ETSI TS 119 142-3 V1.1.1 (2016-12)

TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures;
Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)

Reference

DTS/ESI-000122

Keywords

electronic signature, PAdES, profile, security,
time-stamping

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

The present document is part 3 of a multi-part deliverable covering the PDF digital signatures (PAdES). Full details of the entire series can be found in part 1 [2].

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

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect, digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures supported by PKI and public key certificates, and 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.4].

The present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be applied to any environment e.g. smart cards, SIM cards, special programs for electronic signatures, etc.

1 Scope

The present document specifies a type of PDF digital signatures, as specified in ISO 32000-1 [1], based on time-stamps.

It specifies a format for PAdES digital signatures using a Document Time-stamp - as defined in ETSI EN 319 142-1 [2] - as a digital signature intended to specifically prove the integrity and existence of a PDF document as defined in ISO 32000-1 [1], rather than proving any form of authentication or proof of origin.

NOTE: This format does not meet the requirements of advanced electronic signature and advanced electronic seal as defined in Regulation (EU) No 910/2014 [i.4], as it is not capable of identifying the signer.

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 that 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] ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7".

NOTE: Also available at http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf.

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

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

[i.2] IETF RFC 3161 (2001): "Time-Stamp Protocol (TSP)".

[i.3] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

[i.4] 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.

3 Definitions

For the purposes of the present document, the terms and definitions given in ISO 32000-1 [1], ETSI EN 319 142-1 [2] and the following apply:

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

PAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 142-1 [2] or ETSI EN 319 142-2 [i.1]

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

proof of integrity: evidence that proves the accuracy and completeness of an object

(electronic) time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

NOTE: In the case of IETF RFC 3161 [i.2] updated by IETF RFC 5816 [i.3] protocol, the electronic time-stamp is referring to the `timeStampToken` field within the `TimeStampResp` element (the TSA's response returned to the requesting client).

4 General syntax

4.1 General requirements for PAdES-DTS signatures

The type of PAdES signature defined in the present document is called PAdES-DTS and it builds on PDF signatures as specified in ISO 32000-1 [1].

While other PAdES signature profiles defined in ETSI EN 319 142-1 [2] and ETSI EN 319 142-2 [i.1] incorporate signed and unsigned attributes aimed at proving the authenticity of the signer by means of a digital certificate issued to a natural or legal person, this PAdES signature profile is based on Document Time-stamp as defined in ETSI EN 319 142-1 [2].

This means that instead of authenticating the identity of a user and the document's contents, this type of digital signature provides only a proof of integrity of the content represented in the PDF document, and the use of a Document Time-stamp adds a proof of existence of the document itself.

All the following requirements shall apply:

a) The Signature Dictionary of a PAdES-DTS signature, as defined in ISO 32000-1 [1], clause 12.8.1, table 252, shall be a Document Time-stamp Dictionary as described in clause 5.4.3 of ETSI EN 319 142-1 [2].

b) All the requirements described in clause 5.4.3 of ETSI EN 319 142-1 [2] shall apply.

c) Other requirements for handling PDF Signatures as specified in ISO 32000-1 [1], clause 12.8, shall apply except where overridden by the present document.

4.2 Extending the validity of PAdES-DTS signatures

The lifetime of the protection offered by a PAdES-DTS signature may be further extended beyond the lifetime of its Document time-stamp. In that case, a new Document time-stamp and DSS information shall be added as described in ETSI EN 319 142-1 [2], clause 5.4.

5 Attributes syntax and semantics

5.1 Extensions dictionary

The extensions dictionary (see ISO 32000-1 [1], clause 7.12) should include an entry

```
<</ESIC
    <</BaseVersion /1.7
      /ExtensionLevel 1
     >>
  >>
```

to identify that a PDF document includes extensions as identified in clause 4.1.

NOTE: As an alternative to the above entry, use of extensions as identified in clause 4.1 can also be identified by the following entry from Adobe® defining equivalent extensions to the PDF document format:

```
<</ADBE
<</BaseVersion /1.7
  /ExtensionLevel 8
    >>
>>
```

5.2 Requirements on encryption

A PDF document can be encrypted to protect its contents from unauthorized access. When encryption and signatures are combined together in a single PDF document, encryption shall be applied as described in ETSI EN 319 142-1 [2], clause 5.5.

6 PAdES-DTS signature profiles

6.1 Signature levels

The profiles in this clause define PAdES signatures based on the building blocks defined in ETSI EN 319 142-1 [2]. These profiles define two levels of PAdES-DTS signatures.

PAdES-DTS-BET level defines requirements for the generation of a basic PAdES-DTS signature providing a proof of existence and integrity of the document.

PAdES-DTS-A level defines requirements for the incorporation of electronic time-stamps that allow validation of the PAdES-DTS signature long time after its generation. This level aims to tackle the long term availability and integrity of the validation material.

6.2 General requirements

6.2.1 Requirements from Part 1

The requirements given in clauses 4.1, 5.3, 5.4, 5.5 and 6.2.1 of ETSI EN 319 142-1 [2] (PAdES Part 1) shall apply to all levels in this clause.

6.2.2 Notation for requirements

This clause describes the notation used for defining the requirements of the different PAdES signature levels.

The requirements on the elements and services are expressed in tables. A row in the table either specifies requirements for an element or a service.

These tables contain five columns.

1) Column "Elements/Services":

    a) In the case where the cell identifies a Service, the cell content starts with the keyword "Service:" followed by the name of the service.

    b) In the case where the element provides a service, this cell contains "SPO:" (for Service Provision Option), followed by the name of the element.

    c) Otherwise, this cell contains the name of the element.

2) Column "Presence in DTS-BET level". This cell contains the specification of the presence of element, or the provision of a service, for PAdES-DTS-BET signatures.

3) Column "Presence in DTS-A level". This cell contains the specification of the presence of the element, or the provision of a service, for PAdES-DTS-A signatures.

4) Below follows the values that can appear in columns "Presence in DTS-BET level" and "Presence in DTS-A level":

    - "shall be present": means that the element shall be present, and shall be as specified in the document referenced in column "References", further profiled with the additional requirements referenced in column "Requirements", and with the cardinality indicated in column "Cardinality".

    - "shall be provided": means that the service identified in the first column of the row shall be provided as further specified in the SPO-related rows. This value only appears in rows that contain requirements for services. It does not appear in rows that contain requirements for elements.

    - "conditioned presence": means that the presence of the item identified in the first column is conditioned as per the requirement(s) specified in column "Requirements" and requirements referenced by column "References" with the cardinality indicated in column "Cardinality".

    - "*": means that the attribute or signature field (service) identified in the first column should not be present (provided) in the corresponding level. Upper signature levels may specify other requirements.

5) Column "Cardinality". This cell indicates the cardinality of the attribute or signature field as follows:

    - **0**: The signature shall not incorporate any instance of the attribute or signature field.

    - **1**: The signature shall incorporate exactly one instance of the attribute or signature field.

    - **0 or 1**: The signature shall incorporate zero or one instance of the attribute or signature field.

    - ≥ **0**: The signature shall incorporate zero or more instances of the attribute or signature field.

    - ≥ **1**: The signature shall incorporate one or more instances of the attribute or signature field.

6) Column "Additional notes and requirements". This cell contains numbers referencing notes and/or letters referencing additional requirements on the attribute or signature field. Both notes and additional requirements are listed below the table.

7) Column "Reference". This cell contains either the number of the clause specifying the attribute or signature field in the present document, or a reference to the document and clause that specifies the attribute or signature field.

6.3 Requirements on components and services

This clause defines requirements on elements and services that PAdES signatures have to fulfil.

Table 1 shows the presence and cardinality requirements on the elements and services indicated in the first column for the two PAdES-DTS levels, namely: PAdES-DTS-BET and PAdES-DTS-A. Additional requirements are detailed below the table suitably labelled with the letter indicated in the last column.

Table 1: Requirements for PAdES-DTS-BET and PAdES-DTS-A signatures

Elements/Service	Presence in DTS-BET level	Presence in DTS-A level	Cardinality	Additional requirements and notes	References
SERVICE: proof of integrity	shall be provided	shall be provided	-	a	-
SPO: document-time-stamp	shall be present	shall be present	≥ 1		ETSI EN 319 142-1 [2], clause 5.4.3
SERVICE: provide certificate and revocation values	*	shall be provided	-	b, c	-
SPO: DSS	*	shall be present	DTS-BET: ≥ 0 DTS-A: ≥ 1	d, e, f, g	ETSI EN 319 142-1 [2], clause 5.4.2.2
SPO: DSS / VRI	*	conditioned presence	≥ 0	h	ETSI EN 319 142-1 [2], clause 5.4.2.3
SERVICE: provide trusted time for existence of the validation data	*	shall be provided	-	b, c	-
SPO: document-time-stamp	*	shall be present	DTS-BET: ≥ 0 DTS-A: ≥ 1	a, I, j	ETSI EN 319 142-1 [2], clause 5.4.3

Additional requirements:

a) The value of `SubFilter` shall be **ETSI.RFC3161**.

b) The signature shall contain a document security store as defined in clause 5.4.2 in ETSI EN 319 142-1 [2] followed by a document time-stamp as specified in clause 5.4.3 in ETSI EN 319 142-1 [2].

c) A new Document time-stamp and DSS information shall be added as described in ETSI EN 319 142-1 [2], clause 5.4.

d) The applications should include certificate values within the DSS. The full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the signature and which are not already present shall be included. This set includes certificates required for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

e) Duplication of certificate values within the signature should be avoided.

f) The full set of revocation data (CRL or OCSP responses) that have been used in the validation of the signer and CA certificates used in timestamp shall be included. This set includes all certificate status information required for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

g) The DER encoding shall be used for the certificate-values and the revocation-values.

h) The VRI dictionary should not be used. The inclusion of VRI dictionary entries is optional. All validation material referenced in VRI entries is also referenced in DSS entries.

i) PAdES-DTS-A signatures may have more than one `document-time-stamp` applied after the `DSS` and `DSS/VRI.`

j) Before generating and incorporating a `document-time-stamp` attribute, applications shall include all the validation material, which are not already in the timestamp, required for validating the timestamp. This validation material includes all the certificates and all certificate status information (like CRLs or OCSP responses) required for validating any time-stamp token's signing certificate (i.e. a TSA certificate).

   This validation material should be incorporated within `DSS`.

History

Document history		
V1.1.1	December 2016	Publication