ETSI TR 119 124-1 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures -
Testing Conformance and Interoperability;
Part 1: Overview

Reference
DTR/ESI-0019124-1

Keywords
CAdES, conformance, e-commerce, electronic signature, 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

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 Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering CAdES digital signatures - Testing Conformance and Interoperability, as identified below:

ETSI TR 119 124-1: "Overview";

ETSI TS 119 124-2: "Test suites for testing interoperability of CAdES baseline signatures";

ETSI TS 119 124-3: "Test suites for testing interoperability of extended CAdES signatures";

ETSI TS 119 124-4: "Testing Conformance of CAdES baseline signatures";

ETSI TS 119 124-5: "Testing Conformance of extended CAdES signatures".

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

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

Introduction

The multi-part deliverable defines test suites for testing interoperability and conformance of CAdES signatures. The set of Technical Specifications consist of four documents.

The test suites for testing interoperability of CAdES baseline signatures (Part 2 [i.6]) and the specifications required for building software tools for testing technical conformance of CAdES baseline signatures (Part 4 [i.4]) are defined against ETSI EN 319 122-1 [i.1]. The test suites for testing interoperability of extended CAdES signatures (Part 3 [i.7]) and the specifications required for building software tools for testing technical conformance of extended CAdES signatures (Part 5 [i.8]) are defined against ETSI EN 319 122-2 [i.2].

1 Scope

The present document provides an overview of the set of test suites for testing interoperability and conformance of CAdES signatures.

The present document:

a) provides a general description of the set of test suites for testing interoperability and conformance of CAdES signatures; and

b) lists the features of every test suite for testing interoperability and conformance of CAdES signatures.

The present document is for information only. Normative requirements of each test suite are in other parts of this multi-part deliverable.

2 References

2.1 Normative references

As informative publications shall not contain normative references this clause shall remain empty.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

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

[i.2] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.4] ETSI TS 119 124-4: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing conformance of CAdES baseline signatures".

[i.5] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.6] ETSI TS 119 124-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures".

[i.7] ETSI TS 119 124-3: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures".

[i.8] ETSI TS 119 124-5: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing conformance of extended CAdES signatures".

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.3] and the following apply:

negative test case: test case for a signature whose validation according to ETSI EN 319 102-1 [i.5] 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.3] apply.

4 Testing Conformance and Interoperability

4.1 Part 2: Test suites for testing interoperability of CAdES baseline signatures

ETSI TS 119 124-2 [i.6] specifies the test suites for testing interoperability of CAdES baseline signatures against ETSI EN 319 122-1 [i.1].

ETSI EN 319 122-1 [i.1] defines four different levels of CAdES baseline signatures.

The test suites are defined with different layers reflecting the levels of CAdES baseline signatures specified in [i.1].

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

4.2 Part 3: Test suites for testing interoperability of extended CAdES signatures

ETSI TS 119 124-3 [i.7] specifies the test suites for testing interoperability of extended CAdES signatures against ETSI EN 319 122-2 [i.2].

ETSI EN 319 122-2 [i.2] defines different signature forms.

The test suites are defined with different layers reflecting the forms of Extended CAdES signatures specified in [i.2].

Testing CAdES signatures:

- CAdES-E-BES signatures test cases;
- CAdES-E-EPES signatures test cases;
- CAdES-E-T signatures test cases;
- CAdES-E-C test cases;
- CAdES-E-X test cases;
- CAdES-E-X Long test cases;
- CAdES-E-A signatures (with ATSv2 and ATSv3) built on CAdES-E-T signatures test cases.

Testing negative extended CAdES signatures:

- CAdES-E-BES test cases;
- CAdES-E-EPES test cases;
- CAdES-E-T test cases;
- CAdES-E-A test cases.

Testing augmentation of CAdES signatures:

- augmenting to CAdES-E-C forms test cases;
- augmenting to CAdES-E-X forms test cases;
- augmenting to CAdES-E-XL forms test cases;
- augmenting to CAdES-E-A forms test cases.

4.3 Part 4: Testing Conformance of CAdES baseline signatures

ETSI TS 119 124-4 [i.4] defines the requirements for building software tools for testing technical conformity of CAdES baseline signatures against ETSI EN 319 122-1 [i.1].

ETSI EN 319 122-1 [i.1] defines requirements for building blocks and CAdES baseline signatures. For the purpose of identifying the whole set of test assertions required for testing conformance against CAdES baseline signatures as specified in ETSI EN 319 122-1 [i.1], ETSI TS 119 124-4 [i.4] classifies the whole set of requirements specified in ETSI EN 319 122-1 [i.1] in two groups as follows:

1) requirements specific to CAdES baseline signatures;
2) requirements common to both CAdES baseline signatures as specified in ETSI EN 319 122-1 [i.1] and extended CAdES signatures as specified in ETSI EN 319 122-2 [i.2].

4.4 Part 5: Testing Conformance of extended CAdES signatures

ETSI TS 119 124-5 [i.8] defines the requirements for building software tools for testing technical conformance of extended CAdES signatures against ETSI EN 319 122-2 [i.2].

ETSI EN 319 122-1 [i.1] defines requirements for building blocks and CAdES baseline signatures. For the purpose of identifying the whole set of test assertions required for testing conformance against extended CAdES signatures as specified in ETSI EN 319 122-2 [i.2], ETSI TS 119 124-5 [i.8] classifies the whole set of requirements specified in ETSI EN 319 122-1 [i.1] and in ETSI EN 319 122-2 [i.2] in two groups as follows:

1) requirements common to both CAdES baseline signatures as specified in ETSI EN 319 122-1 [i.1] and extended CAdES signatures as specified in ETSI EN 319 122-2 [i.2] (these requirements are incorporated by references to ETSI TS 119 124-4 [i.4]);

2) requirements specific to extended CAdES signatures.

Annex A: Bibliography

- IETF RFC 5652 (09-2009): "Cryptographic Message Syntax (CMS)".
- ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".
- ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

History

Document history		
V1.1.1	June 2016	Publication