ETSI TS 119 432 V1.1.1 (2019-03)

Electronic Signatures and Infrastructures (ESI);
Protocols for remote digital signature creation

Reference

DTS/ESI-0019432

Keywords

electronic signature, protocol, 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 - 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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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).

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.

Introduction

Standards for digital signatures have generally been developed for a long time considering solutions tailored to the characteristics of devices such as desktop computers and laptops where all signature processing was done in one system locally to the user. These traditional signature solutions assume that the signer uses smart cards or tokens to create any required digital signatures. Given developments in distributed systems, cloud computing, mobile equipment and related technologies, solutions have been emerging in the last few years where the process of digital signature creation and construction of AdES format is done in a distributed way with different steps of the process carried out by different systems/services that may be controlled by different actors.

The present document specifies protocols and interfaces for components providing specific functionalities as part of a process for remote digital signatures creation and construction of AdES formats. The present document aims at supporting electronic signatures and electronic seals, including qualified electronic signatures and qualified electronic seals according to the 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.1] (the eIDAS Regulation).

1 Scope

The present document specifies protocols and interfaces applicable when the process of creating AdES digital signatures as defined by ETSI TS 119 102-1 [i.7] and/or digital signature values, as result of Data To Be Signed Representations signatures, is carried out by a distributed solution comprised of two or more systems/services/components.

The present document is limited to remote server signing, i.e. the signing key is held in a remote shared service.

NOTE: Remote signature creation with local signing, i.e. the signing key is held with the signer's personal device but other steps in the signature creation are carried out by means of networked services, is a possible solution but protocols for such architecture are not covered in the present document.

Finally, the present document specifies two bindings, each one in a different syntax (XML and JSON), for each of the protocols mentioned above.

As far as it has been possible and suitable, the protocols have re-used constructs of CSC JSON and OASIS DSS-X XML specifications. When this has not been possible the present document specifies new components semantically and also syntactically in the two formats: XML and JSON.

The authorized signer's use of its key for signing requires users to provide multiple proofs of their claimed identity before being granted access to the needed set of resources. The way in which the user identity verification process is carried out by the service provider or any suggestion concerning the usage of multi-factor authentication mechanisms is out of the scope of the present document.

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] Cloud Signature Consortium Standard (Version 1.0.3.0): "Architectures and protocols for remote signature applications".

NOTE: Available at https://cloudsignatureconsortium.org/wp-content/uploads/2019/02/CSC_API_V1_1.0.3.0.pdf.

[2] OASIS Standard: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0", Committee Specification Draft 03 / Public Review Draft 03.

NOTE: Available at https://www.oasis-open.org/committees/download.php/64707/dss-core-v2.0-wd12-package-for-CSD03-PRD01.zip.

[3] OASIS Standard: "Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 2.0", Working Draft 02.

NOTE: Available at https://www.oasis-open.org/committees/download.php/63125/oasis-dssx-2.0-profiles-ades%20WD%2002.docx.

[4] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[5] OASIS Standard: "Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0".

NOTE: Available at https://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-asynchronous_processing-spec-cs-v1.0-r1.pdf.

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

[7] IETF RFC 5646: "Tags for Identifying Languages".

[8] IETF RFC 4514: "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names".

[9] IETF RFC 3061: "A URN Namespace of Objects Identifiers".

[10] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures".

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

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

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

[14] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

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] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules – Part 5: Cryptographic Module for Trust Services".

[i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.4] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.5] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[i.6] IETF RFC 7519: "JSON Web Token (JWT)".

[i.7] 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".

[i.8] IETF RFC 8017: "PKCS #1: RSA Cryptography Specifications Version 2.2".

[i.9] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.10] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.11] ETSI TS 103 172: " Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.12] 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.13] 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".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.3] and the following apply:

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

client application: application running in a signer's environment that accesses the services made available by the SCASC and/or the SSASC

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 providing 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 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 SCASC or the SSASC

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 [6].

signature credential: set of the signing key and the corresponding signing certificate

3.2 Symbols

Void.

3.3 Abbreviations

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

API	Application Program Interface
ASN	Abstract Syntax Notation
CA	Certification Authority
CEN	European Committee for Standardization
CRL	Certificate Revocation List
CSC	Cloud Signature Consortium
DSS-X	Digital Signature Services eXtended
DSV	Digital Signature Value
DTBS	Data To Be Signed
DTBSF	Data To Be Signed Formatted
DTBSR	Data To Be Signed Representation
ECDSA	Elliptic Curve Digital Signature Algorithm
EN	European Norm
HTTP	Hyper Text Transfer Protocol
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
JSON	Java Script Object Notation
JWT	JSON Web Token
LT	Long Term
LTA	Long Term Archival
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PNG	Portable Network Graphics
QES	Qualified Electronic Signature
QSCD	Qualified electronic Signature Creation Device
RA	Registration Authority
RSA	Rivest, Shamir, & Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAML	Security Access Markup Language
SCA	Signature Creation Application
SCAL	Sole Control Assurance Level
SCAL1	Sole Control Assurance Level 1

NOTE: As defined in CEN EN 419 241-1 [6].

SCAL2	Sole Control Assurance Level 2

NOTE: As defined in CEN EN 419 241-1 [6].

SCASC	Signature Creation Application Service Component
SCDev	Signature Creation Device
SCS	Signature Creation Service
SCSP	Signature Creation Service Provider
SD	Signer's Document
SDO	Signed Data Object

SDOC	Signed Data Object Composer
SDR	Signer's Document Representation
SSA	Server Signing Application
SSASC	Server Signing Application Service Component
TSP	Trust Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
XML	Extensible Markup Language
XSD	XML Schema Definition

4 Signature creation process, service decomposition

4.1 Signature creation process steps and data elements

Figure 1 (derived from ETSI TS 119 102-1 [i.7], clause 4.2.1) shows the various steps and the related data elements for a signature creation process. For remote signature creation, different steps of this process are carried out according to a decomposition into several components, which will have access to or make available the corresponding data elements. The process illustrated in the figure below is limited to the buildings blocks and information needed for creating a signature without taking in consideration issues such as signer authentication, authorization to the signing key usage or signing certificate availability. The signature activation module in the tamper protected area is needed only when the Signature Creation Service (SCS) complies to the sole control assurance level 2 (SCAL2) signature activation mechanism.

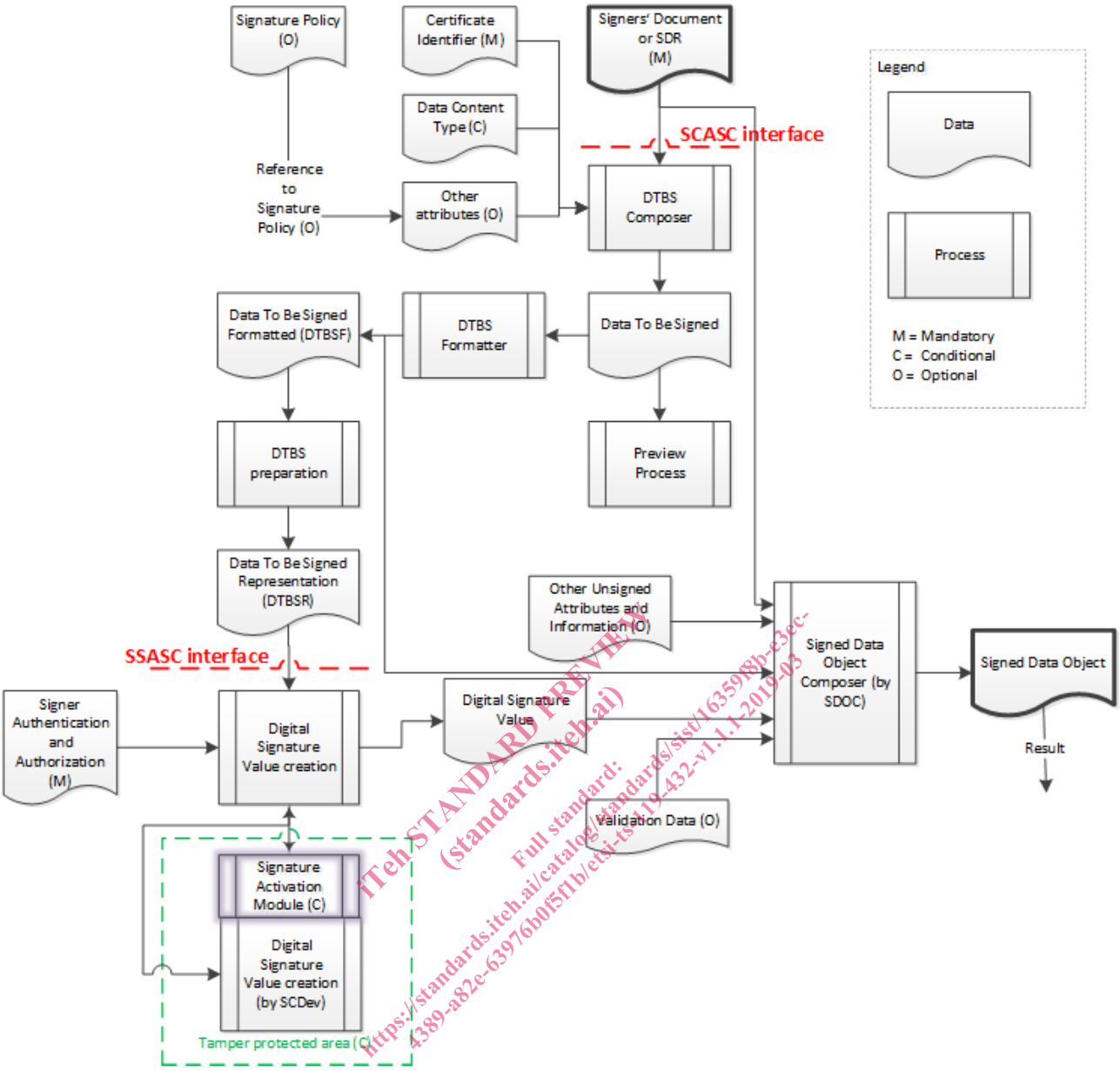

Figure 1: Process Steps and Data Elements in Signature Creation

4.2 Service main components and interfaces

The above process points out scenarios where the AdES and/or Digital Signature Value (DSV) are created using a signing key held within a cryptographic security module named Signature Creation Device (SCDev) operated by a Signature Creation Service Provider (SCSP).

Based on the different types of data managed in requests and responses, two main components can be identified in the above schema providing different interfaces for signing management: the Server Signing Application Service Component (SSASC) and the Signature Creation Application Service Component (SCASC) defined below.

The SSASC is the component supporting digital signature values creation. The SSASC is able to interact with the SCDev holding the signer's private key. When the SSASC uses the SCDev, the authorized signer is able to control the signing key with a certain level of confidence.

The SSASC interface has the Data To Be Signed Representation (DTBSR) and other parameters as main input and the digital signature value as main output.