



SPECIAL REPORT

**Electronic Signatures and Infrastructures (ESI)
Testing interoperability and conformity activities to be run
during the implementation and promotion of the framework of
digital signatures**

Reference

RSR/ESI-0003186v211

Keywords

conformance, e-commerce, electronic signature,
interoperability, 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	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	9
4 Technical Approach and Methodology for Conformance and Interoperability testing.....	10
4.1 Introduction to conformance and interoperability testing.....	10
4.2 Gathering inputs	10
4.3 Standards to be targeted by testing events and criteria to identify them.....	11
4.4 Criteria to identify the scope of testing events	11
4.5 Rules to identify priorities in the testing event scheduling.....	12
5 Standards targeted for Testing and Testing Specifications	12
5.0 Introduction	12
5.1 Identification of standards that benefit from Conformance and Interoperability Testing events	12
5.2 List of Technical Specifications for Testing Conformance and Interoperability.....	13
5.2.0 Introduction.....	13
5.2.1 CAdES Testing Conformance and Interoperability	13
5.2.2 XAdES Testing Conformance and Interoperability.....	14
5.2.3 PAdES Testing Conformance and Interoperability.....	14
5.2.4 ASiC Testing Conformance and Interoperability	14
5.2.5 Testing Conformance of Trusted Lists.....	15
6 Planning of identified activities.....	15
6.1 Proposed scheduling and scoping of testing events.....	15
6.2 Planning for the production of Technical Specifications for Testing Conformance and Interoperability	16
6.2.0 Introduction.....	16
6.2.1 Deliverable D1: Stable Draft for TB Review (SPR).....	16
6.2.2 Deliverables D2: Final Draft for approval (FTB)	18
6.2.3 Deliverables D3: Publication (PTS).....	18
6.3 Production plan for conformity testing tools development	19
Annex A: History of ETSI/ESI Plugtests	20
A.1 AdES Signature Plugtests.....	20
A.2 TSL Plugtests and Conformance tools	21
Annex B: ETSI/ESI Plugtests	22
B.1 Plugtest Portal	22
B.1.0 Introduction	22
B.1.1 Public part of the portal	22
B.1.2 Private part of the portal.....	23
B.1.2.0 Introduction.....	23
B.1.2.1 Contents of Common area of Private part.....	24
B.1.2.1.1 Conducting Plugtests information pages.....	24
B.1.2.1.2 Cryptographic material pages.....	24
B.1.2.1.3 Online PKI-related services pages	25
B.1.2.1.4 Attribute certificate issuance page	25
B.1.2.2 Contents of Signatures Interop Specific areas of Private part.....	25
B.1.2.2.0 Introduction.....	25

B.1.2.2.1	Test Cases Definition Language	25
B.1.2.2.2	Test Cases pages	25
B.1.2.2.3	Individual verification reports.....	26
B.1.2.2.4	Upload pages.....	26
B.1.2.2.5	Download pages	26
B.1.2.2.6	Test data directory pages.....	26
B.2	Conducting ETSI/ESI Plugtests	26
B.2.1	Introduction	26
B.2.2	Generation and Cross-verification.....	27
B.2.3	Only Verification.....	28
B.2.4	Upgrade and Arbitration test	28
Annex C:	Bibliography	30
History		31

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

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 details a proposal for ETSI activities related to testing conformance and interoperability performed in parallel with the building up and promotion of the Rationalized Framework for Electronic Signature Standardization ETSI TR 119 000 [i.1].

The critical deliverables, European Standards and Technical Specifications, of the Framework [i.1] that are in preparation at the time of publication of the present document and whose development, adoption and deployment would largely benefit from the organization of testing events are identified together with the required conformity testing tools.

An appropriate scheduling of events for testing interoperability and conformance is proposed, to help ensure that a reasonable amount of implementations are available in the market for being tested and that these tests may actually impact in due time the standardization process, allowing to fix any problem (interoperability, ambiguity, etc.) present in the deliverables under development that are identified during these events.

Finally, a scheduling of conformity testing tools development and deployment is defined, including also recommendations about when and how they will be made available to the community.

The present document covers the period from Q4 2015 to Q4 2016, schedule for previous events is available in the previous version of the present document.

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.

Not applicable.

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 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.2] CEN CWA 16408: "Testing Framework for Global eBusiness Interoperability Test Beds (GITB)", February 2012.

NOTE: Available at: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA_16408.pdf.

[i.3] OASIS Standard: "Test Assertions Model Version 1.0".

NOTE: Available at: <http://docs.oasis-open.org/tag/model/v1.0/testassertionsmodel-1.0.pdf>.