ETSI TS 119 431-1 V1.3.1 (2024-12)

Electronic Signatures and Trust Infrastructures (ESI);
Policy and security requirements for trust service providers;
Part 1: TSP services operating a remote QSCD / SCDev

Reference
RTS/ESI-0019431-1v131

Keywords
e-commerce, electronic signature, remote,
security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering policy and security requirements for Trust Service Providers providing remote signature, as identified below:

Part 1: "TSP services operating a remote QSCD / SCDev";

Part 2: "TSP service components supporting AdES digital signature creation".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document specifies policy and security requirements for TSP services operating a digital signature creation device, including a Qualified Signature/Seal Creation Device (QSCD) as defined in Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1] to create a digital signature value on behalf of a remote signer.

These requirements are based on the general policy requirements specified in ETSI EN 319 401 [1] and take into account related requirements for certificate issuance in ETSI EN 319 411-1 [2].

The requirements of the present document are aligned with the requirements specified in EN 419241-1 [3].

Introduction

When digital signatures are created in an entirely user-managed environment, it is assumed that the signature creation data is under the control of the signer, who is physically in possession of the signature creation device.

For remote digital signature creation, the signature creation data is maintained and managed by a third party on behalf of the signer. To guarantee that the signature creation environment is reliable and that the signature creation data is used under the control of the signer, the provider of the remote digital signature service has to apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels.

1 Scope

The present document specifies generally applicable policy and security requirements for Trust Service Providers (TSPs) operating a remote Signature Creation Device (SCDev). Specific requirements apply when the device is a remote QSCD as defined in Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1].

The service consists of a server signing application and a QSCD / SCDev. The term used in the present document is Server Signing Application Service (SSAS).

NOTE 1: Regulation (EU) 2024/1183 [i.11] (eIDASv2) defines the management of remote electronic signature/seal creation devices as a trust service. In addition, it introduces the qualified trust service for the management of remote qualified electronic signature/seal creation devices.

The policy and security requirements are defined in terms of requirements for creation, maintenance, life-cycle management and use of signing keys used to create digital signatures.

The present document is aimed to be used by independent bodies as the basis for a conformity assessment that a TSP can be trusted for operating a remote QSCD / SCDev. [i.1].

The present document supports European and other regulatory frameworks.

NOTE 2: Specifically, but not exclusively, the present document is aimed at qualified and non-qualified trust service managing remote qualified and non-qualified electronic signature/seal creation devices supporting electronic signatures and electronic seals (both advanced and qualified) in accordance with the requirements of Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1]. Annex A contains requirements specific for an SSAS in the context of Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1].

The present document does neither specify how fulfilment of the requirements can be assessed by an independent conformity assessment body, nor requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE 3: See ETSI EN 319 403 [i.3] for guidance on assessment of a TSP's processes and services.

NOTE 4: The present document references ETSI EN 319 401 [1] for general policy requirements common to all TSP services covered by ETSI standards.

The present document does not specify protocols used to access the SSAS.

NOTE 5: Protocols for remote digital signature creation are defined in ETSI TS 119 432 [i.4].

The present document identifies specific controls needed to address risks associated with services operating remote QSCD / SCDev.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[3] EN 419241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements", (produced by CEN).

[4] EN 419241-2: " Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing", (produced by CEN).

[5] EN 419221-5: "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services", (produced by CEN).

[6] ETSI TS 119 461: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components for identity proofing of trust service subjects".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.4] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.5] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.6] ISO/IEC 15408: "Information technology — Security techniques — Evaluation criteria for IT security".

[i.7] ISO/IEC 18014-2: "Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens".

[i.8] Void.

[i.9] Void.

[i.10] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.11] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.12] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.2] and the following apply:

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition or in a note.

authentication: provision of assurance in the claimed identity of an entity

NOTE: As defined in ISO/IEC 18014-2 [i.7].

digital signature value: result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

electronic identification (eID): process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

NOTE: As defined in Regulation (EU) No 910/2014 [i.1].

electronic identification means: material and/or immaterial unit containing person identification data and which is used for authentication for an online service

NOTE: As defined in Regulation (EU) No 910/2014 [i.1].

electronic identification means reference: data used in the SSAS as a reference to an electronic identification means in order to authenticate the signer

EXAMPLE: When the eID means uses asymmetric keys, the public key can be the reference.

When a signed assertion is generated after a successful authentication of the signer, the assertion signer id and the user id can be the reference.

When the eID means uses a secret key (e.g. one time password generator) the secret key can be the reference.

one-time signing key: signing key bound, certified, used and disposed based on a single authorization, linked to a single session signing DTBS/R(s)

NOTE 1: The definition is slightly different from the one in EN 419241-2 [4] to allow the usage of pre-generated signing keys.

NOTE 2: Contrary to general signing keys, which may be used in several signing sessions.

person identification data: set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.

NOTE: As defined in Regulation (EU) No 910/2014 [i.1].

Qualified electronic Signature/seal Creation Device (QSCD): As specified in Regulation (EU) No 910/2014 [i.1].

Remote QSCD: As specified in Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1].

remote signature creation device: signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf

Server Signing Application Service (SSAS): trust service consisting of a server signing application and a QSCD / SCDev to create a digital signature value on behalf of a signer

Server Signing Application Service Provider (SSASP): TSP operating a server signing application service component

Signature Creation device (SCDev): configured software or hardware used to implement the signature creation data and to create a digital signature value

trust service: electronic service that enhances trust and confidence in electronic transactions

Trust Service Provider (TSP): entity which provides one or more trust service

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certificate Authority
CID	Commission Implementing Decision
DTBS/R	Data To Be Signed Representation
eID	electronic IDentification
EUDI wallet	European Digital Identity wallet
EUSPv2	EU SSAS Policy
LSP	Lightweight SSAS Policy
NSP	Normalized SSAS Policy
OID	Object IDentifier
PIN	Personal Identification Number
QSCD	Qualified electronic Signature/Seal Creation Device
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCDev	Signature Creation Device
SP	SSAS Policy
SSAS	Server Signing Application Service
SSASP	Server Signing Application Service Provider
TSP	Trust Service Provider
URI	Uniform Resource Identifier

3.4 Notations

The requirements identified in the present document include:

a) requirements applicable to any SSAS policies. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) requirements applicable to the services offered under the applicable SSAS policy. Such requirements are indicated by clauses marked by the applicable SSAS policy as follows:

- "[LSP]", "[NSP]" and "[EUSPv2]".

The requirements in the present document are identified as follows:

- <3 letters service component> - < the clause number> - <2 digit number - incremental>

The SSAS service components are:

- **OVR:** General requirement (requirement applicable to more than 1 service component)
- **GEN:** Signing Key Generation Service
- **LNK:** Certificate/eID means Linking Service
- **SIG:** Signature Activation Service
- **DEL:** Signing Key Deletion Service
- **EID:** eID Means Provision (optional)

The management of the requirement identifiers throughout subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish a new requirement.
- The requirement identifier for deleted requirements are left and completed with "Void".
- The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 General concepts

4.1 General policy requirements concepts

The present document is structured broadly in line with ETSI EN 319 411-1 [2] to assist TSPs in applying these requirements to their own policy and practice statement documentation.

The present document incorporates EN 419241-1 [3] requirements by reference. EN 419241-1 [3] defines levels of assurance for sole control. The term "sole control" does not mean that the requirements are only applicable to electronic signatures as defined in Regulation (EU) No 910/2014 [i.1]. The requirements may be applied mutatis mutandis to electronic seals. In other words, the reader may replace the term "sole control" with "control" as explained in EN 419241-1 [3] clause 5.3.

NOTE 1: Any applicable and referenced requirements on the Trustworthy System Supporting Server Signing (TW4S) in EN 419241-1 [3] is a requirement on the SSAS.

The present document incorporates ETSI EN 319 401 [1] requirements by reference and adds requirements relevant for a SSASP. See ETSI EN 319 401 [1], clause 4 and IETF RFC 3647 [i.5], clauses 3.1 and 3.4 for guidance.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.

NOTE 2: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in operating signing devices. In some cases, reference is made to other more general standards which can be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic can vary.

The present document includes the provision of services for key generation, certificate linking, eID means linking, signature activation, key deletion and device provisioning (see clause 4.4).

4.2 Void

4.3 SSAS applicable documentation

4.3.1 SSAS practice statement

The **Server Signing Application Service Provider (SSASP)** develops, implements, enforces, and updates a **SSAS practice statement**, which is a trust service practice statement as defined in ETSI EN 319 401 [1], instantiated for a SSAS. See clause 6.1.

The SSAS practice statement describes how the SSASP operates its service and is owned by the SSASP. The SSAS practice is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSP. The recipients of the practice statement can be auditors, subscribers and relying parties.

NOTE: The presence of some elements is mandatory in the SSAS practice statement as requested in the present document, however the present document places no restriction on the form of the SSAS practice statement; it can be included in a general TSP practice statement document that covers other services delivered by that TSP or be a standalone document.

The present document provides requirements identified as necessary for SSAS policies defined in clause 4.3.2, to be endorsed by a SSASP and reflected in its **practice statement**.

4.3.2 SSAS policy

A SSAS Policy (SP) describes **what** is offered and can contain diverse information beyond the scope of the present document to indicate the applicability of the SSAS. A SP is defined independently of the specific details of the specific operating environment of a SSASP. The recipients of the SP can be auditors, subscribers and relying parties.

The present document defines three SPs:

1) A Lightweight SSAS Policy (LSP) offering a quality of service less onerous than the NSP (requiring less demanding policy requirements) for use where a risk assessment does not justify the additional burden of meeting all requirements of the NSP (e.g. use of a signature activation module).

2) A Normalized SSAS Policy (NSP) which meets general recognized best practice for TSPs operating a remote SCDev used in support of any type of transaction.

3) An EU SSAS v2 Policy (EUSPv2) which offers the same quality as that offered by the NSP but with specific requirements from the Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1] related to remote QSCD management.

NOTE: EUSPv2 specific requirements are defined in Annex A.

A SP is not necessarily part of the SSASP's documentation (as per ETSI EN 319 401 [1] a practice statement and general terms and conditions are sufficient); e.g. a SP can be shared by a community and not owned by the SSASP. Also, the present document does not put constraints on the form of the SP; a SP can be a stand-alone document or be provided as part of the practice statement and/or the general terms and conditions.

4.3.3 Terms and conditions

In addition to, or as part of, the SCP and the SSAS practice statement, a TSP issues terms and conditions. Terms and conditions can cover a broad range of commercial terms or technical terms. The terms and conditions are specific to a SSASP. The recipients of the terms and conditions are subscribers and relying parties.

NOTE: The presence of some elements is mandatory in the terms and conditions as requested in the present document, however the present document places no restriction on the form of terms and conditions; it can be a standalone document for a public audience, or it can be split over subscriber's agreement(s) and information to relying parties. The form and content of the terms and conditions can also depend on national regulations.

4.4 SSAS component services

NOTE 1: The present document does not mandate any subdivision of the services of a TSP. Requirements are stated in subsequent clauses.

The SSAS services are broken down in the present document into the following component services for the purposes of classifying requirements:

- **Signing key generation service:** generates signing keys in the remote device. The proof of possession of generated signing keys are passed to the registration service of the TSP issuing the associated certificate.
- **Certificate linking service:** links the certificates generated by the certificate generation service of a TSP with the corresponding signing keys.
- **eID means / identity linking service:** links either an eID means references or an identity with the corresponding signing keys in order to provide sole control. The second possibility is only applicable in case of a one-time signing key where it is assured that the identity in the certificate is the same as the one of the signer. The service can be used to support requirement REG-6.3.1-01 in ETSI EN 319 411-1 [2] for a TSP issuing certificates.

EXAMPLE 1: By providing an assertion of the authentication of the signer that is linked to the private key.

- **Signature activation service:** verifies the signature activation data and activates the corresponding signing key in order to create a digital signature.
- **Signing key deletion service:** destroys signing keys in a way that ensures that the signing keys cannot be used anymore.
- **eID means provision service (optional):** prepares and provides or makes eID means available to the signers.

EXAMPLE 2: A service which generates the authentication key and distributes the key to the subject of the certificate (this includes "soft" keys i.e. keys protected by software environment).

A service which prepares the authentication device and enabling codes, and distributes them to the subject of the certificate (this includes keys protected by hardware environment).

This subdivision of services is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the TSP's services.

Figure 1 illustrates the interrelationships between the service components of the present document and relations with external components of the TSP issuing the signing certificates.

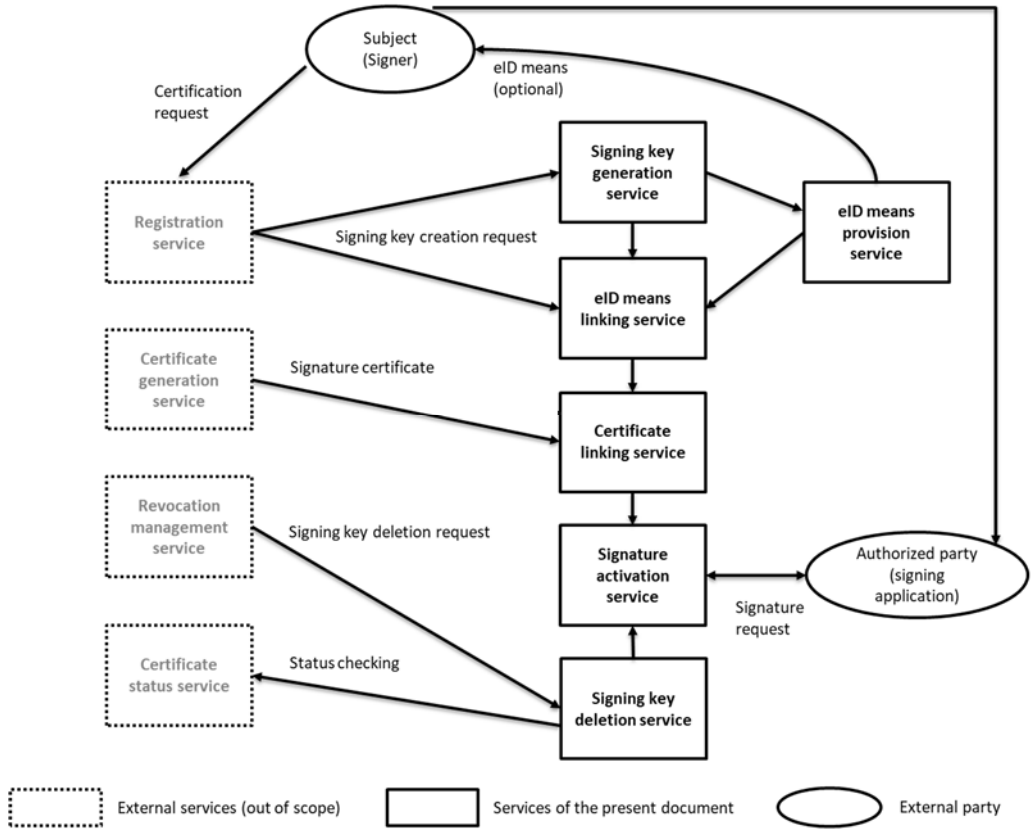

Figure 1: Illustration of subdivision of SSAS components

Figure 2 illustrates the interrelationships between the services of the present document and relations with an authentication process delegated to an external party.

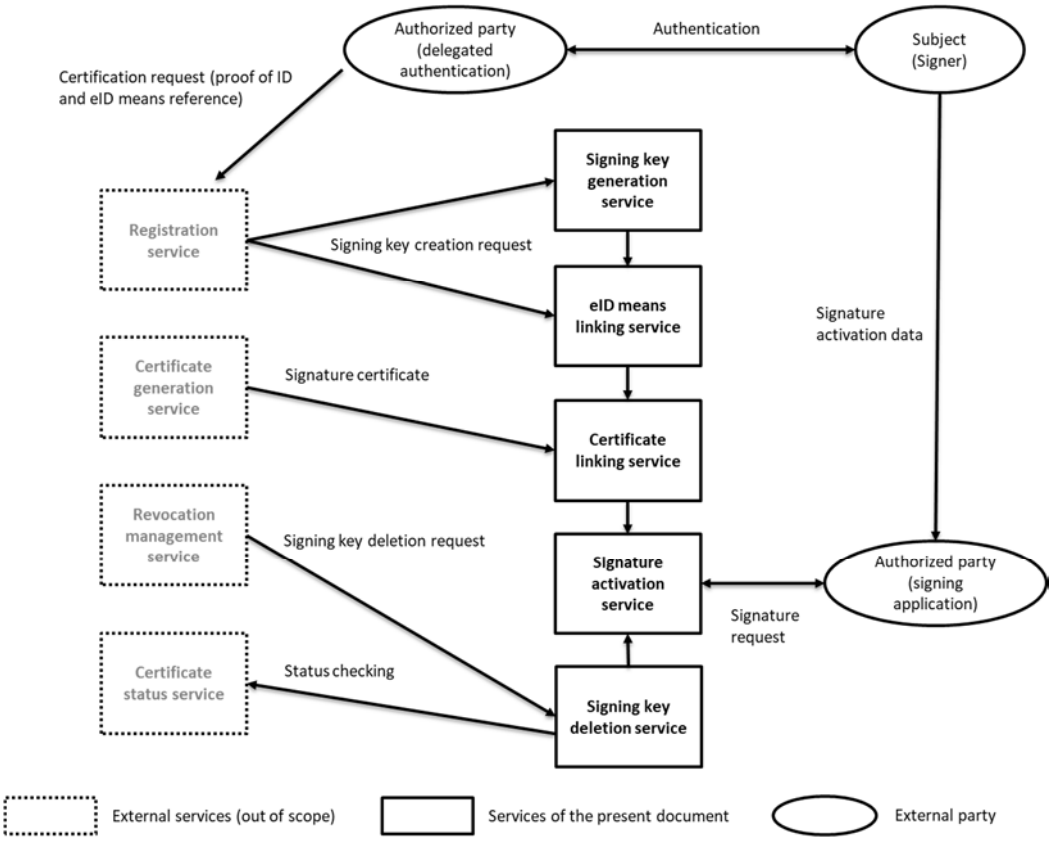

Figure 2: Illustration of subdivision of SSAS components with delegated authentication

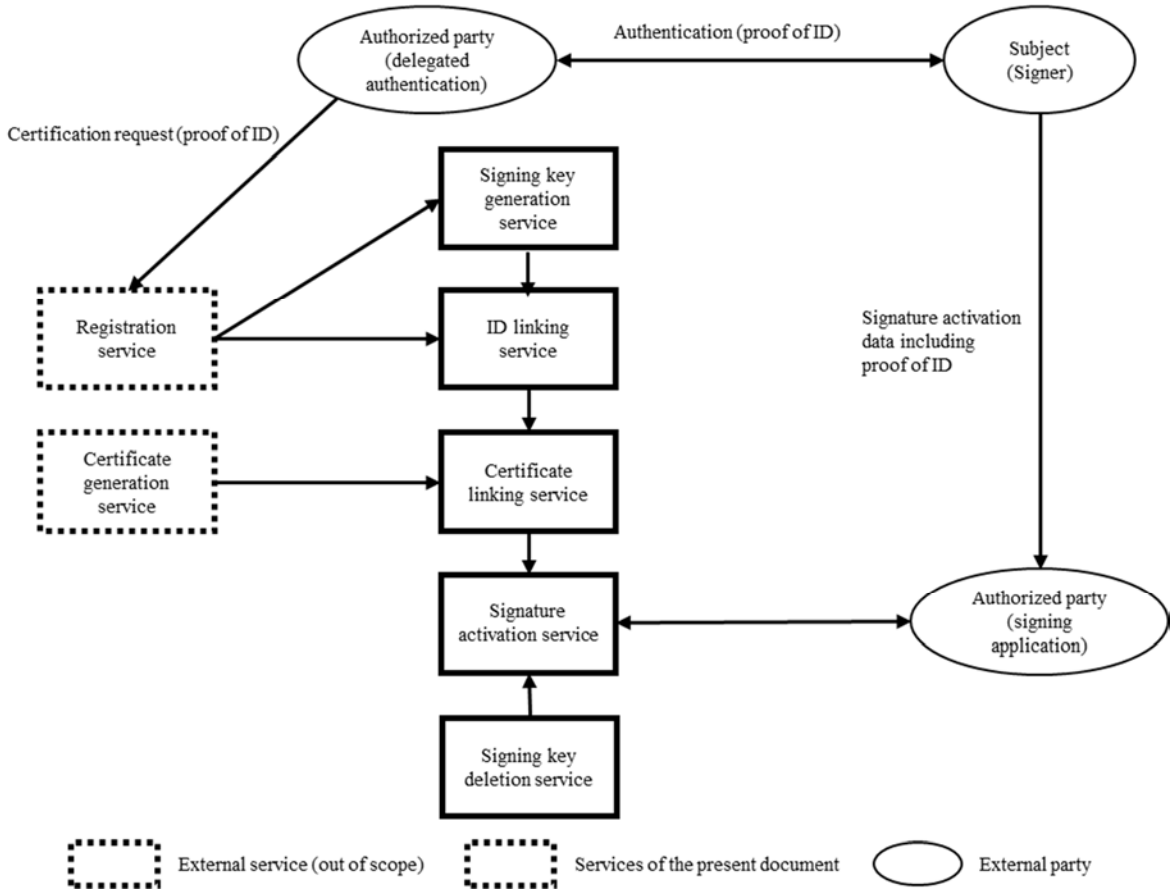

Figure 3: Illustration of subdivision of SSAS components for one-time signing keys with identity proofing without usage of eID means

NOTE 2: In the case of a one-time signing key, the key is deleted directly after the usage, not based on a revocation. The CA can still provide a revocation service and certification status service, but they are not linked to the (Q)SCD management anymore.

NOTE 3: Figures 1, 2 and 3 are for illustrative purposes and do not show a processing flow. Clause 6 specifies the specific requirements for each of the services.

5 General provisions on practice statement and policies

5.1 Practice statement requirements

OVR-5.1-01: The general requirements specified in ETSI EN 319 401 [1], clause 6.1 shall apply.

In addition, the following particular requirements apply:

NOTE 1: A TSP can document practices relating to specific SSAS policy requirements separate from the main practice statement document.

OVR-5.1-02: The TSP's practice statement shall include the signature algorithms and parameters applied, the algorithms applied for key pair generation and any other algorithms and parameters that are critical to the security of the SSAS operation.

OVR-5.1-03: The TSP shall publicly disclose its practice statement through an online means that is available on a 24×7 basis.

NOTE 2: The TSP is not obliged to disclose any aspects containing sensitive information.

5.2 SP name and identification

SSASPs following the present document can claim conformance to the present document via the following specific trust service policy OID:

a) LSP: Lightweight SSAS Policy

```
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops  (1)
policy-identifiers(1) lightweight (1)
```

b) NSP: Normalized SSAS Policy

```
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops(1)
policy-identifiers(1) normalized (2)
```

NOTE: Annex A defines an additional SSAS policy with specific requirements related to Regulation (EU) No 910/2014 [i.1].

OVR-5.2-01: If any changes are made to a SP as described in clause 4.3.2 which affects the applicability then the policy identifier should be changed.

5.3 Participants

5.3.1 SSASP

OVR-5.3.1-01: The SSASP may make use of other parties to provide parts of the service, however, the SSASP always maintains overall responsibility and shall ensure that the policy requirements identified in the present document are met.

NOTE: If the external party uses an eID means issued under a notified scheme that is included in the list published by the Commission pursuant to Article 9 of Regulation (EU) No 910/2014 [i.1], there is no need to demonstrate the conformance to the required level, conformance to the regulatory requirements can be assumed.

5.3.2 Subscriber and signer

In the framework of the present policies, the signer associated to the signing key can be:

- a natural person;
- a natural person identified in association with a legal person;
- a legal person (that can be an organization or a unit or a department identified in association with an organization); or
- a device or system operated by or on behalf of a natural or legal person.

NOTE: The present document does not place any specific restrictions on the legal representation implied by an electronic signature or seal created using the present document.

The relationship between the signer and the subscriber is equivalent to the relationship between subject and subscriber as described in ETSI EN 319 411-1 [2], clause 5.4.2.

6 Trust Service Providers practice

6.1 Publication and repository responsibilities

OVR-6.1-01: The TSP shall make available to subscribers and relying parties the applicable SPs, practice statements and terms and conditions regarding the use of signing keys.

OVR-6.1-02: The applicable terms and conditions shall be readily identifiable for a given signing key or for the associated certificate.

OVR-6.1-03: The information identified in **OVR-6.1-01** and **OVR-6.1-02** above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the SSAS practice statement.

OVR-6.1-04: The information identified in **OVR-6.1-01** above should be publicly and internationally available.

6.2 Signing key initialization

6.2.1 Signing key generation

GEN-6.2.1-01 [LSP]**:** Clause SRG_KM.1.1 of EN 419241-1 [3], specifying signing keys environment, shall apply.

GEN-6.2.1-02 [NSP]**:** Clause SRA_SKM.1.1 of EN 419241-1 [3], specifying signing keys environment, shall apply.

GEN-6.2.1-02A [NSP]**:** Signer's signing key shall be generated and used in a SCDev certified conformant to EN 419221-5 [5].

GEN-6.2.1-03: Clause SRG_KM.1.2 of EN 419241-1 [3], specifying cryptographic algorithms and key lengths, shall apply.

GEN-6.2.1-04: Clause SRG_KM.1.3 of EN 419241-1 [3], specifying key protection, shall apply.

GEN-6.2.1-05: Clause SRG_KM.1.4 of EN 419241-1 [3], specifying device initialization, shall apply.

GEN-6.2.1-06: Clause SRC_SKS.1.1 of EN 419241-1 [3], specifying algorithm parameters, shall apply.

GEN-6.2.1-07: Clause SRC_SKS.1.3 of EN 419241-1 [3], specifying time of generation, shall apply.

GEN-6.2.1-08 [CONDITIONAL]**:** If the SSAS and the certificate generation service are managed separately, then the SSAS shall support the requirement defined in clause REG-6.3.1-01 of ETSI EN 319 411-1 [2].

EXAMPLE: By providing an assertion of the authentication of the signer that is linked to the private key.

GEN-6.2.1-09 [CONDITIONAL]**:** In case of a one-time signing key, the key shall be bound to exactly one signature session.

6.2.2 eID means or identity linking

NOTE 1: The signing key is either linked to an eID means which is linked to the identity or directly to the identity. The latter is only possible in a process using a one-time signing key.

LNK-6.2.2-00 [CONDITIONAL]**:** In case a one-time signing key is used, the key and the authentication may be linked directly to the identity instead of the linking to the eID means.

LNK-6.2.2-01: Void.

LNK-6.2.2-01A [LSP]**:** Clause SRC_SA.1.1 of EN 419241-1 [3], specifying enrolment, shall apply.

LNK-6.2.2-02 [NSP]**:** Void.

LNK-6.2.2-02A [NSP] [CONDITIONAL]**:** If the signer is a natural person, the identity proofing and verification shall be as specified in clause A.1.2 of EN 419241-1 [3], for assurance level substantial or higher.

LNK-6.2.2-02B [NSP] [CONDITIONAL]**:** If the signer is a legal person, the identity proofing and verification shall be as specified in clause A.1.3 of EN 419241-1 [3], for assurance level substantial or higher.

LNK-6.2.2-02C [NSP]**:** The application and registration during enrolment of the signer shall be as specified in clause A.1.1 of EN 419241-1 [3].

LNK-6.2.2-02D [NSP] [CONDITIONAL]**:** In case the authentication is linked to an eID means, the electronic identification means characteristics and design shall be as specified in clause A.2.1 of EN 419241-1 [3], for assurance level substantial or higher.

LNK-6.2.2-02E [NSP] [CONDITIONAL]**:** In case the authentication is linked to an eID means, the authentication mechanism shall be as specified in clause A.2.2 of EN 419241-1 [3], for assurance level substantial or higher.

LNK-6.2.2-03: Void.

LNK-6.2.2-03A [CONDITIONAL]**:** In case the authentication is linked to an eID means, the SSASP shall link signing keys with the appropriate signer's eID means reference.

LNK-6.2.2-03B [CONDITIONAL]**:** In case the authentication is linked directly to the identity, the SSASP shall link the one-time signing key with the specific identity.

LNK-6.2.2-04: The SSASP may generate eID means reference and provide the corresponding eID means to the signer (see clause 6.2.4).

LNK-6.2.2-05: The SSASP shall ensure that the person identification data linked to the eID means reference or the identity is the same as the one linked to the subject of the associated certificate.

NOTE 2: When the eID means reference is provided by the TSP issuing certificates registration service, the conformance to this requirement can be assumed.

LNK-6.2.2-06: The signer's eID means reference may be provided by an authorized (external) party.

LNK-6.2.2-07: Void.

LNK-6.2.2-07A [LSP] [CONDITIONAL]**:** If all or part of the authentication process is delegated to an external party the SSASP shall ensure the external party meets the requirements specified in LNK-6.2.2-01A and LNK-6.2.2-03A or LNK-6.2.2-03B.

NOTE 3: If the external party uses an eID means issued under a notified scheme that is included in the list published by the Commission pursuant to Article 9 of Regulation (EU) No 910/2014 [i.1] or an EUDI wallet as defined in article 5a in Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1] and which correspond to the needed level of assurance, there is no need to demonstrate the conformance to the required level, conformance to the regulatory requirements can be assumed.

LNK-6.2.2-08 [NSP] [CONDITIONAL]**:** If all or part of the authentication process is delegated to an external party the SSASP shall ensure that the external party meets the requirements specified in LNK-6.2.2-02A, LNK-6.2.2-02B, LNK-6.2.2-02C, LNK-6.2.2-02D, LNK-6.2.2-02E and LNK-6.2.2-03A or LNK-6.2.2-03B.

LNK-6.2.2-08A [NSP] [CONDITIONAL]**:** If all of the authentication process is delegated to an external party the SSASP shall ensure that the secret key material used to authenticate the delegated party to the SAM shall reside in a certified cryptographic module consistent with the requirement as defined in SRG_KM.1.1 of EN 419241-1 [3].

EXAMPLE 1: The authentication of the delegated party can be done by using a signed assertion where the key material resides in a certified cryptographic module.

EXAMPLE 2: In case the authentication is linked directly to the identity, the external party can be an identity service provider to whom the authentication process is delegated. In that case the identity service provider is authenticated using the key material.

NOTE 4: A delegation takes place if the authentication process is done outside of the qualified trust service.

LNK-6.2.2-09 [NSP] [CONDITIONAL]**:** If all or part of the authentication process is delegated to an external party the SSASP shall ensure that:

- the external party fulfils all the relevant requirements of the present document and the requirements for registration according to the applicable regulatory requirements; or

NOTE 5: In the context of the European Union, the applicable regulatory requirements are defined in Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1].

- the authentication process delegated to the external party uses an eID means issued under a notified scheme in accordance with the applicable regulatory requirements.

NOTE 6: In the context of the European Union, the list of electronic identification means, issued under notified schemes, is published by the European Commission pursuant to Article 9 of Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1].

NOTE 7: The EUDI wallet as defined in article 5a in Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1] respects the requirements of an electronic identification means of level high.

LNK-6.2.2-10: Void.

LNK-6.2.2-10A: The SSASP shall protect the integrity of links between signer's signing key and its eID means reference if this is used or the provided identity otherwise.

6.2.3 Certificate linking

LNK-6.2.3-01: Clause SRC_SKS.1.2 of EN 419241-1 [3], specifying certificate linking, shall apply to the SSAS.

LNK-6.2.3-02: Clause SRC_SKS.1.4 of EN 419241-1 [3], specifying certificate linking, shall apply to the SSAS.

LNK-6.2.3-03: Clause SRC_SKS.1.5 of EN 419241-1 [3], specifying links protection, shall apply to the SSAS.

6.2.4 eID means provision

EID-6.2.4-01 [CONDITIONAL]**:** If the SSASP provides the signer's eID means, the eID means shall be securely passed to the signer.

EID-6.2.4-02 [CONDITIONAL]**:** If the SSASP personalizes the signer's eID means with an associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signer's eID means.

6.3 Signing key life-cycle operational requirements

6.3.1 Signature activation

SIG-6.3.1-01: Clause SRC_SA.1.2 of EN 419241-1 [3], specifying authentication, shall apply.

SIG-6.3.1-02: Clause SRC_SA.1.3 of EN 419241-1 [3], specifying protocol security, shall apply.

SIG-6.3.1-03: Clause SRC_SA.1.4 of EN 419241-1 [3], specifying access control, shall apply.

SIG-6.3.1-04: Clause SRC_SA.1.5 of EN 419241-1 [3], specifying signing key control, shall apply.

SIG-6.3.1-05 [NSP]**:** Clause SRA_SKM.2.1 of EN 419241-1 [3], specifying signing key activation, shall apply.

SIG-6.3.1-06 [NSP]**:** Clause SRA_SAP.1.2 of EN 419241-1 [3], specifying protocol security, shall apply.

SIG-6.3.1-07 [NSP]**:** Clause SRA_SKM.2.5 of EN 419241-1 [3], specifying signing key control, shall apply.

SIG-6.3.1-08: The SSASP should ensure that the public key certificate is valid before using the corresponding signing key.

NOTE 1: valid = not expired not revoked not suspended, can be met by applying DEL-6.3.2-01 if suspension is not used.

SIG-6.3.1-09: Signing keys shall be usable in only those cases for which the signer's consent has been obtained.

SIG-6.3.1-10: Clause SRC_DSC.1.1 of EN 419241-1 [3], specifying signature creation's algorithm parameters, shall apply.

SIG-6.3.1-11 [CONDITIONAL]**:** In case the authentication is linked directly to the identity, the SAD shall contain the unique identifier of the signature session which shall be uniquely linked to the SSAS.

SIG-6.3.1-12 [CONDITIONAL]**:** In case the authentication is linked directly to the identity, the SAD shall contain the unique identifier of the identity verification process.

SIG-6.3.1-13 [CONDITIONAL]**:** In case the authentication is linked directly to the identity, the signature session shall be linked:

1) either exactly to one SAD which contains the references of all documents that shall be signed within this session;

2) or to multiple SAD values if and only if multiple consecutive signatures are applied to the same document, where each signature covers the previous ones.

EXAMPLE 1: In PAdES each new signature covers the previous ones.

NOTE 2: The unique identifier of the signature session can be used to identify the "default or selected" signing key in the SAD as requested in SRA_SAP.2.3 of EN 419241-1 [3].

NOTE 3: The unique identifier of the identity verification process can be used to identify the authenticated signer in the SAD as requested in SRA_SAP.2.3 of EN 419241-1 [3].

SIG-6.3.1-14 [CONDITIONAL]**:** In case the authentication is linked directly to the identity, the signature session shall end at most 2 hours after the end of the identity verification process.

NOTE 4: The identity verification process includes not only the interaction with the subject of the identity verification, but also all processing needed to have a verified result in the end.

NOTE 5: In case the authentication is linked to an eID, then identity verification of the eID link can be used for longer periods of time, because the authentication factors allow to guarantee a strong link to the identity.

SIG-6.3.1-15 [NSP] [CONDITIONAL]**:** In case the signer is a natural person and the authentication is linked directly to the identity, the SAP shall include an explicit action (not just a checkbox) of the signer to approve the authorization to sign the content of the specific documents referenced in the SAD.

SIG-6.3.1-16 [NSP] [CONDITIONAL]**:** In case the signer is a legal person and the authentication is linked directly to the identity, the SAP shall include an explicit action (not just a checkbox) of the natural person identified during the identity verification process and which is allowed to sign in the name of the legal person to approve the authorization to confirm the origin and integrity of the specific documents referenced in the SAD.

EXAMPLE 2: An explicit action can be scrolling to the end of the document before clicking on an acceptance button or typing "I agree to sign this contract".

6.3.2 Signing key deletion

DEL-6.3.2-01: Clause SRG_KM.7.1 of EN 419241-1 [3] shall apply. If the public key certificate is revoked, the corresponding signing key shall be destroyed.

DEL-6.3.2-02: The SSASP shall destroy a signing key when requested by the signer.

DEL-6.3.2-03: Clause SRG_KM.7.2 of EN 419241-1 [3], specifying session management, shall apply.

DEL-6.3.2-04: Clause SRG_KM.7.3 of EN 419241-1 [3], specifying key backup deletion, shall apply.

DEL-6.3.2-05 [CONDITIONAL]**:** In case of a one-time signing key, the key shall be deleted immediately after the end of the signature session.

6.3.3 Signing key backup and recovery

GEN-6.3.3-01: Clause SRG_KM.2.1 of EN 419241-1 [3], specifying key backup, shall apply.

GEN-6.3.3-02: Clause SRG_KM.2.2 of EN 419241-1 [3], specifying backup protection, shall apply.

GEN-6.3.3-03: Clause SRG_KM.2.3 of EN 419241-1 [3], specifying backup controls, shall apply.

GEN-6.3.3-04: The number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

6.4 Facility, management, and operational controls

6.4.1 General

OVR-6.4.1-01: The requirements identified in ETSI EN 319 401 [1], clauses 5, 6.3 and 7.3 shall apply.

6.4.2 Physical security controls

OVR-6.4.2-01: The requirements identified in ETSI EN 319 401 [1], clause 7.6 shall apply.

In addition, the following particular requirements apply:

OVR-6.4.2-02: The requirements identified in ETSI EN 319 411-1 [2], clause OVR-6.4.2-02 to OVR-6.4.2-10 shall apply mutatis mutandis to signing key generation and activation management services.

6.4.3 Procedural controls

OVR-6.4.3-01: Void.

OVR-6.4.3-01A: The requirements REQ-7.4-03X, REQ-7.4-04X and REQ-7.4-07X to REQ-7.4-12X in ETSI EN 319 401 [1] shall apply.

6.4.4 Personnel controls

OVR-6.4.4-01: The requirements identified in ETSI EN 319 401 [1], clause 7.2 shall apply.

6.4.5 Audit logging procedures

OVR-6.4.5-01: The requirements identified in ETSI EN 319 401 [1], clause 7.10 shall apply.

OVR-6.4.5-02: All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and SSAS system access attempts.

OVR-6.4.5-03: Clause SRG_AA.1 of EN 419241-1 [3], specifying audit data generation, shall apply.

OVR-6.4.5-04: Clause SRG_AA.2 of EN 419241-1 [3], specifying audit data availability, shall apply.

OVR-6.4.5-05: Clause SRG_AA.3 of EN 419241-1 [3], specifying audit data parameters, shall apply.

OVR-6.4.5-06: Clause SRG_AA.7 of EN 419241-1 [3], specifying audit data integrity, shall apply.

OVR-6.4.5-07: Clause SRG_AA.8 of EN 419241-1 [3], specifying audit data timing, shall apply.

6.4.6 Records archival

OVR-6.4.6-01: The SSASP shall retain the audit data records for at least seven years after any certificate based on these records ceases to be valid and within the constraint of applicable legislation.

6.4.7 Key changeover

No policy requirement.

6.4.8 Compromise and disaster recovery

OVR-6.4.8-01: The requirements identified in ETSI EN 319 401 [1], clauses 7.9 and 7.11 shall apply.

6.4.9 SSASP service termination

OVR-6.4.9-01: The requirements identified in ETSI EN 319 401 [1], clause 7.12 shall apply.

6.5 Technical security controls

6.5.1 Systems and security management

OVR-6.5.1-01: The requirements identified in EN 419241-1 [3], clause SRG_M.1 shall apply.

6.5.2 Systems and operations

OVR-6.5.2-01: The requirements identified in EN 419241-1 [3], clause SRG_SO.1 shall apply.

OVR-6.5.2-02: The requirements identified in EN 419241-1 [3], clause SRG_SO.2 shall apply.

6.5.3 Computer security controls

OVR-6.5.3-01: Void.

OVR-6.5.3-01A: The requirements REQ-7.4-01, REQ-7.4-02X, REQ-7.4-05X, REQ-7.4-06X and REQ-7.4-13X in ETSI EN 319 401 [1] shall apply.

NOTE: Requirements for the trustworthy systems can be ensured using, for example, systems conforming to EN 419241-1 [3] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [i.6].

OVR-6.5.3-02: Clause SRG_AA.6.1 of EN 419241-1 [3], regarding system monitoring shall apply.

6.5.4 Life cycle security controls

OVR-6.5.4-01: The requirements identified in ETSI EN 319 401 [1], clause 7.7 and 7.14 shall apply.

6.5.5 Network security controls

OVR-6.5.5-01: The requirements identified in ETSI EN 319 401 [1], clause 7.8 shall apply.

6.6 Compliance audit and other assessment

NOTE: See ETSI EN 319 403 [i.3].

6.7 Other business and legal matters

6.7.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

6.7.2 Financial responsibility

OVR-6.7.2-01: Void.

NOTE: Financial responsibility is covered in clause 6.8.1 of the present document by OVR-6.8.1-01.

6.7.3 Confidentiality of business information

No policy requirement.

6.7.4 Privacy of personal information

OVR-6.7.4-01: The requirement REQ 7.13-05 identified in ETSI EN 319 401 [1] shall apply.

6.7.5 Intellectual property rights

No policy requirement.

6.7.6 Representations and warranties

NOTE 1: Representations and warranties is covered in clause 6.5.4 of the present document by OVR-6.5.4-01 which covers also REQ-7.14.3-01X and REQ-7.14.3-02X identified in ETSI EN 319 401 [1].

NOTE 2: The SSASP has the responsibility for conformance with the procedures prescribed in this policy, even when the SSASP's functionality is undertaken by outsourcers.

6.7.7 Disclaimers of warranties

See clause 6.7.6.

6.7.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.8.4.

6.7.9 Indemnities

No policy requirement.

6.7.10 Term and termination

No policy requirement.

6.7.11 Individual notices and communications with participants

No policy requirement.

6.7.12 Amendments

No policy requirement.

6.7.13 Dispute resolution procedures

OVR-6.7.13-01: Void.

NOTE: Dispute resolution procedures is covered in clause 6.8.1 and 6.8.1 of the present document by OVR-6.8.1-01 and OVR-6.8.4-04.

6.7.14 Governing law

Not in the scope of the present document.

6.7.15 Compliance with applicable law

OVR-6.7.15-01: The requirements REQ-7.13-01 and REQ-7.13-02 identified in ETSI EN 319 401 [1] shall apply.

6.7.16 Miscellaneous provisions

No policy requirement.

6.8 Other provisions

6.8.1 Organizational

OVR-6.8.1-01: The requirements identified in ETSI EN 319 401 [1], clause 7.1 shall apply.

6.8.2 Additional testing

No policy requirement.

6.8.3 Disabilities

OVR-6.8.3-01: The requirements REQ-7.13-03 and REQ-7.13-04 identified in ETSI EN 319 401 [1] shall apply.

6.8.4 Terms and conditions

OVR-6.8.4-01: The requirements identified in ETSI EN 319 401 [1], clause 6.2 shall apply.

7 Framework for definition of server signing application service policy built on the present document

OVR-7-01 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 and 6.

OVR-7-02 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, the policy shall identify any variances it chooses to apply.

OVR-7-03 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, subscribers shall be informed, as part of implementing the terms and conditions, of the ways in which the specific policy adds to or further constrains the requirements of the policy as defined in the present document.

OVR-7-04 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the policy.

OVR-7-05 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, a risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability.

OVR-7-06 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, the policy should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.

OVR-7-07 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, a defined review process should exist to ensure that the policy is supported by the practices statements.

OVR-7-08 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, the TSP should make available the policies supported by the TSP to its user community.

OVR-7-09 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, revisions to policies supported by the TSP should be made available to subscribers.

OVR-7-10 [CONDITIONAL]**:** When building a SP from requirements defined in the present document, a unique object identifier shall be obtained for the policy (e.g. OID or URI).

Annex A (normative): Specific requirements related to Regulation (EU) 2024/1183

A.1 SSASP as a Qualified TSP

The present annex specifies generally applicable policy and security requirements for a Qualified TSP managing a remote QSCD.

OVR-A.1-01: Void.

A.2 Policy name and identification

SSASPs following the present document can claim conformance to the present document via the following specific trust service policy OID:

- EUSPv2: EU SSAS Policy

```
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops  (1)
policy-identifiers(1) eu-remote-qscd-v2 (4)
```

A.3 General requirements

OVR-A.3-01 [EUSPv2]**:** All requirements specified for [NSP] shall apply.

OVR-A.3-02 [EUSPv2]**:** The TSP's practice statement shall include the reference to the certification that the QSCD employed against the requirements of Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [i.1], annex II.

NOTE: CID (EU) 2016/650 [i.12] lays down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014. However, it was published before the publication of EN 419241-1 [3] and EN 419241-2 [4] which are not taken into account.

OVR-A.3-03 [EUSPv2]**:** The SSASP shall comply with any requirements identified in the certification report of the specific remote qualified electronic signature creation device.

A.4 Signing key generation

GEN-A.4-01 [EUSPv2]**:** Signer's signing key shall be generated in a QSCD.

GEN-A.4-02 [EUSPv2]**:** The QSCD shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

A.5 Signature activation

SIG-A.5-01 [EUSPv2]**:** Signer's signing key shall be used in a QSCD.

SIG-A.5-02 [EUSPv2]**:** The QSCD shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

SIG-A.5-03 [EUSPv2]**:** Clause SRA_SAP.1.3 of EN 419241-1 [3], specifying cryptographic strength, shall apply.

SIG-A.5-04 [EUSPv2]**:** Clause SRA_SAP.1.4 of EN 419241-1 [3], specifying threats mitigation, shall apply.

SIG-A.5-05 [EUSPv2]**:** Clause SRA_SAP.1.5 of EN 419241-1 [3], specifying environment protection, shall apply.

SIG-A.5-06 [EUSPv2]**:** Clause SRA_SAP.1.6 of EN 419241-1 [3], specifying protection against tampering, shall apply.

SIG-A.5-07 [EUSPv2]**:** Clause SRA_SAP.1.7 of EN 419241-1 [3], specifying protection against attacker, shall apply.

SIG-A.5-08 [EUSPv2]**:** The SAM should be certified to be conformant to EN 419241-2 [4].

SIG-A.5-09 [EUSPv2] [CONDITIONAL]**:** In case the authentication is linked directly to the identity, the signature session shall end at most 30 minutes after the end of the identity verification process.

A.6 Signature activation data management

SIG-A.6-01 [EUSPv2]**:** Clause SRA_SAP.2.1 of EN 419241-1 [3], specifying signature activation data format, shall apply.

SIG-A.6-02 [EUSPv2]**:** Clause SRA_SAP.2.2 of EN 419241-1 [3], specifying signature activation data collection and generation, shall apply.

SIG-A.6-03 [EUSPv2]**:** Clause SRA_SAP.2.3 of EN 419241-1 [3], specifying signature activation data parameters, shall apply.

SIG-A.6-04 [EUSPv2]**:** Clause SRA_SAP.2.4 of EN 419241-1 [3], specifying signature activation data usage, shall apply.

SIG-A.6-05 [EUSPv2]**:** Clause SRA_SAP.2.5 of EN 419241-1 [3], specifying signature activation data destination, shall apply.

SIG-A.6-06 [EUSPv2]**:** Void.

SIG-A.6-06A [EUSPv2]**:** Clause SRA_SAP.2.6 of EN 419241-1 [3], specifying signature activation data collection and protection, shall apply.

SIG-A.6-07 [EUSPv2] [CONDITIONAL]**:** If the signer is a natural person, clause SRA_SAP.2.7 of EN 419241-1 [3], specifying signature activation data submission under sole control, shall apply.

SIG-A.6-07A [EUSPv2] [CONDITIONAL]**:** If the signer is a legal person, clause SRA_SAP.2.7 of EN 419241-1 [3], specifying signature activation data submission shall apply where "sole control" is replaced by "control".

SIG-A.6-08 [EUSPv2]**:** Clause SRA_SAP.2.8 of EN 419241-1 [3], specifying signature activation data protection after activation, shall apply.

A.7 eID means linking

LNK-A.7-01 [EUSPv2]**:** The identity proofing of the signer shall fulfil the requirements of extended Level of Identity Proofing (LoIP) as defined in ETSI TS 119 461 [6].

Annex B (informative): Regulation and EU SSAS policy mapping

B.1 Void

Table B.1: Void

Table B.2: Void

B.2 Regulation (EU) 2024/1183

Table B.3 identifies how the security controls objectives and other parts of the EU SSAS policy (EUSPv2) defined in the present document address the requirement of TSP managing remote QSCD as defined in Regulation (EU) 2024/1183 [i.11] in the context of electronic signatures or seals.

Table B.3: Electronic signature context

Article 29 Requirements for qualified electronic signature creation devices	**EUv2 SSAS policy reference**
"1a. Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device."	SIG-A.6-01: signature activation data format. SIG-A.6-02: signature activation data collection and generation. SIG-A.6-03: signature activation data parameters. SIG-A.6-04: signature activation data usage. SIG-A.6-05: signature activation data destination. SIG-A.6-06A: signature activation data collection and protection. SIG-A.6-07: signature activation data submission under sole control. SIG-A.6-08: signature activation data protection after activation. SIG-A.7-01: eID means linking.
Article 29a Requirements for a qualified service for the management of remote qualified electronic signature creation devices	**EUv2 SSAS policy reference**
"1. The management of remote qualified electronic signature creation devices as a qualified service shall be carried out only by a qualified trust service provider that: *(a) generates or manages electronic signature creation data on behalf of the signatory;"*	GEN-A.4-01, GEN-A.4-02, SIG-A.5-01 to SIG-A.5-08, SIG-A.6-01 to SIG-A.6-08
"(b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data for back-up purposes only, provided that the following requirements are met: *(i) the security of the duplicated datasets must be at the same level as for the original datasets;* *(ii) the number of duplicated datasets must not exceed the minimum needed to ensure continuity of the service;"*	GEN-6.3.3-02: backup protection. GEN-6.3.3-04: backup minimum datasets.
"(c) complies with any requirements identified in the certification report of the specific remote qualified electronic signature creation device issued pursuant to Article 30."	GEN-A.3-03, GEN-A.4-02, SIG-A.5-02

Article 39	**EUv2 SSAS policy reference**
Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.	SIG-A.6-01: signature activation data format. SIG-A.6-02: signature activation data collection and generation. SIG-A.6-03: signature activation data parameters. SIG-A.6-04: signature activation data usage. SIG-A.6-05: signature activation data destination. SIG-A.6-06A: signature activation data collection and protection. SIG-A.6-07A: signature activation data submission under sole control. SIG-A.6-08: signature activation data protection after activation. SIG-A.7-01: eID means linking.
Article 39a Requirements for a qualified service for the management of remote qualified electronic seal creation devices	**EUv2 SSAS policy reference**
"Article 29a shall apply mutatis mutandis to a qualified service for the management of remote qualified electronic seal creation devices."	GEN-A.4-01, GEN-A.4-02, SIG-A.5-01 to SIG-A.5-08, SIG-A.6-01 to SIG-A.6-08 GEN-6.3.3-02: backup protection. GEN-6.3.3-04: backup minimum datasets. GEN-A.3-03, GEN-A.4-02, SIG-A.5-02
***ANNEX II* Requirements for qualified electronic signature creation devices**	**EUv2 SSAS policy reference**
"1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: *(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;* *(b) the electronic signature creation data used for electronic signature creation can practically occur only once;* *(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;* *(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others."*	GEN-A.4-01: signing keys generated in a QSCD. GEN-A.4-02: QSCD configuration and operation.
"2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing."	SIG-A.5-01: signing keys used in a QSCD. SIG-A.5-02: QSCD configuration and operation.

Annex C (informative): Scope of remote signing standards

C.1 Scope of remote signing standards

Figure C.1 illustrates the different standards applicable for a remote signature creation service.

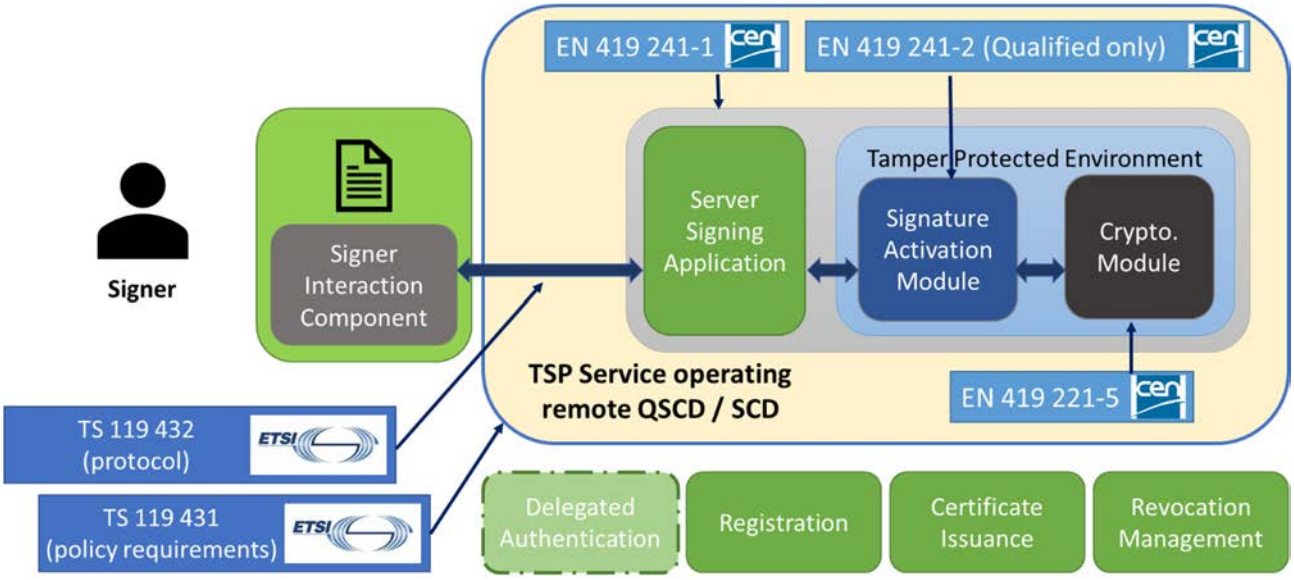

Figure C.1: Scope of standards on the different remote signing components

Annex D (informative): Change history

Date	Version	Information about changes
February 2021	V1.1.2	CR #1 minor changes to clarify the requirements
February 2024	V1.2.2	Draft to align with eIDASv2
September 2024	V1.2.3	CR #1 Several small corrections found when reviewing the document CR #2 Removing the mention of service component CR #4 Changes of identity proofing requirements CR #5 Alignment with latest version of ETSI EN 319 401
October 2024	V1.2.4	CR#3 no mandatory authorization for one-time signing keys Some minor corrections
November 2024	V1.2.5	Some minor changes. The requirement including SAM (**LNK-6.2.2-08A**) is limited to NSP and above

History

Document history		
V1.1.1	December 2018	Publication
V1.2.1	May 2021	Publication
V1.3.1	December 2024	Publication