ETSI SR 003 186 V2.1.1 (2016-04)

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

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This 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.

[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 as amended.

[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 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

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

[i.9] Void.

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

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

[i.12] Void.

[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".

[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".

[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".

[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".

[i.17] Void.

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

[i.19] Void.

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

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

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

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

[i.24] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[i.25] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.26] Void.

[i.27] Void.

[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 ETSI TS 119 134-5 is published, for further details see ETSI TR 119 000 [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 ETSI TR 119 000 [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 ETSI TR 119 000 [i.1].

[i.31] ETSI TS 119 164-2: "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".

[i.34] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.35] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.36] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.37] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.38] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.39] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.40] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.41] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.42] Directive 2014/24/EU of the European Parliament and of the council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

[i.43] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.44] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.45] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.46] 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.47] ETSI TS 119 124 (all parts): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures Testing Conformance and Interoperability".

[i.48] ETSI TS 119 614: "Electronic Signatures and Infrastructures (ESI); Test suites and tests specifications for Technical Conformity & Interoperability Testing of Trusted Lists".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 000 [i.1], CEN CWA 16408 [i.2], OASIS Standard [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 CEN CWA 16408 [i.2].

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

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 CEN CWA 16408 [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 OASIS Standard [i.3].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 000 [i.1] and the following apply:

ASN	Abstract Syntax Notation
EUMS	European Union Member State
FTB	Final draft for Technical Body approval
LDAP	Lightweight Directory Access Protocol
OJ	Official Journal
PKI	Public Key Infrastructure
PTS	Publication of the Technical Specification
RFC	Request For Comment
SPR	Stable Draft for Public Review
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 instruments 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 ETSI TR 119 000 [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 analysing 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 CEN CWA 16408 [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], [i.45] 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: Directive 2014/24/EU on public procurement [i.42] Article 22(6) mandates that contracting authorities requiring advanced electronic signatures in some stage of the procurement procedure establish the required format on the basis of Commission Decision 2011/130/EU [i.4], [i.45], and accept advanced electronic signatures based on qualified certificates issued by certification service providers listed in the trusted lists provided for in Commission Decision 2009/767/EC [i.5]. The conformity and interoperability testing tools will then 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.

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 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

5.0 Introduction

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 events

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 at last conducted Conformance and Interoperability Testing events

Targeted Deliverable	Last Plugtests	Major changes (made or planned) since the last Plugtests event
CAdES building blocks and baseline signatures - ETSI EN 319 122-1 [i.34] and Extended CAdES signatures - ETSI EN 319 122-2 [i.35]	June 2015	Introduction of a new Archive Time Stamp attribute: archive-time-stamp-v3 incorporating ats-hash-index-v3 Introduction of new attributes of the signer: signer-attributes-v2 and claimed-SAML-assertion Introduction of the new signature-policy-store attribute. ETSI EN 319 102-1 [i.46] and certificates based on TC on ETSI EN 319 412-2 [i.23] and ETSI EN 319 412-5 [i.25] Future events should consider the final version of the European Standards. Of special interest will be to test interoperability of archive-time-stamp-v3 incorporating ats-hash-index-v3, specially for cases where a certain attribute may contain more than one attribute value.

Targeted Deliverable	Last Plugtests	Major changes (made or planned) since the last Plugtests event
XAdES ETSI TS 101 903 [i.10] and building blocks and baseline signatures - draft ETSI EN 319 132-1 [i.36] and Extended XAdES signatures- draft ETSI EN 319 132-2 [i.37]	October 2015	Changes related to the management of signed ds:Manifest elements in the long term. Specified new RenewedDigests element. Definition of new properties substituting to SigningCertificate, SignerRole (able now to incorporate signed assertions), CompleteCertificateRefs, RefsOnlyTimeStamp, and SigAndRefsTimeStamp. Specified new property SignaturePolicyStore. ETSI EN 319 102-1 [i.46] and certificates based on TC on ETSI EN 319 412-2 [i.23] and ETSI EN 319 412-5 [i.25] Future events should consider the new defined attributes and the definitive versions of the European Standards.
PAdES building blocks and baseline signatures ETSI EN 319 142-1 [i.38] and Additional PAdES signature profiles ETSI EN 319 142-2 [i.39]	May 2015	Introduction of the new signer-attributes-v2 attribute in CMS data. Clarification of DSS and DTS fields usage, ETSI EN 319 102-1 [i.46] and certificates based on TC on ETSI EN 319 412-2 [i.23] and ETSI EN 319 412-5 [i.25]
ASiC building blocks and baseline containers - ETSI EN 319 162-1 [i.40] and ASiC Additional containers - ETSI EN 319 162-2 [i.41]	June 2016	Long term attributes as specified in the published version of ETSI EN 319 162-1 [i.40] and use of Evidence Records (IETF RFC 4998 [i.43], IETF RFC 6283 [i.44]).
Procedures for Signature Creation and Validation ETSI EN 319 102-1 and ETSI TS 102 853 [i.22]	April 2016	Future Plugtests events should consider: • ETSI EN 319 102-1 [i.46] on Procedures for Creation and Validation of AdES Digital Signatures (when available, see ETSI TR 119 000 [i.1]) in place of ETSI TS 102 853 [i.22]; • ETSI EN 319 412-2 [i.23] on Certificate Profile for certificates issued to natural persons; • ETSI EN 319 412-3 [i.24] on Certificate Profile for certificates issued to legal persons; • ETSI EN 319 412-5 [i.25] on Extension for Qualified Certificate profile.
NOTE: Future events should consider Evidence Records ([i.43] and [i.44]), when applicable.		

The standards that are targeted directly by the Plugtests events whose planning is proposed in clause 6.2 are the baseline and the extended signatures for CAdES, XAdES and PAdES, the baseline and extended containers for ASiC and the Trusted Lists (ETSI TS 119 612 [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

5.2.0 Introduction

This clause lists the set of Technical Specifications defining test suites for testing interoperability and conformance, against the standards of the Framework ETSI TR 119 000 [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 ETSI TS 119 312 [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.

- ETSI TS 119 124 [i.47] (see ETSI TR 119 000 [i.1]): "CAdES Testing Conformance & Interoperability":
  - Part 2: Test suites for testing interoperability of CAdES baseline signatures.
  - Part 3: Test suites for testing interoperability of extended CAdES signatures.
  - Part 4: Specifications for testing conformance of CAdES baseline signatures.
  - Part 5: Specifications for testing conformance of extended CAdES signatures.

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.

- ETSI TS 119 134 [i.28]: "XAdES Testing Conformance & Interoperability":
  - Part 2: Test suites for testing interoperability of XAdES baseline signatures.
  - Part 3: Test suites for testing interoperability of extended XAdES signatures.
  - Part 4: Specifications for testing conformance of XAdES baseline signatures.
  - Part 5: Specifications for testing conformance of extended XAdES signatures.

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.

- ETSI 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 baseline signatures.
  - Part 3: Test suites for testing interoperability of additional PAdES signatures.
  - Part 4: Specifications for testing conformance of PAdES baseline signatures.
  - Part 5: Specifications for testing conformance of additional PAdES signatures.

5.2.4 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.

- ETSI 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 baseline containers.
  - Part 3: Test suites for testing interoperability of ASiC extended containers.
  - Part 4: Specifications for testing conformance of ASiC baseline containers.
  - Reviewed version of Part 5: Specifications for testing conformance of ASiC extended containers.

5.2.5 Testing Conformance of Trusted Lists

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

- ETSI TS 119 614-2 [i.48] (see ETSI TR 119 000 [i.1]): "Specifications for testing compliance of XML representation of Trusted Lists".

The time schedule for TS production is specified in the table in clause 6.2.

6 Planning of identified activities

6.1 Proposed scheduling and scoping of testing events

Table 2 summarizes the schedule and scope of the proposed testing events.

Table 2: Proposed scheduling and scope for testing events

Targeted specification	Proposed date	Supporting PKIs	Interoperability	Conformance
eSignature Validation	April 2016	EUMS Trusted Lists	ETSI EN 319 102-1 [i.46] and certificates valid at time of the plugtests event against ETSI TS 119 612 [i.20] conformant Trusted Lists	Conformance checking against ETSI EN 319 122-1 [i.34], ETSI EN 319 132-1 [i.36], ETSI EN 319 142-1 [i.38], ETSI EN 319 162-1 [i.40] and some previous versions of the signature formats.
CAdES	November 2016	Simple PKI and more complex PKI	TC from previous test events + TC on ETSI EN 319 122 [i.34] and [i.35] including Evidence Records (IETF RFC 4998 [i.43] and IETF RFC 6283 [i.44])	
ASiC	June 2016	Simple PKI and more complex PKI	TC from previous test events + TC on ETSI EN 319 162 including Evidence Records (IETF RFC 4998 [i.43] and IETF RFC 6283 [i.44])	

According to Table 2 the proposed schedule is as follows:

1) E-Signature Validation Plugtest (March 2016), covering the validation of the 4 main Signature formats (XAdES, PAdES, CAdES, ASiC).

2) The action proposed is to organize an interoperability event on e-signature validation between Member States. The interoperability event will allow Member States and the Commission to test their e-signature validation tools to cross-validate e-signatures in whatever format these may be (XAdES, PAdES, CAdES, ASiC), relying on Member States' Trusted Lists and according to new European Standard ETSI EN 319 102-1 [i.46].

   The proposed schedule event date gives the minimum practical period in which Member States can implement the requirements of the new ENs on XAdES, PAdES, CAdES and ASiC. It will also allow time for Member States to test their compliance to the regulation requirements before the date of application of the implementing act under eIDAS and before the event.

3) ASiC (June 2016), covering both baseline and extended ASiC Container formats.

   This remote event aims to conduct conformance and interoperability testing on ASiC Container. The testing will cover ASiC standards ETSI EN 319 162 [i.40] parts 1 and 2. The testing will be based on the test specification ETSI TS 119 164-2 [i.31] ASiC Interoperability testing.

4) CAdES (November 2016), covering both CAdES baseline signatures and extended CAdES signatures.

This remote event aims to conduct conformance and interoperability testing on CAdES digital signatures. The testing will cover CADES standards ETSI EN 319 122-1 [i.34] and ETSI EN 319 122-2 [i.35] and the new TS extending CAdES to include Evidence Records (IETF RFC 4998 [i.43], IETF RFC 6283 [i.44]). They are to be executed according to new draft ETSI EN 319 102-1 [i.46].

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

6.2.0 Introduction

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 TB Review

At this stage the deliverable is ready to be made available to the ETSI ESI members to gather a first set of comments. These drafts will have a high degree of maturity, given the fact that the reference deliverables listed in clause 5.1 have been approved by ETSI ESI and put in public enquiry phase.

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. These versions will reflect any change in the reference deliverables listed in clause 5.1, consequence of the public enquiry phase.

PTS: Publication as TS

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

All the TSs identified in the present clause will be aligned to the new ENs specifying formats for signatures (ETSI EN 319 122 [i.34] and [i.35], ETSI EN 319 132 parts 1 [i.36] and 2 [i.37], ETSI EN 319 142 parts 1 [i.38] and 2 [i.39], and ETSI EN 319 162 parts 1 [i.40] and 2 [i.41]), and the latest version of the TS specifying the XML format for Trusted Lists (ETSI TS 119 612 [i.20]).

6.2.1 Deliverable D1: Stable Draft for TB Review (SPR)

30th March 2016: ETSI TS 119 124 [i.47] (see ETSI TR 119 000 [i.1]): "CAdES Testing Conformance & Interoperability". The following parts will be covered:

- Part 2: Test suites for testing interoperability of CAdES baseline signatures. Test cases covering:
  - interoperability with simple PKIs;
  - negative test cases for simple PKIs;
  - signatures lifecycle involving three steps: signature generation, signature augmentation and signature arbitration;
  - interoperability with more complex PKIs (uncomplete);
  - interoperability with real PKIs based on European Trusted Lists (uncomplete).
- Part 3: Test suites for testing interoperability of extended CAdES signatures. Test cases covering:
  - interoperability with simple PKIs;
  - negative test cases for simple PKIs;
  - signatures lifecycle involving three steps: signature generation, signature augmentation and signature arbitration;
  - interoperability with more complex PKIs (uncomplete);
  - interoperability with real PKIs based on European Trusted Lists (uncomplete).

- Part 4: Specifications for testing conformance of CAdES baseline signatures. Complete set of test assertions for testing conformance of CAdES signatures against CAdES baseline signatures as specified in ETSI EN 319 122-1 [i.34].

- Part 5: Specifications for testing conformance of extended CAdES signatures. ". (Uncomplete) set of test assertions for testing conformance of CAdES signatures against the different levels of extended CAdES signatures as specified in ETSI EN 319 122-2 [i.35].

30th March 2016: ETSI 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 ETSI TS 119 164-2 [i.31] (V1.1.1) 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.

30th March 2016: ETSI TS 119 614 [i.48] (see ETSI TR 119 000 [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.

30th March 2016: ETSI TS 119 144 [i.29]: "PAdES Testing Conformance & Interoperability". The following parts will be covered:

- Part 2: Test suites for testing interoperability of PAdES baseline signatures. Test cases covering:

  - interoperability with simple PKIs;

  - negative test cases for simple PKIs;

  - signatures lifecycle involving three steps: signature generation, signature augmentation and signature arbitration;

  - interoperability with more complex PKIs (uncomplete);

  - interoperability with real PKIs based on European Trusted Lists (uncomplete) ETSI TR 119 000 [i.1].

- Part 3: Test suites for testing interoperability of additional PAdES signatures. Test cases covering:

  - interoperability with simple PKIs;

  - negative test cases for simple PKIs;

  - signatures lifecycle involving three steps: signature generation, signature augmentation and signature arbitration;

  - interoperability with more complex PKIs (uncomplete);

  - interoperability with real PKIs based on European Trusted Lists (uncomplete).

- Part 4: Specifications for testing conformance of PAdES baseline signatures. Complete set of test assertions for testing conformance of PAdES signatures against PAdES baseline signatures as specified in ETSI EN 319 142-1 [i.38].

- Part 5: Specifications for testing conformance of additional PAdES Signatures. (Uncomplete) set of test assertions for testing conformance of PAdES signatures against the different levels of additional PAdES signatures as specified in ETSI EN 319 142-2 [i.39].

30th March 2016: Test suites for XAdES (ETSI TS 119 134 [i.28]):

- Part 2: Test suites for testing interoperability of XAdES baseline signatures.

  Test cases covering:

  - interoperability with simple PKIs;
  - negative test cases for simple PKIs;
  - signatures lifecycles involving three steps: signature generation, signature augmentation and signature arbitration;
  - interoperability with more complex PKIs (uncomplete);
  - interoperability with real PKIs based on European Trusted Lists (uncomplete).

- Part 3: Test suites for testing interoperability of extended XAdES.

  Test cases covering:

  - interoperability with simple PKIs;
  - negative test cases for simple PKIs;
  - signatures lifecycles: involving three steps: signature generation, signature augmentation to different conformance levels, and signature arbitration;
  - interoperability with more complex PKIs (uncomplete);
  - interoperability with real PKIs based on European Trusted Lists (uncomplete).

- Part 4: Specifications for testing conformance of XAdES baseline signatures.

  Complete set of test assertions for testing conformance of XAdES signatures against XAdES baseline signatures as specified in ETSI EN 319 132-1 [i.36].

- Part 5: Specifications for testing conformance of extended XAdES signatures.

  (Uncomplete) set of test assertions for testing conformance of XAdES signatures against the different levels of extended XAdES signatures as specified in ETSI EN 319 132-2 [i.37].

6.2.2 Deliverables D2: Final Draft for approval (FTB)

30th April 2016: All the TSs will be completed and amended according to the comments received from ETSI ESI TB members and be ready for the final approval by the ESI TB.

6.2.3 Deliverables D3: Publication (PTS)

30th June 2016: All the TSs will be published two months later their approval by ETSI ESI TB.

6.3 Production plan for conformity testing tools development

Table 3: Conformity testing tools development plan

Milestone	Milestone Type	Due date	Format/Spec.	Details
Xtool-M1	Internal milestone	Beginning October 2015. Ready for the XAdES test event.	XAdES	The XAdES Conformance Checker (XAdESCC hereinafter) will: 1. Perform complete conformance checks for XAdES baseline signatures. 2. Perform complete conformance checks for the different levels of extended XAdES signatures, with not distributed qualified properties.
Xtool-M2	Internal milestone	End March 2016	XAdES	Complete XAdESCC. This will add the conformance checks for extended XAdES signatures with distributed qualified properties.
Ctool-M1	Internal milestone	Mid March 2016	CAdES	The CAdES Conformance Checker (CAdESCC hereinafter) will: 1. Perform complete conformance checks for CAdES baseline signatures. 2. Perform part of the tests for extended CAdES signatures, including tests on attributes with references to validation material. No LTV attribute check.
Ctool-M2	Internal milestone	Mid April 2016	CAdES	Complete CAdESCC.
Ptool-M1	Internal milestone	End March 2016	PAdES	The PAdES Conformance Checker (PAdESCC hereinafter) will: 1. Perform complete conformance checks for PAdES baseline signatures. 2. Perform part of the tests for additional PAdES profiles based on CAdES signatures.
Ptool-M2	Internal milestone	End April 2016	PAdES	Complete PAdESCC.
Atool-M1	Internal milestone	Mid May 2016	ASiC	The ASiC Conformance Checker (ASiCCC hereinafter) will: 1. Perform complete conformance checks for baseline containers with baseline signatures. 2. Perform part of the tests for additional containers with baseline and extended signatures.
Atool-M2	Internal milestone	End May 2016	ASiC	Complete ASiCCC.
Ttool-M1	Internal milestone	End May 2016	Trusted Lists	Consolidated but uncomplete version of the Trusted Lists Conformance Checker (TLCC hereinafter).
Ttool-M2	Internal milestone	End June 2016	TLCC	Complete TLCC.

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 ETSI TS 101 903 [i.10] (V1.3.2) and CAdES ETSI TS 101 733 [i.8] (V1.7.4).

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 ETSI TS 101 903 [i.10] (V1.4.1) and CAdES ETSI TS 101 733 [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 in 2011 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 this initial activity was to prepare an interoperability test event on PAdES, ASiC and to produce a tool to verify the conformity of signatures to the XAdES Baseline Profile.

ETSI has organized the first Remote Plugtests Event on PAdES (ETSI 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 (ETSI TS 101 903 [i.10]), including the XAdES Baseline Profile (ETSI TS 103 171 [i.11]).

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

Finally, ETSI organized the first remote Plugtests Interoperability 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 ETSI TS 102 918 [i.18]), including a set of specific test cases as defined in the Test Suite ETSI 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) ETSI 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 ETSI TS 102 231 [i.21] (V3.1.1). As a result of the Plugtest a number of issues were fixed and ETSI 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 [i.6] 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

B.1.0 Introduction

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

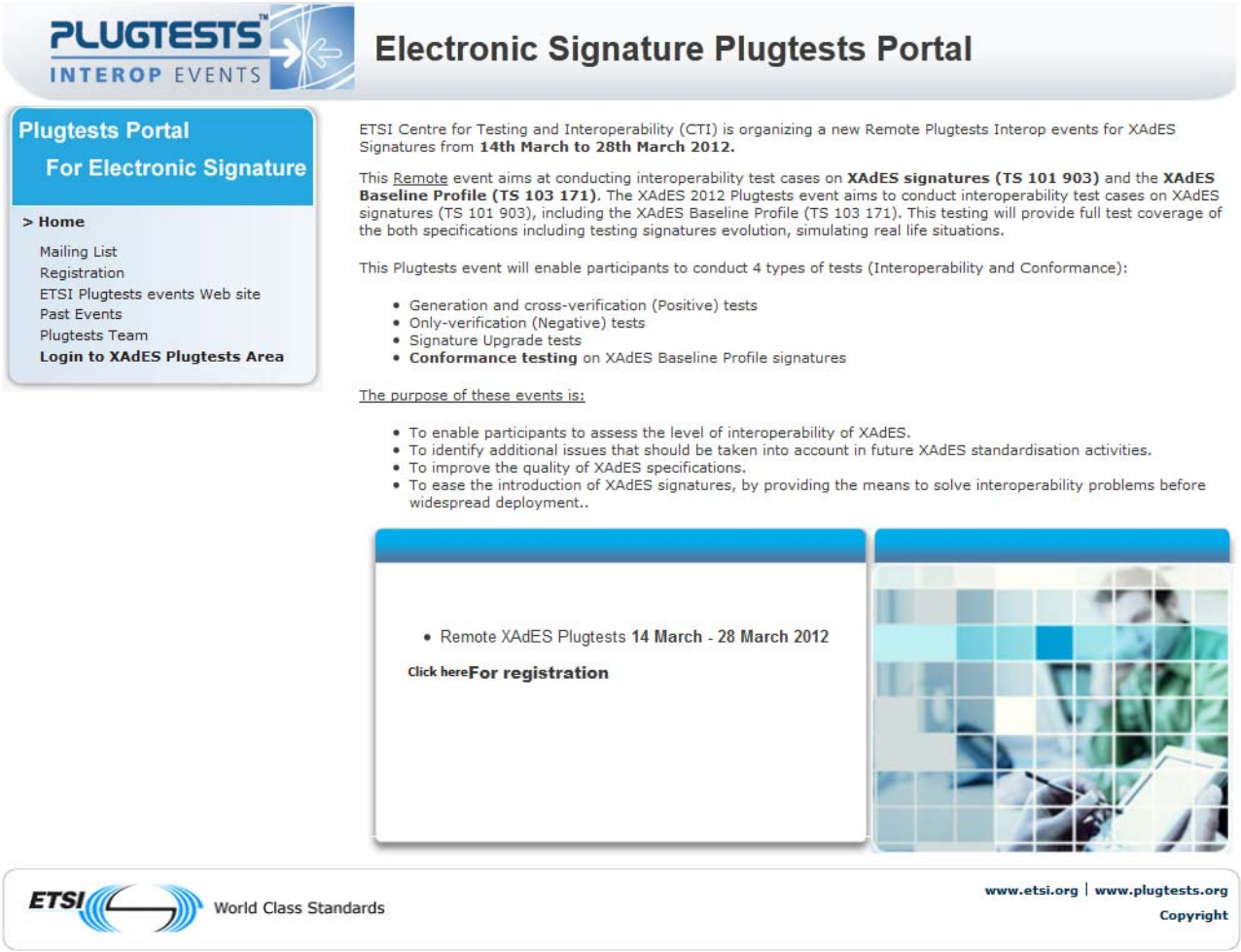

Figure B.1: Public page screenshot (XAdES 2012)

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, targeted 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

B.1.2.0 Introduction

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.

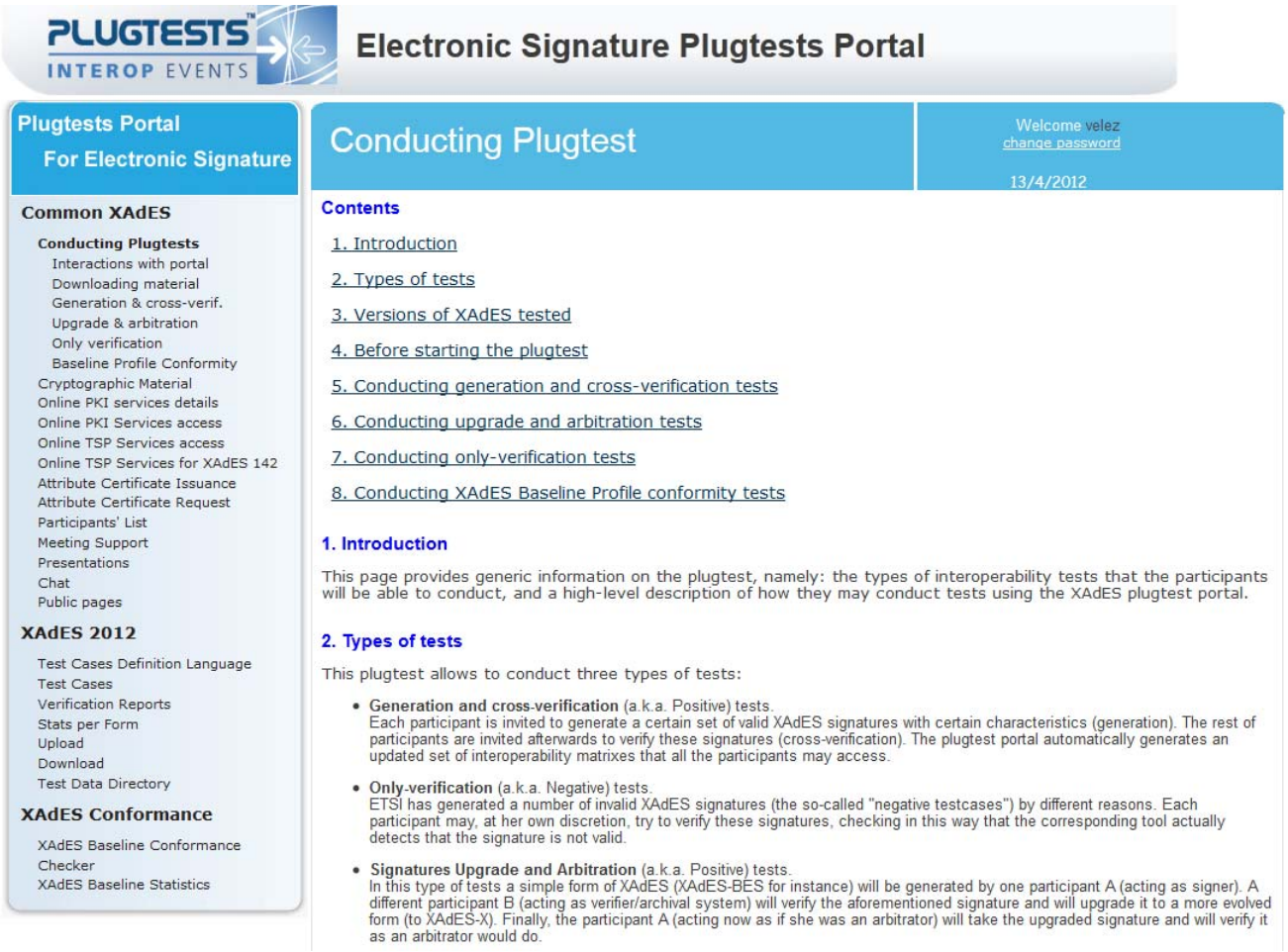

Figure B.2: Private page screenshot (XAdES 2012)

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 IETF 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 (IETF 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

B.1.2.2.0 Introduction

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 the present 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 mentioning 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). ETSI, usually, acts as signer and provides a certain number of simple form of digital signatures by using signing and timestamping certificates generated by a real PKI supported by the EUMS Trusted Lists infrastructure. 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, another participant C, that could be the participant A too (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.

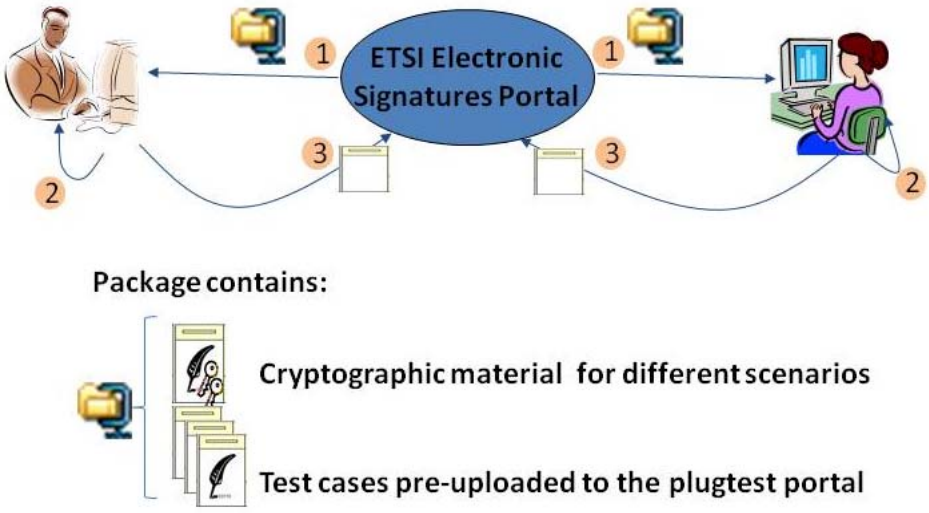

Figure B.3: Generation and Cross-verification process

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.

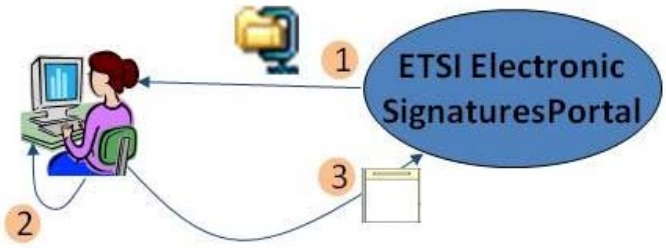

Figure B.4: Only verification process

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.

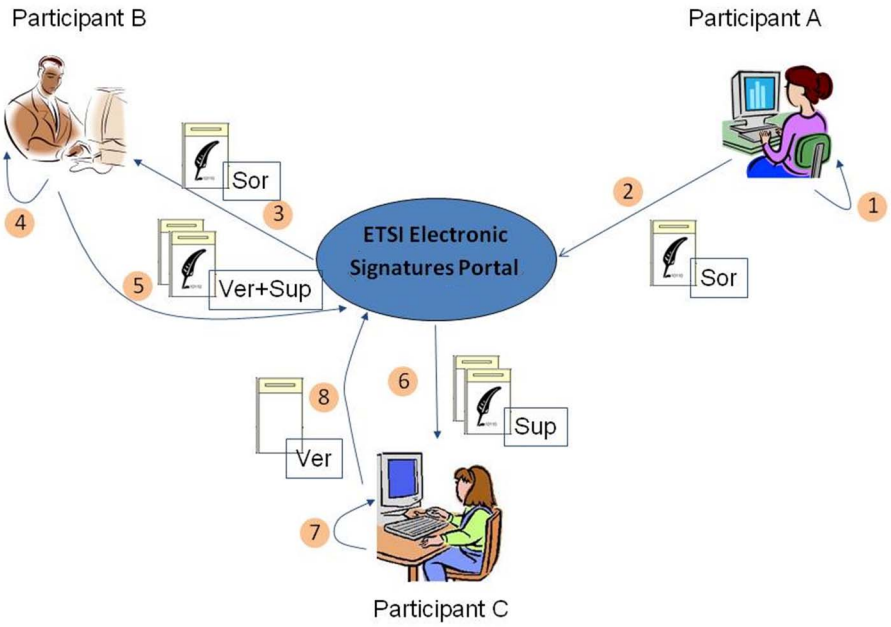

Figure B.5: Only verification process

Steps 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 arbiter. He takes the upgraded signature as generated by Participant -B, verifies it, generates a verification report and upload it to the Plugtests portal.

Annex C: Bibliography

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

ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

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

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

ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

History

Document history		
V1.1.1	December 2013	Publication
V2.1.1	April 2016	Publication