ETSI TS 103 172 V1.1.1 (2011-09)

Electronic Signatures and Infrastructures (ESI);
PAdES Baseline Profile

Reference
DTS/ESI-000092

Keywords
electronic signature, PAdES, profile, security

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

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 (http://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).

Introduction

TS 102 778-3 [1] (PAdES-3 henceforth) specifies formats for Advanced Electronic Signatures built on PDF ISO-32000 [2]. That document defines a number of signed and unsigned optional signature properties, resulting in support for a number of variations in the signature contents and powerful processing requirements.

In order to maximise interoperability in communities applying PAdES to particular environments it is necessary to identify a common set of options that are appropriate to that environment. Such a selection is commonly called a profile.

The present document profiles the use of TS 102 778-3 [1] signatures for its use in the context of the "Directive 2006/123/EC [i.1] of the European Parliament and of the Council of 12 December 2006 on services in the internal market" (EU Services Directive henceforth) and any applicable context where qualified signatures are used.

1 Scope

The present document defines a baseline profile for PAdES, which corresponds to the minimum basic requirements in the context of the EU Services Directive, and provides the same basic features necessary in this context with the minimal number of options. This is required because there is a clear need for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive.

The present document definesa profile that specifies element and property requirements for a PAdES-Signature.

Clause 2 in the present document contains references to the relevant documents and standards.

Clause 3 includes definitions of relevant terms and abbreviations used in the present document.

Clause 4 provides details on the way that the requirements on both signer and verifier will be presented throughout the present document.

Clause 5 specifies the requirements for the short-term electronic signatures, that is, requirements for PAdES-BES and PAdES-EPES forms.

2 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.

2.1 Normative references

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

[1] ETSI TS 102 778-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

NOTE: Available at http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/.

[2] ISO 32000:2008 (all parts): "Document management - Portable document format".

NOTE: Available at http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf.

[3] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

NOTE: Available at "http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/.

[4] IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".

NOTE: Available at http://tools.ietf.org/rfcmarkup/3852.

[5] IETF RFC 2634 (1999): "Enhanced Security Services for S/MIME".

NOTE: Available at http://tools.ietf.org/rfcmarkup/2634.

[6] IETF RFC 5035 (2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

NOTE: Available at http://tools.ietf.org/rfcmarkup/5035.

[7] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[8] ECRYPT II (European Network of Excellence in Cryptology II): "ECRYPT II Yearly Report on Algorithms and Keysizes".

2.2 Informative references

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] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.2] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

3 Definitions and abbreviations

3.1 Definitions

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

generator: any party which creates, or adds attributes to, a signature

NOTE: This may be the signatory or any party which initially verifies or further maintains the signature.

long term signatures: signatures that are expected to be verified beyond the signers' certificate expiration date and, possibly, even after the expiration date of the certificate of the signers' certificate-issuing CA

protocol element: element of the protocol which may be including data elements and / or elements of procedure

service element: element of service that may be provided using one or more protocol elements

NOTE: All alternative protocol elements provide an equivalent service to the users of the protocol.

short term signatures: signatures that are to be verified for a period of time that does not go beyond the signers' certificate expiration date

verifier: entity that validates or verifies an electronic signature

The present document makes use of certain key words to signify requirements. Below follows their definitions:

may: Means that a course of action is permissible within the limits of the present document.

shall: Means that the definition is an absolute requirement of the present document. It has to strictly be followed in order to conform to the present document.

should: Means that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. Implementers **may** know valid reasons in particular circumstances to ignore this recommendation, but the full implications must be understood and carefully weighed before choosing a different course.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in PAdES-3 [1] and the following apply:

TSL Trust Status List

4 General requirements

4.1 Algorithm requirements

Generators are referred to applicable national laws regarding algorithms and key lengths.

Generators are also recommended to take into account the latest version of TS 102 176-1 [7] for guidelines purposes and the latest ECRYPT2 D.SPA.x [8] yearly report for further recommendations, when selecting algorithms and key lengths.

MD5 algorithm **shall not** be used as digest algorithm.

4.2 Compliance requirements

Profiles in the present document define separated requirements for both generator and verifier of PAdES signatures.

The present document defines a profile that specifies which elements/properties **shall** and which **may** be present in a PAdES signature.

A verifier **shall** be able to accept a PAdES signature containing any elements/properties conformant to PAdES [1], but this profile does not specify any processing requirement on such elements/properties present in the signature as it is meant to be used together with a specification describing processing during signature verification.

Requirements are grouped in four different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirement categories

Identifier	Requirement on generator
M	Generator **shall** include the element in the signature.
O	Generator **may** include the element in the signature.

Optional elements defined in PAdES-3 [1**] but not specified in the present document are treated as "O" as above**.

Certain service elements **may** be provided by different protocol elements at user's choice. In these cases the semantics of M and O defined in the table above depend on the requirement for the service element itself. Tables 2 and 3 (each one applies to a different requirement on the service element) define these semantics.

Table 2: Requirements for mandatory service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator
Service = M	Generator **shall** provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	Generator **may** use this protocol element for providing the mandatory service elements.

Table 3: Requirements for optional service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator
Service = O	Generator **may** provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	If the generator decides to provide the service, then she **may** use this protocol element.

The present document shows new requirements for each service and protocol element in tabular form. Below follows the structure of the table.

Table 4: Requirements for optional service with choices

Service / Protocol element	Reference	Requirement on generator	Notes / Additional requirements
Service:			
Choice 1			
Choice 2			

Column **Service / Protocol element** will identify the service element or protocol element the requirement applies to. Service elements that **may** be implemented by different protocol elements (i.e. users **may** make a choice on several protocol elements) build tables with more than one row.

Column **Reference** will reference the relevant clause of the standard where the element is first defined. The reference is to PAdES-3 [1], except where explicitly indicated otherwise.

Column **Requirement on generator** will contain an identifier of the requirement, as defined in table 1, bound to the corresponding protocol element for the generator.

Column **Notes / Additional requirements** will contain numbers referencing notes and/or letters referencing additional requirements. Both notes and additional requirements are listed below the table.

Profiles **may** be affected by applicable regulations; hence implementers **should** check any national regulation that **may** affect these profiles.

5 Requirements for short-term Electronic Signatures

The current clause specifies a compliance requirements for short-term electronic signatures. In consequence it includes requirements for the following forms: PAdES-BES and PAdES-EPES.

All attributes profiled by PAdES Part 3 [1] and specified in ISO 32000-1 [2] apply as stated in those specifications unless mentioned here otherwise. Also PAdES Part 3 states that "Requirements for handling PDF Signatures specified in ISO 32000-1, clause 12.8 apply except where overridden […]". The following sections will apply the same strategy.

NOTE: Given that PAdES signatures are enveloped inside a PDF document and are detached in the sense of a CMS signature, the signature placement is implied by PAdES-3 [1] and ISO 32000 [2]. In ISO 32000 [2] section 12.8.3.3.1 reads "No data shall be encapsulated in the PKCS#7 SignedData field.", no re-statement will be given here, however readers should be aware of the fact that subtle dependencies exist.

Clause 5.1 provides an overview of the CAdES forms profiled in this clause.

5.1 Profiled PAdES Forms

The present clause provides an overview of the PAdES forms profiled in the present clause.

Table 5

Service / Protocol element	PAdES Reference	Generator requirement	Additional requirements / notes
Service: signature		M	
PAdES-BES	[1], clause 4 CAdES [3], clause 4.3.1	O	1
PAdES-EPES	[1], clause 4 CAdES [3], clause 4.3.2	O	2

NOTE 1: Properties leading to PAdES-BES signatures are profiled in clause 5.2.

NOTE 2: Properties leading to PAdES-EPES signatures are profiled in clause 5.3.

5.2 Profile of attributes in Basic PAdES form (PAdES-BES)

5.2.1 Attributes defined in CMS Signature

5.2.1.1 Placement of the signing certificate

Table 6

Service / Protocol element	Reference	Generator requirement	Additional requirements / notes
`SignedData.certificates`	CMS [4], clause 5.1	M	a, b, c

Additional requirement:

a) The generator **shall** include the signer certificate in the SignedData.certificate field.

b) In order to facilitate path building, generators **should** include in the SignedData.certificate field all certificates not available to verifiers that can be used during path building. In the case of signature based on qualified certificates and whose verification is expected to be based on TSLs, (in conformance with Decision 2009/767/EC [i.2]), the generator **should** include all intermediary certificates forming a chain between the signer certificate and a CA present in the TSL which are not available to verifiers.

NOTE 1: A certificate is considered available to the verifier if reliable information about its location is known and allows automated retrieval of the certificate (for instance through an Authority Info Access Extension or equivalent information present in a TSL).

NOTE 2: In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, generators may not know which certificates will be relevant for path building. However, in practice, such certificates can often clearly be identified. In this case, it is advised that generators include them unless they can be automatically retrieved by verifiers. In the specific case of a signature meant to be validated through TSL, it is advised to include at least the unavailable intermediary certificates up to but not including the CAs present in the TSLs, since the TSL is information that is shared globally by all verifiers.

5.2.2 Attributes overridden in PAdES-3

5.2.2.1 Signing time

Table 8

Service / Protocol element	Reference	Generator requirement	Additional requirements / notes
Service: signing time	[1], clauses 5.1 and 4.5.3 CAdES [3], clauses 5.1 and 5.9.1	M	a
M entry in the signature dictionary	ISO 32000-1 [2], clauses 5.1 and 12.8.1	M	

Additional requirements:

a) The generator **shall** include the claimed time of signature as content of this element.

5.2.3 Elements defined in ESS

5.2.3.1 Signing certificate

Table 9

Service / Protocol element	Reference	Generator Requirement	Additional requirements / notes
Service: protection of signing certificate		M	
ESS signing-certificate	ESS [5], clause 5.15.4	O	a, b
ESS signing-certificate v2	ESS [6], clause 5.14	O	a, b

Additional requirement:

a) Generators **shall** use either the signing certificate or the signing-certificate v2 attribute, depending on the hash function using, in accordance with ESS [6], clause 2.

b) Generators **should** migrate to the use of ESS signing-certificate v2 in preference to ESS signing-certificate in line with the guidance regarding limited lifetime for the use of SHA-1 given in clause 9.2 of TS 102 176-1 [7].

5.3 Profile of attributes in Explicit Policy based Electronic Signature CAdES form (CAdES-EPES)

5.3.1 Attributes defined in CAdES

5.3.1.1 Signature policy identifier

Table 10

Service / Protocol element	Reference	Generator requirement	Additional requirements / notes
`signature-policy-identifier`	[1], clauses 5.1 and 4.5.1 CAdES [3], clauses 5.1 and 5.8.1	M	

History

Document history		
V1.1.1	September 2011	Publication