ETSI TS 119 431-2 V1.1.1 (2018-12)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for trust service providers;
Part 2: TSP service components supporting AdES digital signature creation

Reference
DTS/ESI-0019431-2

Keywords
electronic signature, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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

The present document is part 2 of a multi-part deliverable covering Policy and security requirements for trust service providers, as identified below:

Part 1: "TSP service components 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 service components creating AdES digital signatures. The TSP service component relies either on remote server signing or on a signature creation device in the user's environment to create digital signature.

These requirements are based on the general policy requirements specified in ETSI EN 319 401 [9] and consider related requirements from ETSI TS 119 101 [1].

Introduction

The creation of digital signatures can involve different tasks provided by trust service providers. This can cover not only the creation and management of certificates as described in ETSI EN 319 411-1 [i.7] but also the management of signing keys as described in ETSI TS 119 431-1 [i.8] or the creation of the AdES digital signature as described in the present document.

The present document gives no restrictions on where signing key management is done. It can be handled either by a server signing application service component SSASC as described in ETSI TS 119 431-1 [i.8] or directly by the client in a signature creation device (SCDev).

1 Scope

The present document provides policy and security requirements for trust service providers (TSP) implementing a service component supporting AdES digital signature creation. This component contains a signature creation application and is thus called signature creation application service component (SCASC). However, it is more than just the SCA. It contains service elements around which parts of the driving application as defined in ETSI TS 119 102-1 [1] and ETSI TS 119 101 [2] can be implemented. The present document does not give restrictions on whether something is covered within a signature creation application or outside, as long as it is done by the SCASC.

The present document gives no restrictions on the type of TSP implementing such a service component.

The present document aims at supporting the creation of digital signatures in European and other regulatory frameworks.

NOTE 1: Specifically, but not exclusively, the present document is aimed at trust services, supporting the creation of digital signatures in accordance with the requirements of the Regulation (EU) No 910/2014 [i.1] for electronic signatures and electronic seals (both advanced and qualified). Annex B contains specific requirements for SCASC in the context of Regulation (EU) No 910/2014 which aim at providing best practice requirements for the creation of advanced electronic signatures and seals based on X.509 certificates.

NOTE 2: Specifically, but not exclusively, digital signatures in the present document can be used to create electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

The present document may be used by competent bodies as the basis for confirming that an organization is trustworthy in creating AdES digital signatures.

NOTE 3: See ETSI EN 319 403 [i.6] for guidance on assessment of TSP processes and services.

The SCASC has connections with external (trust) services that can be contacted for example for provisioning information to be included within the signature. The present document does not put requirements on the trust service policy applied by such external services.

The present document does not specify any protocol used to access the SCASC or how the SCACS can contact an SSASC or an SCDev.

NOTE 4: Protocols to contact a SCASC or a SSASC are defined in ETSI TS 119 432 [i.9].

The present document identifies specific controls needed to address specific risks associated with services providing AdES signature creation.

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 at https://docbox.etsi.org/Reference.

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 TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[2] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[3] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[4] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[5] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[6] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[7] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[8] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

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

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 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 TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents". .

[i.4] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing; Part 1: General System Security Requirements".

[i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.8] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.9] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

3 Definition of terms, 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:

AdES (digital) signature: digital signature that is either a CAdES signature, or a PAdES signature or a XAdES signature

digital signature: data appended to, or a 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

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

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: application using a remote signature creation device to create a digital signature value on behalf of a signer

server signing application service component: TSP service component employing a server signing application

server signing application service provider: TSP operating a server signing application service component

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose

NOTE: Signature applicability rules can be implicit, or can be stated in a human readable document and/or in a machine processable from. ETSI TS 119 172-1 [i.3] can be used for this purpose.

signature creation application: application within the signature creation system that creates the AdES digital signature and relies on the SCDev to create a digital signature value

NOTE: The SCDev can be managed by the SSASC.

signature creation application service component: TSP service component employing a signature creation application

signature creation application service provider: TSP operating a signature creation application service component

signature creation constraint: criteria used when creating a digital signature

signature creation device: configured software or hardware used to implement the signature creation data and to create a digital signature value

signature creation policy: set of **signature creation constraints** processed or to be processed by the SCA

signature creation service: TSP service implementing a signature creation application and/or a server signing application

signature creation service provider: service provider offering a signature creation service

NOTE: As in CEN EN 419 241-1 i.4.

3.2 Abbreviations

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

CA	Certification Authority
DTBS	Data To Be Signed
DTBSR	Data To Be Signed Representation
OID	Object IDentifier

QES	Qualified Electronic Signature or Qualified Electronic Seal
SAD	Signature Activation Data
SCA	Signature Creation Application
SCASC	Signature Creation Application Service Component
SCASP	Signature Creation Application Service Provider
SCDev	Signature Creation Device
SCS	Signature Creation Service
SCSP	Signature Creation Service Provider
SD	Signer's Document
SDO	Signed Data Object
SLA	Service-Level Agreement
SSA	Server Signing Application
SSASC	Server Signing Application Service Component
SSASP	Server signing application service provider
TSA	Time-Stamping Authority
URI	Uniform Resource Identifier

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any TSP conforming to the present document. 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]".

The requirements in the present document are identified as follows:

<the 3 letters identifying the elements of services > - < the clause number> - <2 digit number - incremental>

The elements of services are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **ASI**: AdES signing interface

The management of the requirement identifiers for 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 new requirements.
- 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 in line with ETSI EN 319 401 [9]. It incorporates ETSI EN 319 401 [9] requirements by reference and adds requirements relevant for a SCASP.

See ETSI EN 319 401 [9], clause 4 for guidance for guidance on general policy requirements.