EPC292-09
Version 2.1 Approved
19 December 2012

Approval Scheme for EPC Approved 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 via the Routing Service to the Validation Service of the Debtor Bank and the e-Mandate validation message is routed from the Validation Service of the Debtor Bank back to the Creditor.

It is a requirement defined by the EPC that these messages could 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 ISO 20022 XML standards as specified in the document "SEPA Core Direct Debit Scheme, E-Mandate Service Implementation Guidelines [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 and the Routing Service Providers without having to establish bilateral agreements between all possible combinations.

According to the EPC Plenary resolution on the recommendation on the establishment and the Governance of "EPC Approved Certification Authorities" in support of the e-Mandates Scheme for SEPA Direct Debit (EPC073-09, 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 technical requirements and specifications for the CA services are described in a separate document "Requirements and Specification for EPC Approved Server CAs for e-Mandate Services" (EPC291-09) [5]. The present document aims to specify the EPC approval process for these CAs.

The EPC follows the general approach of multiple CAs, each offering one or more CA services, with the establishment of a so-called Trust-Service Status List (TSL) for e-Mandate Services based on ETSI 102 231 [12] 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, called in the following the "TSL Trust Body".

2. Recognition of accredited auditors by the EPC

A conformant CA must demonstrate that the management system governing a particular CA Service used for issuing public key certificates fulfils the requirements of the own Certificate Policy for that service. This Certificate Policy must satisfy requirements for CAs as described in ETSI TS 102 042 - "Policy requirements for certification authorities issuing public key certificates" [13]. More details are provided in the document "Requirements and Specification for EPC Approved Server CAs for e-Mandate Services" [5].

The independent body carrying out the audits in the context of "EPC approved CAs" shall be accredited for the purpose of auditing organisations implementing ISO 27001 [15] by an official accreditation body according to ISO/IEC 27006 [16].

The audit body should ideally also confirm compliance to the clause 3.4 of the CEN Workshop agreement CWA 14172-2 [14].

The auditor will provide an exemplary audit report demonstrating the method and evidence followed by the auditor illustrating especially chapter 3 of the Model CA Audit Report [7].

EPC will approve the proposed accredited auditor as part of the approval process and will establish a separate dedicated agreement with the accredited auditor (see [8]). Once approved, the auditor will receive the dedicated EPC label "Recognised Auditor" (see step 2 in Annex I).

The audit of the CA by the EPC Recognised Auditor shall ensure compliance to ISO 27001 [15] and CWA 14172-2 (see [14]) with regard to the establishment, operation and maintenance of the CA. The auditor will use the dedicated template (see [7]) to provide the audit report. Should the CA seeking approval from EPC for the e-Mandate services also operate other CA services, the audit report need to demonstrate that there is appropriate segregation in the trust chain and dedicated resources.

A list of the Recognised Auditors for EPC Approved CAs will be published on the EPC Website.

Subsequent annual audit reports are required in accordance with the standards mentioned above. The costs for all audits are to be borne by the CA. All audit reports shall be provided using the dedicated template (see [7]). The terms and conditions for providing these audit reports to EPC will be laid down in the agreement between EPC and the EPC Approved CA (see [10]).

3. Description of approval process for a new applicant for an EPC approved CA

The basis for the evaluation of applications to the CA approval process are the "Requirements and Specifications for EPC Approved Server CAs for E-Mandate Services" [5].

This section details the steps to be followed under such circumstances (a flowchart giving an overview of this process is provided in Annex I).

Step 1: The CA submits its registration application to the EPC with indication of its auditor using a dedicated EPC template (see [6]) and a copy of its proposed Certificate Policy.

Step 2: EPC will verify if the proposed auditor is already in its list of EPC Recognised Accredited Auditors. If the accredited auditor is not yet recognised by the EPC, the auditor must be approved by the EPC according to the requirements stated in section 2 of this document "Recognition of accredited auditors by the EPC" (see [8]).

Step 3: The EPC will check if the Certificate Policy received satisfies ETSI TS 102 042 [13] for an e-Mandate service (see [5]).

Step 4: If the registration application is accepted by EPC, the candidate CA will mutually sign an agreement with the EPC, clarifying the liabilities of the EPC and the candidate CA, and the CA's Certificate Policy to be used, employing a dedicated EPC template (see [9]). The CA will further unilaterally sign a dedicated document specifying the terms and conditions of the EPC Approved CA mark (see [10]). Subsequently, the CA will receive the "EPC Applicant CA" label.

Step 5: The Applicant CA informs the auditor of its status as an "EPC Applicant CA" and requests the auditor to conduct an audit.

Step 6: The auditor asks for any documents supporting the request and schedules a date to conduct an audit.

Step 7: The Applicant CA proves its conformance to [5] to the auditor.

Step 8: The auditor prepares its report according to [7] (see chapter 2) and provides it to the Applicant CA.

Step 9: The Applicant CA submits the audit report to EPC.

Step 10: EPC reviews the audit report. In case it is satisfactory it will approve the Applicant CA. If the audit report is not satisfactory a few more interactions with the Applicant CA and possibly the auditor might be necessary to improve the audit report until the expected compliance is ensured.

Step 11: EPC countersigns document [10] providing the EPC Approved CA mark (see Step 4) to the CA Applicant.

Step 12: EPC informs the TSL Trust Body.

Step 13: The TSL Trust Body signs a contract with the Approved CA.

Step 14: The TSL Trust Body conducts the appropriate functional testing with the Approved CA in order to verify that the necessary requirements for the CA service's public key certificate laid down in [5] are fulfilled.

Step 15: The TSL Trust Body publishes the public key certificates and CA details in the TSL list of EPC approved CAs according to [11] and sets the service's status to 'In Accordance'.

Step 16: The TSL Trust Body informs both the Approved CA and EPC about this publication.

Step 17: EPC includes the Approved CA in its list of EPC Approved CAs on the EPC website.

Step 18: EPC informs the Approved CA about its publication in the list of EPC Approved CAs on the EPC website.

4. Operational aspects for EPC approved CAs

EPC approval of the CA is granted for an unlimited time period subject to annual audit report accepted by the EPC(see section 2). There may be circumstances that require a re-audit during the annual period as listed for example in the Model agreement for the EPC Registered CA applicants (see [9]).

In accordance with [5], all incidents encountered by the EPC approved CA shall be reported to EPC and the TSL Trust Body within one hour period.

Revocation of public keys, which are issued in the TSL list of EPC Approved CAs, as well as the issuance of new public keys must be notified to the TSL Trust Body.

5. Compromise of CA Public Key

As stated in the previous section, if a key compromise or security incident having an impact on the CA services is detected, the CA shall inform EPC and the TSL Trust Body. This chapter details the steps to be followed under such circumstances (a flowchart giving an overview of this process is provided in Annex II).

Step 1: CA detects (suspected) compromise of its CA service signing key and immediately revokes all relevant public key certificates.

Step 2: CA informs the TSL Trust Body and EPC.

Step 3: TSL Trust Body updates the CA service's status to 'Suspended' and then informs EPC that it has updated the CA service's status. EPC suspends the CA's entry in the list of EPC Approved CAs on the EPC website.

Step 4: EPC evaluates the risk incurred by the key compromise or security incident and whether it requires a re-audit within a specified timeframe.

Step 5: The CA is informed about re-audit request.

Step 6: The CA informs the auditor about the need to have a re-audit.

Step 7: The auditor receives the request for re-audit of the CA.

Step 8: The CA demonstrates to the auditor proof of the incident handling countermeasures taken and proves its continuing conformance to [5].

Step 9: The auditor prepares a new audit report according to [7] and provides it to the CA.

Step 10: The CA submits the report to EPC.

Step 11: EPC reviews the audit report.

Step 12: If the report is satisfactory, the CA is informed and the process continues as of step 12 of Annex I. If the report is not satisfactory or not provided in due time, the CA is informed and the process continues as of step 1 of Annex III.

6. Cancellation of Approved CA by EPC

If EPC has need to cancel the CA's status as "EPC Approved" as provided for in clause 10 of the contract established between EPC and the EPC Approved CA in the chapter headed "**TERM AND TERMINATION**" in the model agreement [10], then EPC will take the following steps (a flowchart giving an overview of the process is provided in Annex III).

Step 1: EPC decides to cancel an EPC Approved CA as above.

Step 2: The CA is notified by EPC about its decision to cancel its EPC Approved status in accordance with the relevant clause in the contract [10].

Step 3: The CA immediately revokes the relevant public key certificates for all of its CA services relating to its EPC approval.

Step 4: EPC removes the Approved CA from its list of EPC Approved CAs on the EPC website.

Step 5: EPC notifies the TSL Trust Body that the relevant CA is no longer EPC Approved.

Step 6: The TSL Trust Body updates the status of all of the CA's services to 'Revoked'.

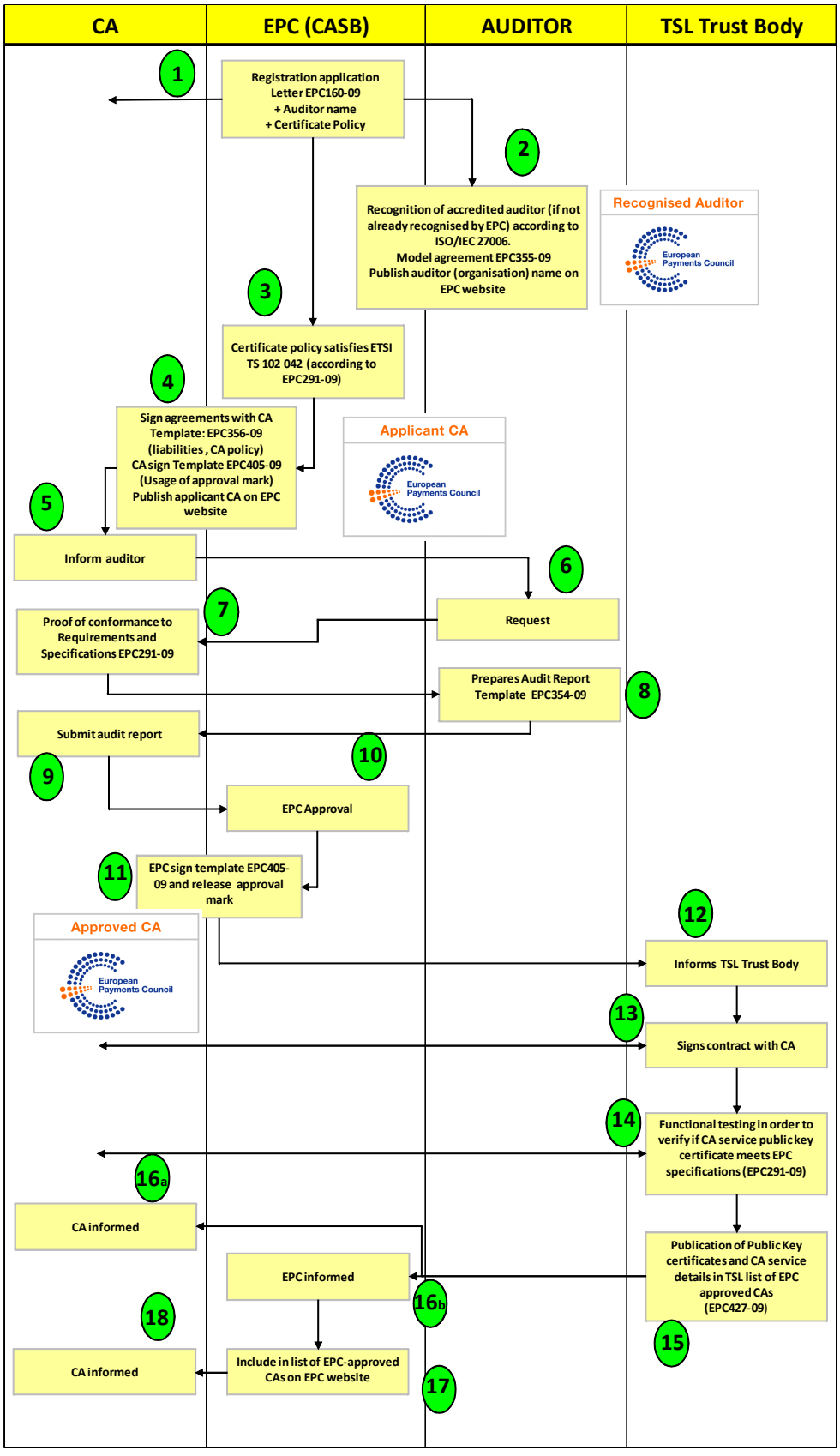
Step 7: The CA is informed by the TSL Trust Body that its entries in the TSL have been updated as requested by EPC and also of any actions that need to be taken in accordance with the contract between the CA and the TSL Trust Body.

Step 8: Also, EPC is informed by the TSL Trust Body that the entries in the TSL have been updated as requested.

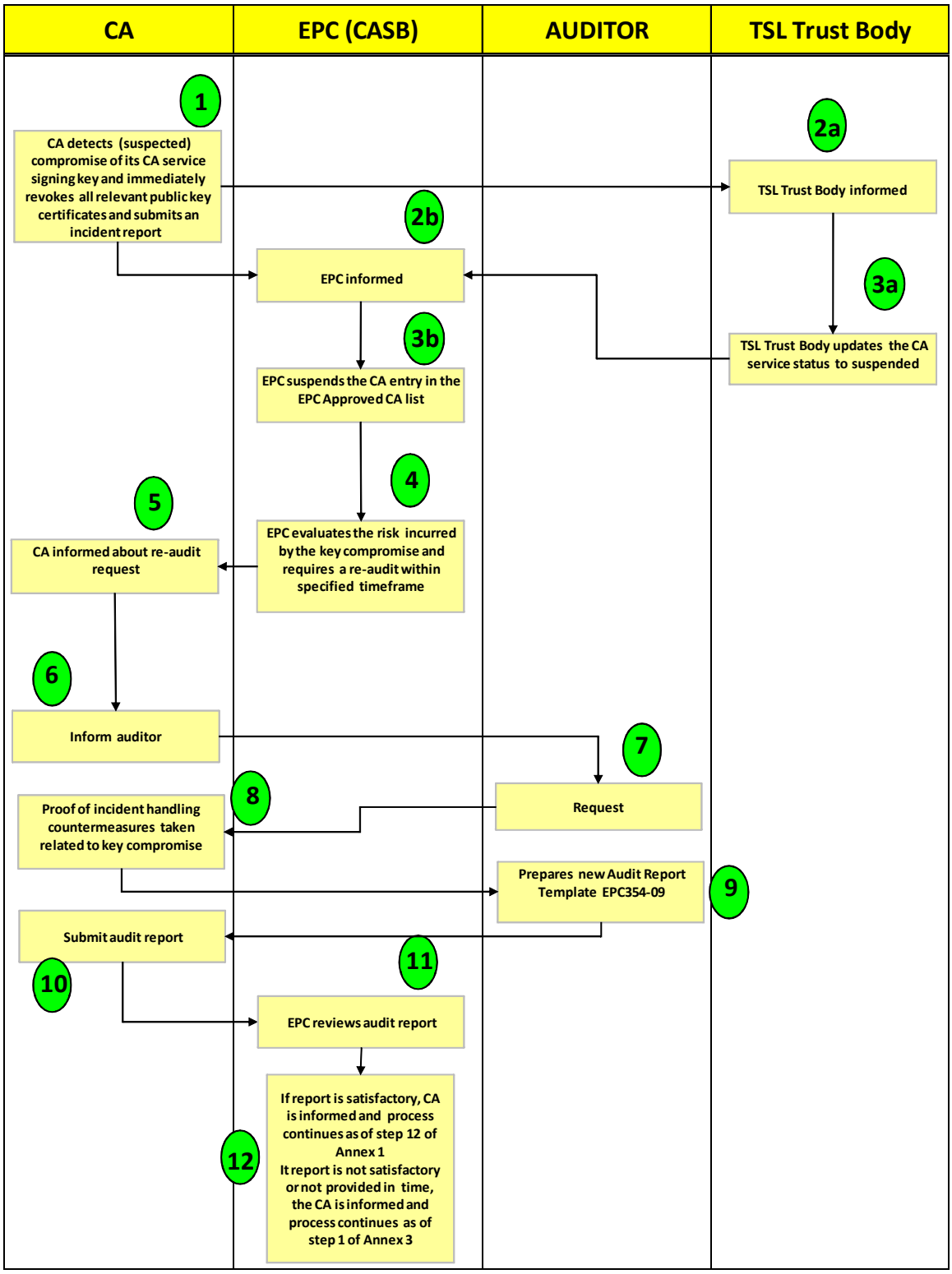
7. References

[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]	EPC291-09	Requirements and Specification for EPC Approved Server CAs for E-Mandate Services	EPC
[6]	Letter EPC160-09	CA Applicant Registration	EPC
[7]	EPC 354-09	Model CA Audit Report	EPC
[8]	EPC 355-09	Model agreement for the EPC recognised auditors	EPC
[9]	EPC 356-09	Model agreement for the EPC Registered CA applicants	EPC
[10]	EPC 405-09	Model agreement permitting Use of the EPC CA Mark	EPC
[11]	EPC 427-09	Detailed Specifications for TSLs for EPC Approved CAs	EPC
[12]	ETSI TS 102 231	Electronic Signatures and Infrastructures (ESI) - Provision of harmonized Trust-service status information (version 2.1.1, March 2006)	ETSI
[13]	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
[14]	CWA 14172-2	EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes (March 2004)	CEN
[15]	ISO 27001	ISO/IEC 27001: Information technology - Security techniques - Information security management systems -- Requirements	ISO
[16]	ISO 27006	ISO/IEC 27006:2007 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems	ISO

Annex I - Approval Scheme Process for EPC Approved CAs



Annex II - Compromise of Public Key of EPC Approved CA



Annex III - Cancellation of Approval status of CA by EPC