ETSI TS 119 144-2 V1.1.1 (2012-03)

Technical Specification

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature (PAdES) Testing Compliance & Interoperability; Part 2: Test Suite for PAdES interoperability test events

Reference

DTS/ESI-000096

Keywords

e-commerce, electronic signature,
interoperability, PAdES, 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

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 (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).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.1].

1 Scope

The present document defines a number of test suites for supporting interoperability tests for PDF Advanced Electronic Signature [7] (PAdES).

The test suites have been defined with four different layers reflecting the multipart structure of PAdES [7]:

Part 2: "PAdES Basic - Profile based on ISO 32000-1";

Part 3: "PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles";

Part 4: "PAdES Long Term - PAdES-LTV Profile";

Part 5: "PAdES for XML Content - Profiles for XAdES signature.

The intention of the test cases is to support software developers in creating interoperable implementations and to get feedback from implementers as input for the PAdES maintenance process and future versions of the present document.

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

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

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

[3] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[4] IETF RFC 2315: "PKCS #7: Cryptographic Message Syntax Version 1.5".

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

[6] IETF RFC 3447 (2003) 'Public-Key Cryptography Standards (PKCS)#1: RSA Cryptography Specifications Version 2.1".

[7] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[8] ETSI TS 102 778-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[9] 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".

[10] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[11] ETSI TS 102 778-5: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

[12] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[13] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

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] ETSI TS 119 144-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature (PAdES) Testing Compliance & Interoperability; Part 1: Overview".

3 Abbreviations

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

BES	Basic Electronic Signature
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DSS	Document Security Store
EPES	Explicit Policy-based Electronic Signature
ESS	Enhanced Security Services
LTV	Long Term Validation
OCSP	Online Certificate Status Protocol
PAdES	PDF Advanced Electronic Signatures
PDF	Portable Document Format
PKCS	Public Key Cryptographic Standard
TSS	Time Stamping Service
VRI	Validation Related Information
XFA	XML Forms Architecture
XML	eXtensible Markup Language

4 Testing PAdES Basic - Profile based on ISO 32000-1

This clause refers to the standard PAdES part 2 defined in [8]. The test cases test PAdES signatures conformance to the PAdES part 2 [8], they test the use of PDF signatures, as described in ISO 32000-1 [1] and based on CMS.

4.1 Testing PAdES-basic

The test cases in this section have been defined for different combinations of CMS/PDF attributes but the following minimum requirements must be satisfied.

A byte range digest shall be computed over a range of bytes in the file, that shall be indicated by the ByteRange entry in the signature dictionary. This range should be the entire file, including the signature dictionary but excluding the signature value itself (the Contents entry). The signature is encoded in CMS defined by PKCS #7 1.5 (RFC 2315 [4]), placed into the Contents entry of the signature dictionary and at minimum contains the signer's X.509 signing certificate. The subfilter entry is adbe.pkcs7.detached. The signature dictionary shall not contain a Cert entry.

The test cases in this section are described in Table 1.

Table 1: Test cases for PAdES-Basic

Test case n°	Description	Notes
P-PK7-1	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and signature dictionary entry M (signing time) and the hashing algorithm SHA256. The signature must be an approval signature as defined in ISO 32000-1 [1].	
P-PK7-2	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and signature dictionary entry M (signing time) and the hashing algorithm SHA1. The signature must be an approval signature as defined in ISO 32000-1 [1].	
P-PK7-3	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and signature dictionary entries Reason, Location, ContactInfo and the hashing algorithm SHA256. Moreover the timestamping of the signature embedded as described in ISO 32000-1 [1] clause 12.8.3.3.1.The signature must be an approval signature as defined in ISO 32000-1 [1].	
P-PK7-4	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and signature dictionary entry M (signing time) and the hashing algorithm SHA256. Moreover the embedded revocation information ISO 32000-1 [1], clause 12.8.3.3.2 with CRL method. The signature must be an approval signature as defined in ISO 32000-1 [1].	CRL: Certificate Revocation List, described in RFC 3280 [12].
P-PK7-5	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and signature dictionary entry M (signing time) and the hashing algorithm SHA256. Moreover the embedded revocation information ISO 32000-1 [1], clause 12.8.3.3.2 with OCSP method. The signature must be an approval signature as defined in ISO 32000-1 [1].	OCSP: Online Certificate Status Protocol response, described in RFC 2560 [13].
P-PK7-6	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and signature dictionary entries M (signing time), reason, and seed value dictionary entries. The signature must be an approval signature as defined in ISO 32000-1 [1].	the value of the hashing algorithm to be chosen depending of a seed value dictionary, it could assume the value of SHA1 or SHA256 depending of the relative entry in the seed value dictionary.
P-PK7-7	This test case tests PAdES signatures conformance to the PAdES part 2 [8], with minimum requirements and with signature dictionary entry M (signing time) and the hashing algorithm SHA256. It contains also "legal content attestation" as defined in ISO 32000-1 [1], clause 12.8.5. The signature must be a certification signature as defined in ISO 32000-1 [1].	
P-PK7-8	This test case tests PAdES signatures conformance to the PAdES part 2 [8], when a second serial signature is added to a signed PDF file. The serial signature must have the minimum requirements and signature dictionary entry M (signing time) and the hashing algorithm SHA256. The signature must be an approval signature as defined in ISO 32000-1 [1].	Possible input could be a P-PK7-1 test case file.

4.2 Negative test cases

Negative test cases are performed on wrong and not conformant PDF signed files to test the correctness of the negative response. Possible tests are:

- Verify a signed (pades basic) pdf document having a seed value that specify use of PKCS#1 [6]
- Verify a signed pdf document having a wrong byte range

- Verify a signed pdf document having a wrong signature (the hash that was signed is not the hash of the specified byte range)
- Verify a pdf document signed with an untrusted signing certificate
- Verify a pdf document signed with an expired signing certificate
- Verify a pdf document signed with a revoked/suspended signing certificate
- Verify a signed pdf document containing an untrusted signature timestamp
- Verify a signed pdf document containing an expired signature timestamp
- Verify a signed pdf document containing a revoked signature timestamp
- Verify a signed pdf document containing a wrong format in signing time
- Verify a signed pdf document not containing the signing certificate inside the PKCS#7

5 Testing PAdES Enhanced - PAdES-BES/EPES Profile

This clause refers to the standard PAdES part 3 [9]. The test cases test PAdES signatures conformance to the PAdES part 3 [9], they test the use of PDF signatures those formats are equivalent to the signature forms CAdES-BES, CAdES-EPES and CAdES-T as specified in TS 101 733 [2].

5.1 Testing PAdES-BES

The test cases in this section have been defined for different combinations of CADES-BES attributes but the following minimum requirements must be satisfied.

A byte range digest shall be computed over a range of bytes in the file, which shall be indicated by the ByteRange entry in the signature dictionary. This range should be the entire file, including the signature dictionary but excluding the signature value itself (the Contents entry). A DER-encoded SignedData object as specified in CMS (RFC 3852 [5]) shall be included as the PDF signature in the entry with the key Content of the signature dictionary. The signature dictionary shall contain a value of "ETSI.CAdES.detached" for the key SubFilter. The signature dictionary shall not contain a Cert entry.

Mandatory attributes for PADES-BES described in [9] profile, clauses 4.4.1, 4.4.2 and 4.4.3, should be present.

The test cases in this section are described in Table 2.

Table 2: Test cases PADES-BES

Test case n°	Description	Notes
P-BES-1	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements, signature dictionary entry M (signing time), ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2] and the hashing algorithm SHA256.	
P-BES-2	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256 and signature dictionary entries: Reason, Location, ContactInfo and M (signing time).	
P-BES-3	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256 and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2].	
P-BES-4	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256, ClaimedAttributes of the signer as defined in clause 5.11.3 of CAdES [2] and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2].	The implementation may add any value of a claimed attribute as far as respecting PadES and CadES.
P-BES-5	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256, CertifiedAttributes of the signer as defined in clause 5.11.3 of CAdES [2] and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2].	
P-BES-6	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256, content time stamp of the signer as defined in clause 5.11.4 of CAdES [2] and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2].	Content-time-stamp indicates that the signed information was formed before the date included in the content-time-stamp.
P-BES-7	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate attribute as defined in clause 5.7.3.1 of CAdES [2], the hashing algorithm SHA1, commitment-type-indication as defined in clause 5.11.11 of CAdES [2] and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2].	

5.2 Testing PAdES-EPES

The test cases in this section have been defined for different combinations of CADES-EPES attributes but the following minimum requirements must be satisfied.

A byte range digest shall be computed over a range of bytes in the file, which shall be indicated by the ByteRange entry in the signature dictionary. This range should be the entire file, including the signature dictionary but excluding the signature value itself (the Contents entry). A DER-encoded SignedData object as specified in CMS (RFC 3852 [5]) shall be included as the PDF signature in the entry with the key Content of the signature dictionary. The signature dictionary shall contain a value of ETSI.CAdES.detached for the key SubFilter. The signature dictionary shall not contain a Cert entry.

Mandatory attributes for PADES-BES described in [9] profile, clauses 4.4.1, 4.4.2 and 4.4.3, should be present.

The test cases in this section are described in Table 3.

Table 3: Test cases PADES-EPES

Test case n°	Description	Notes
P-EPES-1	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-v2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256, signature dictionary entries: Reason, Location, ContactInfo and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2]. The signature-policy-identifier attribute shall be present as a signed attribute. The rules from clause 5.8.1 in CAdES [2].	
P-EPES-2	This test case tests PAdES signatures conformance to the PAdES part 3 [9], with minimum requirements and ESS signing-certificate-V2 attribute as defined in clause 5.7.3.2 of CAdES [2], the hashing algorithm SHA256, commitment-type-indication as defined in clause 5.11.11 of CAdES [2] and the unsigned attribute signature-time-stamp as defined in clause 6.1 of CADES-T [2]. The signature-policy-identifier attribute shall be present as a signed attribute. The rules from clause 5.8.1 in CAdES [2].	

5.3 Negative test cases

Negative test cases are performed on wrong and not conformant PDF signed files to test the correctness of the negative response. Possible tests are:

- Verify a signed pdf document having a wrong byte range
- Verify a signed pdf document having a wrong signature (the hash that was signed is not the hash of the specified byte range)
- Verify a signed pdf document having a wrong time stamp signature (the signature that was timestamped is not pdf document signature)
- Verify a pdf document signed with an untrusted signing certificate
- Verify a pdf document signed with an expired signing certificate
- Verify a pdf document signed with a revoked/suspended signing certificate
- Verify a signed pdf document containing an untrusted signature timestamp
- Verify a signed pdf document containing an expired signature timestamp
- Verify a signed pdf document containing a revoked signature timestamp
- Verify a signed pdf document in which the hash value of the signing certificate is different from the hash value in signing certificate or ESS signing certificate V2 attribute
- Verify a signed pdf document containing signing-time attribute (PAdESs part 3 [9], clause 4.5)
- Verify a signed pdf document containing signing-location attribute (PAdESs part 3 [9], clause 4.5)
- Verify a signed pdf document containing counter-signature attribute (PAdESs part 3 [9], clause 4.5)
- Verify a signed pdf document containing content-reference attribute (PAdESs part 3 [9], clause 4.5)
- Verify a signed pdf document containing content-identifier attribute (PAdESs part 3 [9], clause 4.5)
- Verify a signed pdf document containing content-hints attribute (PAdESs part 3 [9], clause 4.5)
- Verify a signed pdf document containing commitment-type-indication attribute and the attribute reason of the dictionary (PAdESs part 3 [9], clause 4.5)

- Verify a signed pdf document containing signer-location attribute (PAdESs part 3 [9], clause 4.5)

6 Testing PAdES LongTerm - PAdES-LTV Profile

This clause refers to the standard PAdES part 4 [10]. The test cases test PAdES signatures conformance to the PAdES part 4 [10].

The PAdES part 4 [10] profile supports Long Term Validation (LTV) of PDF Signatures using some extensions from ISO 32000-1 [1]. They are:

- Document Security Store (DSS) that is able to carry validation data necessary to validate a signature, optionally with.
- Validation Related Information (VRI) which relates the validation data to a specific signature.
- Document time-stamp that is able to extend document life-time.

6.1 Testing PAdES-LTV

Those test cases start from different input PDF signed file. Those test cases generate validation stuff on different PDF signed file.

The test cases in this section are described in Table 4.

Table 4: Test cases PADES-LTV

Test case n°	Description	Notes
P-LTV-1	This test case verifies signature and generates subsequent PadES-LTV [10] based on DSS with Certificates and CRLs. Then only one Document time-stamp must be applied and then verified.	Generate validation stuff on PAdES part. 2 signed file, possible input: P-PK7-1 CRL: Certificate Revocation List, described in RFC 3280 [12].
P-LTV-2	This test case verifies signature and timestamp then generates subsequent PadES-LTV [10] based on DSS with Certificates and OCSP. Then only one Document time-stamp must be applied and then verified.	Generate validation stuff on PAdES part. 2 signed file with timestamping, possible input: P-PK7-3 OCSP: Online Certificate Status Protocol response, described in RFC 2560 [13].
P-LTV-3	This test case verifies signature and timestamp then generates subsequent PadES-LTV [10] based on DSS with Certificates and CRLs.	Generate validation stuff on PAdES part. 3 signed file with signature-time-stamping, possible input P-BES-3.
P-LTV-4	This test case verifies signature and generates subsequent PadES-LTV [10] based on DSS with VRI entry and VRI dictionary with Certificate and CRL entries and then verifies it. Then only Document time-stamp must be applied and verified.	Generate validation stuff on PAdES part. 3 signed file, possible input P-BES-1.
P-LTV-5	This test case verifies signatures (the input contains a serial signature) and generates subsequent PadES-LTV based on DSS with Certs and VRI entries and VRI dictionaries with OCSP entries and then verifies it. Then only one Document time-stamp must be applied and verified.	Generate validation stuff on PAdES part. 2 signed file with a serial signature, possible input P-PK7-8.
P-LTV-6	This test case applies a Document time-stamp and verifies.	Add a document timestamp.
P-LTV-7	This test case verifies signatures (the input contains a serial signature) and generates subsequent PadES-LTV based on DSS with VRI entries, a VRI dict with Cert and OCSP entries for one signature, and a VRI dict with Cert and CRL entries for the other signature and then verifies them.	Generate validation stuff on PAdES part. 3 signed file with a serial signature, possible input P-BES-8.

Test case n°	Description	Notes
P-LTV-8	This test case verifies and generates subsequent verifies a P-LTV-6 signatures and Document time-stamp and generates subsequent PadES-LTV updating DSS entries. Then a second Document time-stamp must be applied and verified.	Add a document timestamp on a document with a previous document time stamp, possible input P-LTV-6.
P-LTV-9	This test case applies a Document time-stamp and verifies on unsigned PDF document.	Any PDF document as input.
P-LTV-10	This test case applies a Document time-stamp and verifies on unsigned PDF document with a previous Document time-stamp.	Possible input: P-LTV-9.
P-LTV-11	This test case verifies and generates subsequent verifies a P-LTV-9 Document time-stamp and generates subsequent PadES-LTV updating DSS entries based on VRI with Certificates and OCSPs for Document time-stamp. And then apply a new Document time-stamp.	Possible input: P-LTV-9.
P-LTV-12	This test case verifies and generates subsequent verifies a P-LTV-9 Document time-stamp and generates subsequent PadES-LTV updating DSS entries based on VRI with Certificates and CRLs for Document time-stamp. And then apply a new Document time-stamp.	Possible input: P-LTV-9.

6.2 Negative test cases

Negative test cases are performed on wrong and not conformant PDF signed files to test the correctness of the negative response. Possible tests are:

- Verify a signed pdf in which one timestamp is invalid at the time of the successive (in time) timestamp (TSS certificate expired or revoked)
- Verify a signed pdf in which the signature of one timestamp is not valid in respect of validation data stored in the DSS
- Verify a signed pdf document in which the signature is not valid in respect of validation data stored in the DSS

7 Testing: PAdES for XML Content

This clause refers to the standard PAdES part 5 [11]. The test cases test PAdES signatures conformance to the PAdES part 5 [11], they deal with signing XML content within the PDF containers.

An XML document created and signed with XAdES (forms XAdES-BES, XAdES-EPES, XAdES-T) according to [3] out of PDF framework can be embedded within a PDF container and transported within it.

For the purpose to verify the signatures of an XML document signed with XAdES [3] and embedded within a PDF container long after their creation, a verifier may extracts the XML document, verify the XAdES signature, upgrade the XAdES signature itself (to more evolved forms) and embeds again the modified XML document within the PDF container.

Minimum requirement: The xades;SigningCertificate or the ds:KeyInfo element must be used to secure the signing certificate.

The test cases in this section are described in Table 5.

Table 5: Test cases PADES-XML

Test case n°	Description	Notes
P-XML-1	This test case tests PAdES signatures conformance to the PAdES part 5 [11] clause 4, with minimum requirements and SigningTime, SignaturePolicyIdentifier, SignatureProductionPlace,SignerRole elements (clause 4.2.5 PAdES part 5 [11])	
P-XML-2	This test case tests a PAdES signatures conformance to the PAdES part 5 [11] clause 4, with minimum requirements and DataObjectFormat,CommitmentTypeIndication, AllDataObjectsTimeStamping, IndividualDataObjectsTimeStamp, SignatureTimeStamp elements (clause 4.2.5 PAdES part 5 [11])	
P-XML-3	This test case tests a PAdES signatures conformance to the PAdES part 5 [11] clause 4, with a counter signature	Possible input P-XML-1
P-XML-4	This test case tests a PAdES signatures conformance to the PAdES part 5 [11] clause 4, with XADES-C CompleteCertificateRefs, CompleteRevocationRefs elements	Possible input P-XML-2
P-XML-5	This test case tests a PAdES signatures conformance to the PAdES part 5 [11] clause 4, with XADES-X SigAndRefsTimeStamp elements	Possible input P-XML-2
P-XML-6	This test case tests a PAdES signatures conformance to the PAdES part 5 [11] clause 4, with XADES-A ArchiveTimeStamp element	Possible input P-XML-2

7.1 Testing Basic XAdES signatures on XFA forms

The XAdES signature will be able to sign XFA data only or any XML content from XFA allowed by XFA specification, Signature is encoded as XAdES-BES and XAdES-T forms.

The xades:SigningCertificate or the ds:KeyInfo element must be used to secure the signing certificate.

For long-term validation XAdES signatures on XFA use the LTV technology (XADES-LTV).

The test cases in this section are described in Table 6.

Table 6 Test cases PADES-XFA

Test case n°	Description	Notes
P-XFA-1	This test case tests a PAdES signatures conformance to the PAdES part 5 clause 5 [11], with minimum requirements and SigningTime, SignaturePolicyIdentifier, SignatureProductionPlace,SignerRole elements (clause 5.2.4 PAdES part 5 [11]) and a SignatureTimeStamp.	
P- XFA -2	This test case tests a PAdES signatures conformance to the PAdES part 5 clause 5 [11], with minimum requirements and DataObjectFormat,CommitmentTypeIndication, AllDataObjectsTimeStamping, IndividualDataObjectsTimeStamp elements(clause 5.2.4 PAdES part 5 [11]).	
P- XFA -3	This test case tests a PAdES signatures conformance to the PAdES part 5 clause 5 [11], with a CounterSignature.	Possible input: P-XFA-2.
P- XFA -4	This test case tests a PAdES signatures conformance to the PAdES part 5 clause 5 [11] with a PADES-LTV This test case verifies signature and generates subsequent PadES-LTV based on DSS with VRI entries, a VRI dict with Cert and CRLs entries for one signature and then verifies them.	Possible input P-XFA-1.
P- XFA -5	This test case tests a PAdES signatures conformance to the PAdES part 5 clause 5 [11] with a PADES-LTV This test case verifies signature and generates subsequent PadES-LTV based on DSS with VRI entries, a VRI dict with Cert and CRLs entries for one signature and then verifies them. Then a Document time-stamp must be applied and verified.	Possible input P-XFA-1.

7.2 Negative test cases

Negative test cases are performed on wrong and not conformant PDF signed files to test the correctness of the negative response. Possible tests are:

- Verify a pdf document signed with XAdES signatures on XFA Forms with SigningTime (SigningTime shall not be used).
- Verify a pdf document signed with XAdES-BES signatures and CommitmentTypeIndication.
- Verify a pdf document where both XFA template and XFA data are signed.

History

Document history		
V1.1.1	March 2012	Publication