ETSI EN 319 102-1 V1.1.1 (2016-05)

Electronic Signatures and Infrastructures (ESI);
Procedures for Creation and Validation
of AdES Digital Signatures;
Part 1: Creation and Validation

Reference
DEN/ESI-0019102-1

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

IPRs essential or potentially essential to the present document 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.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering Procedures for Creation and Validation of AdES Digital Signatures, as identified below:

Part 1: "Creation and Validation";

Part 2: "Signature Validation Report".

National transposition dates	
Date of adoption of this EN:	29 April 2016
Date of latest announcement of this EN (doa):	31 July 2016
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2017
Date of withdrawal of any conflicting National Standard (dow):	31 January 2017

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

The present document aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.15].

1 Scope

The present document specifies procedures for:

- the creation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.2], ETSI EN 319 132-1 [i.4], ETSI EN 319 142-1 [i.6] respectively);
- establishing whether an AdES digital signature is technically valid;

whenever the AdES digital signature is based on public key cryptography and supported by public key certificates. To improve readability of the present document, *AdES digital signatures* are meant when the term *signature* is being used.

NOTE 1: Regulation (EU) No 910/2014 [i.15] defines the terms electronic signature, advanced electronic signature, electronic seals and advanced electronic seal. These signatures and seals are usually created using digital signature technology. The present document aims at supporting the Regulation (EU) No 910/2014 [i.15] for creation and validation of advanced electronic signatures and seals when they are implemented as AdES digital signatures.

The present document introduces general principles, objects and functions relevant when creating or validating signatures based on signature creation and validation constraints and defines general classes of signatures that allow for verifiability over long periods.

The following aspects are considered to be out of scope:

- generation and distribution of Signature Creation Data (keys, etc.), and the selection and use of cryptographic algorithms;
- format, syntax or encoding of data objects involved, specifically format or encoding for documents to be signed or signatures created; and
- the legal interpretation of any signature, especially the legal validity of a signature.

NOTE 2: The signature creation and validation procedures specified in the present document provide several options and possibilities. The selection of these options is driven by a signature creation policy, a signature augmentation policy or a signature validation policy respectively. Note that legal requirements can be provided through specific policies, e.g. in the context of qualified electronic signatures as defined in the Regulation (EU) 910/2014 [i.15].

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

[2] ISO/IEC 9594-8:2014: "Information technology -- Open Systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks".

[3] IETF RFC 3161: "Internet X.509 Public Key Infrastructure; Time Stamp Protocol (TSP)".

[4] 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".

[5] Common PKI Specifications for Interoperable Applications from T7 & Teletrust, Specification Part 9 SigG-Profile, Version 2.0, 20 January 2009.

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] IETF RFC 4158: "Internet X.509 Public Key Infrastructure: Certification Path Building".

[i.2] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.3] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.4] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.5] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.6] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.7] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.8] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".

[i.9] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.10] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.11] Void.

[i.12] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.13] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.14] ECRYPT II Yearly Report on Algorithms and Keysizes (2010-2011), Revision 1.0, 30. June 2011.

[i.15] 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.16] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

attribute authority: authority which assigns privileges by issuing attribute certificates

attribute certificate: data structure, digitally signed by an attribute authority, that binds some attribute values with identification information about its holder

certificate: See public key certificate.

certificate identifier: unambiguous identifier of a certificate

certificate path (chain) validation: process of verifying and confirming that a certificate path (chain) is valid

certificate revocation list: signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

certificate validation: process of verifying and confirming that a certificate is valid

certification authority: authority trusted by one or more users to create and assign public-key certificates

chain model: model for validation of X.509 certificate chains where all CA certificates have to be valid at the time they were used for issuing a certificate and the end-entity certificate was valid when creating the signature

claimed signing time: time of signing claimed by the signer which on its own does not provide independent evidence of the actual signing time

(signature) commitment type: signer-selected indication of the exact implication of a digital signature

(signature) creation constraints: abstract formulation of rules, values, ranges and computation results that are used when creating a digital signature

cryptographic suite: combination of a signature scheme with a padding method and a cryptographic hash function

detached (digital) signature: digital signature that, with respect to the signed data object, is neither enveloping nor enveloped

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

driving application: application that uses a signature creation system to create a signature or a signature validation application in order to validate digital signatures or a signature augmentation application to augment digital signatures

electronic document: any content stored in electronic form, in particular text or sound, visual or audiovisual recording

enveloped (digital) signature: digital signature embedded within the signed data object

enveloping (digital) signature: digital signature embedding the signed data object

evidence: information that can be used to resolve a dispute about various aspects of authenticity of archived data objects

evidence record: unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time

NOTE: See IETF RFC 4998 [i.9] and IETF RFC 6283 [i.10].

proof of existence: evidence that proves that an object existed at a specific date/time

prospective certificate chain: sequence of n certificates which satisfies the conditions (a) to (c) in IETF RFC 5280 [1] clause 6.1, and the trust anchor is trusted according to the signature validation policy in use

public key certificate: public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it

shell model: model for validation of X.509 certificate chains where all certificates have to be valid at a given time

NOTE: The given time is an input parameter to the validation.

signature attribute: signature property

signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

NOTE: Augmenting signatures is a co-lateral process to the validation of signatures, namely the process by which certain material (e.g. time-stamps, validation data and even archival-related material) is incorporated to the signatures for making them more resilient to change or for enlarging their longevity.

signature augmentation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their augmentation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

(signature) constraints: abstract formulation of rules, values, ranges and computation results that a digital signature can be validated against

NOTE: Constraints can be defined in a formal signature policy, can be given in configuration parameter files or implied by the behaviour of the SVA.

signature creation application: application within the signature creation system, complementing the signature creation device, that creates a signature data object

signature creation data: unique data, such as codes or private cryptographic keys, which are used by the signer to create a digital signature value

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

signature creation environment: physical, geographical and computational environment of the signature creation system

signature creation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

signature creation system: overall system, consisting of the signature creation application and the signature creation device, that creates a digital signature

signature invocation: non-trivial interaction between the signer and the SCA or SCDev that is necessary to invoke the start of the signing process

NOTE: It is the 'Wilful Act' of the signer.

signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures

signature scheme: triplet of three algorithms composed of a signature creation algorithm, a signature verification algorithm and a key generation algorithm

signature validation: process of verifying and confirming that a signature is valid

signature validation application: application that implements signature validation

signature validation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their validation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be valid

signature verification: process of checking the cryptographic value of a signature using signature verification data

signature verification data: data, such as codes or public cryptographic keys, used for the purpose of verifying a signature

signed data object: data structure containing the signature value, signature attributes and other information (see clause 4.2.10)

signer: entity being the creator of a digital signature

time-assertion: time-stamp token or evidence record

time-stamp token: data object defined in IETF RFC 3161 [3], representing a time-stamp

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

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

trust service status list: form of a signed list as the basis for presentation of trust service status information

validation: process of verifying and confirming that a certificate or a digital signature is valid

validation data: data that is used to validate a digital signature

verifier: entity that wants to validate or verify a digital signature

3.2 Abbreviations

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

AC	Attribute Certificate
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DA	Driving Application
DTBS	Data To Be Signed
DTBSF	Data To Be Signed (Formatted)
DTBSR	Data To Be Signed Representation
ER	Evidence Record
ERS	Evidence Record Syntax
HTML	HyperText Markup Language
LDAP	Lightweight Directory Access Protocol
LT	Long Term
LTV	Long Term Validation
OCSP	Online Certificate Status Protocol
ODA	Office Document Architecture
OID	Object Identifier
PC	Personal Computer
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X. 509
POE	Proof Of Existence
RSA	Rivest, Shamir and Adleman algorithm
SAV	Signature Acceptance Validation
SCA	Signature Creation Application
SCDev	Signature Creation Device
SCE	Signature Creation Environment
SCS	Signature Creation System
SD	Signer's Document
SDO	Signed Data Object
SDR	Signer's Document Representation
SGML	Standard Generalized Markup Language
SVA	Signature Validation Application
TSA	Time-Stamping Authority

TSL	Trust-service Status List
TSP	Trust Service Provider
URI	Uniform Resource Identifier
XML	Extensible Mark-up Language
XSL	eXtensible Stylesheet Language

4 Signature creation

4.1 Signature creation model

The objective of signature creation is to generate a signature covering the Signer's Document (SD), the signing certificate or a reference to it, as well as signature attributes supporting the signature and its interpretation and purpose.

The present document uses the functional model of a Signature Creation Environment (SCE) consisting of:

- a signer that wants to create a signature in a document;
- a Driving Application (DA) which represents a user environment (e.g. a business application) that the signer uses to access signing functionality; and
- a Signature Creation System (SCS) which implements the signing functionality.

NOTE: The involvement of a human signer is not always needed; signing can be an automated process implemented in the DA.

Figure 1 illustrates this model. It does not distinguish between hardware or software implementations, and the model does not specify the nature of any inputs/outputs or information transfer paths between the different components (which might take the form of direct I/O devices, hardwired connections or be distributed over communications links). Also, it makes no statement about the distribution of the functions over different platforms. These aspects are implementation issues which are out of scope of the present document.

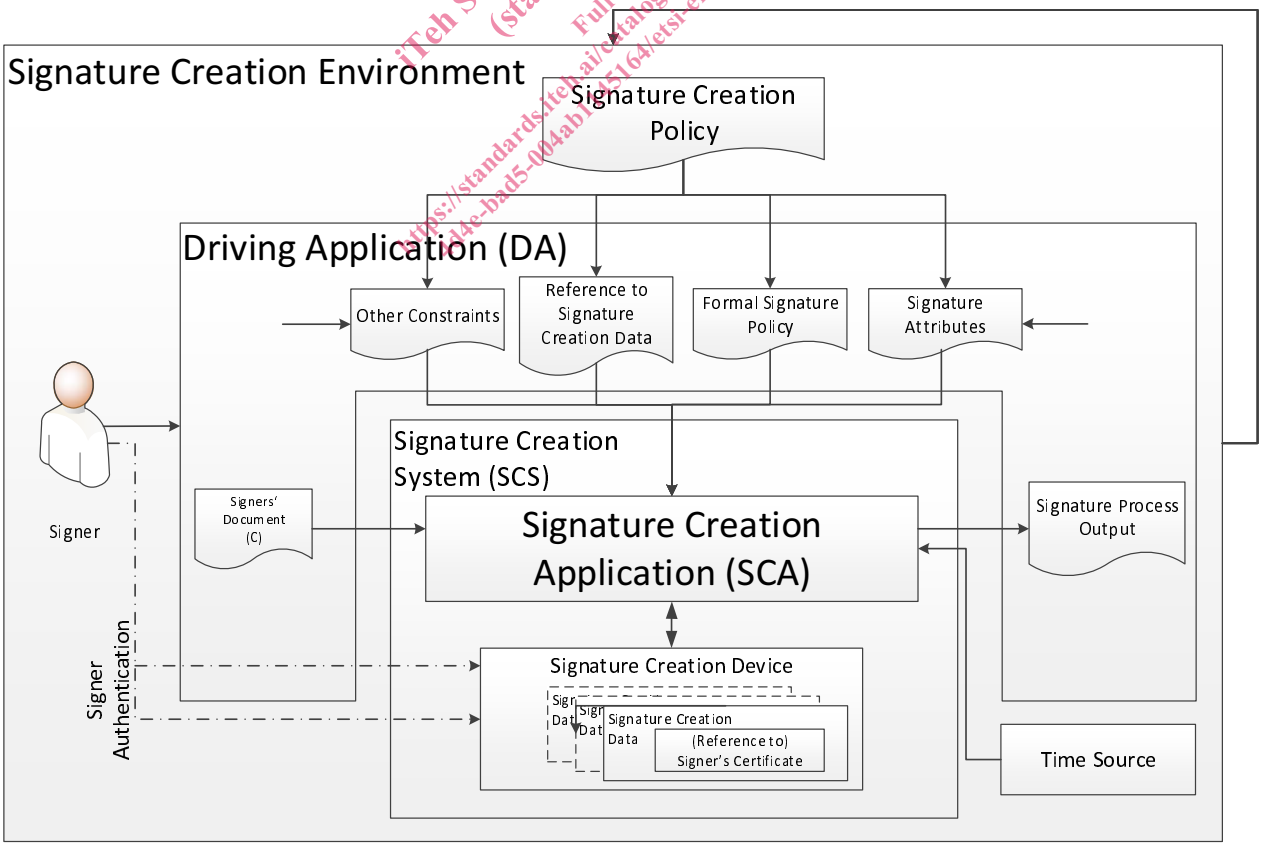

Figure 1: Functional Model of Signature Creation

The Signature Creation System (SCS) contains:

- a Signature Creation Application (SCA); and
- a Signature Creation Device (SCDev).

Clauses 4.2 and 4.3 specify the details of the signing process, which consist of the following steps:

- the SCS receives the document to be signed together with other input from the DA;
- composes this into Data To Be Signed (DTBS);
- formats this into Data To Be Signed (Formatted) (DTBSF);
- produces a signature over the DTBSF;
- formats the result into a Signed Data Object (SDO) conforming to the desired signature format (e.g. CAdES [i.2], XAdES [i.4] and PAdES [i.6]); and
- returns the SDO and a status indication to the DA.

In case of an error, the SCS should return additional information allowing the DA or the signer to properly deal with the error.

The signature creation device (SCDev):

- shall hold the signing certificates (or unambiguous references to them);
- shall hold the corresponding signature creation data;
- shall be able to authenticate the signer; and
- shall create the signature value using the signer's signature creation data.

NOTE: There are varieties of ways to implement the signature creation procedures, such as:

- running as (part of) an application software on a device like a PC with a graphical user interface;
- as a web service;
- a web application;
- a command-line tool;
- an integrated library or a middleware for other applications.

4.2 Signature creation information model

4.2.1 Introduction

Figure 2 outlines the building blocks for creating a signature and illustrates the data flow for the process of the generation of a signature. Clauses 4.2.2 to 4.2.11 specify information objects used in this process.