Requirements and Specifications for EPC Approved Server CAs for e-Mandate Services

Circulation: Publicly available
Restricted: No

1 Introduction

The SEPA Core Direct Debit ("SDD") Scheme owned by the European Payments Council ("EPC") supports the optional use of electronic Mandates ("e-Mandates"). The e-Mandate proposal message is routed from the Creditor to the Debtor Bank and the e-Mandate validation message is routed from the Debtor Bank to the Creditor.

It is a requirement defined by the EPC that these messages must be routed via open networks by making use of the Internet. In order to make this message exchange reliable and secure the EPC has defined a standard for this messaging which is called the "e-Operating Model".

The EPC e-Operating Model is defined across the following three documents:

1. The **High-level definition of the EPC e-Operating Model** presents a broad description of the e-Mandate EPC e-Operating Model, message flows, data model and general requirements for the solution and for the parties [1].

2. The **Security Concept of the EPC e-Operating Model** has the objective of establishing a security platform via the definition of security requirements that must be fulfilled by the detailed specification in order to mitigate risks evaluated through a risk assessment [2].

3. The **Detailed Specification of the EPC e-Operating Model** has the objective to make a comprehensive description of each requirement allowing an unambiguous implementation. It includes the implementation guidelines and a complete XML schema for the EPC e-Operating Model [3].

In addition, the messages exchanged via the e-Operating Model are to be compliant with the UNIFI (ISO 20022) XML standards as specified in the document "SEPA Core Direct Debit Scheme, E-Mandate Service Implementation Guidelines, Version 1.0 Approved 3 April 2009" [4].

In the detailed specification of the e-Operating Model there are a number of references to EPC approved Certification Authorities (CAs). For example, the Management Summary states that "…EPC approved Certification Authorities are used to securely qualify legitimate Validation Service providers and Routing Service providers." The primary role of these EPC approved CAs is to provide a common trust (and hence liability) model enabling secure message flows between the

Validation Service Providers (SPs) and the Routing SPs without having to establish bilateral agreements between all possible combinations.

According to a resolution approved at the EPC Plenary in June 2009, EPC will allow any established CA which has been approved by the EPC according to the dedicated approval process for e-Mandate Service CAs to provide certificates (as specified in [3]) to the market.

The EPC follows the general approach of multiple CAs with the establishment of a so-called Trust-Service Status List (TSL) for e-Mandate Services based on ETSI 102 231 [11] that contains all relevant public key certificates of all EPC approved CAs for e-Mandate Services. EPC has contracted a Trust Body to establish and maintain this TSL.

This document defines the EPC technical requirements and specifications for these "EPC approved CAs for e-Mandate Services. The actual approval process will be defined in a separate document.

2 General requirements

Requirements for CAs are described in 'ETSI TS 102 042 - "Policy requirements for certification authorities issuing public key certificates" [10]. A conformant CA must demonstrate that its management system for issuing public key certificates fulfills the requirements of its Certificate Policy.

The CA must comply with the following requirements:

a) It shall have an ISMS system compliant with IS27000 which is audited according to IS27006 the scope of which shall cover the CA operation

b) It meets its obligations as defined in clause 6 of TS 102 042: Certification authority obligations.

c) It has implemented controls which meet the requirements specified in clause 7 of TS 102 042:

- Certification practice statement
- Public key infrastructure – Key management life cycle
- Public key infrastructure – Certificate management life cycle
- CA security management and operation
- Organizational requirements.

More details are provided in the next clauses.

3. Functional requirements

3.1 Certificate Policy (CP)

The CA shall be required to produce a Certificate Policy (CP) in accordance with ETSI TS 102 042 [10] using the Extended Normalized Certificate Policy (NCP+) as the reference policy. In particular:

1. Clause 5.4.1 – items b), c) and d) will be required;
2. Clause 6.2 – conditional items d), e) and g) will be required;
3. Clauses 7.2.1, 7.2.2 – should be amended with the inclusion of ISO/IEC 19790:2006 [9]. The conformance with the latter is recommended.
4. Clause 7.2.8, 7.2.9 –will not be required as the CA will not generate the subject's keys;
5. Clause 7.3.1 – the CA will verify the subject's identity in accordance with the requirements given in annex D of the Detailed Specification of EPC e-Mandates e-Operating Model [3] (EPC will provide a mechanism for identifying authorized persons in this context);
6. Clause 7.3.3 – conditional item d) will not be required;
7. Clauses 7.3.5, 7.3.6 – the CA will not be issuing certificates to the public under this CP, it will be up to the CA to determine the conditions for the dissemination of the certificates and agree with EPC accordingly;
8. Clause 7.3.6 - support for certificate suspension will be required, under circumstances to be agreed with EPC.

   As soon as key compromise or security incident having an impact on the CA services is detected, the CA shall inform EPC and the TSL Trust Body with:

   i. a short incident report within 1 hour. The CA decides if the CA key needs to be suspended or revoked immediately;
   ii. a full analysis report within the 48 hours. The CA will inform the TSL Trust Body and EPC about the re-activation of the suspended key, or the revocation followed by the submission of a new key, possibly after a successful re-auditing.
   iii. EPC has the right to request suspension or revocation under to be agreed circumstances.

The proposed Certificate Policy must be submitted to EPC with the application for registration. Review of adherence to the Certificate Policy shall be part of the audit report.

3.2 Certificate Practice Statement (CPS)

The CA shall be required to prepare a Certification Practice Statement (CPS) in accordance with RFC 3647[6] against which it must be successfully audited. If the CPS cannot be published for reasons agreed with EPC, then the CA shall be required to produce a PKI Disclosure Statement (PDS) in accordance with Annex B of ETSI TS 102 042 [10] that will be published as appropriate.

The description of the certificate profiles to be issued by the CA is specified in Annex E of the Detailed Specification of EPC e-Mandates e-Operating Model [3]. These profiles address the:

- Routing Service authentication certificate;
- Validation Service authentication certificate;
- Validation Service signing certificate.

In these profiles the EPC_BASE_OID (see Annex E in [3]) must hold the value 1.xxxxx.NNNNN[1] (tbd) in order to refer to the EPC Approved CAs for e-Mandate Services.

Review of adherence to the Certificate Practice Statement shall be part of the audit report.

4. Operational requirements

The CA shall be required to be conformant with ETSI TS 102 042 [10] Clause 7.4 "CA Management and operation". In addition, the following requirements must be complied with:

1. Clause 7.4.5 Operations management
   - The [NCP] option should used in g)
   - All incidents shall be reported to EPC within a one hour period. EPC will notify the Trust Body in order to respond according to the incident.
2. Clause 7.4.8 Business continuity management and incident handling
   - Item f) first bullet – insert “EPC,” before “all subscribers”.
3. Clause 7.4.9 Trustworthy systems deployment and maintenance
   - The CA shall agree with EPC, suitable plans to ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings,

[1] Value to be defined by the Internet Assigned Numbers Authority (IANA) via registration form: http://pen.iana.org/pen/PenApplication.page

5. References

[1]	EPC109-08	e-Mandates e-Operating Model - High-level Definition	EPC
[2]	EPC159-08	e-Mandates e-Operating Model - Security Concept	EPC
[3]	EPC208-08	e-Mandates e-Operating Model – Detailed Specification	EPC
[4]	EPC002-09	SEPA Core Direct Debit Scheme, E-Mandate Service Implementation Guidelines	EPC
[5]	ISSG033-09	Approval Scheme for EPC Approved CAs for E-Mandate Services	EPC
[6]	IETF RFC 3647	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework	IETF
[7]	CWA 14169	Secure signature-creation devices “EAL 4+” (March 2004)	CEN
[8]	FIPS PUB140-02	Security Requirements for Cryptographic Modules (2001)	NIST
[9]	ISO/IEC19790	Information technology -- Security techniques -- Security requirements for cryptographic modules (2006)	ISO
[10]	ETSI TS 102 042	Electronic Signatures and Infrastructures (ESI) - Policy requirements for certification authorities issuing public key certificates, (version 2.1.1, May 2009)	ETSI
[11]	ETSI TS 102 231	Electronic Signatures and Infrastructures (ESI) - Provision of harmonized Trust-service status information (version 2.1.1, March 2006)	ETSI