ETSI TS 119 144-2 V2.1.1 (2016-06)



Electronic Signatures and Infrastructures (ESI); PAdES digital signatures -Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of PAdES baseline signatures Reference

RTS/ESI-0019144-2

Keywords

e-commerce, electronic signature, interoperability, PAdES, profile, security, testing

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: <u>http://www.etsi.org/standards-search</u>

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 <u>https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx</u>

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI. The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016. All rights reserved.

DECT[™], PLUGTESTS[™], UMTS[™] and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP**[™] and LTE[™] are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intell	lectual Property Rights	4
Fore	word	4
Mod	al verbs terminology	4
1	Scope	5
2 2.1 2.2	References Normative references Informative references	5 5 5
3 3.1 3.2	Definitions and abbreviations Definitions Abbreviations	6 6 6
4	Overview	6
5	Testing interoperability of PAdES-B-B signatures	6
6	Testing interoperability of PAdES-B-T signatures	9
7	Testing interoperability of PAdES-B-LT signatures	11
8	Testing interoperability of PAdES-B-LTA signatures	12
9	Testing PAdES baseline signatures augmentation interoperability	15
10 10.1 10.2 10.3	Testing negative PAdES baseline signatures PAdES-B-B signatures test cases PAdES-B-T signatures test cases PAdES-B-LTA signatures test cases	17 17 17 17
Histo	Dry	

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 2 of a multi-part deliverable covering PAdES digital signatures - Testing Conformance and Interoperability. Full details of the entire series can be found in part 1 [i.1].

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 <u>ETSI Drafting Rules</u> (Verbal forms for the expression of provisions).

"must" and "must not" are NOT allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines a number of test suites to assess the interoperability between implementations claiming conformance to PAdES baseline signatures [2].

The test suites are defined with four different layers reflecting the four different levels of PAdES baseline signatures:

- Tests suite addressing interoperability between applications claiming B-B level conformance.
- Tests suite addressing interoperability between applications claiming B-T level conformance.
- Tests suite addressing interoperability between applications claiming B-LT level conformance.
- Tests suite addressing interoperability between applications claiming B-LTA level conformance.

Test suites also cover augmentation of PAdES baseline signatures and negative test cases.

These test suites are agnostic of the PKI infrastructure. Any PKI infrastructure can be used including the one based on EU Member States Trusted Lists.

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] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
- [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 TR 119 144-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures -Testing Conformance and Interoperability; Part 1: Overview".
- [i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

6

3 Definitions and abbreviations

3.1 Definitions

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

negative test case: test case for a signature whose validation according to ETSI EN 319 102-1 [i.3] would not result in TOTAL-PASSED

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.2] apply.

4 Overview

This clause describes the overall approach used throughout the present document to specify test suites for PAdES baseline signatures interoperability testing.

ETSI EN 319 142-1 [2] defines four different levels of PAdES baseline signatures.

The test suites are defined with different layers reflecting the levels of PAdES baseline signatures specified in ETSI EN 319 142-1 [2]:

- Testing PAdES signatures interoperability between applications claiming B-B level conformance.
- Testing PAdES signatures interoperability between applications claiming B-T level conformance.
- Testing PAdES signatures interoperability between applications claiming B-LT level conformance.
- Testing PAdES signatures interoperability between applications claiming B-LTA level conformance.
- Testing augmentation of PAdES signatures from B-T level to B-LTA level.
- Negative test cases for PAdES baseline signatures:
 - PAdES-B-B signatures test cases.
 - PAdES-B-T signatures test cases.
 - PAdES-B-LTA signatures test cases.

5 Testing interoperability of PAdES-B-B signatures

The test cases in this clause have been defined for different combinations of PAdES-B-B signatures attributes.

Mandatory attributes for PAdES-B-B signatures described in ETSI EN 319 142-1 [2], clauses 6.2 and 6.3, shall be present.

Table 1 shows which attributes are required to generate PAdES-B-B signatures for each test case.

TC ID	Description	Pass criteria	Signature attributes
PAdES/BB/1	This is the simplest PAdES- B-B signatures interoperability test case. The signature ONLY CONTAINS the mandatory PAdES attributes.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, ESSSigningCertificateV2 and MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2
PAdES/BB/2	In this PAdES-B-B signatures interoperability test case the signature dictionary contains the same entries used in test case PAdES/BB/1 with the addition of Location, ContactInfo and Reason entries. ContentType, ESSSigningCertificateV2 and MessageDigest attributes shall be added to the PDF signature included in the Contents entry as specified in CAdES [1].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M, Location, Reason and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, ESSSigningCertificateV2 and MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache M Location ContactInfo Reason ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat
PAdES/BB/3	In this PAdES-B-B signatures interoperability test case the PDF signature contains ContentTimeStamp attribute in addition to ContentType, ESSSigningCertificateV2 and MessageDigest attributes included to the PDF signature included in the Contents entry as specified in CAdES [1].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, ESSSigningCertificateV2, ContentTimeStamp and MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 ContentTimeStamp

Table 1: Test cases for PAdES-B-B signatures

TC ID	Description	Pass criteria	Signature attributes
PAdES/BB/4	This test case tests a PAdES-B-B signature with an instance of ClaimedAttribute of SignerAttributesV2 attribute. ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes shall also be added to the PDF signature included in the Contents entry as specified in CAdES [1].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, M, SubFilter and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, ClaimedAttribute (included in SignerAttributesV2), ESSSigningCertificateV2, MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter Adobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 SignerAttributesV2 ClaimedAttribute
PAdES/BB/5	This test case tests a PAdES-B-B signature with an instance of CertifiedAttributeV2 of SignerAttributesV2 attribute. ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes shall also be added to the PDF signature included in the Contents entry as specified in CAdES [1].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, M, SubFilter and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, CertifiedAttributesV2 (included in SignerAttributesV2), ESSSigningCertificateV2, MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 SignerAttributesV2 CertifiedAttributeV2
PAdES/BB/6	This test case tests a PAdES-B-B signature with M, Reason, and Location entries in signature dictionary and MessageDigest, SignaturePolicyIdentifier, ContentType and ESSSigningCertificateV2 attributes in the CAdES [1] signature included in the Contents entry.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M, Reason, Location and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, ESSSigningCertificateV2, SignaturePolicyIdentifier and MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache d Reason Location M ByteRange Contents (DER CMS) SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 SignaturePolicyIdentifier

TC ID	Description	Pass criteria	Signature attribu	ites
PAdES/BB/7	This test case tests a PAdES-B-B signature in which digest algorithm SHA1 is used to digest data to be signed. The signature ONLY CONTAINS the mandatory PAdES properties.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, ESSSigningCertificate and MessageDigest attributes	 SignatureDictionary Type Sig Filter Adobe.PPF SubFilter ETSI.CAdE M ByteRange Contents (DER C Certificates SigningCer ContentTyp MessageD ESSSigning 	(Lite S.detache CMS) tificate be gest gCertificat

6

Testing interoperability of PAdES-B-T signatures

The test cases in this clause have been defined for different combinations of PAdES-B-T signatures attributes. PAdES baseline signatures claiming conformance to B-T level of ETSI EN 319 142-1 [2] shall be built on baseline signatures conformant to B-B level.

A PAdES baseline signature conformant to B-T level shall be a baseline signature conformant to B-B level for which a Trust Service Provider has generated a trusted token (time-stamp token) proving that the signature itself actually existed at a certain date and time.

Mandatory attributes for PAdES-B-T signatures described in ETSI EN 319 142-1 [2], clauses 6.2 and 6.3, shall be present.

Table 2 shows which attributes are required to generate PAdES-B-T signatures for each test case.

TC ID	Description	Pass criteria	Signature attributes	
PAdES/BT/1	This is the simplest PAdES-	Positive validation.	•	SignatureDictionary
	B-T signatures	The signature dictionary shall		о Туре
	interoperability test case	contain Type, Contents, Filter, M,		o Sig
	with M entry in signature	SubFilter and ByteRange entries.		o Filter
	dictionary. ContentType,	The DER-encoded CMS binary		 Adobe.PPKLite
	ESSSigningCertificateV2,	data object included in the		o SubFilter
	MessageDigest and	Contents entry shall include the		 ETSI.CAdES.detache
	SignatureTimeStamp	SigningCertificate (in		d
	attributes shall be added to	SignedData.certificates field)		o M
	the PDF signature included	attribute, ContentType,		 ByteRange
	in the Contents entry as	ESSSigningCertificateV2,		 Contents (DER CMS)
	specified in CAdES [1].	MessageDigest signed attributes		 Certificates
		and SignatureTimeStamp		SigningCertificate
		unsigned attribute.		 ContentType
				 MessageDigest
				 ESSSigningCertificat
				eV2
				 SignatureTimeStamp

Table 2: Test cases for PAdES-B-T signatures

TC ID	Description	Pass criteria	Signature attributes
PAdES/BT/2	This test case tests a PAdES-B-T signature with an instance of ClaimedAttribute of SignerAttributesV2 attribute. ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes are included in PDF signature included in the Contents entry as specified in CAdES [1].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, M, SubFilter and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field) attribute, ContentType, ClaimedAttribute (included in SignerAttributesV2), ESSSigningCertificateV2, MessageDigest signed attributes and SignatureTimeStamp unsigned attribute.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache ByteRange Contents (DER CMS) Certificates
PAdES/BT/3	This test case tests a PAdES-B-T signature with MessageDigest, ContentType, SignaturePolicyIdentifier, SignatureTimeStamp, CommitmentTypeIndication and ESSSigningCertificateV2 attributes in the CAdES [1] signature included in the Contents entry.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, M, SubFilter and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field) attribute, ContentType, ESSSigningCertificateV2, SignatureTimeStamp, SignaturePolicyIdentifier, CommitmentTypeIndication and MessageDigest attributes.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 SignaturePolicyIdentifier CommitmentTypeIndication SignatureTimeStamp
PAdES/BT/4	This test case tests a PAdES-B-T signature with a ContentTimeStamp attribute which provides time-stamp token of the signed data content before it is signed. ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes shall also be added to the CAdES signature [1] included in the Contents entry.	Positive validation. The signature dictionary shall contain Type, M, Contents, Filter, SubFilter and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field) attribute, ContentType, MessageDigest, ESSSigningCertificateV2, ContentTimeStamp signed attributes and SignatureTimeStamp unsigned attribute.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter Adobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 ContentTimeStamp SignatureTimeStamp

7 Testing interoperability of PAdES-B-LT signatures

The test cases in this clause have been defined for different combinations of PAdES-B-LT signatures attributes. PAdES baseline signatures claiming conformance to B-LT level of ETSI EN 319 142-1 [2] shall be built on baseline signatures conformant to B-T level.

A PAdES baseline signature conformant to B-LT level shall be a baseline signature conformant to B-T level to which values of certificates and values of certificate status used to validate the signature have been added in the DSS and eventually VRI dictionaries.

Mandatory attributes for PAdES-B-LT signatures described in ETSI EN 319 142-1 [2], clauses 6.2 and 6.3, shall be present.

Table 3 shows which attributes are required to generate PAdES-B-LT signatures for each test case.

ite
S.detache
MS)
ficate
9
jest
Certificat
neStamp
_ite
2 data ah a
5.detache
MS)
100)
ficate
a a
iest
Certificat
neStamp
- ··· P

Table 3: Test cases for PAdES-B-LT signatures

	Description	Pass criteria			Signature attributes
	This PAdES_B_LT signature	Positive validation	-	Sia	naturoDictionary
TAULO/DEI/S	contains Type Contents	The signature dictionary shall	•	Sig	
	Filter SubFilter M and	contain Type Contents Filter		0	
	ByteRange entries in	SubFilter M and ByteRange		0	Filter
	signature dictionary, CMS	entries.		0	
	signature, included in the	The DER-encoded CMS binary		0	SubFilter
	Contents entry, contains	data object included in the		0	• ETSI.CAdES.detache
	ContentType,	Contents entry shall include the			d
	ESSSigningCertificateV2,	SigningCertificate (in		0	Μ
	MessageDigest and	SignedData.certificates field)		0	ByteRange
	SignatureTimeStamp	attribute, ContentType,		0	Contents (DER CMS)
	attributes. The DSS	MessageDigest,			 Certificates
	dictionary includes Certs,	ESSSigningCertificateV2 signed			SigningCertificate
	CRLs and VRI entries. The	attributes and			 ContentType
	VRI dictionary includes Cert	Signature limeStamp unsigned			 MessageDigest
	and CRL entries.	attribute.			 ESSSigningCertificat
		the Type Corte CPL and VPL			ev2 Sign at una Time a Starrag
		entries The VPI dictionary shall		50	
		contain the Type. Cert and CRI	•	05	
		entries		0	Corts
				0	CRIs
				0	VRI
				VR	
				0	Type
				0	Cert
				0	CRL
PAdES/BLT/4	This PAdES-B-LT signature	Positive validation.	•	Sig	natureDictionary
	contains Type, Contents,	The signature dictionary shall		0	Туре
	Filter, SubFilter, M and	contain Type, Contents, Filter,			o Sig
	ByteRange entries in	SubFilter, M and ByteRange		0	Filter
	signature dictionary. CMS	entries.			
	Signature, included in the	deta object included in the		0	
		Contents entry shall include the			o ETSI.CAdES.detache
	ESSSigningCertificate//2	SigningCertificate (in		0	M
	MessageDigest and	SignedData certificates field)		0	ByteRange
	SignatureTimeStamp	attribute, ContentType,		0	Contents (DER CMS)
	attributes. The DSS	MessageDigest,		-	 Certificates
	dictionary includes Certs,	ESSSigningCertificateV2 signed			SigningCertificate
	OCSPs and VRI entries.	attributes and			 ContentType
	The VRI dictionary includes	SignatureTimeStamp unsigned			 MessageDigest
	Cert and OCSP entries.	attribute.			 ESSSigningCertificat
		The DSS dictionary shall contain			eV2
		the type, Certs and OCSPs		D 0	
			•	08	
				0	rype Corts
				0	OCSPs
				0	VRI
			•	VR	 I
				0	Туре
				0	Cert
				0	OCSP

8

Testing interoperability of PAdES-B-LTA signatures

The test cases in this clause have been defined for different combinations of PAdES-B-LTA signatures attributes. PAdES baseline signatures claiming conformance to B-LTA level of ETSI EN 319 142-1 [2] shall be built on baseline signatures conformant to B-LT level.

A PAdES baseline signature conformant to B-LTA level shall be a baseline signature conformant to B-LT level to which one or more DTS dictionaries have been added.

Mandatory attributes for PAdES-B-LTA signatures described in ETSI EN 319 142-1 [2], clauses 6.2 and 6.3, shall be present.

Table 4 shows which attributes are required to generate PAdES-B-LTA signatures for each test case.

TC ID	Description	Pass criteria	Signature attributes
PAdES/BLTA/1	This is the simplest PAdES- B-LTA signatures interoperability test case with Type, Contents, Filter, SubFilter, M and ByteRange entries in signature dictionary. CMS signature, included in the Contents entry, contains ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes. The DSS dictionary includes Certs and CRLs entries. Then one Document Time Stamp shall be applied and verified.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field) attribute, ContentType, MessageDigest, ESSSigningCertificateV2 signed attributes and SignatureTimeStamp unsigned attribute. The DSS dictionary shall contain the Type, Certs and CRLs entries. The DTS dictionary shall contain the Type, SubFilter and Contents entries.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter Adobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) Certificates SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 SignatureTimeStamp DSS Type Certs CRLs
PAdES/BLTA/2	This PAdES-B-LTA signature contains Type, Contents, Filter, SubFilter, M and ByteRange entries in signature dictionary. CMS signature, included in the Contents entry, contains ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes. The DSS dictionary includes Certs and OCSPs. Then one Document Time Stamp shall be applied and verified.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded CMS binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field) attribute, ContentType, MessageDigest, ESSSigningCertificateV2 signed attributes and SignatureTimeStamp unsigned attribute. The DSS dictionary shall contain the Type, Certs and OCSPs entries. The DTS dictionary shall contain the Type, SubFilter and Contents entries.	 SignatureDictionary Type Sig Filter Adobe.PPKLite SubFilter Atobe.PPKLite SubFilter ETSI.CAdES.detache M ByteRange Contents (DER CMS) SigningCertificate ContentType MessageDigest ESSSigningCertificat eV2 SignatureTimeStamp DSS Type Certs OCSPs DTS Type SubFilter Contents

Table 4: Test cases for	PAdES-B-LTA	signatures
-------------------------	-------------	------------

TC ID	Description	Pass criteria	Signature attributes
PAdES/BLTA/3	This PAdES-B-LTA	Positive validation.	SignatureDictionary
	signature contains Type,	The signature dictionary shall	о Туре
	Contents, Filter, SubFilter,	contain Type, Contents, Filter,	o Sig
	M and ByteRange entries in	SubFilter, M and ByteRange	• Filter
	signature dictionary. CMS	entries.	o Adobe.PPKLite
	Signature, included in the	The DER-encoded CMS binary	• SubFilter
		Contents entry shall include the	
	EssigningCertificate//2	SigningCertificate (in	
	MessageDigest and	SignedData.certificates field)	o ByteRange
	SignatureTimeStamp	attribute, ContentType,	 Contents (DER CMS)
	attributes. The DSS	MessageDigest,	 Certificates
	dictionary includes Certs,	ESSSigningCertificateV2 signed	SigningCertificate
	CRLs and VRI entries. The	attributes and	 ContentType
	VRI dictionary includes Cert	Signature limeStamp unsigned	 MessageDigest
	and CRL entries. Then one	attribute.	
	be applied and verified	the Type Certs CRI's and VRI	
	be applied and vermed.	entries The VRI dictionary shall	
		contain the Type, Cert and CRL	
		entries. The DTS dictionary shall	o Certs
		contain the Type, SubFilter and	o CRLs
		Contents entries.	o VRI
			• VRI
			o Type
			o Cert
			o SubFilter
			 Contents
PAdES/BLTA/4	This PAdES-B-LTA	Positive validation.	SignatureDictionary
	signature contains Type,	The signature dictionary shall	o Type
	Contents, Filter, SubFilter,	contain Type, Contents, Filter,	o Sig
	M and ByteRange entries in	SubFilter, M and ByteRange	• Filter
	signature dictionary. CMS	entries.	o Adobe.PPKLite
	Contents entry contains	data object included in the	
	ContentType	Contents entry shall include the	d
	ESSSigningCertificateV2,	SigningCertificate (in	0 M
	MessageDigest and	SignedData.certificates field)	o ByteRange
	SignatureTimeStamp	attribute, ContentType,	 Contents (DER CMS)
	attributes. The DSS	MessageDigest,	o Certificates
	dictionary includes Certs,	ESSSigningCertificateV2 signed	SigningCertificate
	CCSPs and VRI entries.	attributes and	• Content lype
	Cert and OCSP entries	attribute	
	Then one Document Time	The DSS dictionary shall contain	eV/2
	Stamp shall be applied and	the Type, Certs and OCSPs	 SignatureTimeStamp
	verified.	entries. The DTS dictionary shall	• DSS
		contain the Type, SubFilter and	о Туре
		Contents entries.	o Certs
			o OCSPs
			o iype
			• DTS
			о Туре
			o SubFilter
			o Contents

9 Testing PAdES baseline signatures augmentation interoperability

The test cases in this clause have been defined for testing augmentation of PAdES-B-T signatures to PAdES-B-LTA signatures and subsequent validation of the augmented signatures.

A PAdES baseline signature conformant to B-LTA level shall be a baseline signature conformant to B-T level to which one or more DSS and eventually VRI dictionaries containing values of certificates and values of certificates status used to validate the signature and one or more DTS dictionaries have been added.

Table 5 shows which attributes are required to augment a PAdES-B-T signature to a PAdES-B-LTA signature for each test case.

TC ID	Description	Pass criteria	Signature attributes
PAdES/Aug/1	The PAdES-B-T signature,	Positive validation.	PAdES-B-T signature
	passed as input, shall be	The signature shall contain a	• DSS
	validated, the validation	PAdES-B-T signature with a	о Туре
	material concerning the	signature dictionary containing	 Certs
	signing certificate and the	Type, Contents, Filter, M,	o CRLs
	certificate that generated	SubFilter and ByteRange entries	• DTS
	the signature timestamp	and a DER-encoded CMS binary	о Туре
	shall be added (the	data object included in the	 SubFilter
	revocation data used are	Contents entry including the	 Contents
	CRLS) and, alter that, one	SigningCertificate (In SignedDate cortificates field)	
	be applied	attribute ContentType	
	be applied.	ESSSigningCertificate\/2	
		MessageDigest signed attributes	
		and SignatureTimeStamp	
		unsigned attribute. A DSS	
		dictionary containing the Type,	
		Certs and CRLs entries and a	
		DTS dictionary containing the	
		Type, SubFilter and Contents	
		entries are added to the PAdES-	
		B-T signature.	
PAdES/Aug/2	The PAdES-B-T signature,	Positive validation.	 PAdES-B-T signature
	passed as input, shall be	The signature shall contain a	• DSS
	validated, the validation	PAGES-B-T Signature with a	o lype
	signing certificate and the	Type Contents Filter M	
	certificate that generated	SubFilter and ByteRange entries	
	the signature timestamp	and a DER-encoded CMS binary	
	shall be added (the	data object included in the	 SubFilter
	revocation data used are	Contents entry including the	 Contents
	OCSP responses) and, after	SigningCertificate (in	
	that, one Document Time	SignedData.certificates field)	
	Stamp shall be applied.	attribute, ContentType,	
		ESSSigningCertificateV2,	
		MessageDigest signed attributes	
		and SignatureTimeStamp	
		unsigned attribute. A DSS	
		Corta and OCSPa antrian and a	
		DTS dictionary containing the	
		Type SubFilter and Contents	
		entries are added to the PAdES-	
		B-T signature.	
L	1		

Table 5: Test cases for augmentation of PAdES-B-T signatures to B-LTA signatures

TC ID	Description	Pass criteria	Signature attributes
PAdES/Aug/3	The input to this test case is a PAdES-B-LTA signature. The signature, passed as input, shall be validated, the validation material concerning the certificate that generated the timestamp included in the Contents entry of the DTS dictionary shall be added (the revocation data used are CRLs) to the DSS dictionary and, after that, one Document Time Stamp shall be applied too.	Positive validation. The signature shall contain a PAdES-B-LTA signature with a signature dictionary containing Type, Contents, Filter, M, SubFilter and ByteRange entries, a DER-encoded CMS binary data object included in the Contents entry including the SigningCertificate (in SignedData.certificates field) attribute, ContentType, ESSSigningCertificateV2, MessageDigest signed attributes and SignatureTimeStamp unsigned attribute, a DSS dictionary containing the Type, Certs and CRLs entries and a DTS dictionary containing the Type, SubFilter and Contents entries. A new DSS dictionary containing the validation material concerning the certificate that generated the timestamp included in the Contents entry of the DTS dictionary and a new DTS dictionary containing the Type, SubFilter and Contents entries shall be added to the PAdES-B-LTA signature.	 PAdES-B-T signature DSS Type Certs CRLs DTS Type SubFilter Contents DTS Type SubFilter Contents
PAdES/Aug/4	The input to this test case is a PAdES-B-LTA signature. The signature, passed as input, shall be validated, the validation material concerning the certificate that generated the timestamp included in the Contents entry of the DTS dictionary shall be added (the revocation data used are OCSPs) to the DSS dictionary and, after that, one Document Time Stamp shall be applied too.	Positive validation. The signature shall contain a PAdES-B-LTA signature with a signature dictionary containing Type, Contents, Filter, M, SubFilter and ByteRange entries, a DER-encoded CMS binary data object included in the Contents entry including the SigningCertificate (in SignedData.certificates field) attribute, ContentType, ESSSigningCertificateV2, MessageDigest signed attributes and SignatureTimeStamp unsigned attribute, a DSS dictionary containing the Type, Certs and OCSPs entries and a DTS dictionary containing the Type, SubFilter and Contents entries. A new DSS dictionary containing the validation material concerning the certificate that generated the timestamp included in the Contents entry of the DTS dictionary and a new DTS dictionary containing the Type, SubFilter and Contents entries shall be added to the PAdES-B-LTA signature.	 PAdES-B-T signature DSS Type Certs OCSPs DTS Type SubFilter Contents DTS Type SubFilter Contents

10 Testing negative PAdES baseline signatures

10.1 PAdES-B-B signatures test cases

The test cases in this clause have been defined for PAdES-B-B signatures.

Table 6 summarizes negative test cases for PAdES-B-B signatures.

Table 6: Negative test cases for PAdES-B-B signatures

TC ID	Description		
PAdES/BBN/1	Verify a PAdES-B-B signature having a wrong signature (the hash that was signed isn't the hash		
	computed on the specified byte range).		
PAdES/BBN/2	Verify a PAdES-B-B signature created with an untrusted signing certificate.		
PAdES/BBN/3	Verify a PAdES-B-B signature created with an expired signing certificate.		
PAdES/BBN/4	Verify a PAdES-B-B signature created with a revoked/suspended signing certificate.		
PAdES/BBN/5	Verify a PAdES-B-B signature created with a signing certificate generated by a CA whose certificate		
	is revoked/suspended.		
PAdES/BBN/6	Verify a PAdES-B-B signature having a wrong byte range.		

10.2 PAdES-B-T signatures test cases

The test cases in this clause have been defined for PAdES-B-T signatures.

Table 7 summarizes negative test cases for PAdES-B-T signatures.

Table 7: Negative test cases for PAdES-B-T signatures

TC ID	Description		
PAdES/BTN/1	Verify a PAdES-B-T signature in which, at the time in SignatureTimeStamp, the signer certificate had		
	been already expired		
PAdES/BTN/2	Verify a PAdES-B-T signature in which, at the time in SignatureTimeStamp, the signer certificate had		
	been already revoked		
PAdES/BTN/3	Verify a PAdES-B-T signature in which the hash value of messageImprint in SignatureTimeStamp		
	does *NOT* match to the hash value of corresponding signature value in signerInfo		
PAdES/BTN/4	Verify a PAdES-B-T signature in which, at the time in SignatureTimeStamp, the timestamp signer		
	certificate had been already revoked		
PAdES/BTN/5	Verify a PAdES-B-T signature in which, at the time in SignatureTimeStamp, the timestamp signer		
	certificate had been already expired		
PAdES/BTN/6	Verify a PAdES-B-T signature in which the timestamp signer certificate was generated by an		
	untrusted CA		
PAdES/BTN/7	Verify a PAdES-B-T signature in which the timestamp signer certificate was generated by a CA whose		
	certificate is revoked/suspended		

10.3 PAdES-B-LTA signatures test cases

The test cases in this clause have been defined for PAdES-B-LTA signatures.

Table 8 summarizes negative test cases for PAdES-B-LTA signatures.

Table 8: Negative test cases for PAdES-B-LTA signatures

TC ID	Description	
PAdES/BLTAN/1	Verify a PAdES-B-LTA signature in which the time in the SignatureTimeStamp is ulterior than the	
	time in Document Time Stamp	
PAdES/BLTAN/2	2 Verify a PAdES-B-LTA signature in which the Document Time Stamp has a wrong signature (th	
	hash that was signed isn't the hash computed on the specified byte range)	

History

Document history				
V1.1.1	March 2012	Publication		
V2.1.1	June 2016	Publication		

18