ETSI SR 003 186 V1.1.1 (2013-12)

Special Report

Testing interoperability and conformity activities to be run during the implementation and promotion of the Rationalized Framework of Electronic Signatures

Reference

DSR/ESI-00125

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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

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 [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.

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 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.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

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 SR 001 604: "Rationalised Framework for Electronic Signature Standardisation".

NOTE: This Special Report includes a description and plans for publication for all the deliverables mentioned in the present document and not yet available. The reader is adviced that [i.1] at present is under revision and will be replaced by TR 119 000.

[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.

[i.4] Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.5] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.6] Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

[i.7] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

NOTE: This document will be replaced by TS 119 312.

[i.8] ETSI TS 101 733 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

NOTE: This document will be replaced by EN 319 122-1.

[i.9] ETSI TS 103 173 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

NOTE: This document will be replaced by EN 319 122-2.

[i.10] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

NOTE: This document will be replaced by EN 319 132-1.

[i.11] ETSI TS 103 171 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

NOTE: This document will be replaced by EN 319 132-2.

[i.12] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.13] ETSI TS 102 778-2 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

NOTE: This document will be replaced by EN 319 142-2.

[i.14] ETSI TS 102 778-3 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

NOTE: This document will be replaced by EN 319 142-3.

[i.15] ETSI TS 102 778-4 (V1.1.2): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

NOTE: This document will be replaced by EN 319 142-4.

[i.16] ETSI TS 102 778-5 (V1.1.2): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

NOTE: This document will be replaced by EN 319 142-5.

[i.17] ETSI TS 103 172 (V2.2.2): "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

NOTE: This document will be replaced by EN 319 142-7.

[i.18] ETSI TS 102 918 (V1.3.1): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

NOTE: This document will be replaced by EN 319 162-2.

[i.19] ETSI TS 103 174 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

NOTE: This document will be replaced by EN 319 162-3.

[i.20] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

NOTE: This document will be replaced by EN 319 612.

[i.21] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.22] ETSI TS 102 853 (V1.1.2): "Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies".

[i.23] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons".

[i.24] ETSI TS 119 412-2 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons".

[i.25] ETSI EN 319 412-5 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile".

[i.26] ETSI TR 102 038 (V1.1.1): "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[i.27] ETSI TR 102 272 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

[i.28] ETSI TS 119 134 (all parts): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signature (XAdES) Testing Compliance & Interoperability".

NOTE: At present only TS 119 134-5 is published, for further details see [i.1].

[i.29] ETSI TS 119 144 (all parts): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature (PAdES) Testing Compliance & Interoperability".

NOTE: At present only TS 119 144-2 is published, for further details see [i.1].

[i.30] ETSI TS 119 164 (all parts): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Testing Compliance & Interoperability".

NOTE: At present only TS 119 164-2 is published, for further details see [i.1].

[i.31] ETSI TS 119 164-2 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Testing Compliance & Interoperability; Part 2: Test Suite for ASiC interoperability test events".

[i.32] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".

[i.33] IETF RFC 3281: "An Internet Attribute Certificate Profile for Authorization".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [i.1], [i.2], [i.3] and the following apply (with precedence, in case of conflict, to the terms and definitions given in the present document):

conformance testing: process of verifying that a single implementation conforms to the individual requirements of one or more standards or specifications or profiles

interoperability testing: process for verifying that several implementations can interoperate while conforming to one or more standards or specifications or profiles

NOTE: Derived from [i.2].

Plugfest: interoperability testing event about a standard or a profile where the participants test each other their implementation

Plugtests: testing events, similar to a plugfest, developed and hosted by ETSI where the participants can test the interoperability or the conformance of their implementations

NOTE: The term "Plugtests" is an ETSI trademark and a general description of Plugtests is available here: http://www.etsi.org/services/plugtests/about-plugtests.

profile: agreed upon subset or interpretation of one or more norms or technical specifications, intended to achieve interoperability while adapting to specific needs of a user community or purpose

NOTE: Derived from [i.2].

test assertion: testable or measurable expression for evaluating the adherence of an implementation (or part of it) to one or more normative statements in a specification that describe the expected output or behaviour for the implementation within specific operation conditions, in a way that can be measured or tested

NOTE: Derived from [i.3].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in [i.1] and the following apply:

ASN	Abstract Syntax Notation
ATSv3	Archive Time-stamp v3 (attribute)
CPR	Complete draft for Public Review
DSS-X	Digital Signature Services eXtended (OASIS Technical Committee)
EUMS	European Union Member State
FTB	Final draft for Technical Body approval
LDAP	Lightweight Directory Access Protocol
LTA	Long Term Attribute
OJ	Official Journal
PKI	Public Key Infrastructure
PTS	Publication of the Technical Specification
RFC	Request For Comment
SPR	Stable Draft for Public Review
STF	Specialist Task Force
TC	Test Case
TSA	Time Stamping Authority
XSLT	eXtensible Stylesheet Language Transformations

4 Technical Approach and Methodology for Conformance and Interoperability testing

4.1 Introduction to conformance and interoperability testing

The purpose of standardizing systems, services, protocols and interfaces is to enable the inter-working of similar or associated products made by different manufacturers. The absence of interoperability is often the reason why final services for which there is great demand do not come into being.

Interoperability is one of the main goals of standardization and conformance and interoperability testing are fundamental instrument to achieve this target.

Testing the conformance of an implementation to a standard is considered to be essential in order to verify that this implementation can interoperate with other implementations that implement the same standard or a complementary one: in fact the purpose of such testing is to assess how much an implementation of one or more standards or profiles conforms to the individual requirements provided there.

Conformance testing concentrates on specific implementations, often related to a single standard or set of related standards. It is unit testing rather than system testing. Conformance tests are executed under controlled conditions using a dedicated test system. Each test case within a test suite is related to one or more conformance requirements or clauses of the standard, providing for the tester a high degree of control and observability. It is methodical and precise but limited in scope. It gives a high-level of confidence that key components of a system are working as they were specified and designed to do, but a conformant implementation will not necessarily always interoperate with other implementations.

Interoperability testing in this sense is complementary to conformance testing as it allows the structured testing of different implementations. It is not the detailed verification of requirements specified in a conformance test suite but concentrates on the interactions between different implementations, it is system testing rather than unit testing.

It is most commonly applied to end-to-end testing and shows that functionality is accomplished but not how. It gives anyway a high-level of confidence that different implementations are able to interoperate increasing the possibility to also ensure interoperability with other implementations not included in the testing process. But running such interoperability testing at a plugfest or at a series of plugfests is the most cost effective way to guarantee that the system has a correct implementation of the standard and will be interoperable with other systems implementing the same standard.

Conformance and interoperability are complementary and are both important and useful approaches for testing implementations based on standards.

4.2 Gathering inputs

The present document has been developed taking into account:

- the Plugtests events that ETSI ran in the past;
- the critical deliverables of the Framework [i.1] that are in preparation at the time of publication of the present document;
- the ongoing standardization activities and plans to develop these deliverables.

The final aim for analyzing these documents is to:

- identify the standards whose development, adoption and deployment can mostly benefit from the organization of testing events;
- plan the development of the required conformity testing tools.

Also external relevant works on standardization of testing such as [i.2] and [i.3] were considered.

4.3 Standards to be targeted by testing events and criteria to identify them

The criteria used for identifying the standards that should be targeted by testing events are: the relevance of the standards to the framework and the expected eagerness of stakeholders to participate in events targeting the standards. The following list of standards is considered to meet the criteria adopted:

- Standards concerning signature formats, in support of the Commission Decision 2011/130/EU [i.4] and future amendments also dealing with long term attributes of the signature formats;
- Standards concerning trusted list management and usage, in support of the Commission Decision 2009/767/EC [i.5] and following amendments [i.6];
- Standards concerning Electronic Delivery and other TASPs/TSPs as specified in the new proposed Regulation
- Standards concerning electronic procurement and business in general.

NOTE: A new European Directive is expected on electronic procurement: the conformity and interoperability testing tools will provide a common basis of tools to be used to guarantee the acceptance of signed documents in public e-procurement applications especially in cross border contexts. The testing activities can also support the requirement of the ongoing standardization activities in this field.

At the present stage of the development of the Rationalized Framework for Electronic Signature Standardization [i.1] some of the standards that could benefit by testing events are not yet developed enough to propose a complete plan for the production of testing specification, the development of the related testing tools and scheduling testing events; this includes the specifications for AdES on mobile environment, Electronic Delivery and other TASPs/TSPs, standards listed in clause 5.1 (table 1) not directly targeted by test events such as Certificate profiles and Signature Policies. Those standards will be reconsidered and possibly included in a future release of the present document, see also the note in clause 5.1.

4.4 Criteria to identify the scope of testing events

A testing event can be devoted to signature formats or to the provision of trust services. The contents and the scope of a testing event are fully specified grouping one or more components. Each component is defined by a full set of the applicable criteria in the following list:

1) the format tested;

2) the specific part of the related standard: core specification, baseline profile or other potential profiles;

3) the type of tests: interoperability or conformance testing;

4) the supporting PKI(s), e.g. a simple PKI, a more complex PKI including one or more hierarchies, a real PKI supported by the EUMS Trusted Lists infrastructure;

5) the set of tests to be carried out (test suites).

The experience gained from past Plugtests organized and supported by ETSI demonstrated that it was difficult for the participants to deal with tests on different formats during the same event, for this reason in the present document each event is always related to a single format.

On the other hand it is considered beneficial to include in the proposed scheduling of the testing events as in clause 6.2 different testing event components on the same format, according to the expected availability of the tools and the standards, as this should allow more effective and comprehensive testing events.

4.5 Rules to identify priorities in the testing event scheduling

The scheduling of test events for signature formats specified in clause 7 has been specified giving priority to the available specifications matching the following criteria:

- long time elapsed since an event on the same format (see annex A for a list of past events);
- the presence of new substantial features in the signature format specification to be tested, that were not present at the time of the last test event on the same format; or
- the availability of new substantial features during the ongoing development of the standards;
- updates to the test suites and availability of the related testing tools.

5 Standards targeted for Testing and Testing Specifications

This clause identifies the standards that are targeted for testing and the Technical Specifications that will be produced to specify conformance and interoperability testing.

5.1 Identification of standards that benefit from Conformance and Interoperability Testing

Table 1 identifies the standards that are expected will benefit from the testing events, according to the criteria specified in clause 4.3.

Table 1: Targeted standards for Conformance and Interoperability Testing

Deliverable	Current publication	Last Plugtests	Major changes (made or planned) since the last Plugtests event
CAdES core specification - EN 319 122-2 (see [i.1])	TS 101 733 [i.8] V2.2.1	Nov 2010	Introduction of a new Archive Time Stamp attribute: archive-time-stamp-v3
CAdES baseline profile - EN 319 122-3 (see [i.1])	TS 103 173 [i.9] V2.2.1	N/A	N/A
XAdES core specification - EN 319 132-2 (see [i.1])	TS 101 903 [i.10] V1.4.2	Apr 2012	Changes related to the management of signed ds:Manifest elements in the long term
XAdES baseline profile - EN 319 132-3 (see [i.1])	TS 103 171 [i.11] V2.1.1	Apr 2012	Changes required to align to core specification
PAdES Basic - Profile based on ISO 32000-1 [i.12] EN 319 142-2 (see [i.1])	TS 102 778-2 [i.13] V1.2.1	Dec 2011	
PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles - EN 319 142-3 (see [i.1])	TS 102 778-3 [i.14] V1.2.1	Dec 2011	
PAdES Long Term - PAdES-LTV Profile - EN 319 142-4 (see [i.1])	TS 102 778-4 [i.15] V1.1.2	Dec 2011	
PAdES for XML Content - Profiles for XAdES signatures - EN 319 142-5 (see [i.1])	TS 102 778-5 [i.16] V1.1.2	Dec 2011	
PAdES baseline profile - EN 319 142-7 (see [i.1])	TS 103 172 [i.17] V2.2.2	N/A	N/A
ASiC core specification - EN 319 162-1 (see [i.1])	TS 102 918 [i.18] V1.3.1	Dec 2012	It is planned to add long term attributes.
ASiC baseline profile - EN 319 162-2 (see [i.1])	TS 103 174 [i.19] V2.2.1	N/A	It is planned to align this with the ASiC core specification to add long term attributes.
Trusted Lists EN 319 612 see [i.20]	TS 119 612 [i.20]	Dec 2009	TS 119 612 [i.20] is mostly based on TS 102 231 [i.21] V3.1.2 but with some major changes
Procedures for Signature Creation and Validation EN 319 102 (see [i.1])	TS 102 853 [i.22] V1.1.2	N/A	N/A
Certificate Profile for certificates issued to natural persons EN 319 412-2 (see [i.1])	TS 119 412-2 [i.24] V1.1.1	N/A	N/A
Extension for Qualified Certificate profile EN 319 412-5 [i.25]	EN 319 412-5 [i.25] V1.1.1	N/A	N/A
XML format for Signature Policies EN 319 172-2 (see [i.1])	TR 102 038 [i.26] V1.1.1	N/A	N/A
ASN.1 format for Signature Policies EN 319 172-3 (see [i.1])	TR 102 272 [i.27] V1.1.1	N/A	

The standards that are targeted directly by the plugtests events whose planning is proposed in clause 6.2 are the core specifications and the baseline profiles for all the signature formats (CAdES, XAdES, PAdES and ASiC) and the Trusted Lists ([i.20]). All the other standards listed can benefit because it is proposed that the test events at a late stage incorporate test cases and PKI support for testing them (e.g. use of certificates conformant to the relevant profiles, use of signature policies, use of the validation process).

NOTE: ETSI/ESI TC will update the present document to propose a plan for development of Technical Specifications, conformance testing tools and test events for other standards that are not mature enough at the date of publishing of the present document.

5.2 List of Technical Specifications for Testing Conformance and Interoperability

This clause lists the set of Technical Specifications defining test suites for testing interoperability and conformance, against the standards of the Framework [i.1] identified in the previous clause and specifies the scheduling for their production.

Test execution may require the use of cryptographic algorithms and/or hashing functions, for example when creating and verifying electronic signatures. The algorithms and/or hashing functions whose use is proposed during a certain test event execution can be selected according to test specifications and/or during the test event preparation. It is recommended that the algorithms and functions selection takes into account [i.7].

5.2.1 CAdES Testing Conformance and Interoperability

A set of Technical Specifications defining test suites for testing interoperability and conformity of CAdES signatures is planned, consisting of the following documents.

- TS 119 124 (see [i.1]) "CAdES Testing Conformance& Interoperability":
  - Part 2: Test suites for testing interoperability of CAdES signatures as defined in CAdES core specification.
  - Part 3: Test suites for testing interoperability of Baseline CAdES signatures as defined in the CAdES Baseline Profile.
  - Part 4: Specifications for testing conformance of CAdES Signatures against CAdES core specification.
  - Part 5: Specifications for testing conformance of Baseline CAdES Signatures against CAdES Baseline Profile.

5.2.2 XAdES Testing Conformance and Interoperability

A set of Technical Specifications defining test suites for testing interoperability and conformity of XAdES signatures is planned, consisting of the following documents.

- TS 119 134 [i.28]: "XAdES Testing Conformance & Interoperability":
  - Part 2: Test suites for testing interoperability of XAdES signatures as defined in XAdES core specification.
  - Part 3: Test suites for testing interoperability of Baseline XAdES signatures as defined in the XAdES Baseline Profile.
  - Part 4: Specifications for testing conformance of XAdES Signatures against XAdES core specification.
  - Reviewed version of Part 5: Specifications for testing conformance of Baseline XAdES Signatures against XAdES Baseline Profile.

5.2.3 PAdES Testing Conformance and Interoperability

A set of Technical Specifications defining test suites for testing interoperability and conformity of PAdES signatures is planned, consisting of the following documents.

- TS 119 144 [i.29]: "PAdES Testing Conformance & Interoperability". The following parts will be covered:
    - Reviewed version of Part 2: Test suites for testing interoperability of PAdES signatures as defined in PAdES core specification.
    - Part 3: Test suites for testing interoperability of Baseline PAdES signatures as defined in the PAdES Baseline Profile.
    - Part 4: Specifications for testing conformance of PAdES Signatures against PAdES core specification.
    - Part 5: specifications for testing conformance of Baseline PAdES Signatures against PAdES Baseline Profile.

5.2.4 AdES signatures in Mobile environments Testing Conformance and Interoperability

A set of Technical Specifications defining test suites for testing interoperability and conformity of AdES signatures in Mobile environments is planned, consisting of the following documents.

- TS 119 154 (see [i.1]): "Testing Conformance & Interoperability of AdES signatures in Mobile environments".

NOTE: No standard is available on AdES signatures in Mobile Environment at the time of publication of the present document, for this reason in the following clauses in the present document no further details are provided on the planning for the test specifications and for the related testing events. A new version of this document will be provided by ETSI/ESI TC when STF458 will make available the required deliverables. Another identified source of information for the update of this document could be the work undertaken by OASIS DSS-X Technical Committee, which is planning tests on the DSS protocol, as this is relevant to AdES signatures in Mobile environments.

5.2.5 ASiC Testing Conformance and Interoperability

A set of Technical Specifications defining test suites for testing interoperability and conformity of ASiC containers is planned, consisting of the following documents.

- TS 119 164 [i.30]: "ASiC Testing Conformance & Interoperability". The following parts will be covered:
    - Reviewed version of Part 2: Test suites for testing interoperability of ASiC containers as defined in ASiC core specification.
    - Part 3: Test suites for testing interoperability of Baseline ASiC containers as defined in the ASiC Baseline Profile.
    - Part 4: Specifications for testing conformance of ASiC containers against ASiC core specification.
    - Reviewed version of Part 5: Specifications for testing conformance of Baseline ASiC containers against ASiC Baseline Profile.

5.2.6 Testing Conformance of Trusted Lists

A Technical Specification defining test suites for testing conformity of ASiC containers is planned, consisting of the following document:

- TS 119 614-2 (see [i.1]): Specifications for testing conformance of XML representation of Trusted Lists.

The time schedule for TS production is specified in the table in clause 6.3.

6 Planning of identified activities

6.1 Calendar of activities

Table 2 shows a calendar for all the activities to be carried out by this STF as well as for the proposed test events. The table has 11 columns, whose descriptions are provided below:

- First column (header **"Format / Spec."**). It indicates the signature format or the (set of) specification(s) target of the STF activity. Cells in this column will stretch over the equivalent to three rows.
- Second column (header **"Work-plan for"**). Cells within this column are used for showing the details of three different activities to be performed or planned by this STF for the format or (set of) specification(s) indicated by cells within the first column (as mentioned before, one cell in the first column stretches over the equivalent of three rows in the table). Each row shows the proposed calendar for a certain type of activity as indicated below:
    - Rows headed by cell **"TS"** within this column show the calendar that the STF will follow for producing the ETSI Technical Specifications defining test suites for testing interoperability and conformance corresponding to the signature format or (set of) specification(s) identified in the stretched cells within the first column. More details on this planning are available in clause 6.3.
    - Rows headed by cell **"Software Tools"** within this column show the calendar that the STF will follow for developing the software conformance testing tools corresponding to the signature format or (set of) specification(s) identified in the stretched cell within the first column.
    - Rows headed by cell **"Proposed Test Events"** within this column show the calendar that the STF proposes for conducting test events for the signature format or (set of) specification(s) identified in the stretched cell within the first column.
- Columns 3 to 11. Each column represents one term of one year. Cells within these columns identify, in consequence a period of three months. These cells include details of:
    - **Test events**. They are denoted by the legend [XXX] Event , where [XXX] indicates the format or (set of) specification(s) (e.g. "CAdES Event ").
    - **Milestones**. Milestones for the ETSI TS to be produced by the STF are denoted **[W]TS-M[Z]**. Milestones for the software tools testing conformance are denoted by **[W]Tool-M[Z]**. [W] identifies the targeted format or (set of) specification(s), as follows: "A" for ASiC, "C" for CAdES, "P" for PAdES, "X" for XAdES, "TL" for Trusted Lists. Finally [Z] is the milestone number.

Table 2 does not include the formal milestones specified in the STF's terms of reference for these tasks. These official milestones are established at the end of years 2013, 2014 and 2015.

Table 2: Calendar of activities related to testing

Specification under test	Work-plan for	2013-Q3	2013-Q4	2014-Q1	2014-Q2	2014-Q3	2014-Q4	2015-Q1	2015-Q2	2015-Q3	2015-Q4
ASiC	TS 119 164 [i.30] (all parts)			SPR			CPR			FTB	PTS
	Software Tools		🟦	Atool-M1	🟦	🟦	🟦	🟦	🟦	Atool-M2	Atool-M3
	Proposed Test Events			ASiC Event★						ASiC Event★	
CAdES	TS 119 124-2 & TS 119 124-3 (see [i.1])	SPR					CPR			FTB	PTS
	TS 119 124-4 & TS 119 124-5 (see [i.1])			SPR						FTB	PTS
	Software Tools	🟦	Ctool-M1	🟦	🟦	🟦	🟦	🟦	Ctool-M2	🟦	Ctool-M3
	Proposed Test Events		CAdES Event★						CAdES Event★		
XAdES	TS 119 134 [i.28] (all parts)			SPR	XTS-M1		CPR			FTB	PTS
	Software Tools	🟦	🟦	🟦	🟦	Xtool-M1	🟦	🟦	🟦	🟦	Xtool-M2
	Proposed Test Events					XAdES Event★					
PAdES	TS 119 144 [i.29] (all parts)			SPR			CPR	PTS-M1		FTB	PTS
	Software Tools			🟦	🟦	🟦	🟦	Ptool-M1	🟦	🟦	Ptool-M2
	Proposed Test Events							PAdES Event★			
TSL	TS 119 614-2 (see [i.1])			SPR			CPR			FTB	PTS
	Software Tools	🟦	🟦	TLTool-M1							
	Proposed Test Events			Trusted Lists Event★							

6.2 Proposed scheduling and scoping of testing events

Table 3 summarizes the schedule and scope of the proposed testing events.

Table 3: Proposed scheduling and scope for testing events

Targeted specification	Proposed date	Supporting PKIs	Interoperability	Conformance
CAdES	Dec 2013	Simple PKI	TC from previous test events + ATSv3	ATSv3
Trusted Lists	Feb 2014	Simple PKI	N/A	Trusted List [i.20]
ASiC	Mar 2014	Simple PKI	TC from previous test events +LTA	Basic conformance checks on signatures within the container
XAdES	Sep 2014	Simple PKI and more complex PKI	TC from previous test events + TC on EN 319 102 (see [i.1])	XAdES Baseline Profile, not distributed XAdES Core Specification including management of signed ds:Manifest in the long term
PAdES	Mar 2015	Simple PKI, more complex PKI and real PKI supported by EUMS TLs	TC from previous test events + TC on EN 319 102 (see [i.1]) + TC on EN 319 412-2 [i.23] and EN 319 412-5 [i.25]	PAdES Baseline Profile, PAdES Core Specification part 2, 3 and 4
CAdES	Second half 2015	Simple PKI, more complex PKI and real PKI supported by EUMS TLs	TC from previous test events + TC on EN 319 102 (see [i.1]) + TC on EN 319 412-2 [i.23] and EN 319 412-5 [i.25]	CAdES Baseline Profile, CAdES Core Specification
ASiC	Second half 2015	Simple PKI, more complex PKI and real PKI supported by EUMS TLs	TC from previous test events + TC on EN 319 102 (see [i.1]) + TC on EN 319 412-2 [i.23] and EN 319 412-5 [i.25] + TC on EN 319 172 (see [i.1])	ASiC Baseline Profile, ASiC Core Specification

6.2.1 Proposed testing events for signature formats

Proposed schedule:

1) CAdES interoperability event, baseline & core specification including the new Archive Time-stamp v3 (ATSv3) attribute, including some conformance testing: December 2013.

2) ASiC currently does not include long term attributes but their specification is already planned to be present in the related Ens. It is however important to allow implementers to develop and test these attributes at a stage where the EN production process can still benefit from this feedback. It is then proposed to proceed as follows:

   a) To have intermediate publicly available specification for ASiC core specification and baseline profile available in October 2013 (either as a draft EN or as a TS) including the long term attributes.

   b) Implementation by implementers and in parallel development of the test specifications and testing tools.

   c) Have a new Plugtests event for the core and baseline specification including the new long term attributes and basic conformance testing tools by march 2014 as detailed in clause 6.1.

3) XAdES (Sep 2014).

4) PAdES (march 2015).

5) New CAdES/ASiC events including full conformance testing (second half 2015).

6.2.2 Testing events for signature formats TSL Providers

Proposed schedule:

1) TSL (Jan 2014).

NOTE: The date for this is estimated taking into account that a new Decision updating 2009/767/EC [i.5] is expected to be published in September 2013 having effect from March 2014 and will be updated when the actual dates will be available.

6.3 Planning for the production of Technical Specifications for Testing Conformance and Interoperability

Below follows some production details of the Technical Specifications on testing conformance and interoperability and the explanation of the acronyms used in the table in clause 6.1 related to the general activity calendar.

SPR: Stable draft for Public Review

At this stage the deliverable is ready to be made available to all the interested parties to gather a first set of comments.

NOTE 1: The degree of maturity of each deliverable at this stage depends on the production of stable drafts for the reference deliverables indicated in clause 5.1 and on the requirements for the development of the tools as identified in clause 6.4. Nevertheless, each part draft should include clear indications of the scope covered by each test suite.

CPR: Complete draft for Public Review

At this stage the deliverable is complete as specified in clause 5.2 and is made available to all the interested parties to gather the comments that will be considered for the final version of the deliverable.

FTB: Final draft for Technical Body approval.

At this stage the deliverable is ready for the final approval from the technical approval and, if achieved, can progress to the publication stage.

PTS: Publication as TS

At this stage the deliverable is verified for eventual editorial issues and published.

NOTE 2: The SPR for CAdES conformance testing (TS 119 124 (see [i.1]) part 4 and 5) should cover the new `archive-time-stamp-v3` attribute.

NOTE 3: The SPR for ASiC part 4 and 5 should cover at least the conformance testing on containers with a single XAdES signature and, for part 4, XAdES signatures managing the signed ds:Manifest elements in the long term.

6.3.1 Milestone M1: Stable Draft for Public Review (SPR)

TS 119 124 (see [i.1]): "CAdES Testing Conformance & Interoperability". The following parts will be covered:

- Part 2: Test suites for testing interoperability of CAdES signatures as defined in CAdES core specification. Test cases covering:
  - interoperability with simple PKIs
  - negative test cases for simple PKIs
  - signatures lifecycle involving electronic signatures that can remain valid over long periods
- Part 3: Test suites for testing interoperability of Baseline CAdES signatures as defined in the CAdES Baseline Profile. Test cases will cover the four different conformance levels defined in CAdES Baseline Profile.

- Part 4: Specifications for testing conformance of CAdES Signatures against CAdES core specification. The set of defined checks will cover CAdES-BES, CAdES-EPES, CAdES-T, CAdES-A (with ATSv2 and ATSv3) signature formats.

- Part 5: Specifications for testing conformance of Baseline CAdES Signatures against CAdES Baseline Profile. The set of defined checks will cover the four different conformance levels defined in CAdES Baseline Profile.

TS 119 164 [i.30]: "ASiC Testing Conformance & Interoperability". The following parts will be covered:

- Part 2: Test suites for testing interoperability of ASiC signatures update of TS 119 164-2 (V1.1.1) [i.31] including long term attributes with simple PKIs.

- Part 3: Test suites for testing interoperability of Baseline ASiC containers as defined in the ASiC Baseline Profile. Test cases will cover the four different conformance levels defined in ASiC Baseline Profile.

- Part 4: Specifications for testing conformance of ASiC containers against ASiC core specification. Complete set of test assertions for the ASiC core specification.

- Part 5: Specifications for testing conformance of Baseline ASiC containers against ASiC Baseline Profile. Complete set of test assertions for the four different conformance levels defined in ASiC Baseline Profile.

TS 119 614 (see [i.1]) Testing Conformance & Interoperability of Trusted Lists:

- Part 2: Specifications for testing conformance of XML representation of Trusted Lists.

- Test assertions covering the parts of the European Standard that specify the European Trusted Lists. No test assertions will appear for testing requirements for Trusted Lists issued outside the EU.

TS 119 144 [i.29]: "PAdES Testing Conformance & Interoperability". The following parts will be covered:

- Part 2: Test suites for testing interoperability of PAdES signatures as defined in PAdES core specification. Test cases covering:

  - interoperability with simple PKIs

  - negative test cases for simple PKIs

  - signatures lifecycle involving electronic signatures that can remain valid over long periods

- Part 3: Test suites for testing interoperability of Baseline PAdES signatures as defined in the PAdES Baseline Profile. Test cases will cover the four different conformance levels defined in PAdES Baseline Profile.

- Part 4: Specifications for testing conformance of PAdES Signatures against PAdES core specification. The set of defined checks will cover the PAdES Basic, PAdES-BES, PAdES-EPES, PAdES-T, PAdES-LTV signature profiles.

- Part 5: Specifications for testing conformance of Baseline PAdES Signatures against PAdES Baseline Profile. The set of defined checks will cover the four different conformance levels defined in PAdES Baseline Profile.

Test suites for XAdES (TS 119 134 [i.28]):

- Part 2: Test suites for testing interoperability of XAdES signatures as defined in XAdES core specification.

  Test cases covering:

  - interoperability with simple PKIs

  - negative test cases for simple PKIs

  - signatures lifecycles involving three steps: signature generation, signature upgrade and signature arbitration

- Part 3: Test suites for testing interoperability of Baseline XAdES signatures as defined in the XAdES Baseline Profile.

Test cases covering:

- interoperability with simple PKIs
- negative test cases for simple PKIs
- signatures lifecycles: involving three steps: signature generation, signature upgrade to different conformance levels, and signature arbitration

- Part 4: Specifications for testing conformance of XAdES Signatures against XAdES core specification.

  Test assertions for non distributed incorporation of qualifying properties of XAdES.

- Part 5: specifications for testing conformance of Baseline XAdES Signatures against XAdES Baseline Profile.

  Complete set of test assertions for the XAdES Baseline Profile.

6.3.2 Milestone M2: Complete Draft for Public Review (CPR)

All the TSs will fully cover at this stage the content specified in clause 5.2 and the comments received after their first public review (SPR) and will be ready for the second public review.

6.3.3 Milestone M3: Final Draft for approval (FTB)

All the TSs will be amended according to the comments received from the second public review and be ready for the final approval by the ESI TB.

6.4 Production plan for conformity testing tools development

In order to maximize stakeholders' benefit, the test events scheduled should incorporate interoperability and conformance testing. In consequence, the conformance testing tools development calendar should be aligned with the test events calendar. Although it will be impossible to use complete versions of the aforementioned conformance testing tools in all the events, their development calendar should ensure that in all the events the stakeholders could use partial versions allowing them to test conformance against certain critical aspects of the specifications being targeted at those events. Obviously, the last events scheduled in the calendar should be supported by full versions of the corresponding conformance testing tools.

Below follows a detailed explanation of the plan for the development of the software conformance testing tools, based on the calendar contained in clause 6.1. This plan is presented in a tabular form. The table identifies all the internal and official milestones, the due date, the format or (set of) specification(s) affected, and details of the milestones. This table shows both internal and official milestones aforementioned. This table actually refines the official milestones, which in the STF terms of reference were left open because the development calendar strongly depends on the test events calendar.

Table 4: Plan for conformity testing tools development

Milestone	Milestone Type	Due date	Format / Spec.	Details
Ctool-M1	Internal milestone	Last term of 2013. Ready for the CAdES test event.	CAdES	Before the actual conduction of the test event on CAdES an initial version of the CAdES conformance testing tool will be ready. It will incorporate, at least the following features: • Conformance testing against the new `archive-time-stamp-v3` attribute. • Trace of the contributions to `archive-time-stamp-v3`'s message imprint computation. These features should accelerate the correct implementation of the aforementioned attribute.

Milestone	Milestone Type	Due date	Format / Spec.	Details
Atool-M1	Internal milestone	First term of 2014. Ready for first ASiC test event.	ASiC	Due to the fact that this test event is scheduled very early, the ASiC conformance testing tool will be in a very early stage. The STF opted for quickly testing the new long-term related attributes, instead delaying the test event for also incorporating a more evolved conformance testing tool. This results in that for this test event it is planned that the tool will be able to do some conformance testing on individual XAdES signatures. The foreseen set of tests are those required for XAdES Baseline Profile. In consequence the tool will not be able to carry out conformance testing on the internal structure of the package or on the interrelationships between the different files, etc. All these tests will be incorporated in ulterior phases of the development.
M1	Formal STF-459 Milestone	End December 2013	ASiC, XAdES, CAdES, Trusted Lists	Hereby, this formal STF-459 milestone is refined as follows: • CAdES conformance testing tool will be able to perform conformance testing against the new `archive-time-stamp-v3` attribute; and to trace the contributions to `archive-time-stamp-v3`'s message imprint computation. • ASiC conformance testing tool: **on its way** for being able to carry, on XAdES signatures found within the package, the set of tests required for testing conformance against XAdES Baseline Profile. Not yet completed by the indicated date. • Trusted Lists conformance testing tool: **on its way** to being able to test conformance of EU Trusted Lists against the latest version of [i.20] "Trusted Lists". Tests on non EU TLs will not be incorporated at this stage.
TLTool-M1	Internal milestone	First term of 2014. Ready for first TL test event.	Trusted Lists	A complete Trusted Lists conformance testing tool is planned for this first Trusted Lists test event. At this point in time this tool will only test conformance against the part of the European Standard specifying European Trusted Lists. No conformance test will be done on requirements for Trusted Lists issued outside the EU.
Xtool-M1	Internal milestone	Mid 2014. Ready for first XAdES event	XAdES	At this time, the STF is aiming to have completed the two following tools: • Complete XAdES Baseline Profile conformance testing tool, targeting specifications in EN 319 132 (see [i.1]) Part 3 (standard version of former TS 103 171 [i.11]). • Complete XAdES conformance testing tool targeting specifications in EN 319 132 (see [i.1]) Part 2 (standard version of TS 101 903 [i.10]) These tools should be used during the test event proposed for this term. The STF will, after this event, keep working on the tools until the end of the project for both, keeping them aligned with any potential change in the reference specifications and for dealing with any issue uncovered during the aforementioned test event.

Milestone	Milestone Type	Due date	Format / Spec.	Details
M2	Formal STF-459 Milestone	End December 2014	ASiC, XAdES, CAdES, PAdES, Trusted Lists	Hereby, this formal STF-459 milestone is refined as follows: • CAdES conformance testing tool will be able to perform conformance testing against the new `archive-time-stamp-v3` attribute; and to trace the contributions to `archive-time-stamp-v3`'s message imprint computation. • ASiC conformance testing tool: **on its way** for being able to carry, on XAdES signatures found within the package, the set of tests required for testing conformance against XAdES Baseline Profile. Not yet completed by the indicated date. • Trusted Lists conformance testing tool: **on its way** to being able to test conformance of EU Trusted Lists against the latest version of [i.20] "Trusted Lists". Tests on non EU TLs will not be incorporated at this stage.
Ptool-M1	Internal milestone	First term 2015	PAdES	At this time the STF is aiming to have completed a first version of the two following tools: • Complete PAdES Baseline Profile conformance testing tool, targeting specifications in EN 319 142 (see [i.1]) Part 7 (standard version of former TS 103 172 [i.17]). • Complete PAdES conformance testing tool targeting specifications in EN 319 132 (see [i.1]) Parts 2, 3, and 4 (standard version of TS 102 778 [i.13] Parts 2, 3 and 4). These tools should be used during the test event proposed for this term. The STF will, after this event, keep working on the tools until the end of the project for both, keeping them aligned with any potential change in the reference specifications and for dealing with any issue uncovered during the aforementioned test event.
Ctool-M2	Internal milestone	Second term of 2015	CAdES	At this time the STF is aiming to have completed a first version of the two following tools: • Complete CAdES Baseline Profile conformance testing tool, targeting specifications in EN 319 122 (see [i.1]) Part 3 (standard version of former TS 103 173 [i.9]). • Complete CAdES conformance testing tool targeting specifications in EN 319 122 (see [i.1]) Part 2 (standard version of TS 101 733 [i.8]). These tools should be used during the test event proposed for this term. The STF will, after this event, keep working on the tools until the end of the project for both, keeping them aligned with any potential change in the reference specifications and for dealing with any issue uncovered during the aforementioned test event.

Milestone	Milestone Type	Due date	Format / Spec.	Details
Atool-M2	Internal milestone	Third term of 2015	ASiC	At this time the STF is aiming yo have completed a first version of the two following tools: • Complete ASiC Baseline Profile conformance testing tool, targeting specifications in EN 319 162 (see [i.1]) Part 3 (standard version of former TS 103 174 [i.19]). • Complete ASiC conformance testing tool targeting specifications in EN 319 162 (see [i.1]) Part 2 (standard version of TS 102 918 [i.18]). These tools should be used during the test event proposed for this term. The STF will, after this event, keep working on the tools until the end of the project for both, keeping them aligned with any potential change in the reference specifications and for dealing with any issue uncovered during the aforementioned test event.
M3	Formal STF-459 Milestone	End December 2015	ASiC, XAdES, CAdES, PAdES, Trusted Lists	As stated in the terms of reference of this project, by this time the STF will have the final version of all the tools: • Complete CAdES Baseline Profile conformance testing tool, targeting specifications in EN 319 122 (see [i.1]) Part 3 (standard version of former TS 103 173 [i.9]). • Complete CAdES conformance testing tool targeting specifications in EN 319 122 (see [i.1]) Part 2 (standard version of TS 101 733 [i.8]). • Complete XAdES Baseline Profile conformance testing tool, targeting specifications in EN 319 132 (see [i.1]) Part 3 (standard version of former TS 103 171 [i.11]). • Complete XAdES conformance testing tool targeting specifications in EN 319 132 (see [i.1]) Part 2 (standard version of TS 101 903 [i.10]) • Complete ASiC Baseline Profile conformance testing tool, targeting specifications in EN 319 162 (see [i.1]) Part 3(standard version of former TS 103 174 [i.19]). • Complete ASiC conformance testing tool targeting specifications in EN 319 162 Part 2 (standard version of TS 102 918 [i.18]). • Complete PAdES Baseline Profile conformance testing tool, targeting specifications in EN 319 142 (see [i.1]) Part 7(standard version of former TS 103 172 [i.17]). • Complete PAdES conformance testing tool targeting specifications in EN 319 132 (see [i.1]) Parts 2, 3, and 4 (standard version of TS 102 778 Parts 2, 3 and 4). • Trusted Lists conformance testing tool testing conformance against [i.20] "Trusted Lists", including conformance tests against those requirements defined in this document for non EU Trusted Lists.

Annex A: History of ETSI/ESI Plugtests

A.1 AdES Signature Plugtests

ETSI has organized 10 Interoperability Plugtests Events in the past. The first two were not remote and participants were required to travel to Sophia Antipolis and stay one week in ETSI's headquarters.

The first Plugtests Event was a face to face Event and took place in 2003 from 3 to 7 November, where a number of XAdES implementers tested the interoperability of their XAdES products, had discussion on different aspects of the specification and rose recommendations for future standardization activities. Between 2003 and 2004 ETSI TC ESI reviewed XAdES specifications and, based on feedback got from implementers, XAdES v1.2.2 was published in April 2004.

The 2nd Plugtests Event also was a face to face Event. It also was a joint PKI-XAdES Plugtest Event and took place in Sophia-Antipolis from 24 to 28 May 2004. Based on the feedback coming from this event and from other sources, ETSI TC ESI produced XAdES v1.3.2.

The 3rd XAdES Plugtests Event was a remote Event supported by the ETSI Remote Plugtest Portal on (http://xades-portal.etsi.org). Around thirty different entities participated in that event, which was conducted from 3 to 18 March 2008.

All the following Electronic Signatures events have been performed remotely, using a dedicated web portal, which has been continuously improved to fulfil the needs and requirements of the participants. It has been demonstrated along the years that it is an effective way to reduce costs for participants avoiding travel to the event. Moreover, as the testing is not real time, the companies from different time zones can participate effectively.

The 4th Plugtests Event, held between 8 and 18 September 2008, was a remote Event supported by an enhanced version of ETSI's Remote Plugtest Portal, offering cryptographic materials and PKI-related Online services (Certificates, CRL, Time-stamp Authority server, OCSP responders, LDAP, etc.). An internal chat tool has also been implemented to allow easy and efficient communication between participants during the event.

The 5th Plugtests Event was held from 16 to 27 February 2009. It was a combined XAdES and CAdES interoperability remote event, testing XAdES TS 101 903 [i.10] V1.3.2 and CAdES TS 101 733 [i.8] 1.7.4.

The 6th Plugtests Event held from 25 October to 22 November 2010 was a combined XAdES and CAdES interoperability remote event. The test scenarios were based on previous event with additional new testcases and the support of the new specifications XAdES [i.10] V1.4.1 and CAdES [i.8] V1.8.1. There were 27 different organizations and 66 people participating in the event.

In answer to the European Commission Mandate 460 on Electronic Signatures Standardization, ETSI has initiated several Specialist Task Forces projects (STF). The STF 428 addressed the needs of Testing activities being performed rapidly leading to a quick and easy improvement of the functionality of the existing e-Signature standardization deliverables, bringing them up to date with current practices. One of the purposes of the STF428 was to prepare a interoperability test event on PAdES, ASiC and to produce a tool to verify the conformity of signatures to the XAdES Baseline Profile.

Following the STF 428, ETSI has organized the first Remote Plugtests Event on PAdES (TS 102 778 part 2 [i.13], part 3 [i.14], part 4 [i.15] and part 5 [i.16]), held from 24 November to 19 December 2011. There were 38 different organizations and 75 people participating in the event.

In 2012, ETSI organized a XAdES Remote Plugtests Event from 14 March to 13 April 2012. It gathered 27 different organizations and 51 people participating in the event. The event aimed to conduct interoperability test cases on XAdES signatures (TS 101 903 [i.10]), including the XAdES Baseline Profile (TS 103 171 [i.11]).

In addition to the Interoperability, the XAdES baseline profile conformance checker tool produced by STF 428, was provided to the participants to perform conformance testing.

Finally, still as an outcome of the STF 428, ETSI organized the first remote Plugtests Interop event for ASiC Signatures from 19 November to 7 December 2012. This Remote event aimed at conducting interoperability test cases on ASiC signatures (Associated Signature Container TS 102 918 [i.18]), including a set of specific test cases as defined in the Test Suite TS 119 164-2 [i.31]. It provided full test coverage of the specification related to the ASiC standard, including both Simple and Extended container forms with CAdES and XAdES signatures. 13 different organizations and 26 people participated in the event.

A.2 TSL Plugtests and Conformance tools

In 2009, ETSI and the European Commission have organized an Interoperability event of TSL (Trust-service Status List) TS 102 231 [i.21], from 19 October to 28 December 2009. For this occasion, the Electronic Signatures Plugtests portal has been fully updated with new functionalities and dedicated tools. This event allowed restricted Member State representatives to test the conformity and interoperability of the Trusted Lists that the Member States have created in accordance with Commission Decision 2009/767/EC [i.5] and TS 102 231 [i.21] V3.1.1. As a result of the plugtest a number of issues were fixed and TS 102 231 [i.21] V3.1.2 was published in December 2009.

There were 22 organizations participating in the event including 20 Member States and ETSI and European Commission representatives. This makes a total of 64 persons involved in the daily activities of the event.

Following the outcomes of the ETSI TSL Interoperability event end of 2009, it was demonstrated that some technical changes are needed in the technical specifications in the Annex to Decision 2009/767/EC [i.5], to ensure functioning and interoperable trusted lists.

The Commission has published the Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC [i.5] as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States (OJ L 199 of 31.07.2010)".

ETSI continued its work on Trust-service Status List (TSL) signatures testing in cooperation with the European Commission (EC) by providing a portal containing several tools to allow Member States to modify their Trusted Lists to make them compliant with the amended Decision and to check their conformity to the new Trusted List Technical Specifications.

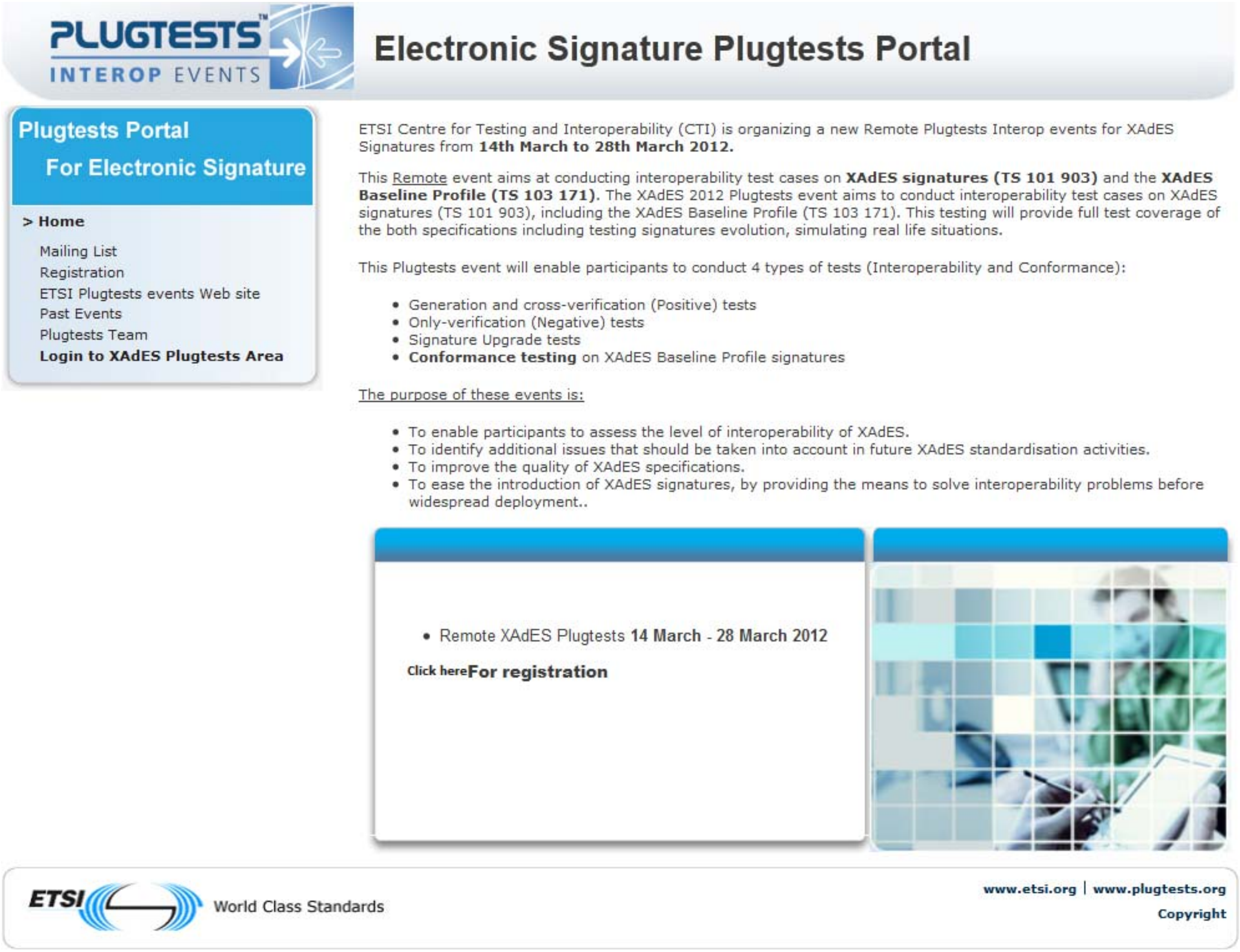
Annex B: ETSI/ESI Plugtests

B.1 Plugtest Portal

Since March 2008, all the Electronic Signatures interop events have been conducted remotely, using a dedicated portal developed by ETSI, allowing signature exchanges between participants and offering cryptographic materials and PKI-related Online services.

The portal has usually two different parts, namely one public part, that anybody may visit, and a private part accessible only for the participants subscribed to the Plugtests event.

B.1.1 Public part of the portal



ETSI Centre for Testing and Interoperability (CTI) is organizing a new Remote Plugtests Interop events for XAdES Signatures from **14th March to 28th March 2012.**

This Remote event aims at conducting interoperability test cases on **XAdES signatures (TS 101 903)** and the **XAdES Baseline Profile (TS 103 171)**. The XAdES 2012 Plugtests event aims to conduct interoperability test cases on XAdES signatures (TS 101 903), including the XAdES Baseline Profile (TS 103 171). This testing will provide full test coverage of the both specifications including testing signatures evolution, simulating real life situations.

This Plugtests event will enable participants to conduct 4 types of tests (Interoperability and Conformance):

- Generation and cross-verification (Positive) tests
- Only-verification (Negative) tests
- Signature Upgrade tests
- **Conformance testing** on XAdES Baseline Profile signatures

The purpose of these events is:

- To enable participants to assess the level of interoperability of XAdES.
- To identify additional issues that should be taken into account in future XAdES standardisation activities.
- To improve the quality of XAdES specifications.
- To ease the introduction of XAdES signatures, by providing the means to solve interoperability problems before widespread deployment..

- Remote XAdES Plugtests **14 March - 28 March 2012**

Click here**For registration**

Figure B.1: Public page screenshot (XAdES 2012)

As mentioned above, this part remains as it was for previous events. It includes the following contents:

- The Plugtests page, providing some more details on the event itself, namely targeted specification, targetted audience, some general info on how to conduct such events, etc.
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating exchange of information.

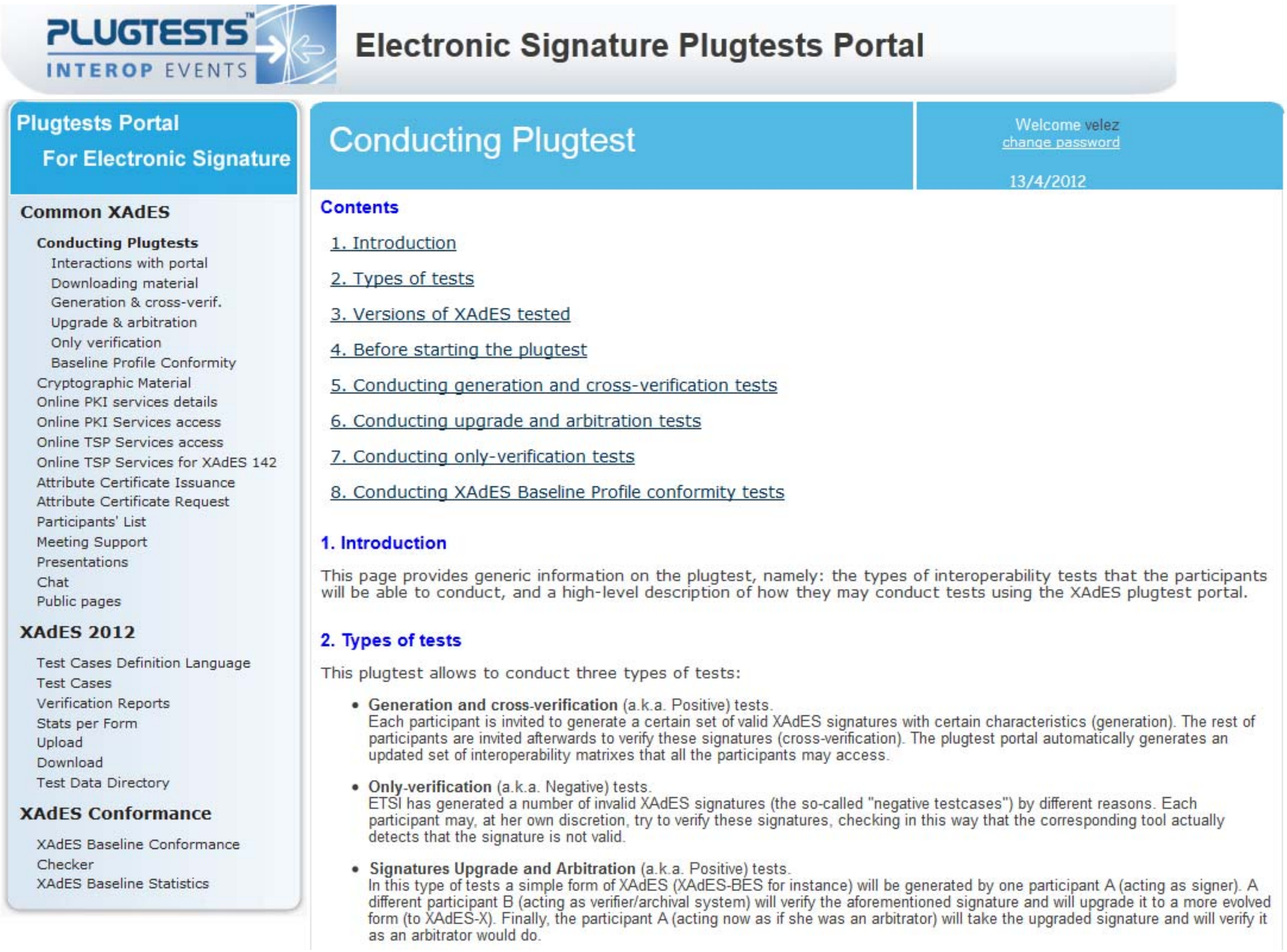
- The Registration page, providing details on the Plugtests registration process.
- The Presentation of the Plugtests team.
- The Presentation of some past events (XAdES, CAdES, PAdES, etc.).
- The **Login to Plugtests Area** page, access to the **protected area** of the portal.

B.1.2 Private part of the portal

This part is visible only for the participants of the Plugtests event. It is structured in three main areas:

- **Common area**. This area contains a number of pages that provide generic information to the participants, which is relevant to participants of signature interoperability tests.
- **Signature specific area**. This area contains a number of pages that support the interoperability tests on tested Signature.
- **Signature Conformance Checker tool.** This area provides a tool for verifying the conformity of signatures.

Clauses below provide details of the contents of these pages.



Contents

1. Introduction
2. Types of tests
3. Versions of XAdES tested
4. Before starting the plugtest
5. Conducting generation and cross-verification tests
6. Conducting upgrade and arbitration tests
7. Conducting only-verification tests
8. Conducting XAdES Baseline Profile conformity tests

1. Introduction

This page provides generic information on the plugtest, namely: the types of interoperability tests that the participants will be able to conduct, and a high-level description of how they may conduct tests using the XAdES plugtest portal.

2. Types of tests

This plugtest allows to conduct three types of tests:

- **Generation and cross-verification** (a.k.a. Positive) tests.
  Each participant is invited to generate a certain set of valid XAdES signatures with certain characteristics (generation). The rest of participants are invited afterwards to verify these signatures (cross-verification). The plugtest portal automatically generates an updated set of interoperability matrixes that all the participants may access.
- **Only-verification** (a.k.a. Negative) tests.
  ETSI has generated a number of invalid XAdES signatures (the so-called "negative testcases") by different reasons. Each participant may, at her own discretion, try to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.
- **Signatures Upgrade and Arbitration** (a.k.a. Positive) tests.
  In this type of tests a simple form of XAdES (XAdES-BES for instance) will be generated by one participant A (acting as signer). A different participant B (acting as verifier/archival system) will verify the aforementioned signature and will upgrade it to a more evolved form (to XAdES-X). Finally, the participant A (acting now as if she was an arbitrator) will take the upgraded signature and will verify it as an arbitrator would do.

Figure B.2: Private page screenshot (XAdES 2012)

B.1.2.1 Contents of Common area of Private part

B.1.2.1.1 Conducting plugtests information pages

The Conducting Plugtests pages provide detailed explanations on how to conduct interoperability and conformance tests on signatures during the event.

Four types of tests are usually provided at the Plugtests events:

- Generation and cross-verification (a.k.a. Positive) tests.
- Only-verification (a.k.a. Negative) tests.
- Signatures Upgrade and Arbitration tests.
- Signatures Conformance Checking tools.

It also provides high level descriptions of the steps that participants need to perform for conducting the three different types of interoperability tests aforementioned and the Conformance checker tool.

The rest of pages of the set provide details on:

- How to download material from the portal for starting conducting the Plugtests (**Downloading material page**). This material is usually a zip file enclosing a well defined folder structure containing both signatures and verification reports on signatures.
- How to generate signatures and to upload them to the corresponding section of the portal so that the rest of participants at the interoperability tests may download and verify them (**Generating Signatures page**).
- How to verify other participants' signatures, report on verification results and uploading of these reports to the portal so that the portal keeps track of the current status of the Plugtests (**Verifying Signatures page**).

B.1.2.1.2 Cryptographic material pages

The Cryptographic Material pages provide details on the cryptographic material that the participants have to deal with while conducting the Plugtests and also on the trust frameworks specified for this Plugtests event.

This cryptographic material consists of:

- P12 files containing private keys and their corresponding certificates for generating and verifying test cases signatures.
- Certificate files containing the CA certificates up to a trust anchor represented by the root CA. These certificates are published in the LDAP server and in the HTTP server deployed in the Plugtests portal.
- CRLs issued by the Cas operating in the Plugtests trust frameworks. These CRLs are re-issued several times during the Plugtests with a certain periodicity, so that all of them are up to date. The CRLs are published in the LDAP server and in the HTTP server deployed in the Plugtests portal.
- The certificate for the Time-stamping server issued by the root CA. As above, this material is published in the LDAP server and in the HTTP server deployed in the Plugtests portal.

The portal deploys trust frameworks for the plugtest, each one having a different Root CA. Within each trust framework different scenarios are defined. ETSI will define groups of test cases for each scenario.

Participants will use the cryptographic material in a certain scenario for generating (and/or verifying) the signatures corresponding to this group. In consequence each scenario will incorporate a set of cryptographic items that the participants will use while working with one of the aforementioned groups of test cases.

Each CA also provides **OCSP** responses reporting the status of the certificates issued by that CA. In addition to that, each CA issued **CRLs** reporting the revoked certificates.

The portal also includes a **Timestamping Authority** able to generate time-stamp tokens on request by the participants.

B.1.2.1.3 Online PKI-related services pages

The Plugtests portal incorporates a number of online PKI-related services.

The **Online PKI services details page** describe all of them and provides details on how the participants may access them.

The on-line PKI-related services deployed are listed below:

- **CA-related services**. This service provides issuance of certificates; generation of CRLs; publication of CRLs. Participants should use this service for getting their corresponding certificates for generating signatures.
- **Time-stamp Authority server**. This server generates RFC 3161 [i.32] time-stamp tokens as per request of the participants in the plugtest.
- **OCSP responders**, which are able to generate OCSP responses to OCSP requests submitted by the participants on the status of a certain certificate generated by the ETSI portal infrastructure. During this Plugtest, these OCSP responders are actually the Cas issuing certificates (Direct Trust Model).
- **LDAP server**. This server acts as central repository for CA and TSA certificates, and CRLs.
- **Http server**. This server acts as alternative central repository for CA and TSA certificates, and CRLs.

This page also contains a link to a Java class implementing basic login/password authentication mechanism required for accessing these services, so that participants had not to develop such a mechanisms in their tools.

B.1.2.1.4 Attribute certificate issuance page

Depending on the testing, the participants may need X509 V2 attribute certificate (RFC 3281 [i.33]) for their signing public key certificate. The private key and certificate of the attribute authority which issues your attribute certificate can be found in the CryptographicMaterial.

Thus the participants can issue their own attribute certificate for themselves by some security toolkits. However the Plugtests service can also issue the attribute certificate if participants need. The portal has integrated a tool allowing participants to upload their X509 certificates and generate the corresponding attribute certificates.

B.1.2.2 Contents of Signatures Interop Specific areas of Private part

The portal contains, within the private part of the portal, a specific area for Signature specification that is tested in these Plugtests.

B.1.2.2.1 Test Cases Definition Language

These pages describe the structure of a signature test case definition. It is intended to be a simple and straight forward way to define all necessary inputs for the creation of a signature.

B.1.2.2.2 Test Cases pages

These are pages containing documents with the complete specification of the test cases for Signature specification.

The documents are written in XML and incorporate XSLT stylesheets and javascript technologies. These technologies allow:

- To browse the aforementioned test definition documents and build pieces of text and tables corresponding to each test case within this document.
- To browse reports of verification (simple XML documents) of each single signature verified by each participant, process them and keep up to date the interoperability matrixes, which show what signatures of each participant have been verified by what other participants and the results of such verifications.

The test case document actually incorporates the whole set of interoperability matrixes resulting from the uploading of the participants of their verification report. It is worth mentionning that XSLT and javascript technologies allow that each time a participant uploads a set of signatures and/or verification reports, the interoperability matrixes shown within the signature test case document, are updated, so that participants always see the up to date information on interoperability tests carried so far.

B.1.2.2.3 Individual verification reports

This area contains a page where each participant may find its own interoperability matrixes, i.e. matrixes that report the verification results obtained by the rest of the participants after trying to verify each of his/her signatures.

These matrixes include links to the signature files and to the verification report files, as well an indication of the verification result.

Each participant has access from the main page of the portal to their own verification reports page, and from there, each participant may directly access to the verification reports pages of the rest of the participants.

B.1.2.2.4 Upload pages

This area contains a page that participants use for uploading their signatures and/or verification reports.

The Upload pages provide mechanisms for uploading new signatures, new verification reports or both.

Once uploaded, the portal re-builds a new downloading package and makes it available for all the participants at the Download page. Within this package, participants will find all the signatures and verification reports generated up to that instant in the Plugtests. It is a way to archive all the different uploads and keep a complete history of the Interop testing of the event.

As it has been already mentioned, the upload of a package has the immediate effect of updating the corresponding interoperability matrixes and the individual verification reports within the suitable specific area.

B.1.2.2.5 Download pages

This area contains a page that participants use for downloading the corresponding initial package that includes cryptographic material, test-definition files, and a folder structure suitable for uploading signatures and verification reports.

These pages are also used for downloading the whole material generated by the participants at a certain instant of the plugtest, including all the signatures and verification reports generated so far.

B.1.2.2.6 Test data directory pages

The page is used by the participants for browsing the folders structure where the portal stores the signatures and the verification files generated by all the participants.

This allows a detailed inspection of the files uploaded in a certain instant to the portal.

B.2 Conducting ETSI/ESI Plugtests

B.2.1 Introduction

The present document provides details on how the participants need to interact with the portal for conducting the different types of interoperability tests, namely:

- Generation and cross-verification (a.k.a. Positive) tests.
  Each participant is invited to generate a certain set of valid signatures with certain characteristics (generation). The rest of participants are invited afterwards to verify these signatures (cross-verification). The Plugtests portal automatically generates an updated set of interoperability matrixes that all the participants may access.

- Only-verification (a.k.a. Negative) tests.
  ETSI has generated a number of invalid signatures (the so-called "negative testcases") by different reasons. Each participant may, at their own discretion, try to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.

- Signatures Upgrade and Arbitration tests.
  In this type of test a simple form of AdES (XAdES-BES for instance) will be generated by one participant A (acting as signer). A different participant B (acting as verifier/archival system) will verify the aforementioned signature and will upgrade it to a more evolved form (to XAdES-X for instance). Finally, the participant A (acting now as if they were an arbitrator) will take the upgraded signature and will verify it as an arbitrator would do.

- Signature Conformance Checking tools.
  The portal incorporates an AdES conformity-testing tool, which tests conformity of signatures against the requirements defined in the standard.

B.2.2 Generation and Cross-verification

Figure B.3 shows two participants interacting with the portal for downloading the material present in the portal, locally performing the required operations for signature generation and cross-verification plugtests type, and uploading to the portal the obtained results.

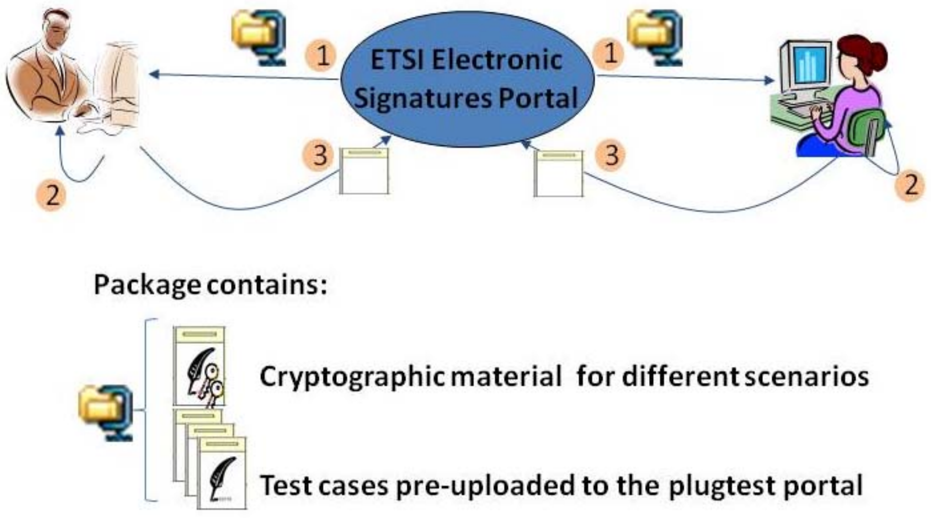

1
ETSI Electronic Signatures Portal
1
3
3
2
2
Package contains:
Cryptographic material for different scenarios
Test cases pre-uploaded to the plugtest portal

Figure B.3: Generation and Cross-verification process

Each participant:

1 downloads the initial package containing cryptographic material, pre-generated signature corresponding to the **only-verification** test cases, and the xml files specifying the different test-cases.

2 locally runs the corresponding generation and cross-verification testcases with the suitable cryptographic material included in this initial package locally on their equipment and with their own tools. Two types of operation are possible here: generation of signature or verification of other participants' signatures.

3 uploads the results to the Plugtests portal. Two types of results are possible for this type of test: generated signatures or other participants' verification reports.

B.2.3 Only Verification

Figure B.4 shows one participant interacting with the portal for downloading the material present in the portal, locally performing the required operations for the **only verification** test sets, and uploading to the portal the obtained results.

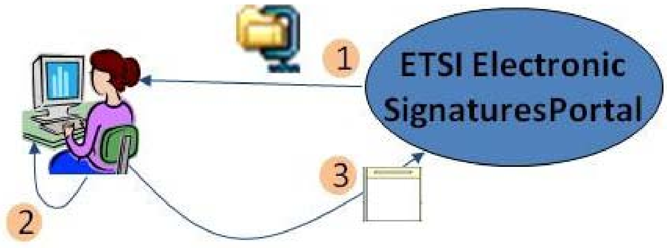


Figure B.4: Only verification process

Each participant:

1 downloads the initial package containing cryptographic material, and the pre-generated signatures corresponding to the **only-verification** test cases, and the xml files specifying the different test-cases.

2 locally runs the corresponding **only verification** testcases with the suitable cryptographic material included in this initial package locally on their equipment and with their own tools.

3 uploads the verification reports obtained in the former step to the Plugtests portal.

B.2.4 Upgrade and Arbitration test

Figure B.5 shows 3 participants interacting with the portal for conducting the signature **upgrade and arbitration** interoperability tests.

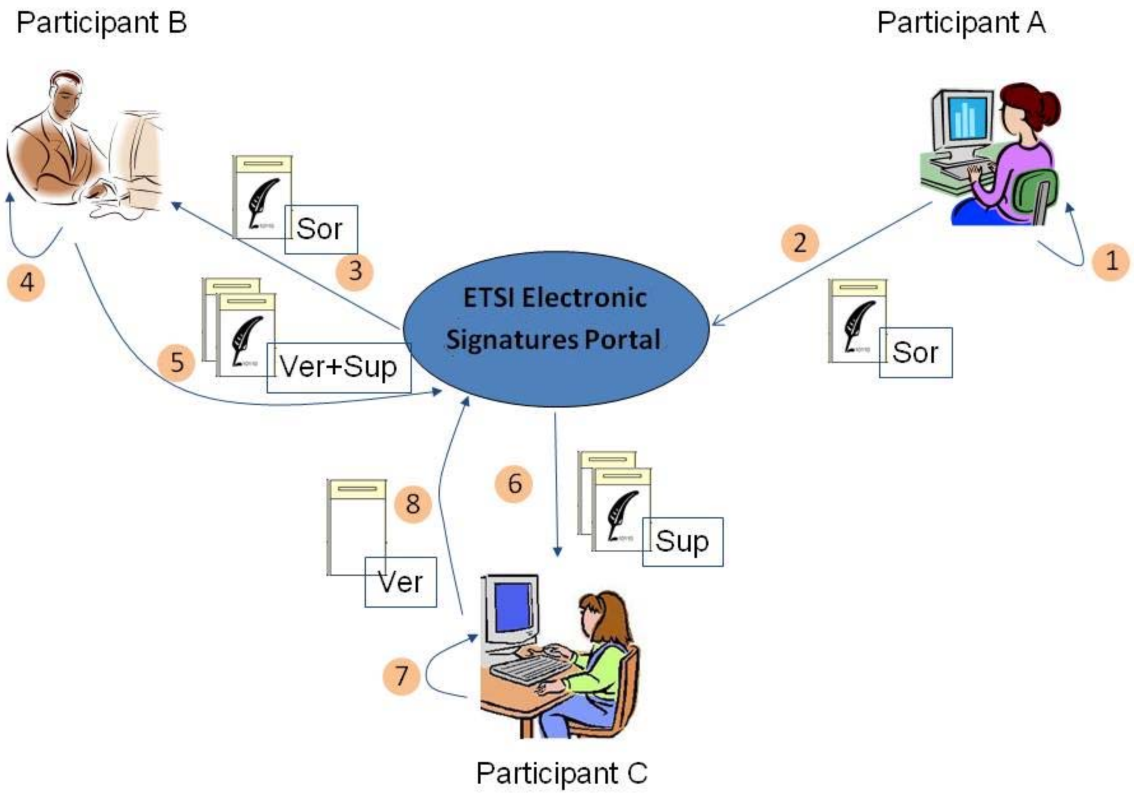


Figure B.5: Only verification process

Step 1 and 2: Participant-A generates a signature according to a certain test case and A uploads it to the Plugtests portal.

Steps 3 to 5: Participant -B downloads the original signature generated by Participant -A and upgrades it to a more complex form. He uploads it to the portal.

Steps 6 to 8: Participant -C acts as an arbitror. He takes the upgraded signature as generated by Participant -B, verifies it, generates a verification report and upload it to the Plugtests portal.

History

Document history		
V1.1.1	December 2013	Publication