



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

---

Reference

DTS/ESI-0019124-3

---

Keywords

CAdES, e-commerce, electronic signature, interoperability, 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**

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

Intellectual Property Rights .....	4
Foreword.....	4
Modal verbs terminology.....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references.....	5
3 Definitions and abbreviations.....	6
3.1 Definitions .....	6
3.2 Abbreviations .....	6
4 Overview .....	6
5 Testing extended CAAdES signatures interoperability.....	7
5.1 CAAdES-E-BES test cases .....	7
5.2 CAAdES-E-EPES test cases .....	8
5.3 CAAdES-E-T test cases .....	9
5.4 CAAdES-E-C test cases .....	9
5.5 CAAdES-E-X test cases.....	11
5.6 CAAdES-E-XL test cases .....	12
5.7 CAAdES-E-A test cases.....	14
6 Testing extended CAAdES signatures augmentation interoperability.....	18
6.1 Introduction .....	18
6.2 Augmentation to CAAdES-E-C signatures test cases .....	18
6.3 Augmentation to CAAdES-E-X signatures test cases .....	19
6.4 Augmentation to CAAdES-E-XL signatures test cases .....	20
6.5 Augmentation to CAAdES-E-A signatures test cases.....	21
7 Testing negative extended CAAdES signatures.....	22
7.1 CAAdES-E-BES test cases .....	22
7.2 CAAdES-E-EPES test cases .....	23
7.3 CAAdES-E-T test cases .....	23
7.4 CAAdES-E-A test cases.....	25
History .....	27

---

## 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 CADES 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 extended CAAdES signatures [2].

The present document defines test suites for each level defined in ETSI EN 319 122-2 [2].

Test suites also cover augmentation of extended CAAdES 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 <https://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); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures".
- [2] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 2: Extended CAAdES 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 119 124-1: "Electronic Signatures and Infrastructures (ESI); CAAdES 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".
- [i.4] IETF RFC 3125 (09-2001): "Electronic Signature Policies".