Technical Report of the XAdES Remote Plugtests™ Event (Oct/Nov 2015)

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

Reference

Keywords
Electronic Signature,

February 2016

Version 1.0

Author:

Luigi Rizzo, InfoCert
Juan Carlos Cruellas, UPC
Laurent Velez, ETSI

Editor:

Laurent Velez, ETSI laurent.velez@etsi.org

Abstract

This document is the technical report of the 2015 remote Plugtests event on XAdES Digital Signature. (XML Advanced Electronic Signature ETSI TS 101 903 and EN 319 132), organized by ETSI' s Centre of Testing and Interoperability (CTI) conducted using the specifically designed ETSI portal which supports remote interoperability Plugtests.

For reasons of confidentiality this report does not list the results of each testcase, it only shows the overall and anonymous statistics, without any link to the company names.

Status of this Document

This document is provided by ETSI Centre of Testing and Interoperability (CTI). For further details on Plugtests services, please see: http://www.etsi.org/Website/OurServices/Plugtests/home.aspx .

.

Contents

1 Introduction

In answer to phase 2 of the European Commission Mandate 460 on Electronic Signatures Standardization, ETSI has initiated 3 Specialist Task Force projects (STF).

The ETSI STF-459 is one of the three STFs that are implementing Phase 2 of the Electronic Signature Mandate/460 requirement for a "rationalised European eSignature standardization framework (the other two are STF-457 and STF-458).

The STF 459 addresses the needs of testing interoperability and conformance. In this area, the STF aims at producing a set of ETSI Technical Specifications (ETSI TSs) and software tools that will help to accelerate the generation and deployment of systems that ensure true interoperability of electronic signatures across the European Union. The STF aims at generating a set of ETSI TSs that defines test suites for testing interoperability of Advanced Electronic Signatures (including their Baseline Profiles) in their different formats, Containers of those signatures, and also Trusted Lists of Certification Services Providers.

The ETSI TS 119 134 part 1-5 "XAdES Testing Conformance & Interoperability" produced by the STF 459 is the basis of the testing proposed at the XAdES Plugtests 2015 interoperability event.

This Plugtests event is the 6th of the series of interoperability events scheduled to run for 2 years, as defined in the ETSI SR 003 186. This series of events will address interoperability and conformance needs for all the AdES signatures defined by ETSI.

ETSI has organized the remote Plugtests event on XAdES, held from 1st October to 18th Nov 2015 This remote event aims to conduct conformance and interoperability testing on XAdES digital signatures. The testing will cover TS 101 903 but also the draft ETSI EN 319 132.

A special focus will be performed on the augmentation of XAdES signatures. The tests included creation and verification of signature and were executed according to new draft EN 319 102 (Procedures for Signature Creation and Validation).

The XAdES specifications are in the process of becoming EN 319 132, but drafts are publicly available for review, so the participants were invited to take in account and to implement the new EN 319 132.

- 319 132-1 XAdES digital signatures; Part 1: XAdES baseline signatures
- 319 132-2 XAdES digital signatures; Part 2: XAdES Extended signatures

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

- Generation and cross-verification (Positive) tests
- Only-verification (Negative) tests
- Augmentation and Arbitration (Positive) tests
- Conformance testing

The present document is the report from the 2015 remote Plugtests Event on XAdES Digital Signatures. It also provides details on the specification, design and implementation of the portal supporting remote Plugtests events on XAdES specification, including an overview of the contents of the portal as well as the on-line PKI-related services provided to the participants of the XAdES Remote Plugtests.

The present report provides details on:

- Specification, design and implementation of those testcases description, including cross-verification and negative testcases for XAdES Digital signatures, based on ETSI TS 119 134 "XAdES Testing Conformance& Interoperability

- The Remote Plugtests Event on XAdES was organized by ETSI and held from 1st October to 18th November 2015.

In order to give participants time to prepare the testing, ETSI opened the portal to participants in "read-only" mode, a couple of days before the official start date of the Plugtests event. An introduction web conference took place on 1st October to present the portal and the testing.

The event was initially planned to run until 31st October but it was extended to 18th November on request from the participants. The reason being that the amount of testing activities was extremely high within the initial scheduled period, due to the large number of participants.

The present document is organized as indicated below.

Section 2 provides details on how the material of the portal is organized and the services it provides to the participants of the Plugtests Events.

Section 3 lists the participants to the 2015 XAdES Remote Plugtests Event.

Section 4 provides an overview of the most interesting results and conclusions of the Plugtests.

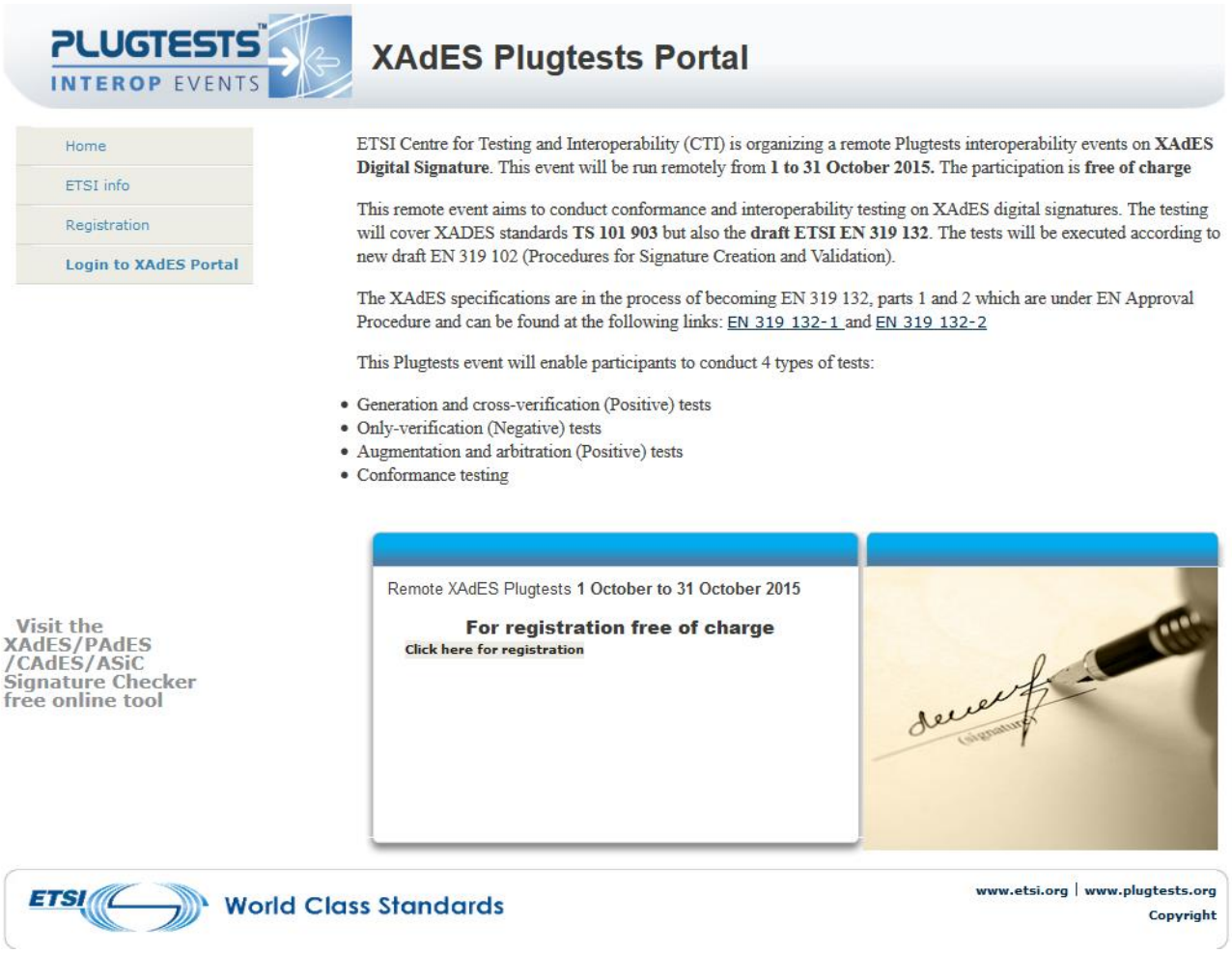
Section 5 provides details on a number of issues related to the XAdES specifications as identified by the participants. These issues have been raised to the ETSI TC ESI, with the recommendation that they are taken into consideration for future XAdES standardization activities, especially for the Draft EN 319 132.

Section 6 shows some overall statistics on the test results and also the testcases defined for the Plugtests event.

2 Organization and contents of the portal

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

2.1 Public part of the portal



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

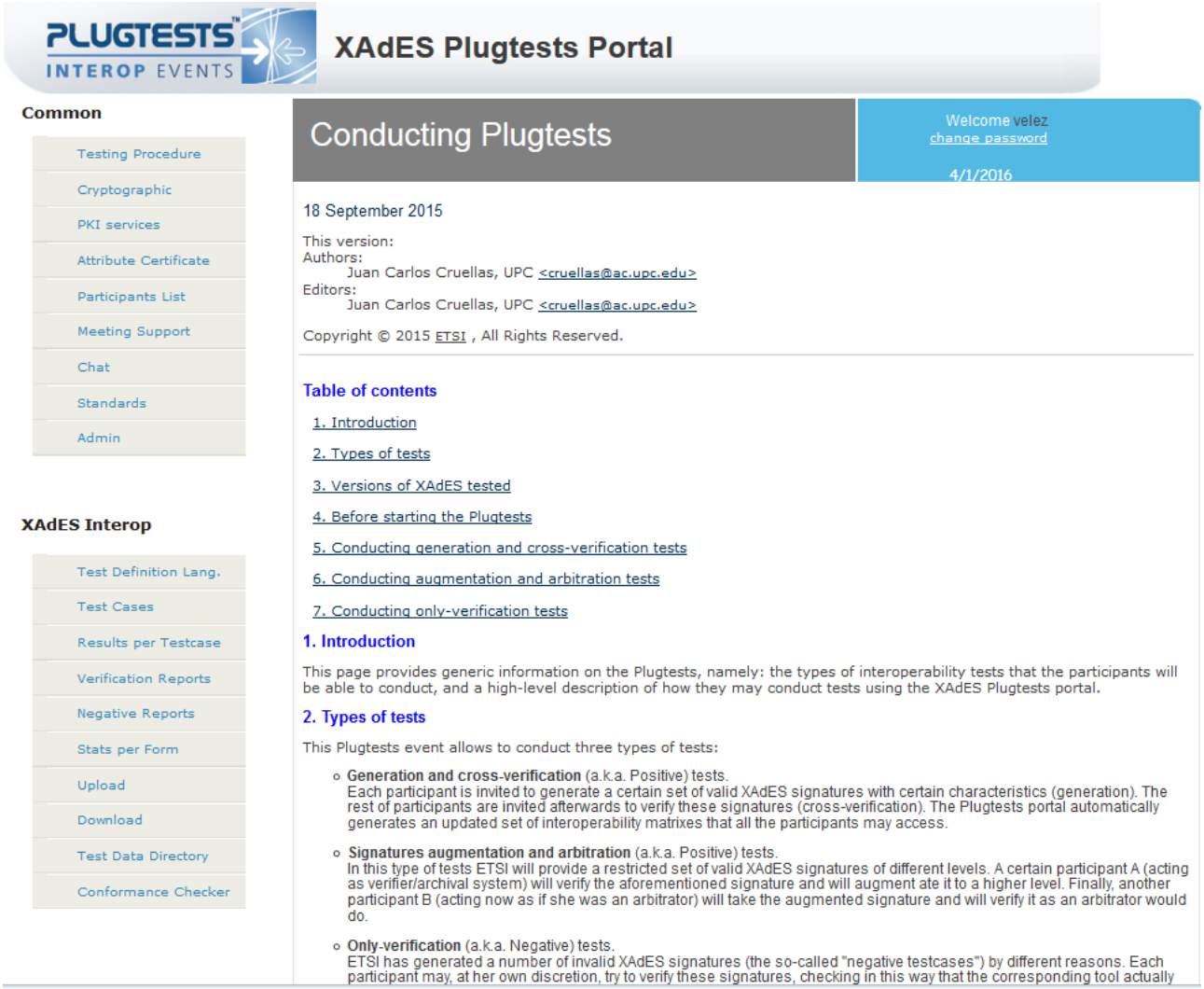
- The XAdES Plugtests page, providing some more details on the event itself, namely targeted specification, targeted audience, some general info on how to conduct such event, etc.
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating 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, PAdES, XAdES, ASiC)
- The **Login to Plugtests Area** page gives access to the **protected area** of the portal.

2.2 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 XAdES interoperability tests.
- **XAdES Interop area**. This area contains a number of pages that support the interoperability tests on XAdES.

Sub-clauses below provide details of the contents of these pages.



2.2.1 Contents of Common area of Private part

2.2.1.1 Conducting Plugtests information pages

The Conducting Plugtests page is the first of a set of 7 pages providing detailed explanations on how to conduct interoperability and conformance tests on XAdES during this event.

This first page details the 4 types of tests provided at this Plugtests event:

- 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 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 XAdES signatures (the so-called "negative testcases") with different reasons. Each participant may, at his/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 Augmentation and Arbitration (a.k.a. Positive) tests.
  In this type of tests a simple form of XAdES (XAdES-B-B 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-B-T for instance). Finally, the participant A (acting now as if he/she was an arbitrator) will take the upgraded signature and will verify it as an arbitrator would do.

- Conformance testing.
  In this type of tests, participants will have to upload XAdES signatures to the portal Conformance checker.

This section also provides details on the versions of XAdES specifications:

- ETSI pre EN 319 132 v1.0.0. The test suite defined in Test Cases includes test cases for:

  - Part 1. XAdES Baseline signatures XAdES-B-B, XAdES-B-T, XAdES-B-LT, and XAdES-B-LTA levels.

  - Part 2. XAdES Extended signatures XAdES-E-BES, XAdES-E-C, XAdES-E-X, XAdES-E-XL, and XAdES-E-A.

- XAdES ETSI TS 103 171v2.2.1. The test suite defined in Test Cases includes test cases for the four conformance levels, identified within this document as XAdES-B conformance level, XAdES-T conformance level, XAdES-LT conformance level, and XAdES-LTA conformance level.

- XAdES ETSI TS 101 903v1.4.2. The test suite defined in Test Cases includes test cases for XAdES-BES, XAdES-C, XAdES-X, XAdES-XL, and XAdES-A.

They aim at providing a good coverage of the different XAdES specifications existing today:

- The pair formed by the existing ETSI TSs, namely ETSI TS 101 903v1.42, ETSI TS 103 731v2.1.1. The test cases defined in this test suite lead to XAdES signatures that, in most of the cases, are compliant at the same time with both ETSI TS 101 903v1.42, ETSI TS 103 731v2.1.1.

- The new ETSI pre EN 319 132 v1.0.0 parts 1 and 2. The test cases defined in this test suite lead to XAdES signatures that, in most of the cases, are compliant at the same time with both ETSI TS 101 903v1.42, ETSI pre EN 319 132-1 v1.0.0 and ETSI pre EN 319 132-2 v1.0.0.

It also provides high level description of the steps that participants must perform for conducting the 4 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 XAdES 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**).

2.2.1.2 Cryptographic material pages

The Cryptographic Material page is the first one of a set of three pages providing 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 in:

- 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 (there will be two different root CAs, namely: RootCAOK and RootCAOK2). These certificates will be published in the LDAP server (details for accessing to the LDAP server may be found in the Online PKI services details page) and in the HTTP server deployed in the Plugtest portal.

- CRLs issued by the CAs operating in the Plugtest trust frameworks. These CRLs will be re-issued several times during the Plugtest with a certain periodicity, so that all of them are up to date. The CRLs will be published in the LDAP server and in the HTTP server deployed in the Plugtest portal.

- The certificate for the Time-stamping servers issued by different CAs. As above, this material will be published in the the LDAP server and in the HTTP server deployed in the Plugtest portal.

The portal deployed trust frameworks for this Plugtests, allowing different scenarios.

Trust framework and scenarios:

ETSI has defined a number of trust frameworks, within which different scenarios are defined. ETSI has defined groups of test cases (for instance a group defining different test cases for XAdES baseline signatures compliant with level B) for each scenario (they will be grouped within the folder XAdES-B-B).

Participants will use the cryptographic material in a certain scenario (as per ETSI indications) 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.

There are two trust frameworks: the one whose root CA is RootCAOK and the other whose root CA is RootCAOK2. These two trust frameworks support three scenarios, which are detailed below:

- Scenario SCOK. This scenario will include the first root CA (RootCAOK), one intermediate CA (LevelACAOK), one final CA, which issues certificates for end-entities (LevelBCAOK), and a Time Stamp Authority (TSA1), certified by RootCAOK. Participants will use its cryptographic material for both generating and verifying the signatures corresponding to the generation and cross-verification.In this scenario there are the certificates managed during the generation and verification of the signature, including the end-entities certificates issued by the CA deployed in the portal to the participants, that are valid. CAs within this scenario issuing certificates will issue the CRLs including references to the revoked certificate. CAs within this scenario will also generate OCSP responses reporting on the status of these certificates whenever it is requested by the participants. This scenario is intended to check implementations behavior when verifying signatures that will be provided by the other participants.
- Scenario SCOK2. This scenario is formed by the second root CA RootCAOK2 and a Time Stamp Authority (TSA3) certified by RootCAOK2, which issues correct time-stamp tokens. This scenario allows that signatures generated following the specifications of certain test cases, incorporate time-stamp tokens coming from two correct and different TSAs (namely TSA1 certified by RootCAOK, and TSA3 certified by RootCAOK2). This has impact on the contents of XAdES properties carrying validation material of time-stamp tokens.

- Scenario SCUN. This scenario will include the following services:

1. RootCAOK, LevelACAOK, and LevelBCAOK.
2. A CA, issuing certificates to end entities, whose certificate shall be revoked by the time the Plugtest will start (LevelBCARev, certified by LevelACAOK).
3. A Time Stamp Authority, certified by LevelBCARev(TSA2).
4. A Time Stamp Authority, certified by RootCAOK, whose certificate shall be revoked by the time the Plugtest will start (TSA_Rev).
5. A Time Stamp Authority, certified by RootCAOK, whose certificate shall be expired by the time the Plugtest will start (TSA_Exp).

Participants will use its cryptographic material for verifying signatures pre-generated by ETSI corresponding to the only-verification test cases. Furthermore, in this scenario there are the certificates managed during the verification of the signature, including:

1. One pre-generated signing certificate, issued by LevelBCAOK, which by the time the Plugtest will start will be revoked.
2. One pre-generated signing certificate, issued by LevelBCAOK, which by the time the Plugtest will start will be expired.

   CAs within this scenario issuing the certificates will issue the CRLs including references to the revoked certificate. CAs within this scenario will also generate OCSP responses reporting on the status of these certificates whenever it is requested by the participants. ETSI will pre-generate one XAdES signature using the revoked certificate and another one using the expired certificate. This scenario is intended to check implementations behavior when verifying not valid signatures.

2.2.1.3 Online PKI-related services page

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

The **Online PKI services details page** describes 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 XAdES signatures.
- **Time-stamp Authority server**. This server generates RFC 3161 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 will actually be 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 have not to develop such a mechanisms in their tools.

2.2.1.4 Online PKI services access page

The Online PKI Services access page allows to access to most of the on-line PKI-related services provided by the portal, namely: access to the CA software for requesting generation of a key-pair and the corresponding end-entity

certificate for generating signatures, connection details for accessing the LDAP server where CRLs and CA certificates are stored, etc.

2.2.1.5 Online TSA services access page

The Online TSP Services access page allows to access to the TSA server deployed in the server for requesting generation of time-stamp tokens.

2.2.1.6 Attribute certificate issuance page

This tool is available in case the participants need X509 V2 attribute certificate ([RFC3281]) for their signing public key certificate. The private key and certificate of the attribute authority which issues the attribute certificate can be found in the Cryptographic Material.

Therefore 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 required by the participants. The portal has integrated a tool allowing participants to upload their X509 certificates and generate the corresponding attribute certificates ('Attribute Certificate Request' section on the left menubar)

2.2.1.7 Participants' List page

This page lists the details of all the companies and people that participated in the Plugtests as well as their email addresses and login name.

2.2.1.8 Meeting Support page

The Meeting Support page contains all the information related to the meetings that took place during the Plugtests event. It includes:

- Introduction presentation. This presentation was made available before the start of the Plugtests, and it provides the most relevant information on the event, including structure of the portal, relevant URLs, rules to be followed during the participation, etc
- Calendar for the meetings (Gotowebinar conference calls).
- URL for accessing a chat server accessible through a Web browser where the calls were minuted and participants could write their comments, questions and statements.
- The agenda for each meeting.
- Links to the minutes of each meeting.

2.2.1.9 Mailing list

A mailing list, with archives, was set up which was restricted to participants of the event and this was used to exchange messages, questions and clarifications. This was the main medium for putting questions to the Plugtests support team and initiating technical discussion between participants

After each upload of signatures or verifications, an email was sent to all participants via this mailing list so that the participants were made aware each time that a company has performed an upload with the related content.

2.2.1.10 Chat page

The Chat page provides access to a web-based chat that participants use during the conference calls for sharing notes. It is also used for taking notes of the meetings. These notes are the core component of the meetings minutes.

2.2.1.11 Known issues pages

This page lists all the known issues related to the portal which were waiting for resolution by the Plugtests support team.

2.2.2 Contents of XAdES Interop Specific areas of Private part

Within the private area of the portal there is a specific area for the XAdES specification that is tested during this event.

2.2.2.1 Test Cases Definition Language

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

2.2.2.2 Test Cases pages

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

It is worth noting that the use of XSLT and JavaScript enable an automatic update of the interoperability matrixes within the XAdES test case document each time a set of signatures or verification report is uploaded. This ensures that the participants always have access to the complete and up to date information on the interoperability tests which have been carried out at any time.

2.2.2.3 Individual verification reports

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

These matrixes include links to the signature files and to the verification report files as well as 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 the verification reports pages of the other participants.

2.2.2.4 InteropMatrix reports

This area contains a page where each participant may find interoperability matrixes per testcase.

For each testcase, the matrix displays the signatures from the signers and the corresponding verification results from the verifiers. This is similar to the verification reports but built per testcase and not per company. This matrix is also rebuilt after each upload.

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

2.2.2.5 Statistics per signature form

The Statistics page contains 3 tables that summarize the number of XAdES signatures generated and verified at each moment of the Plugtests.

The tables show how many signatures of a certain XAdES form have been generated or verified per company and also the number of verified negative testcase signatures.

2.2.2.6 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 in the XAdES area 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 moment 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 already mentioned, the upload of a package has the immediate effect of updating the corresponding interoperability matrixes and the individual verification reports within the related area.

2.2.2.7 Download pages

This area contains a page that participants use for downloading the 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 entire material generated by the participants at any precise moment during the event including all the XAdES signatures and verification reports generated thus far.

2.2.2.8 Test data directory pages

The page is used by the participants for browsing the folders structure where the portal stores the XAdES signatures and the verification files generated by all the participants. This allows a detailed inspection of the files uploaded to the portal at any moment during the event.

3 Participants list

The table below shows the details of all the organizations and people who have participated in the 2015 XAdES remote Plugtests event.

There were **67 different organizations** and 116 people participating in the event.

#	Registered Company	Country
1	Agency for Digital Agenda of Romania	RO
2	Ardaco, a.s.	SK
3	ARhS	LU
4	AS Sertifitseerimiskeskus	EE
5	Ascertia Limited.	UK
6	AULOCE, S.A.	ES
7	Borica - Bankservice AD	BG
8	BULL	FR

#	Registered Company	Country
9	Central Bank of Costa Rica	CR
10	Certisign	BR
11	Connective	BE
12	Cryptolog	FR
13	DIAN: Income Tax, Import & Export Services in Colombia	CO
14	DIGNITA, sro	CZ
15	Disig, a.s.	SK
16	Ditec, a.s.	SK
17	EldoS Corporation	UK
18	Estina	LT
19	EUSO	LV
20	EVAL Tecnologia	BR
21	EVICERTIA	ES
22	EXPLAND UAB	LI
23	Gemalto	CZ
24	Governikus GmbH & Co KG	DE
25	Indenova SL	ES
26	Infocert S.p.A.	IT
27	Insiel S.p.A.	IT
28	intarsys GmbH	DE
29	Intesi Group	IT
30	Kale Yazilim A.S.	TR
31	Lacuna Software	BR
32	LangEdge,Inc.	JP
33	LEX PERSONA	FR
34	Lombardia Informatica S.p.A.	IT
35	Mentana-Claimsoft GmbH	DE
36	Microsec ltd.	HU
37	MORPHO	FR
38	National Security Authority	SK
39	Noreg Ltd.	HU
40	Nowina Solutions	LU
41	Peculiar Ventures	RU
42	Polish Security Printing Works	PL
43	POLYSYS	HU
44	První certifikacní autorita, a.s.	CZ
45	Real.not	FR
46	Safelayer Secure Communications, S.A.	ES
47	Safelayer Secure Communications, S.A.	ES
48	SecCommerce Informationssysteme GmbH	DE
49	Secure Information and Communication Technologies	AT
50	SEFIRA spol. s r.o.	CZ
51	SeguriData Privada, S. A. de C. V.	MX
52	Servicios Avanzados Para las Instituciones S.A.	ES

#	Registered Company	Country
53	SIA	ES
54	Software602 a.s.	CZ
55	Solvo	CR
56	TECSIDEL	ES
57	Tessaris Integrated Security AG	CH
58	Thales UK	UK
59	TrustWeaver AB	SE
60	UAB "MIT-SOFT"	LT
61	Unimatica S.p.A.	IT
62	Universidad Politécnica de Cataluña	ES
63	Unizeto Technologies SA	PL
64	Viafirma S.L.	ES
65	NISZ National Infocommunications Services Company	HU
66	Secrypt GmbH	DE
67	xades4j	PT

4 Plugtests conclusions

4.1 Remote vs. Face to Face

ETSI CTI reinforces its opinion on the usefulness of remote Plugtests as a way of reducing costs to participants.

With 67 organizations from Europe, Central and South Americas, Turkey and Japan participating, it would have been difficult to organise a face to face event.

4.2 Communication supporting technologies

The utilization of Web conference (GotoWebinar) has been very much appreciated by participants. It has allowed the participants to get very interactive conferences by sharing the same document or application. At the welcome meeting the team explained how to conduct the testing by carrying out a real case demonstration.

The chat feature of the portal has also been very important for the participants to write their questions or request and also it has been used to record meeting minutes.

4.3 Event duration

In order to let participants read all the documentations and prepare the testing, ETSI has opened the portal 2 days before the official beginning of the interoperability event.

Initially, 4 weeks of testing have been planned for this event, starting from 1st Oct to 31st Oct 2015. 67 companies were registered. As each company has to verify the signature of the others, the time needed increases with the number of companies and it was agreed that 4 weeks was definitely too short. On the request from participants, the Plugtests has been extended until the 18th November 2015.

5 XAdES related Issues

5.1 Introduction

The present section lists some of the issues raised during the XAdES Plugtests event in October and November 2015. This technical report will be provided to ETSI TC ESI which is the technical committee in charge of the standardization of the XAdES Digital Signature.

5.2 Usage of URI attribute in TimeStampValidationData element

At the Plugtest it was discussed about the error raised by the XAdES conformance checker when checking an ETSI TS 101 903 v1.4.2 XAdES signature containing a SignatureTimestamp element because of the presence of the URI attribute in the TimestampValidationData element incorporated immediately after the SignatureTimestamp element. It was pointed out that ETSI TS 101 903 v1.4.2 doesn't prohibit the URI attribute inclusion in a TimeStampValidationData element incorporated immediately after the respective electronic timestamp container element even if such inclusion should be avoided in these cases because this URI attribute is not needed and adding a wrong value that doesn't refer the correct timestamp container could create mistakes when validating the XAdES signature. The XAdES conformance checker was amended for being able to accept the above specified signature. In the latest version of EN 319 132-1 a note was added in the clause defining the use of URI attribute in TimeStampValidationData element pointing how to manage XAdES signatures validation containing wrong URI attribute values in TimestampValidation data.

5.3 Expiration date of "old" algorithms to be checked in validation procedures

At the Plugtest it was suggested to provide some positive and negative test cases in which testing the expiration of an algorithm, such as SHA1 hashing algorithm, or key size, such as RSA 1024 bits, at a certain date. In such way the signatures created after the set expiration date would not pass the validation check concerning crypto constraints while the signatures created before such set expiration date would pass the check.

5.4 Usage of DataObjectFormat element with ObjectReference attribute that refers to <ds:KeyInfo> element

At the Plugtest there were some XAdES signatures containing a xades:DataObjectFormat element including an ObjectReference attribute referring to the ds:KeyInfo element. It was asked if xades:DataObjetFormat elements could refer to elements different than ds:Object ones. The xades:DataObjectFormat is a property providing information on the type of any of the objects signed by the signature, except the XAdES signed properties (for obvious reasons) and, in case of a countersignature, except the countersigned signature (also for obvious reasons). As the signed object may be located in places different than ds:Object containers (detached documents in servers, for instance), xades:DataObjectFormat may point to ds:Reference elements referencing other objects than ds:Object elements.

5.5 IssuerSerialV2 encoding

At the Plugtest it was requested a clarification concerning the IssuerSerialV2 element definition. Because it contains a DER-encoded instance of type IssuerSerial it seemed more logical that its type was EncapsulatedPKIData (which is normally used to represent DER encoded data) instead of base64Binary. It was stated that the type EncapsulatedPKIData is base64Binary with an attribute name="Encoding". The value of IssuerSerial is always DER-encoded and for this reason the Encoding attribute is never used. So the IssuerSerialV2 type is directly base64Binary.

5.6 External signed contents and DataObjectFormat

At the Plugtest a participant asked a clarification concerning references pointing to an external content, and the associated xades:DataObjectFormat elements. The participant generated these signatures making the external signed content pointed by a ds:Reference included in the ds:SignedInfo or pointed by a ds:Reference which included in a ds:Manifest. The conformance checker returned errors while checking a XAdES signature which used a ds:Manifest. It was stated that the XAdESCC in its current status was able only to deal with:

Enveloping signatures

Detached signatures where the signed data objects and the signatures are part of the same XML documents and are detached ones from the others.

Detached signatures where the signed data objects are referenced from the signatures through non relative URI references.

5.7 Signing certificate identification

Some participants had signing certificate detection problems when validating XAdES signatures including multiple certificates in ds:KeyInfo element. These participants were advised to identify the signing certificate included in the ds:KeyInfo certification chain as the end certificate having no descendants and/or considering the first <xades:Cert> element of the <xades:SigningCertificate> element as the signing certificate.

5.8 OCSPIdentifier element URI attribute

A participant noticed a little mistake in ETSI EN 319 132-1 Annex A.1.2 about OCSPIdentifier element URI attribute. It was stated:

The OCSPIdentifier child of OCSPRef element shall include the generation time of the OCSP response in its ProducedAt child.

The value in ProducedAt child of OCSPIdentifier shall indicate the same time as the time indicated by the ProducedAt field of the referenced OCSP response.

URI attribute of CRLRef element indicates one place where the referenced OCSP response can be archived.

The last sentence was modified in the latest draft of ETSI EN 319 132-1 as:

URI attribute of OCSPIdentifier element indicates one place where the referenced OCSP response can be archived.

5.9 IssuerAndSerialV2 element validation

Some debate was devoted to the negative checking and validation of XAdES signatures containing the SigningCertificateV2 element including the IssuerSerialV2 element.

It was pointed out the requirement for SigningCertificateV2, CompleteCertificateRefsV2, and AttributeCertificateRefsV2 elements: “the references to certificates shall not include the IssuerSerialV2 element”.

5.10 Signature core validation

Some participants encountered some problems when checking signatures integrity. It was stated that any modifications of ds:SignedInfo element (such as deleting or adding whitespaces) shall be avoided to solve the issue of validation check failures.

5.11 References included in CompleteCertificateRefs

At the Plugtest it was asked a clarification concerning the possibility to put TSU's certification path references and data in the CompleteCertificateRefs and CertificateValues elements (mixed with the signer's certification path references anda data).

It was stated that the references in these elements have to be references to validation material for the signature's signing certificate, not to the validation material for RFC3161 timestamp signing certificates.

5.12 Countersignature format

Some participants asked to clarify if the DataObjectFormat element should be included in a CounterSignature element being the CounterSignature element itself a XAdES baseline signature. The current implementation of EN 319 132-1 states in requirement k) in clause 6.3 that if the signature is a baseline signature countersigning another signature, and if it only signs its own signed properties and the countersigned signature, then it shall not include any DataObjectFormat signed property. If the signature is a baseline signature countersigning another signature and if it signs its own signed properties, the countersigned signature, and other data object(s), then it shall include one DataObjectFormat signed property for each of these other signed data object(s) aforementioned.

5.13 CompleteCertificateRefs and CompleteRevocationRefs

A participant asked

- if CompleteCertificateRefs element should contain only references to CA certificates in certificate path or to all CA certificates used during validation (such as indirect CRL certificate path and/or OCSP responder certificate path)
- if, when CompleteRevocationRefs element is present, a verifier should check that only referenced data was used during validation.

It was stated that CompleteCertificateRefs shall include references to every certificate and revocation data used to validate the signature. It means, e.g., including certificates of the OCSP signing certificate path too.

If the CompleteRevocationRefs element is present, a verifier should use only referenced data during validation. Revocation data should be collected after SignatureTimeStamp

6 XAdES Plugtests testing

6.1 Overall statistics

Here is a table of the overall number of **GENERATED** XAdES signatures containers per test case sets

Tests	B-B	B-LT	B-LTA	B-T	E-BES	E-A	E-C	E-X	E-XL	UpdArb
Total	212	55	119	52	26	78	28	52	48	8

Here is a table of the overall number of **VERIFIIED** XAdES signatures containers per test case sets

Tests	B-B	B-LT	B-LTA	B-T	E-BES	E-A	E-C	E-X	E-XL	UpdArb
Total	1848	340	893	663	170	313	118	169	265	27

Here is a table of the overall number of **VERIFIIED** XAdES signatures containers per **Negative** test case sets

Tests	B-BN	B-TN	B-LTAN	E-AN	E-CN	E-XN	E-XLN
Total	87	71	16	24	6	24	49

6.2 Generation and Verifications testcases

6.2.1 Test case XAdES-B-B and XAdES-EN_B-B levels

The test cases in this section deal with signatures conformant to XAdES Baseline Profile Conformance Level B as specified in ETSI TS 103 171 v2.1.1 and XAdES baseline signatures level B as specified in ETSI pre EN 319 132 Part 1.

- X-B-B-1.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat

Description:

This is the simplest XAdES Baseline Profile conformance level B test case. The signature ONLY CONTAINS the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-B-B-2.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat

Description:

This is the simplest XAdES Baseline Profile conformance level B test case, with TWO signed data objects apart from the signed XAdES properties. This brings the presence of two xades:DataObjectFormat elements.

- X-B-B-3.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlace

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-B-B-4.xml

+SigningCertificate
+xades:SigningTime

+xades:DataObjectFormat
+xades:SignatureProductionPlace
+SignerRole
++ClaimedRoles

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:SignerRole containing one claimed role (XML encoded). The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-B-B-5.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlace
+SignerRole
++CertifiedRoles

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:SignerRole containing one certified role. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-B-B-6.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlace
+xades:CommitmentTypeIndication

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:CommitmentTypeIndication. The signature only signs the XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The CommitmentTypeIndication applies to one of the signed data objects, indicates commitment "ProofOfOrigin", and includes one commitment qualifier privately defined.

- X-B-B-7.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlace
+IndividualDataObjectsTimeStamp
+xadesv141TimeStampValidationData

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace, xades:IndividualDataObjectsTimeStamp and xadesv141:TimeStampValidationData. The signature only signs the

XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The xades:IndividualDataObjectsTimeStamp time-stamps one of the signed data objects. The xadesv141:TimeStampValidation data contains the validation data for the time-stamp token encapsulated in xades:IndividualDataObjectsTimeStamp. The revocation data are CRLs.

- X-B-B-8.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlace
+AllDataObjectsTimeStamp
+xadesv141TimeStampValidationData

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace, xades:AllDataObjectsTimeStamp and xadesv141:TimeStampValidationData. containing The signature only signs the XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The xades:AllDataObjectsTimeStamp time-stamps all the signed data objects. The xades:AllDataObjectsTimeStamp time-stamps one of the signed data objects. The xadesv141:TimeStampValidation data contains the validation data for the time-stamp token encapsulated in xades:AllDataObjectsTimeStamp. The revocation data are OCSP responses.

- X-B-B-9.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlace
++CounterSignature

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:CounterSignature. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-B-B-10.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlace
+SignerRole
++CertifiedRoles
+xades:CommitmentTypeIndication
+IndividualDataObjectsTimeStamp
+xadesv141TimeStampValidationData

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace, xades:SignerRole with one certified role, xades:CommitmentTypeIndication, xades:IndividualDataObjectsTimeStamp and xadesv141:TimeStampValidationData. containing The signature only signs the XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The CommitmentTypeIndication applies to one of the signed data objects, indicates

commitment "ProofOfOrigin", and includes one commitment qualifier privately defined. The xades:IndividualDataObjectsTimeStamp time-stamps one of the signed data objects. The xadesv141:TimeStampValidation data contains the validation data for the time-stamp token encapsulated in xades:IndividualDataObjectsTimeStamp. The revocation data are OCSP responses.

- X-B-B-11.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlace

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:SignaturePolicyIdentifier. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-B-1.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat

Description:

This is the simplest XAdES-B-B baseline signature. The signature ONLY CONTAINS the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertificateV2, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-B-2.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat

Description:

This is the simplest XAdES-B-B baseline signature test case, with TWO signed data objects apart from the signed XAdES properties. This brings the presence of two xades:DataObjectFormat elements.

- X-EN_B-B-3.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-B-4.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
+SignerRoleV2
++ClaimedRoles

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:SignerRoleV2 containing one claimed role (XML encoded). The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-B-5.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
+SignerRoleV2
++CertifiedRolesV2

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:SignerRoleV2 containing one certified role within a X509 attribute certificate. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-B-6.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
+xades:CommitmentTypeIndication

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:CommitmentTypeIndication. The signature only signs the XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The CommitmentTypeIndication applies to one of the signed data objects, indicates commitment "ProofOfOrigin", and includes one commitment qualifier privately defined.

- X-EN_B-B-7.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
+IndividualDataObjectsTimeStamp
+xadesv141TimeStampValidationData

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2, xades:IndividualDataObjectsTimeStamp and xadesv141:TimeStampValidationData. The signature only signs the

XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The xades:IndividualDataObjectsTimeStamp time-stamps one of the signed data objects. The xadesv141:TimeStampValidation data contains the validation data for the time-stamp token encapsulated in xades:IndividualDataObjectsTimeStamp. The revocation data are CRLs.

- X-EN_B-B-8.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
+AllDataObjectsTimeStamp
+xadesv141TimeStampValidationData

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2, xades:AllDataObjectsTimeStamp and xadesv141:TimeStampValidationData. containing The signature only signs the XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The xades:AllDataObjectsTimeStamp time-stamps all the signed data objects. The xades:AllDataObjectsTimeStamp time-stamps one of the signed data objects. The xadesv141:TimeStampValidation data contains the validation data for the time-stamp token encapsulated in xades:AllDataObjectsTimeStamp. The revocation data are OCSP responses.

- X-EN_B-B-9.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
++CounterSignature

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:CounterSignature. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-B-10.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2
+SignerRoleV2
++CertifiedRolesV2
+xades:CommitmentTypeIndication
+IndividualDataObjectsTimeStamp
+xadesv141TimeStampValidationData

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2, xades:SignerRoleV2 with one certified role within a X509 attribute certificate, xades:CommitmentTypeIndication, xades:IndividualDataObjectsTimeStamp and xadesv141:TimeStampValidationData. containing The signature only signs the XAdES signed properties and TWO documents: text files. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to these signed simple text files. The CommitmentTypeIndication applies to

one of the signed data objects, indicates commitment "ProofOfOrigin", and includes one commitment qualifier privately defined. The xades:IndividualDataObjectsTimeStamp time-stamps one of the signed data objects. The xadesv141:TimeStampValidation data contains the validation data for the time-stamp token encapsulated in xades:IndividualDataObjectsTimeStamp. The revocation data are OCSP responses.

- X-EN_B-B-11.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignatureProductionPlaceV2

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:SignaturePolicyIdentifier. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

6.2.2 Test cases for XAdES-B-T and XAdES-EN_B-T levels.

The test cases in this section deal with signatures conformant to XAdES Baseline Profile Conformance Level T as specified in ETSI TS 103 171 v2.1.1 and XAdES baseline signatures level LT as specified in ETSI pre EN 319 132 Part 1.

- X-B-T-1.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp

Description:

This is the simplest test case for testing signatures conformants to XAdES Baseline Profile conformance level. The signature ONLY CONTAINS the mandatory XAdES properties, (xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat) and xades:SignatureTimeStamp. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-B-T-2.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+SignatureTimeStamp

Description:

This is a test case for testing a signature conformant to XAdES Baseline Profile conformance level B with two xades:SignatureTimeStamp. The signature ONLY CONTAINS the mandatory XAdES properties, (xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat) and TWO xades:SignatureTimeStamp. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-T-1.xml

+SigningCertificateV2
+xades:SigningTime

+xades:DataObjectFormat
+SignatureTimeStamp

Description:

This is the simplest test case for testing XAdES-B-T baseline signatures. The signature ONLY CONTAINS the mandatory XAdES properties, (xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat) and xades:SignatureTimeStamp. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_B-T-2.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+SignatureTimeStamp

Description:

This is a test case for testing XAdES-B-B baseline signatures with two xades:SignatureTimeStamp. The signature ONLY CONTAINS the mandatory XAdES properties, (xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat) and TWO xades:SignatureTimeStamp. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

6.2.3 Test cases for XAdES-B-LT and XAdES-EN_B-LT levels.

The test cases in this section deal with signatures conformant to XAdES Baseline Profile Conformance Level LT as specified in ETSI TS 103 171 v2.1.1 and XAdES baseline signatures level LT as specified in ETSI pre EN 319 132 Part 1.

- X-B-LT-1.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+CertificateValues
+RevocationValues

Description:

Test case for testing the simplest signature conformant to XAdES Baseline Profile conformance level LT. The signature signs ONE signed data object, incorporates ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are CRLs.

- X-B-LT-2.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+CertificateValues
+RevocationValues

Description:

Another signature for testing the simplest case of XAdES Baseline Profile conformance level LT. ONE signed data object, ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are OCSP responses.

- X-B-LT-3.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignerRole
++CertifiedRoles
+SignatureTimeStamp
+CertificateValues
+AttrAuthoritiesCertValues
+RevocationValues

Description:

A signature for testing XAdES Baseline Profile conformance level LT that incorporates certified attributes. The signature has one signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, and one xades:RevocationValues. The revocation material used are CRLs.

- X-B-LT-4.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignerRole
++CertifiedRoles
+SignatureTimeStamp
+CertificateValues
+AttrAuthoritiesCertValues
+RevocationValues
+AttributeRevocationValues

Description:

A signature for testing XAdES Baseline Profile conformance level LT that incorporates certified attributes. The signature incorporates one signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, one xades:RevocationValues, and one xades:AttributeRevocationValues. The revocation material used are OCSP responses.

- X-EN_B-LT-1.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+CertificateValues
+RevocationValues

Description:

Test case for testing the simplest XAdES-B-LT baseline signatures. The signature signs ONE signed data object, incorporates ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are CRLs.

- X-EN_B-LT-2.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+CertificateValues
+RevocationValues

Description:

Another test case for testing the simplest XAdES-B-LT baseline signatures. The signature signs ONE signed data object, incorporates ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are OCSP responses.

- X-EN_B-LT-3.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignerRoleV2
++CertifiedRolesV2
+SignatureTimeStamp
+CertificateValues
+AttrAuthoritiesCertValues
+RevocationValues

Description:

A test case for testing XAdES-B-LT baseline signatures that incorporate certified attributes. The signature has one signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, and one xades:RevocationValues. The revocation material used are CRLs.

- X-EN_B-LT-4.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignerRoleV2
++CertifiedRolesV2
+SignatureTimeStamp
+CertificateValues
+AttrAuthoritiesCertValues
+RevocationValues
+AttributeRevocationValues

Description:

A test case for testing XAdES-B-LT baseline signature that incorporates certified attributes. The signature incorporates one signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, one xades:RevocationValues, and one xades:AttributeRevocationValues. The revocation material used are OCSP responses.

- X-EN_B-LT-5.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+xades:SignaturePolicyIdentifier
+SignatureTimeStamp
+CertificateValues
+RevocationValues

Description:

This XAdES baseline signature contains the mandatory XAdES properties plus xades:SignaturePolicyIdentifier, xades:SignatureTimeStamp, xades:CertificateValues, xades:RevocationValues, and xadesv141:SignaturePolicyStore. The xadesv141:SignaturePolicyStore contains the signature policy document base-64 encoded.

6.2.4 Test cases for XAdES-B-LTA and XAdES-EN_B-LTA levels.

The test cases in this section deal with signatures conformant to XAdES Baseline Profile Conformance Level LTA as specified in ETSI TS 103 171 v2.1.1 and XAdES baseline signatures level LTA as specified in ETSI pre EN 319 132 Part 1.

- X-B-LTA-1.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA1), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-B-LTA-2.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA1), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-B-LTA-3.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the

certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-B-LTA-4.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-B-LTA-5.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp issued by TSA1.

- X-B-LTA-6.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData

++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including one OCSP response reporting the status of TSA1's certificate , and a second xadesv141:ArchiveTimeStamp issued by TSA1.

- X-B-LTA-7.xml

+SigningCertificate
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA1), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including one OCSP response reporting the status of TSA1's certificate , and a second xadesv141:ArchiveTimeStamp issued by TSA1.

- X-EN_B-LTA-1.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA baseline signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA1), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_B-LTA-2.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData

++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES Baseline Profile conformance level LTA. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA1), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_B-LTA-3.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA baseline signatures. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_B-LTA-4.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA baseline signatures. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_B-LTA-5.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues

+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA baseline signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp issued by TSA1.

- X-EN_B-LTA-6.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA signatures. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including one OCSP response reporting the status of TSA1's certificate , and a second xadesv141:ArchiveTimeStamp issued by TSA1.

- X-EN_B-LTA-7.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA signatures. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA1), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by this CA), xades:CertificateValues, xades:RevocationValues (OCSP responses), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including one OCSP response reporting the status of TSA1's certificate , and a second xadesv141:ArchiveTimeStamp issued by TSA1.

- X-EN_B-LTA-8.xml

+SigningCertificateV2
+xades:SigningTime
+xades:DataObjectFormat
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141TimeStampValidationData
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-B-LTA baseline signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp issued by TSA1.

6.2.5 Test cases for XAdES-BES and XAdES-E-BES levels.

The test cases in this section deal with XAdES-BES signatures specified in ETSI TS 101 903 v1.4.2 and XAdES-E-BES as specified in ETSI pre EN 319 132 Part 2.

- X-BES-1.xml

+xades:SigningTime
+xades:DataObjectFormat

Description:

This is a XAdES-E-BES signature. The signature CONTAINS the XAdES properties xades:SigningTime and xades:DataObjectFormat and the element ds:KeyInfo containing the signer certificate in X509Certificate. The signature signs the XAdES signed properties, the ds:KeyInfo element and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-BES-3.xml

+SigningCertificate
+xades:DataObjectFormat

Description:

This is a XAdES-E-BES signature. The signature ONLY CONTAINS the XAdES properties xades:SigningCertificate, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

- X-EN_E-BES-2.xml

+SigningCertificateV2
+xades:DataObjectFormat

Description:

This is a XAdES-E-BES signature. The signature ONLY CONTAINS the XAdES properties xades:SigningCertificateV2, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

6.2.6 Test cases for XAdES-C and XAdES-E-C levels.

The test cases in this section deal with XAdES-C signatures specified in ETSI TS 101 903 v1.4.2 and XAdES-E-C as specified in ETSI pre EN 319 132 Part 2.

- X-C-1.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs

Description:

This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefs and the corresponding CRLs in CompleteRevocationRefs.

- X-C-2.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs

Description:

This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefs and the corresponding OCSP responses in CompleteRevocationRefs.

- X-C-3.xml

+xades:SigningTime
+SigningCertificate
+SignerRole
++CertifiedRoles
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+AttributeCertificateRefs
+AttributeRevocationRefs

Description:

This test case tests the use of AttributeCertificateRefs.

- X-C-4.xml

+xades:SigningTime
+SigningCertificate
+SignerRole
++CertifiedRoles
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+AttributeCertificateRefs
+AttributeRevocationRefs

Description:

This test case tests the use of AttributeCertificateRefs.

- X-EN_E-C-5.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs

Description:

This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefsV2 and the corresponding CRLs in CompleteRevocationRefs.

- X-EN_E-C-6.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs

Description:

This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefsV2 and the corresponding OCSP responses in CompleteRevocationRefs.

- X-EN_E-C-7.xml

+xades:SigningTime
+SigningCertificateV2
+SignerRole
++CertifiedRoles
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+AttributeCertificateRefsV2
+AttributeRevocationRefs

Description:

This test case tests the use of AttributeCertificateRefsV2 and AttributeRevocationRefs.

- X-EN_E-C-8.xml

+xades:SigningTime
+SigningCertificateV2
+SignerRole
++CertifiedRoles
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+AttributeCertificateRefsV2
+AttributeRevocationRefs

Description:

This test case tests the use of AttributeCertificateRefsV2 and AttributeRevocationRefs.

6.2.6 Test cases for XAdES-X and XAdES-E-X levels.

The test cases in this section deal with XAdES-X signatures specified in ETSI TS 101 903 v1.4.2 and XAdES-E-X as specified in ETSI pre EN 319 132 Part 2.

- X-X-1.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-X-2.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-X-3.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs (OCSP), xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-X-4.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs (OCSP), xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-X-5.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues

Description:

This test case tests CompleteCertificteRefs and CompleteRevocationRefs based on OCSP responses. Also SigAndRefsTimeStamp and TimeStampValidationData for this timestamp. TimeStampValidationData uses OCSP responses.

- X-X-6.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues

Description:

This test case tests CompleteCertificateRefs and CompleteRevocationRefs based on CRLs. Also RefsOnlyTimeStamp and TimeStampValidationData for this timestamp. TimeStampValidationData uses CRL values.

- X-EN_E-X-7.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-X-8.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp

+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-X-9.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs (OCSP), xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-X-10.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2

Description:

Test case for testing XAdES-X signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs (OCSP), xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-X-11.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues

Description:

This test case tests CompleteCertificteRefsV2 and CompleteRevocationRefs based on OCSP responses. Also SigAndRefsTimeStampV2 and TimeStampValidationData for this timestamp. TimeStampValidationData uses OCSP responses.

- X-EN_E-X-12.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues

Description:

This test case tests CompleteCertificateRefsV2 and CompleteRevocationRefs based on CRLs. Also RefsOnlyTimeStampV2 and TimeStampValidationData for this timestamp. TimeStampValidationData uses CRL values.

6.2.7 Test cases for XAdES-XL and XAdES-E-XL levels.

The test cases in this section deal with XAdES-XL signatures specified in ETSI TS 101 903 v1.4.2 and XAdES-E-XL as specified in ETSI pre EN 319 132 Part 2.

- X-XL-1.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs (CRLs), xades:CompleteRevocationRefs, xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (CRLs).

- X-XL-2.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs (CRLs), xades:CompleteRevocationRefs, xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (CRLs).

- X-XL-3.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs (OCSP), xades:CompleteRevocationRefs, xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (OCSP).

- X-XL-4.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs (OCSP), xades:CompleteRevocationRefs, xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (OCSP).

- X-EN_E-XL-5.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2 (CRLs), xades:CompleteRevocationRefs, xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (CRLs).

- X-EN_E-XL-6.xml

+xades:SigningTime

+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2 (CRLs), xades:CompleteRevocationRefs, xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (CRLs).

- X-EN_E-XL-7.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2 (OCSP), xades:CompleteRevocationRefs, xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (OCSP).

- X-EN_E-XL-8.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+CertificateValues
+RevocationValues

Description:

Test case for testing XAdES-XL signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2 (OCSP), xades:CompleteRevocationRefs, xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA1), xades:CertificateValues, xades:RevocationValues (OCSP).

6.2.8 Test cases for XAdES-A and XAdES-E-A levels

The test cases in this section deal with XAdES-A signatures specified in ETSI TS 101 903 v1.4.2 and XAdES-E-A as specified in ETSI pre EN 319 132 Part 2.

- X-A-1.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-2.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-3.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs (OCSP Responses), xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (OCSP Responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-4.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs (OCSP Responses), xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (OCSP Responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-5.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

This test case checks the usage of <xadesv141:ArchiveTimeStamp> and <xadesv141:TimeStampValidationData> elements when CRLs are used as validation data

- X-A-6.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

This test case checks the usage of <xadesv141:ArchiveTimeStamp> and <xadesv141:TimeStampValidationData> elements when OCSP responses are used as validation data

- X-A-7.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-8.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues

+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-9.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+RefsOnlyTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the OCSP responses reporting the status of TSA1's certificate (in real life, it could be different from the OCSP responses present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-A-10.xml

+xades:SigningTime
+SigningCertificate
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefs
+CompleteRevocationRefs
+SigAndRefsTimeStamp

+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CompleteCertificateRefs, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the OCSP responses reporting the status of TSA1's certificate (in real life, it could be different from the OCSP responses present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-11.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-12.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs,

xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (CRLs), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-13.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs (OCSP Responses), xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (OCSP Responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-14.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing a XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs (OCSP Responses), xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xades:CertificateValues, xades:RevocationValues (OCSP Responses), and xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-15.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues

+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

This test case checks the usage of <xadesv141:ArchiveTimeStamp> and <xadesv141:TimeStampValidationData> elements when CRLs are used as validation data

- X-EN_E-A-16.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp

Description:

This test case checks the usage of <xadesv141:ArchiveTimeStamp> and <xadesv141:TimeStampValidationData> elements when OCSP responses are used as validation data

- X-EN_E-A-17.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA3),

xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-18.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the CRL issued by this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the CRL reporting the status of TSA1's certificate (in real life, it could be different from the CRL present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-19.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+RefsOnlyTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues

++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:RefsOnlyTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the OCSP responses reporting the status of TSA1's certificate (in real life, it could be different from the OCSP responses present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

- X-EN_E-A-20.xml

+xades:SigningTime
+SigningCertificateV2
+SignatureTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CompleteCertificateRefsV2
+CompleteRevocationRefs
+SigAndRefsTimeStampV2
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+CertificateValues
+RevocationValues
+xadesv141ArchiveTimeStamp
+xadesv141TimeStampValidationData
++CertificateValues
++RevocationValues
+xadesv141ArchiveTimeStamp

Description:

Test case for testing XAdES-A signature. Signature with: xades:SignatureTimeStamp (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CompleteCertificateRefsV2, xades:CompleteRevocationRefs, xades:SigAndRefsTimeStampV2 (encapsulating one time-stamp token generated by TSA3), xadesv141:TimeStampValidationData (encapsulating the certificate of RootCA2OK and the OCSP responses issued for this CA), xades:CertificateValues, xades:RevocationValues (CRLs), one first xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1), one xadesv141:TimeStampValidationData, including the OCSP responses reporting the status of TSA1's certificate (in real life, it could be different from the OCSP responses present within RevocationValues property), and a second xadesv141:ArchiveTimeStamp (encapsulating one time-stamp token generated by TSA1).

6.3 Test cases for augmentation & arbitration for ETSI TS 103 171 v2.1.1 and ETSI pre EN 319 132 Part 1

The following section contains test cases for augmentation and arbitration for XAdES signatures compliant with XAdES Baseline Profile as specified in ETSI TS 103 171 v2.1.1 and XAdES baseline signatures as specified in ETSI pre EN 319 132 Part 1.

- X-AugArb-1.xml

Description:

This test case tests a XAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_TS_EU_TL.xml (signed according TS 103 171 specifications) and generate a XAdES-B-LTA based on xadesv141ArchiveTimeStamp. Before adding the xadesv141ArchiveTimeStamp, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added.

- X-AugArb-2.xml

Description:

This test case tests a XAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_TS_EU_TL.xml (signed according TS 103 171 specifications) and generate a XAdES-B-LTA based on xadesv141ArchiveTimeStamp. Before adding the xadesv141ArchiveTimeStamp, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added.

- X-EN_AugArb-3.xml

Description:

This test case tests a XAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EN_EU_TL.xml (signed according EN 319 132-1 specifications) and generate a XAdES-B-LTA based on xadesv141ArchiveTimeStamp. Before adding the xadesv141ArchiveTimeStamp, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added.

X-EN_AugArb-4.xml

Description:

This test case tests a XAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EN_EU_TL.xml (signed according EN 319 132-1 specifications) and generate a XAdES-B-LTA based on xadesv141ArchiveTimeStamp. Before adding the xadesv141ArchiveTimeStamp, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added.

6.4 Negative test cases for verification for XAdES

6.4.1 Negative test cases for XAdES-B-B signatures.

- X-B-BN-1.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature that DOES NOT CONTAIN the mandatory xades:SigningTime element.

- X-B-BN-2.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature that DOES NOT CONTAIN the mandatory xades:SigningCertificate element.

- X-B-BN-3.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature that DOES NOT CONTAIN the mandatory xades:DataObjectFormat element qualifying the signed data object.

- X-B-BN-4.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature having a wrong signature (the hash that was signed isn't the hash computed on the content being signed together with the signed properties).

- X-B-BN-5.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature created with an untrusted signing certificate.

- X-B-BN-6.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature created with an expired signing certificate.

- X-B-BN-7.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature created with a revoked/suspended signing certificate.

- X-B-BN-8.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature created with a signing certificate generated by a CA whose certificate is revoked/suspended.

- X-B-BN-9.xml

Description:

This test case tests the verification of a XAdES Baseline level B signature with a SigningCertificate property where digest does not match with the actual digest of the signer certificate.

6.4.2 Negative test cases for XAdES-B-T signatures as specified in ETSI TS 103 171 v2.1.1

- X-B-TN-1.xml

Description:

This is a negative test case for verifying signer certificate at the time in SignatureTimeStamp. At the time in xades:SignatureTimeStamp, the signer certificate had been already expired.

- X-B-TN-2.xml

Description:

This is a negative test case for verifying signer certificate at the time in SignatureTimeStamp. At the time in xades:SignatureTimeStamp, the signer certificate had been already revoked.

- X-B-TN-3.xml

Description:

This is a negative test case for SignatureTimeStamp. The hash value of messageImprint in xades:SignatureTimeStamp does *NOT* match to the hash value of the canonicalized ds:SignatureValue element.

- X-B-TN-4.xml

Description:

This is a negative test case for verifying timestamp signer certificate at the time in SignatureTimeStamp. At the time in xades:SignatureTimeStamp, the timestamp signer certificate had been already revoked.

- X-B-TN-5.xml

Description:

This is a negative test case for verifying timestamp signer certificate at the time in SignatureTimeStamp. At the time in xades:SignatureTimeStamp, the timestamp signer certificate had been already expired.

- X-B-TN-6.xml

Description:

This is a negative test case for verifying timestamp signer certificate. The timestamp signer certificate has been generated by an untrusted CA.

- X-B-TN-7.xml

Description:

This is a negative test case for verifying timestamp signer certificate. The timestamp signer certificate has been generated by a CA whose certificate is revoked/suspended.

6.4.3 Negative test cases for XAdES-B-LT signatures as specified in ETSI TS 103 171 v2.1.1

- X-B-LTN-1.xml

Description:

The signature corresponding to this test case is not conformant against the XAdES Baseline Profile conformance level LT because it DOES CONTAIN the banned xades:CompleteCertificateRefs element.

- X-B-LTN-2.xml

Description:

The signature corresponding to this test case is not conformant against the XAdES Baseline Profile conformance level LT because it DOES CONTAIN the banned xades:CompleteRevocationRefs element.

6.4.4 Negative test cases for XAdES-B-LTA signatures as specified in ETSI TS 103 171 v2.1.1

- X-B-LTAN-1.xml

Description:

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the SignatureTimeStamp is ulterior than the time in xadesv141ArchiveTimeStamp.

- X-B-LTAN-2.xml

Description:

This is a negative test case for verifying xadesv141ArchiveTimeStamp content. In this test case, the hash value of messageImprint in xadesv141ArchiveTimeStamp element does *NOT* match to the hash value of all the time-stamped data objects.

6.4.5 Negative test cases for generation and verification of XAdES signatures compliant with ETSI TS 101 903 v1.4.2

This section defines negative test cases for the specification identified in its header.

8.1 Negative test cases for `XAdES-E-C` signatures as specified in ETSI TS 101 903 v1.4.2.

The following tests have at least one aspect that should cause verification to fail, you will not have to generate them (verification only).

The following table shows the properties of the `XAdES-CN` level and wich test cases test them.

The validation of the signatures pregenerated for these test cases should be negative.

- X-CN-1.xml

Description:

The signature corresponding to this test case include a CompleteCertificateRefs element such that the references do not reference a complete cert paht for signing certificate.

- X-CN-2.xml

Description:

The signature corresponding to this test case include a CompleteRevocationRefs element such that the references do not reference a complete CRLs group for signing certificate chain.

6.4.6 Negative test cases for XAdES-E-X signatures as specified in ETSI TS 101 903 v1.4.2.

The following tests have at least one aspect that should cause verification to fail, you will not have to generate them (verification only).

The following table shows the properties of the `XAdES-XN` level and wich test cases test them.

The validation of the signatures pregenerated for these test cases should be negative.

- X-XN-1.xml

Description:

In the signature corresponding to this test case the time in xades:SignatureTimeStamp is ulterior to the time in xades:RefsOnlyTimeStamp.

- X-XN-2.xml

Description:

In the signature corresponding to this test case the time in xades:SignatureTimeStamp is ulterior to the time in xades:SigAndRefsTimeStamp.

- X-XN-3.xml

Description:

In the signature corresponding to this test case the time-stamp token in xades:RefsOnlyTimeStamp does not time-stamp the canonicalized xades:CompleteCertificateRefs and xades:CompleteRevocationRefs.

- X-XN-4.xml

Description:

In the signature corresponding to this test case the time-stamp token in xades:SigAndRefsTimeStamp does not time-stamp the canonicalized ds:SignatureValue element, xades:SignatureTimeStamp element, xades:CompleteCertificateRefs and xades:CompleteRevocationRefs.

6.4.7 Negative test cases for XAdES-E-XL signatures as specified in ETSI TS 101 903 v1.4.2.

The following tests have at least one aspect that should cause verification to fail, you will not have to generate them (verification only).

The following table shows the properties of the `XAdES-XLN` level and wich test cases test them.

The validation of the signatures pregenerated for these test cases should be negative.

- X-XLN-1.xml

Description:

This is a negative test case with a xades:CompleteRevocationRefs that contains a CRL reference whose IssueTime element is not equal to the thisUpdate field of the CRL identified by the Issuer and the crlNumber.

- X-XLN-2.xml

Description:

This is a negative test case with a xades:CompleteRevocationRefs that contains a CRL reference whose crlNumber element is not equal to the Number field of the CRL identified by the Issuer and the issueTime.

- X-XLN-3.xml

Description:

This is a negative test case with a xades:CompleteRevocationRefs that contains a CRL reference whose digest is not equal to the digest value computed on the CRL identified by the Issuer and the issueTime.

- X-XLN-4.xml

Description:

This is a negative test case with a xades:CompleteRevocationRefs that contains an OCSP resp reference whose ProducedAt element is not equal to the producedAt field of the OCSP responses generated by responderID.

- X-XLN-5.xml

Description:

This is a negative test case with a xades:CompleteRevocationRefs that contains an OCSP resp reference whose digest element is not equal to the digest value computed on the OCSP response identified by the responderID and the ProducedAt elements.

- X-XLN-6.xml

Description:

This is a negative test case with a xades:CompleteRevocationValues that does not contain all the CRLs referenced in xades:CompleteRevocationRefs.

- X-XLN-7.xml

Description:

This is a negative test case with a xades:CompleteRevocationValues does not contain all the OCSP responses referenced in xades:CompleteRevocationRefs.

6.4.8 Negative test cases for `XAdES-E-A` signatures as specified in ETSI TS 101 903 v1.4.2.

The following tests have at least one aspect that should cause verification to fail, you will not have to generate them (verification only).

The following table shows the properties of the `XAdES-AN` level and wich test cases test them.

The validation of the signatures pregenerated for these test cases should be negative.

- X-AN-1.xml

Description:

This is a negative test case in which the time in xades:RefsOnlyTimeStamp is ulterior to the time in xadesv141ArchiveTimeStamp.

- X-AN-2.xml

Description:

This is a negative test case in which the time in xades:SigAndRefsTimeStamp is ulterior to the time in xadesv141ArchiveTimeStamp.

- X-AN-3.xml

Description:

This is a negative test case in which no property xades:CertificateValues is present.

- X-AN-4.xml

Description:

This is a negative test case in which no property xades:RevocationValues is present.

History

Document history		
v0.1	Jan 2016	Initial draft
v1.0	Feb 2016	Final version