EPC427-09EPC427-09
Version 1.0
8 October 2013
EPC

# Detailed Specifications for TSLs for EPC Approved Certification Authorities (CAs) in support of SEPA e-Mandate Services

**Circulation:** Publicly available
**Restricted:** No

Within this document the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [3].

The present specifications are relying on the specifications and requirements stated in ETSI TS 102 231 v2.1.1 [1]. When no specific requirement is stated in the present specifications, requirements from [1] SHALL apply entirely. When specific requirements are stated in the present specifications, they SHALL prevail over the corresponding requirements from [1] while being completed by format specifications specified in [1]. In case of discrepancies between the present specifications and specifications from [1], the present specifications SHALL be the normative ones.

Date-time indication SHALL be compliant with clause 5.1.4 of [1].

Use of URIs SHALL be compliant with clause 5.1.5 of [1].

Notes are provided for further clarifications during the finalisation process of the present detailed specifications.

## Information on the TSL Issuing Scheme

### Trust-service Status List tag

**TSL tag** (clause 5.2.1)

This field is REQUIRED and SHALL comply with clause 5.2.1 of [1].

### Scheme Information

**TSL version identifier** (clause 5.3.1)

This field is REQUIRED and SHALL be set to « 2 » (integer).

**TSL sequence number** (clause 5.3.2)

This field is REQUIRED. It SHALL specify the sequence number of the TSL. Starting from “1” at the first release of the TSL, this integer value SHALL be incremented by 1 at each subsequent release of the TSL. It SHALL NOT be recycled to "1" when the "TSL version identifier" above is incremented.

**TSL type** (clause 5.3.3)

This field is REQUIRED specifying the type of TSL. It SHALL be set to http://uri.etsi.org/TrstSvc/TSLtype/generic/EPC-ApprovedList .

**Note (1)**: In order to comply with [1] clause 5.3.3, and to indicate the specific type of TSL as referring to the existence of the relevant specifications governing the establishment of the TSL implementation of the list of EPC-approved CAs, the above specific URI SHALL be registered and described as follows:

*"URI: (Generic)*[1]

*http://uri.etsi.org/TrstSvc/TSLtype/generic/EPC-ApprovedList*

*Description: A TSL implementation of a list of services from CAs that are approved by the EPC to support the e-Mandate Service, through a voluntary process of direct oversight."*

**Scheme operator name** (clause 5.3.4)

This field is REQUIRED. It SHALL specify the name of the Body in charge of establishing, publishing and maintaining this TSL. It SHALL specify the formal name under which the associated legal entity or mandated organization associated with this Body operates. It MUST be the name used in formal legal registration or authorisation and to which any formal communication should be addressed.

The named Scheme Operator is expected to sign the TSL.

**Scheme operator address** (clause 5.3.5)

This field is REQUIRED. It SHALL specify the address of the legal entity or mandated organization identified in the "Scheme operator name" field (clause 5.3.4) for both postal and electronic communications. It SHALL include both "PostalAddress" (i.e. street address, locality, [state or province], [postal code] and ISO 3166-1 [8] alpha-2 country code) as compliant with clause 5.3.5.1; and "ElectronicAddress" (i.e. email and/or website URI) as compliant with clause 5.3.5.2.

**Scheme name** (clause 5.3.6)

This field is REQUIRED. It SHALL specify the name of the scheme as "EPC_Approved CA Services".

**Scheme information URI** (clause 5.3.7)

This field is REQUIRED and SHALL specify the URI(s) where users (relying parties) can obtain information about the EPC approval process.

**Status determination approach** (clause 5.3.8)

This field is REQUIRED and SHALL specify the identifier of the status determination approach. The URI SHALL be "Active":

http://uri.etsi.org/TrstSvc/TSLType/StatusDetn/active.

**Scheme type/community/rules** (clause 5.3.9)

This field is OPTIONAL and is not used in the context of the present specification.

**Scheme territory** (clause 5.3.10)

[1] This URI shall be preferably registered and described at ETSI but in the event this registration process leads to unacceptable delays, an alternative registration process shall be performed.

This field is OPTIONAL and is not used in the context of the present specification.

**TSL policy/legal notice** (clause 5.3.11)

This field is OPTIONAL. *Its content and whether it will be present is to be decided.*

**Historical information period** (clause 5.3.12)

This field is REQUIRED and SHALL specify the duration (integer) over which historical information in the TSL is provided. This integer value is to be provided in number of days and in the context of the present specifications it SHALL be greater or equal to 3653 (i.e. meaning that the list MUST contain historical information for a minimum of ten years).

**Pointers to other TSLs** (clause 5.3.13)

This field is OPTIONAL and is not used in the context of the present specification.

**List issue date and time** (clause 5.3.14)

This field is REQUIRED and SHALL specify the date and time (UTC expressed as Zulu) on which the TSL was issued using Date-time value as specified in [1] clause 5.1.4.

**Next update** (clause 5.3.15)

This field is REQUIRED and SHALL specify the latest date and time (UTC expressed as Zulu) by which the next TSL will be issued or be null to indicate a closed TSL (using Date-time value as specified in [1] clause 5.1.4).

In the event of no interim status changes to any TSP or service covered by the scheme, the TSL MUST be re-issued by the time of expiration of the last TSL issued.

In the context of the present specifications, the difference between the “Next update” date and time and the “List issue date and time” SHALL NOT exceed six (6) months.

Scheme extensions (clause 5.3.16)

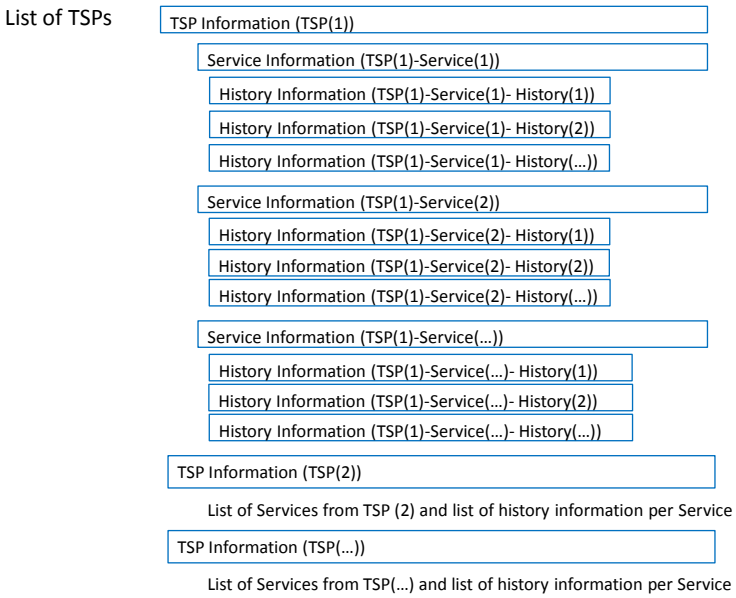
This field is OPTIONAL and is not used in the context of the present specification.

**List of Trust Service Providers** (clause 5.3.17)

This field is OPTIONAL.

In the case where no CA’s services are or have been approved by the EPC, this field SHALL be absent. Note, in order to maintain past history for CAs that may no longer be approved then even if there are no currently approved CAs this field SHALL be present.

In the case where one or more CA’s services are or have been approved by the EPC, then the field SHALL contain a sequence identifying each CA providing one or more of those EPC-Approved services, with details on the status and status history of each of the CA’s services (see the Figure below, extracted from [1], where TSP is synonymous with CA).




The list of CAs is organised as depicted in the above Figure. For each CA, there is a sequence of fields holding information on the CA ("**TSP Information**"), followed by a list of services. For each of such listed services, there is a sequence of fields holding information on the service ("**Service Information**"), and a sequence of fields on the approval status history of the service ("**Service Approval History Information**").

## TSP Information

### TSP(1)

**TSP name** (clause 5.4.1)

This field is REQUIRED and SHALL specify the name of the **legal entity** responsible for the CA's services that are or were approved under the EPC_Approval scheme. This name MUST be the name that is used in formal legal registrations and to which any formal communication would be addressed.

**TSP trade name** (clause 5.4.2)

This field is OPTIONAL and, if present, SHALL specify an alternative name under which the CA identifies itself in the specific context of the provision of those of its services that are to be found in this TSL under this "TSP name" entry.

**Note**: In the event a single CA legal entity is providing services under different trade names or under different specific contexts, each and every CA (legal entity) shall only be listed once and provide service specific context information.

**TSP address** (clause 5.4.3)

This field is REQUIRED and SHALL specify the address of the legal entity or mandated organization identified in the "TSP name" field (clause 5.4.1) for both postal and electronic communications. It SHALL include both "PostalAddress" (i.e. street address, locality, [state or province], [postal code] and ISO 3166-1 alpha-2 country code) as compliant with clause 5.3.5.1; and "ElectronicAddress" (i.e. email and/or website URI) as compliant with clause 5.3.5.2.

**TSP information URI** (clause 5.4.4)

This field is REQUIRED and SHALL specify the URI(s) where users (e.g., relying parties) can obtain CA-specific information. This SHALL be a sequence of multilingual pointers (with EN as the mandatory language, and with potentially one or more national languages). The referenced URI(s) MUST provide a path to information describing the general terms and conditions of the CA, its practices, legal issues, its customer care policies and other generic information which apply to all of its services listed under its CA entry in the TSL.

**Note**: In the event a single CA legal entity is providing services under different trade names or under different specific contexts, and this has been reflected in as many TSP entries as such specific contexts, this field SHALL specify information related to the specific set of services listed under a particular "TSP name"/"TSP trade name" entry.

**TSP information extensions** (clause 5.4.5)

This field is OPTIONAL and, if present, MAY be used by the EPC, in compliance with ETSI TS 102 231 specifications (clause 5.4.5), to provide specific information, to be interpreted according to the EPC-Approval scheme's rules.

**List of services** (clause 5.4.5)

This field is REQUIRED and SHALL contain a sequence identifying each of the CA's EPC-Approved services and the approval status (and history of that status) of that service. At least one service must be listed (even if the information held is entirely historical).

As the retention of historical information about listed services is REQUIRED under the present specifications, that historical information MUST be retained even if the service's present status would not normally require it to be listed (e.g. the service is withdrawn). Thus a CA MUST be included even when its only listed service is in such a state, so as to preserve the history.

### Service Information

**TSP(1) Service(1)**

**Service type identifier** (clause 5.5.1)

This field is REQUIRED and SHALL indicate a Certification Authority issuing public key certificates http://uri.etsi.org/TrstSvc/Svctype/CA/PKC.

**Service name** (clause 5.5.2)

This field is REQUIRED and SHALL specify the name under which the CA identified in "TSP name" (clause 5.4.1) provides the service identified in "Service type identifier" (clause 5.5.1).

**Service digital identity** (clause 5.5.3)

This field is REQUIRED and SHALL specify a digital identifier unique to the service whose type is specified in "Service type identifier" (clause 5.5.1) by which the service can be unambiguously identified.

In the present specifications, the digital identifier used in this field SHALL be the relevant X.509v3 [2] Certificate being a representation of the public key(s) that the CA uses for providing the service whose type is specified by the "Service type identifier" (clause 5.5.1) (i.e. the key used for signing certificates).

As a general default principle, the digital identifier (i.e. the related X.509v3 certificate, see [2]) SHALL NOT be present more than once in the TSL.

Implementations are ASN.1 or XML dependent and SHALL comply with ETSI TS 102 231 specifications [1] (for ASN.1 see Annex A and for XML see Annex B).

**Service current status** (clause 5.5.4)

This field is REQUIRED and SHALL specify the identifier of the status of the service through one of the following URIs:

- **In Accordance**

  (http://uri.etsi.org/TrstSvc/Svcstatus/inaccord)

  The subject service is approved by the EPC according to the dedicated approval process for the e-Mandate Service;

- **Expired**

  (http://uri.etsi.org/TrstSvc/Svcstatus/expired)

The subject service is no longer EPC-Approved, e.g. due to non-renewal or withdrawal by the CA, or cessation of the service;

- **Suspended**

  (http://uri.etsi.org/TrstSvc/Svcstatus/suspended)

The subject service's status is temporarily uncertain whilst checks are made by the EPC (typically e.g. while a revocation request is being investigated or if action is required to resolve a deficiency in the service fulfilling the EPC-Approval scheme's criteria;

- **Revoked**

  (http://uri.etsi.org/TrstSvc/Svcstatus/revoked)

The subject service's EPC-Approved status has been revoked because it is no longer in accordance with the EPC-Approval scheme.

> **Note (1)**: The status value "**Revoked**" can be a definitive status, even if the CA then completely ceases its activity; there is no need to migrate to "**Expired**" status in this case. The only way to change the "**Revoked**" status is to recover from non-compliance to compliance with the provisions laid down in the EPC Approval scheme.

**Current status starting date and time** (clause 5.5.5)

This field is REQUIRED and SHALL specify the date and time on which the current approval status became effective (date and time value as defined in [1] clause 5.1.4).

**Scheme service definition URI** (clause 5.5.6)

This field is OPTIONAL and is not used in the context of the present specification.

**Service supply points** (clause 5.5.7)

This field is REQUIRED and SHALL specify the URI(s) where relying parties can access the service through a sequence of character strings whose syntax MUST be compliant with RFC 3986 [16].

**TSP service definition URI** (clause 5.5.8)

This field is REQUIRED and SHALL specify the URI(s) where relying parties can obtain service-specific information provided by the CA as a sequence of multilingual pointers (with EN as the mandatory language and potentially with one or more national languages). The referenced URI(s) MUST provide a path to information describing the service as specified by the CA (see section 2.5 in the RFP).

**Service information extensions** (clause 5.5.9)

This field is OPTIONAL and is not used in the context of the present specification.

**Service approval history** (clause 5.5.10)

Since the "Historical information period" (clause 5.3.12) is non-zero this field is REQUIRED. In the case where the service has no history prior to the current status (i.e. a first recorded status or history information not retained by the scheme operator) this field SHALL be empty. Otherwise, for each change in "Service current status" (clause 5.5.4) that occurred within the "Historical information period" (clause 5.3.12), information on the previous approval status SHALL be provided in descending order of status change date and time (i.e. the date and time on which the subsequent approval status became effective).

This SHALL be a sequence of history information as defined here after.

### Service Approval History

**TSP(1) Service(1) History(1)**

**Service type identifier** (clause 5.6.1)

This field is REQUIRED and SHALL be the value used in "TSP Service Information – Service type identifier" (clause 5.5.1) when this field represented the current status.

**Service name** (clause 5.6.2)

This field is REQUIRED and SHALL be the value used in "TSP Service Information – Service name" (clause 5.5.2) when this field represented the current status. This clause does not require that the name be the same as that currently specified in clause 5.5.2 as a change of name MAY be one of the circumstances requiring a new status.

**Service digital identity** (clause 5.6.3)

This field is REQUIRED and SHALL be the value used in "TSP Service Information – Service digital identity" (clause 5.5.3) when this field represented the current status.

**Service previous status** (clause 5.6.4)

This field is REQUIRED and SHALL be the value used in "TSP Service Information – Service current status" (clause 5.5.4) when this field represented the current status.

**Previous status starting date and time** (clause 5.6.5)

This field is REQUIRED and SHALL specify the date and time on which the previous status in question became effective, with the format and meaning used in "TSP Service Information – Service current status starting date and time" (clause 5.5.5).

**Service information extensions** (clause 5.6.6)

This field is OPTIONAL and is not used in the context of the present specification.

**TSP(1) Service(1) History(2)**

Idem for TSP(1) Service(1) History(2) (prior to History(1))

**TSP(1) Service(2)**

Idem for TSP(1) Service(2) (as applicable)

**TSP(1) Service(2) History(1)**

**TSP(2)**

Idem for TSP(2) (as applicable)

Idem for TSP(2) Service(1)

Idem for TSP(2) Service(1) History(1)

### Signature

**Signed TSL** (clause 5.7.1)

The TSL, established under these specifications, SHALL be signed by the "Scheme operator name" (clause 5.3.4) to ensure its authenticity and integrity.

It is recommended that the format of the signature SHALL be CAdES BES/EPES for ASN.1 implementations, and XAdES BES/EPES as defined by ETSI TS 101 903 [5] specifications for XML implementations[2]. Such electronic signature implementations SHALL meet requirements as stated in ETSI TS 102 231 Annexes A or B [1] respectively.

Additional general requirements regarding the signature are stated in the following sections.

**Scheme identification** (clause 5.7.2)

This field is REQUIRED and SHALL specify a reference assigned by the scheme operator that uniquely identifies the scheme described in the present specifications and the established TSL, and MUST be included in the calculation of the signature. This is expected to be a character string or bit string.

[2] It is mandatory to protect the Scheme Operator signing certificate with the signature in one of the ways specified by ETSI TS 101 733 [4] or ETSI TS 101 903 [5] respectively.

In the context of the present specifications the assigned reference SHALL be the concatenation of the "TSL type" (clause 5.3.3), the "Scheme name" (clause 5.3.6) and the value of the SubjectKeyIdentifier extension of the certificate used by the Scheme operator to electronically sign the TSL.

**Signature algorithm identifier** (clause 5.7.3)

This field is REQUIRED and SHALL specify the cryptographic algorithm that has been used to create the signature. Depending on the algorithm used, this field MAY require additional parameters. This field MUST be included in the calculation of the signature.

**Signature value** (clause 5.7.4)

This field is REQUIRED and SHALL contain the actual value of the digital signature. All fields of the TSL (except the signature value itself) MUST be included in the calculation of the signature.

**References**


| | | |
|---|---|---|
| 1 | ETSI TS 102 231 v2.1.1 (2006) | Technical Specification for a Trust-service Status List |
| 2 | ISO/IEC 9594-8 (ITU-T X.509) (2001) | Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks |
| 3 | RFC 2119 (1997) | Key words for use in RFCs to Indicate Requirement Levels |