organisations for assisting the EDPS in the development of this security audit based on their expertise and availability. The audit team was composed of representatives from the EDPS, the BSI - Federal Office for Information Security of Germany, and from the DCSSI (Direction centrale de la sécurité des systèmes d'information) from France. ENISA reviewed the quality standards of the report and its advice has been taken into account in the present document.

---

1 In January 2004 the former Joint Supervisory Body of EURODAC was replaced by the European Data Protection Supervisor ("EDPS"), pursuant to Article 20(11) of Regulation (EC) 2725/2000

2 Regulation (EC) 2725/2000 of the Council of 28 February 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention

3 European Networks and Information Security Agency, www.enisa.europa.eu

3. Audit Methodology

The audit of EURODAC is based on the “IT-Grundschutz” methodology according to the following standards: BSI100-2, BSI100-3, ISO/IEC 27001, IT-Grundschutz catalogues, edition 2004 and 2005.

After consultations with the audit team and ENISA, the EDPS decided to use the "IT-Grundschutz" as it represented the most appropriate tool for the EURODAC situation. Indeed, part of the audit team already had developed a high level of expertise with respect to this methodology. The protection profiles of the forthcoming large scale IT systems (VIS and SIS II) the supervision of which will be provided by the EDPS, have been defined using this tool. The methodology which offers a systematic and efficient approach has been developed based on international well recognised standards.
This choice raised some procedural and interoperability issues during the audit as the EURODAC security measures had not initially been defined following the "IT-Grundschutz". This point required adjustments and additional efforts which were only possible due to the flexibility and proactive contribution of the EURODAC team of the European Commission.

According to the “IT-Grundschutz” methodology, an initial modelling of the EURODAC-application took place - based on documentation of the following IT-assets: buildings and rooms, networks, IT systems and applications.

As part of the methodology, appropriate protection requirements (normal, high, or very high) for all relevant aspects listed above had to be defined by the owner of the application. The EURODAC team decided to set “normal” protection requirements with respect to confidentiality, integrity and availability of all relevant data. Hence, a “Supplementary Risk Analysis” was not applied.

Prior to the on-site audit-activities, a formal verification of the network plan and the list of all components of the IT-assets defined above were carried out. In this step a number of minor inconsistencies were clarified.

Furthermore, the EURODAC team was asked to carry out the “Basic Security Check”. Within this step, the EURODAC team checked the implementation of all safeguards arising from the IT-Grundschutz-modelling.

A penetration test on components of the EURODAC application was not foreseen for this audit.

Based on the above information and a preliminary visit to the premises that had already taken place at the end of 2006, a set of 10 specific modules was chosen for the on-site audit in the premises. Additionally, for each module, one appropriate component was assigned.

Number (2006-de)	Number (2004-en)	Name of Module	Status	Tier
M 1.000	M 3.0	IT Security Management	(Mandatory)	I
M 1.003	M 3.3	Contingency Planning Concept	(Random)	I
M 1.013	M 3.13	IT Security Awareness and Training	(Selected)	I
M 2.004	M 4.3.2	Server Rooms	(Random)	II
M 3.102	M 6.2	Unix Servers	(Random)	III
M 3.301	M 7.3	Security Gateway (Firewall)	(Selected)	III
M 4.001	M 6.7	Heterogeneous Networks	(Random)	IV
M 5.003	M 7.4	E-Mail	(Selected)	V
M 5.007	M 9.2	Databases	(Random)	V
M 5.012	M 7.10	Exchange/Outlook 2000	(Selected)	V

The on-site audit took place between 26 and 29 June 2007.

4. Conclusion

The security measures initially implemented with respect to the EURODAC system and the way they have been maintained during these first four years of activity have provided a fair level of protection to date. However, some parts of the systems and the organizational security present some weaknesses which will have to be addressed in order for EURODAC to fully comply with best practices and the implementation of best available techniques.

The EDPS will review the proper implementation of the follow-up measures which will be elaborated on the basis of the present report.