ETSI TS 119 144-3 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures -
Testing Conformance and Interoperability;
Part 3: Test suites for testing interoperability of additional PAdES signatures

Reference

DTS/ESI-0019144-3

Keywords

conformance, e-commerce, electronic signature, 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:
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 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 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.

1 Scope

The present document defines a number of test suites to assess the interoperability between implementations claiming conformance to additional PAdES signatures profiles [3].

The present document defines test suites for each profile defined in ETSI EN 319 142-2 [3].

Test suites also cover augmentation of additional PAdES 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] 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 EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

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

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

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

[6] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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".

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] and the following apply:

XFA XML Forms Architecture

4 Testing CMS digital signatures in PDF interoperability

4.1 Introduction

This clause refers to clause 4 of ETSI EN 319 142-2 [3]. The test cases in this clause have been defined for different combinations of CMS digital signatures in PDF attributes. They test the use of PDF signatures, as described in ISO 32000-1 [1] and based on CMS.

Mandatory attributes for CMS digital signatures in PDF described in ETSI EN 319 142-2 [3], clause 4.2, shall be present.

4.2 Testing CMS digital signatures in PDF

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

Mandatory attributes for CMS digital signatures in PDF described in ETSI EN 319 142-2 [3], clause 4, shall be present.

Table 1 shows which attributes are required to generate CMS digital signatures in PDF for each test case.

Table 1: Test cases for CMS digital signatures in PDF

TC ID	Description	Pass criteria	Signature attributes
PAdES/CMS/1	This is the simplest CMS digital signatures in PDF with minimum requirements and signature dictionary entry M (signing time). The signature shall be an approval signature as defined in ISO 32000-1 [1].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded PKCS #7 binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType and SignerInfo attributes.	• SignatureDictionary o Type o Sig o Filter o Adobe.PPKLite o SubFilter o adbe.pkcs7.detached o M o ByteRange o Contents (DER PKCS #7) o Certificates o SigningCertificate o ContentType o SignerInfo
PAdES/CMS/2	This test case tests a CMS digital signature in PDF with signature time stamp attribute which ensures the time of signing, Location attribute which describes where the data was signed (CPU host name or physical location), Reason attribute that describes the reason for the signing, ContactInfo attribute that provides information to enable a recipient to contact the signer to verify the signature.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, Reason, Location, ContactInfo and ByteRange entries. The DER-encoded PKCS #7 binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, SignerInfo and SignatureTimestamp attributes.	• SignatureDictionary o Type o Sig o Filter o Adobe.PPKLite o SubFilter o adbe.pkcs7.detached o Reason o Location o ContactInfo o ByteRange o Contents (DER PKCS #7) o Certificates o SigningCertificate o ContentType o SignerInfo o SignatureTS
PAdES/CMS/3	This test case tests a CMS digital signature in PDF with signature time stamp attribute which ensures the time of signing and adbe Revocation Information attribute to ensure revocation checks for the signing certificate and its issuer certificates. Certificate revocation list, described in IETF RFC 5280 [6] shall be used.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, and ByteRange entries. The DER-encoded PKCS #7 binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, SignerInfo, SignatureTimestamp and RevocationInfo attributes.	• SignatureDictionary o Type o Sig o Filter o Adobe.PPKLite o SubFilter o adbe.pkcs7.detached o ByteRange o Contents (DER PKCS #7) o Certificates o SigningCertificate o ContentType o SignerInfo o SignatureTS o RevocationInfo ▪ Crls

TC ID	Description	Pass criteria	Signature attributes
PAdES/CMS/4	This test case tests a CMS digital signature in PDF with signature time stamp attribute which ensures the time of signing and adbe Revocation Information attribute to ensure revocation checks for the signer's certificate and its issuer certificates. OCSP responses, described in IETF RFC 6960 [5] shall be used.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, and ByteRange entries. The DER-encoded PKCS #7 binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType, SignerInfo, SignatureTimestamp and RevocationInfo attributes.	• SignatureDictionary o Type o Sig o Filter o Adobe.PPKLite o SubFilter o adbe.pkcs7.detached o ByteRange o Contents (DER PKCS #7) o Certificates o SigningCertificate o ContentType o SignerInfo o SignatureTS o RevocationInfo ▪ OCSP resp
PAdES/CMS/5	This test case tests a CMS serial digital signature in PDF. The signed document shall include 2 serial signatures.	Positive validation. The signed document shall contain 2 serial signatures. The signature dictionary of every signature shall contain Type, Contents, Filter, SubFilter, M and ByteRange entries. The DER-encoded PKCS #7 binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType and SignerInfo attributes.	• SignatureDictionary (2 entries) o Type o Sig o Filter o Adobe.PPKLite o SubFilter o adbe.pkcs7.detached o ByteRange o M o Contents (DER PKCS #7) o Certificates o SigningCertificate o ContentType o SignerInfo
PAdES/CMS/6	This test case tests a CMS certification digital signature in PDF with signing time and LegalContentAttestation attributes.	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M, Reference and ByteRange entries. The DER-encoded PKCS #7 binary data object included in the Contents entry shall include the SigningCertificate (in SignedData.certificates field), ContentType and SignerInfo attributes. The attestation entry in the LegalAttestationDictionary shall be valued.	• LegalAttestationDictionary • SignatureDictionary o Type o Sig o Filter o Adobe.PPKLite o SubFilter o adbe.pkcs7.detached o ByteRange o M o Reference o DocMDP o Contents (DER PKCS #7) o Certificates o SigningCertificate o ContentType o SignerInfo

5 Testing interoperability of PAdES-E-BES and PAdES-E-EPES signatures

5.1 Introduction

This clause refers to clauses 5.3 of ETSI EN 319 142-2 [3]. The test cases in this clause have been defined for different combinations of PAdES-E-BES and PAdES-E-EPES signatures attributes.

Mandatory attributes for PAdES-E-BES and PAdES-E-EPES signatures described in ETSI EN 319 142-2 [3], clauses 5.2, 5.3 and 5.4, shall be present.

5.2 Testing PAdES-E-BES signatures

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

Table 2: Test cases for PAdES-E-BES signatures

TC ID	Description	Pass criteria	Signature attributes
PAdES/BES/1	This test case tests the simplest PAdES-E-BES signature without signature-time-stamp and with M entry in signature dictionary. ContentType, ESSSigningCertificateV2 and MessageDigest attributes shall be added to the PDF signature as specified in CAdES [4].	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 o Type o Sig o Filter o Adobe.PPKLite o SubFilter o ETSI.CAdES.detached o M o ByteRange o Contents (DER CMS) o Certificates o SigningCertificate o ContentType o MessageDigest o ESSSigningCertificateV2
PAdES/BES/2	This test case tests a PAdES-E-BES signature without signature-time-stamp and with M, Location, Reason and ContactInfo entries in signature dictionary. ContentType, ESSSigningCertificateV2 and MessageDigest attributes shall be added to the PDF signature as specified in CAdES [4].	Positive validation. The signature dictionary shall contain Type, Contents, Filter, SubFilter, M, Location, Reason, ContactInfo 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 o Type o Sig o Filter o Adobe.PPKLite o SubFilter o ETSI.CAdES.detached o M o Location o Reason o ContactInfo o ByteRange o Contents (DER CMS)) o Certificates o SigningCertificate o ContentType o MessageDigest o ESSSigningCertificateV2
PAdES/BES/3	This test case tests the simplest PAdES-E-BES signature with signature-time-stamp attribute. ContentType, ESSSigningCertificateV2, MessageDigest and SignatureTimeStamp attributes shall be added to the PDF signature as specified in CAdES [4].	Positive validation. The signature dictionary shall contain Type, 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, ESSSigningCertificateV2, MessageDigest signed attributes and SignatureTimeStamp unsigned attribute.	• SignatureDictionary o Type o Sig o Filter o Adobe.PPKLite o SubFilter o ETSI.CAdES.detached o ByteRange o Contents (DER CMS) o Certificates SigningCertificate o ContentType o MessageDigest o ESSSigningCertificateV2 o SignatureTimeStamp