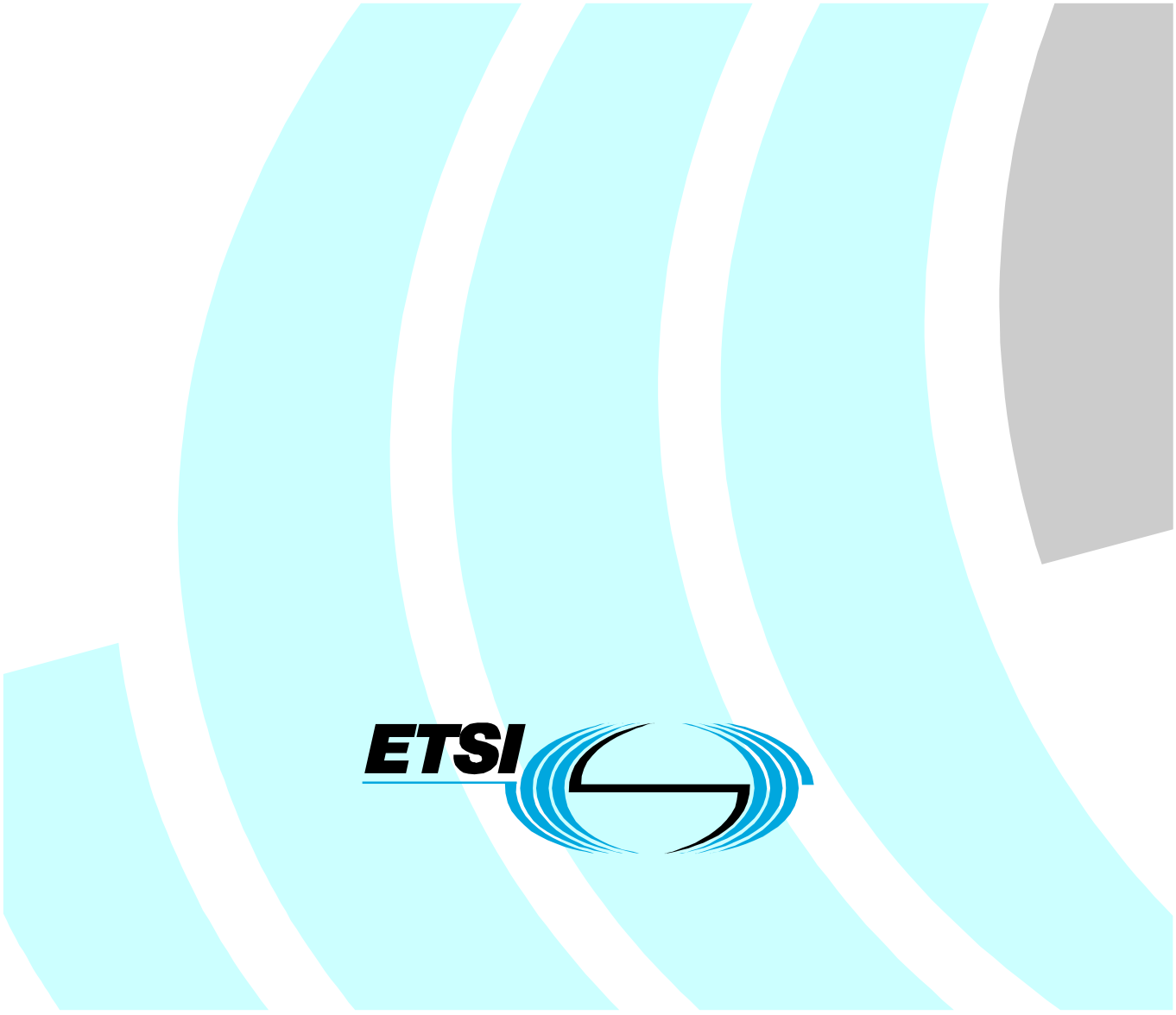
External Report of the 2012 XAdES Remote Plugtests™ Event (March-April 2012)



Reference

<Workitem>

Keywords

< XAdES>

ETSI

650 Route des Lucioles

F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C

Association à but non lucratif enregistrée à la

Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

1 Authors

Laurent Velez, ETSI laurent.velez@etsi.org

Juan Carlos Cruellas, UPC cruellas@ac.upc.edu

Konrad Lanz, A-SIT Konrad.Lanz@iaik.tugraz.at

2 Editors

Laurent Velez, ETSI laurent.velez@etsi.org

4 Contents

Intellectual Property Rights

Abstract

This document is the external report of the 2012 Remote Plugtests Event on XAdES (ETSI TS 101 903) and XAdES Baseline Profile (ETSI TS 103 171), organized by ETSI Centre of Testing and Interoperability (CTI) conducted using the ETSI portal supporting remote interoperability Plugtests.

For Non Disclosure Agreement reason, the report does not list the results of each testcases. It only show the overall and anonymous statistics, without link to the company names.

Status of this Document

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

1 Introduction

The present document aims at reporting the 2012 Remote Plugtests© Event on XAdES Signatures, including new XAdES Baseline Profile.

In anwer to the European Commission Mandate 460 on Electronic Signatures Standardization, ETSI has initiated several Specialist Task Forces projects (STF). The STF428 addressed the needs of Testing activities be performed rapidly leading to a quick and easy improvement of the functionality of the existing e-Signature standardization deliverables, bringing them up to date with current practices. One of the purposes of the STF428 was to develop a conformance testing tool for the XAdES baseline profile developed in order to enable EU Member States implementers to perform conformance testing of the aforementioned profile.

The tool has been integrated into the Electronic Signature Plugtests portal. It gave the opportunity to the Plugtests participants to conduct conformance tests to quickly assess the alignment of the signatures generated by their tools to the XAdES Baseline profile, significantly reducing the time and the cost of putting these tools in the market.

The document 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 descrtiption, including cross-verification, upgrade and arbitration testcases and negative testcases for XAdES signatures
- The Remote Plugtests© Event on XAdES organized by ETSI and held from Wednesday 14th March to Friday 13th April 2012 (The event was initially planned until 28th March but it has been extended to 13rd April due to high 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 kind of services it provides to the participants of the Plugtests© Events.

Section 3 lists the participants to the 2012 XAdES Remote Plugtests© Event.

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

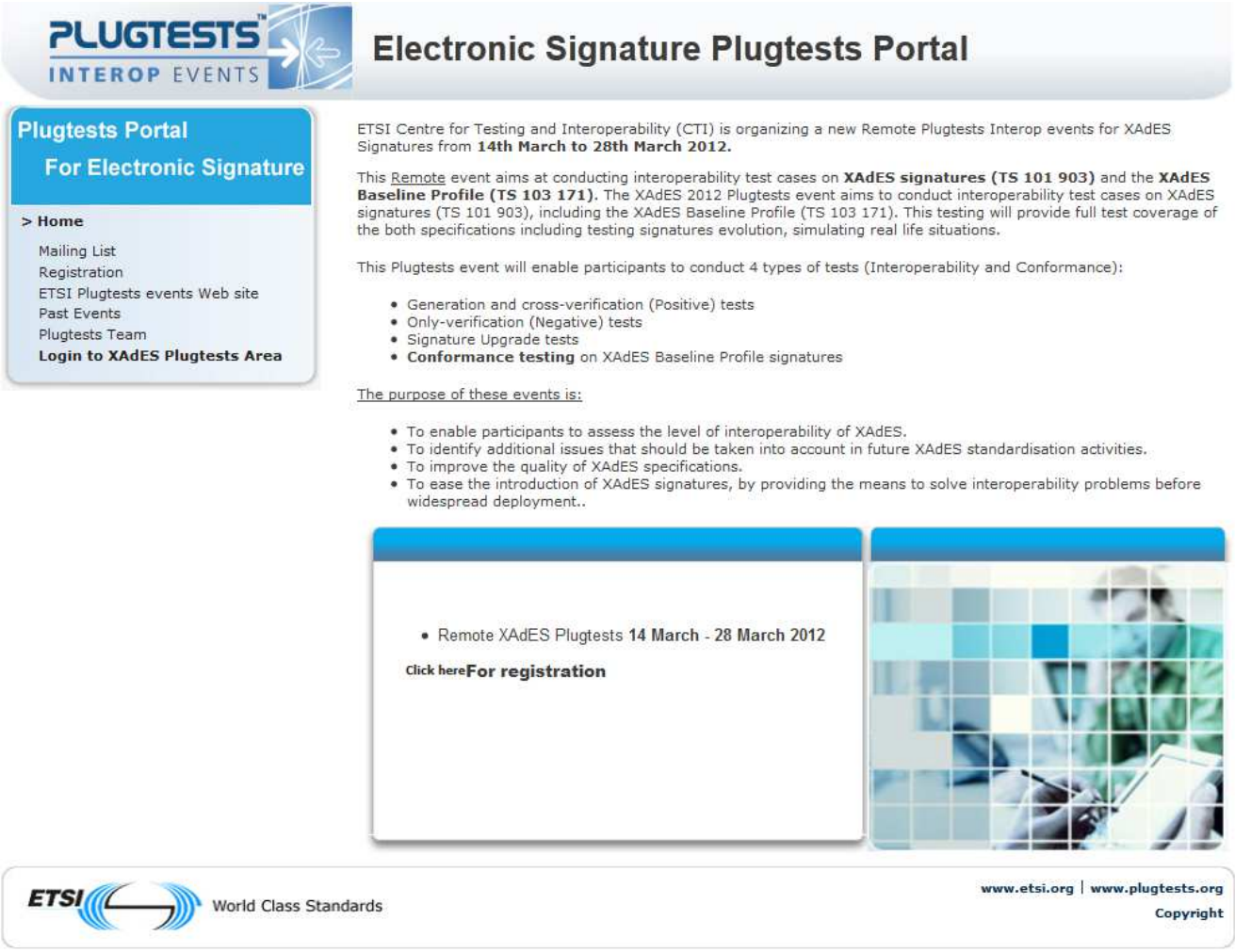
Section 5 provides details on a number of issues related to the XAdES and Baseline profile specifications as identified by the participants. These issues have been raised to the ETSI TC ESI requesting to take them into consideration for future XAdES standardization activities.

Section 6 shows the interoperability matrixes for the test-cases that were defined for the Plugtests event, and for XAdES specifications.

2 Organization and contents of the portal

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

2.1 Public part of the portal



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

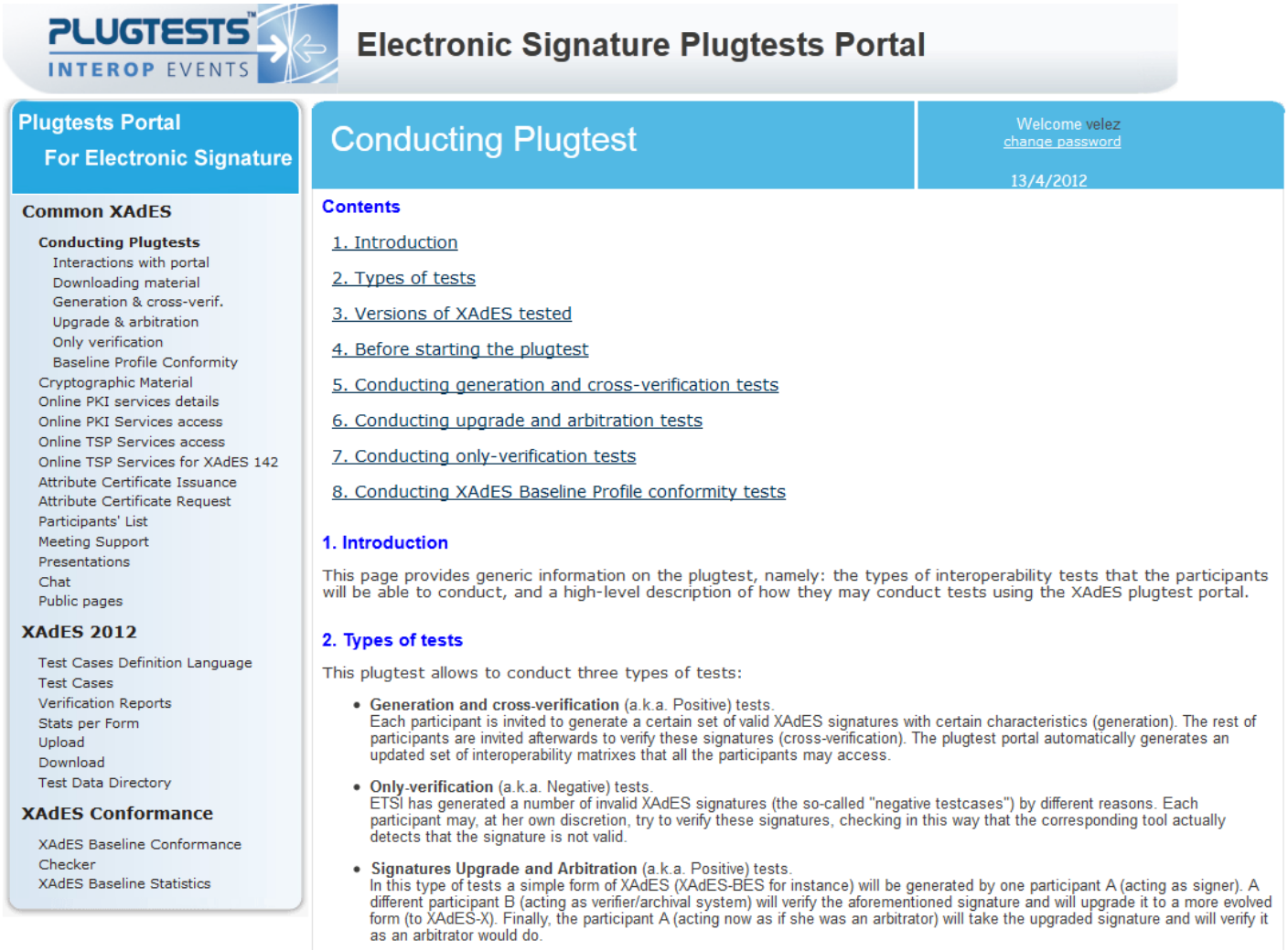
- The XAdES Plugtests page, providing some more details on the event itself, namely targetted specification, targetted audience, some general info on how to conduct such event, etc.
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating 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, CAdES, PAdES)
- The **Login to Plugtests Area** page,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 specific area**. This area contains a number of pages that support the interoperability tests on PAdES.
- **XAdES Baseline Conformance Checker.** This area provides a tool for verifying the conformity of signatures to ETSI TS 103 171

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 six 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") by different reasons. Each participant may, at her own discretion, try to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.

- Signatures Upgrade and Arbitration tests.

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

- XAdES Baseline Profile Conformance Checking.

The portal incorporates a XAdES Baseline Profile conformity-testing tool, which tests conformity of signatures against the requirements defined in ETSI TS 103 171.

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

- XAdES mother specification as per ETSI TS 101 903 v1.3.2.
  - Generation and cross-verification.
  - Only-verification.
  - Signatures Upgrade and Arbitration.
- XAdES mother specification as per ETSI TS 101 903 v1.4.1 and v1.4.2.
  - Generation and cross-verification.
  - Only-verification.
- XAdES Baseline Profile as per ETSI TS 103 171.
  - Generation and cross-verification.
  - Only-verification.
  - Conformity tests.

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

The rest of pages of the set provide details on:

- How to download material from the portal for starting conducting the Plugtests (**Downloading material page**). This material is usually a zip file enclosing a well defined folder structure containing both signatures and verification reports on signatures.
- How to generate 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 (Root_CA_OK). 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 server issued by Root_CA_OK. 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 two trust frameworks for this plugtests, each one having a different Root CA.

Within each trust framework different scenarios are defined. ETSI will define groups of test cases (for instance a group defining different test cases for XAdES-A signatures) for each scenario.

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.

The two frameworks have been defined as detailed below:

- **Trust framework. Root_CA_OK as Root CA.** This framework is used for conducting tests on PAdES signatures usingusing time-stamp tokens issued by only one TSA. For this trust framework, two different scenarios have been defined:

  - **Scenario SCOK.** Participants will use its cryptographic material for both generating and verifying the signatures corresponding to the generation and cross-verification test cases. In this scenario all 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, are valid.

  - **Scenario SC1.** Participants will use its cryptographic material only for verifying signatures pre-generated by ETSI corresponding to the only-verification tests cases. In this scenario, ETSI will include a pre-generated signing certificate, which by the time the plugtest will start will be revoked, and also a pre-generated signing certificate, which by the time the plugtest will start will be expired. The CA issuing both certificates (Level_B_CA_OK) will issue the CRLs including references to the revoked certificate. This CA will also generate OCSP responses reporting on the status of these certificates whenever it is requested by the participants. ETSI will generate one XAdES signature using the revoked certificate and another one using the expired certificate. This scenario is intended to check implementations behaviour when verifying not valid signatures, which will be provided by the ETSI portal

- **Second trust framework. Root_CA_2OK as Root CA**. This framework will be used for conducting the tests on new features introduced by XAdES v1.4.1, namelly and unsigned properties. Only one scenario has been

defined for this framework, consisting in one Root CA (Root_CA_2OK) which issues certificate for a TSA (TSA2), which issues the time-stamp tokens for the signatures generated. This scenario does not provides end user certificates and participants will use signing certificates in the the first trust framework, which results in certificates and validation material coming from different trust frameworks appearing within the same AdES signature.

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

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

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** describe all of them and provides details on how the participants may access them.

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

- **CA-related services**. This service provides issuance of certificates; generation of CRLs; publication of CRLs. Participants should use this service for getting their corresponding certificates for generating XAdES/CAdES 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 had 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 an 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

In the XAdES CertifiedRoles test (X-BES-5), particpants may need X509 V2 attribute certificate ([RFC3281]) for their signing public key certificate. The private key and certificate of the attribute authority which issues your attribute certificate can be found in the CryptographicMaterial.

Thus the particpants can issue their own attribute certificate for themselve by some security toolkits. However the Plugtests service can also issue the attribute certificate if particpants need. 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 emails 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 were 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 Electronic mail list with archival capabilities, whose use was restricted to the participants in the Plugtests©, was set up for supporting exchange of messages among them. This was the main medium for putting questions to the Plugtest support team and initiatetechnical discussion between particpants

After each upload of signatures or verifcations , an email is sent to all particpants via this mailing list to inform them. So the particpants are notified 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 of the portal waiting their resolution by the Plugtests support team.

2.2.2 Contents of XAdES Interop Specific areas of Private part

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

2.2.2.1 Test Cases Definition Language

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

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

2.2.2.3 Individual verification reports

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

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

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

2.2.2.4 Statistics per signature form

The Statistics page contains 3 tables that summarize the number of XAdES signatures generated and verifed at each instant of the Plugtests©.

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

2.2.2.5 Upload pages

The XAdES 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 instant in the Plugtests. It is way to archive all the different uploads and keep a complete history of the Interop testing of the event.

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

2.2.2.6 Download pages

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

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

2.2.2.7 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.

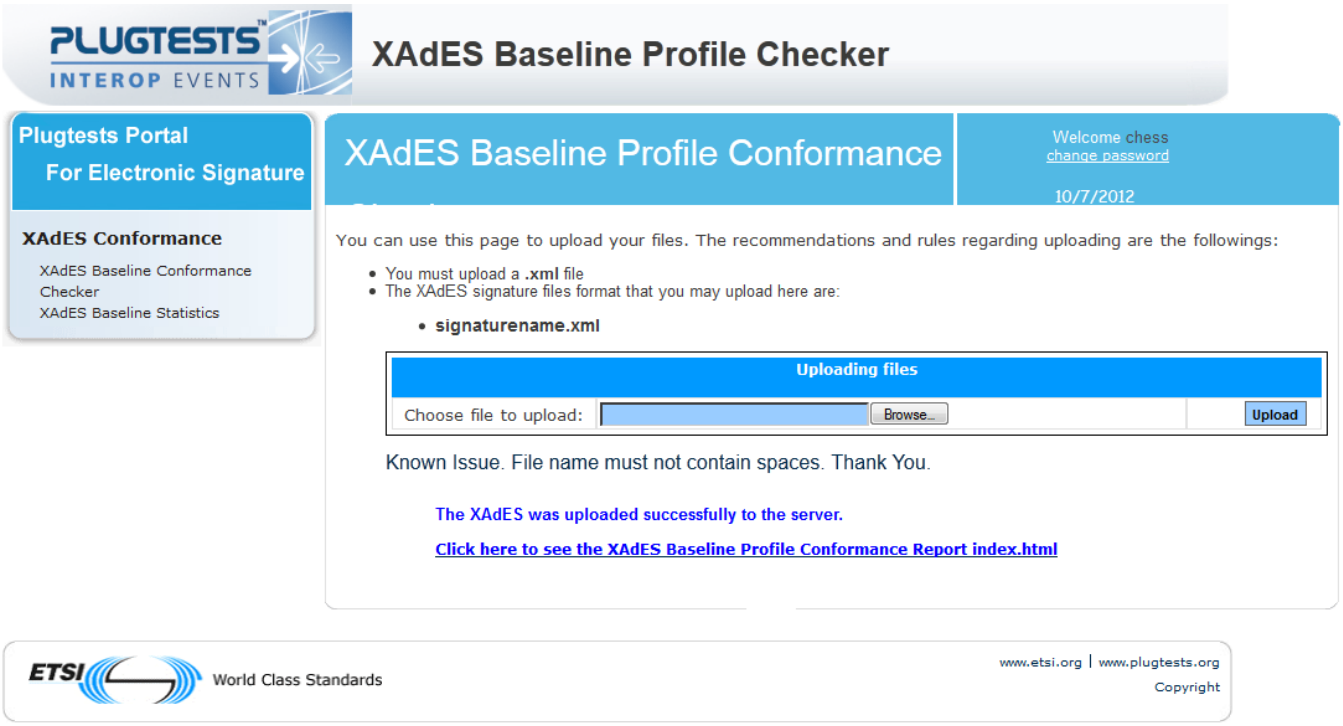
This allows a detailed inspection of the files uploaded in a certain instant to the portal.

2.2.3 XAdES Baseline Profile checker

The portal contains, within the private part of the portal, an online tool for testing conformity of XAdES signatures against the requirements defined in new standard ETSI TS 103 171 (XAdES Baseline Profile). This profile corresponds to the minimum basic requirements in the context of the "Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market".

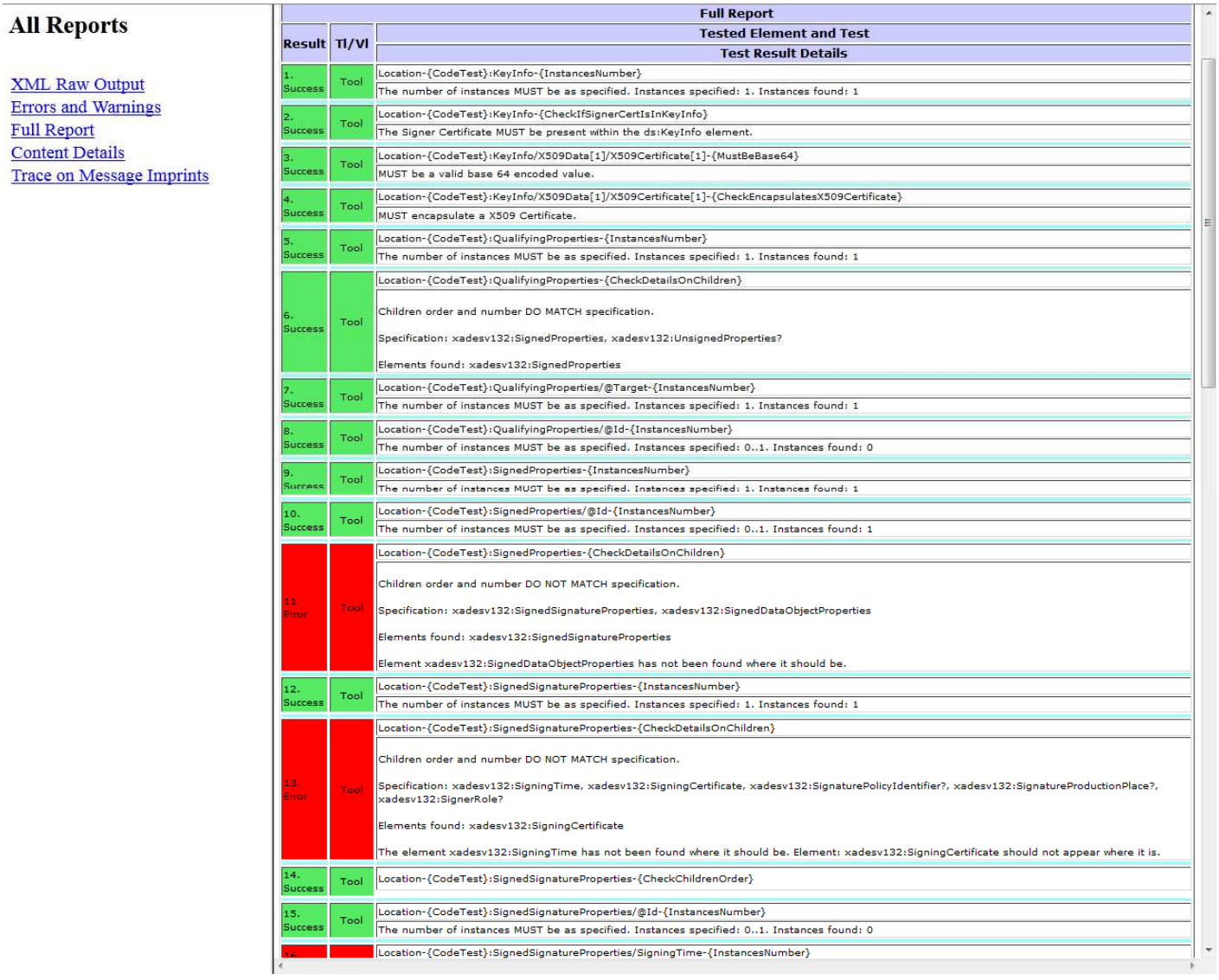
2.2.3.1 Online tool

These section gives access to the tool and describe how to upload XAdES Signatures to to server.



The tool performs numerous checkings against the requirements defined in new standard ETSI TS 103 171 and provides several reports as follows:

- XML Raw Output
- Errors and Warnings
- A full conformance report
- Signature Content Details, providing details of the elements an PKI data present in the signature
- Trace Details, showing the contributions to the Message Imprint computation for time-stamps.



All Reports

XML Raw Output
Errors and Warnings
Full Report
Content Details
Trace on Message Imprints

Full Report

Result	TI/VI	Tested Element and Test / Test Result Details
1. Success	Tool	Location-{CodeTest}:KeyInfo-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 1. Instances found: 1
2. Success	Tool	Location-{CodeTest}:KeyInfo-{CheckIfSignerCertIsInKeyInfo} The Signer Certificate MUST be present within the ds:KeyInfo element.
3. Success	Tool	Location-{CodeTest}:KeyInfo/X509Data[1]/X509Certificate[1]-{MustBeBase64} MUST be a valid base 64 encoded value.
4. Success	Tool	Location-{CodeTest}:KeyInfo/X509Data[1]/X509Certificate[1]-{CheckEncapsulatesX509Certificate} MUST encapsulate a X509 Certificate.
5. Success	Tool	Location-{CodeTest}:QualifyingProperties-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 1. Instances found: 1
6. Success	Tool	Location-{CodeTest}:QualifyingProperties-{CheckDetailsOnChildren} Children order and number DO MATCH specification. Specification: xadesv132:SignedProperties, xadesv132:UnsignedProperties? Elements found: xadesv132:SignedProperties
7. Success	Tool	Location-{CodeTest}:QualifyingProperties/@Target-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 1. Instances found: 1
8. Success	Tool	Location-{CodeTest}:QualifyingProperties/@Id-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 0..1. Instances found: 0
9. Success	Tool	Location-{CodeTest}:SignedProperties-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 1. Instances found: 1
10. Success	Tool	Location-{CodeTest}:SignedProperties/@Id-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 0..1. Instances found: 1
11. Error	Tool	Location-{CodeTest}:SignedProperties-{CheckDetailsOnChildren} Children order and number DO NOT MATCH specification. Specification: xadesv132:SignedSignatureProperties, xadesv132:SignedDataObjectProperties Elements found: xadesv132:SignedSignatureProperties Element xadesv132:SignedDataObjectProperties has not been found where it should be.
12. Success	Tool	Location-{CodeTest}:SignedSignatureProperties-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 1. Instances found: 1
13. Error	Tool	Location-{CodeTest}:SignedSignatureProperties-{CheckDetailsOnChildren} Children order and number DO NOT MATCH specification. Specification: xadesv132:SigningTime, xadesv132:SigningCertificate, xadesv132:SignaturePolicyIdentifier?, xadesv132:SignatureProductionPlace?, xadesv132:SignerRole? Elements found: xadesv132:SigningCertificate The element xadesv132:SigningTime has not been found where it should be. Element: xadesv132:SigningCertificate should not appear where it is.
14. Success	Tool	Location-{CodeTest}:SignedSignatureProperties-{CheckChildrenOrder}
15. Success	Tool	Location-{CodeTest}:SignedSignatureProperties/@Id-{InstancesNumber} The number of instances MUST be as specified. Instances specified: 0..1. Instances found: 0
16.		Location-{CodeTest}:SignedSignatureProperties/SigningTime-{InstancesNumber}

2.2.3.2 Statistics

This page displays a table of numbers of generated reports for XAdES Baseline profile per participating company.

3 Participants list

The table below shows the details of all the organizations and persons that have participated in the 2012 XAdES Remote Plugtests© Event.

There have been **27 different organizations** and 51 people participating in the event.

Company	Acronym	First Name	Surname
Appli.Not / Groupe ADSN	APP	Philippe	Pellegrin
		Yann	Mathieu
Ascertia Ltd	ASC	Liaquat	Khan
		Israr	Ahmed
		Yasir	Khan
		Farooq	Rashed
ATOS	ATOS	François	Leclercq
		Christophe	Brunet
Bit4id	BIT	Marco	Scognamiglio
		Fabrizio	Balsamo
		Davide	Bertelli
		Rodrigo	Lopez
Bremen Online Services	BOS	Hartje	Bruns
		Alexander	Funk
		Thomas	Chojeki
Bull SAS	BULL	Pierre-Jean	Aubourg
		Dominique	Pierson
		Vincent	Kahoul
Cryptolog International	CRY	Moez	Benmbarka
DAC-UPC	UPC	Alberto	Alonso
		Juan Carlos	Cruellas
Dictao SA	DIC	Mehdi	Ben Abdallah
European Commission	EC	David	Naramski
		Anneli	Andresson-Bourgey
ETSI	ETSI	Karen	Hughes
		Laurent	Velez
E-VAL Tecnologia	EVAL	Emerson	Tozette
		Renato	Fonseca
		Adilson	Atalla
		Carolina	Davanzzo
FedICT	FED	Frank	Cornelis
IAIK	IAIK	Birgit	Haas
		Konrad	Lanz
Indenova	IND	Sergio	Serrano

LangEdge	LAN	Naoto	Miyachi
Microsec Ltd	MIC	Balazs	Czekmany
Ministry of Industry, Energy and Tourism	MIET	Rafael	Perez-Galindo
MitSoft	MIT	Antanas	Mitasiunas
		Adomas	Birstunas
		Orestas	Miskivas
Ministry of Public Administration of Slovenia	MJU	Maks	Romih
mTrust sro	MTR	Pavol	Harhovsky
Polysys	POL	Agnes	Juhasz
SafeLayer Secure Communications	SAF	Susanna	Alvarez
SAGE AYTOS	SAGE	Ramiro	Oliva Navas
		Alfonso	Coherán Pérez
Trustweaver	TRU	Martin	Aparicio
		Daniel	Granath
Tubitak Uekae	TUB	Ahmet	Yetgin
		Murat Yasin	Kubilay
Unizeto Technologies SmartSign	UNIS	Robert	Hospodarysko
Unizeto Technologies WebNotarius	UNIW	Robert	Hospodarysko
Viafirma S.L.	VIA	Javier	Echeverria
		Diego	Fajardo
		Felix	Garcia Borrego

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.

27companies registered from Europe, Brazil and Japan. That would have been difficult to organise in a face to face event

4.2 Communication supporting technologies

The utilization of Web conference (GotoWebinar) has been very 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 making a real case demo.

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

4.3 Event duration

Initially, 2 weeks of testing have been planned for this event. Starting from 14th March to 28th March 2012.

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.

Moreover, for this event, 27 companies were registered, testing 28 products. As each company has to verify the signature of the other ones, the time needed increases with the amount of companies. 2 weeks were definitely too short.

For this reasons, the Plugtests team has decided to extend the duration of the event until the 13th April 2012.

5 XAdES related Issues

The present section lists some of the issues raised during the conduction of the XAdES Plugtests ™ Event in 2012.

Additionally to the contents of the present clause, a document “TimeStampRevocationDataInclusion” , generated by Adomas Birstunas, is added in Annex A) to the present report including specific questions on including revocation status data in XAdES signatures.

5.1 XAdES Baseline Profile, Commission Decision and versioning

A comment was raising mentioning that there could be two approaches for dealing with the XAdES Baseline Profile, namely:

1. Those ones following the Commission Decision text and having as only reference ETSI TS 101 903 v.1.4.1.
2. Those ones reading the ETSI TS 103 171, where an explicit reference is made to ETSI TS 101 903 v1.4.2.

It must be commented that when the Commission Decision was approved, the latest official published version of ETSI TS 101 903 was v1.4.1. However that version contained some early and well identified detected errors that version v1.4.2 fixed. In fact, as early as the first XAdES interoperability event conducted after the publication of v1.4.1, a kind of consensus on the resolution of these errors was achieved among participants, and this consensus was afterwards implemented in v1.4.2.

The major conclusion is that implementations should follow ETSI TS 103 171 and by doing this, use ETSI TS 101 903 v1.4.2; in addition to that, a future amended version of the Commission Decission should make a reference to the ETSI TS 103 171.

5.2 Inclusion of trust anchor, when it is a selfsigned certificate, in the set of certificates present in the signature

A comment was raised questioning the inclusion of the trust anchor in the form of a selfsigned certificate in the test cases.

This inclusion has been an issue visited a number of times before the production of the Baseline Profiles. The final decision, implemented in the set of Baseline Profiles after a consultance to the experts group on the services directive, was to require its inclusion.

5.3 Computation of messageImprint for Archive Time-stamps

An important amount of messages were exchanged among participants discussing technical details on how to compute the messageImprint for the different versions of Archive Time-stamps. Reproducing all the technical details in this report would be cumbersome.

What is relevant though, for the purposes of the present report is to report that these discussions had two major outcomes:

1. They led to review the first version of the XAdES Baseline Profile Conformance Tool, available by the participants at the portal, and fix a bug in that implementation.
2. Once this bug was fixed, the doubts on how to compute the aforementioned messageImprint field, were quickly solved because the tool itself generates a trace showing the different components that contribute to compute the input to the digest process whose result is the messageImprint subject of discussion. In fact, after that fixing, the discussions took as reference this kind of traces and implementers had a reference result that clarified most of their doubts.

5.4 Inclusion of revocation data in signatures

Mr. Adomas Birstunas kindly generated and distributed to the rest of participants a document on the topic identified in the headline of the present clause. This document is put in Annex A) as mentioned before. This document will also be handed to the ETSI ESI TC.

5.5 Need to improve wording of ETSI TS 101 903 regarding usage of ds:Canonicalization in certain time-stamp containers properties

A number of comments were raised related to what the ETSI TS 101 903 identifies as ds:Canonicalization element within time-stamp container properties.

1. A comment was raised on clause "8.2.1 Not distributed case" (of xadesv141:ArchiveTimeStamp). More specifically on the following requirement:

   "(…)If ds:Canonicalization is present, the algorithm indicated by this element is used".

   The actual name of the element is ds:CanonicalizationMethod. This is an editorial error that has to be fixed in the new version of the specification.

   The second comment is that according to the person who rose the comment it should be clarified whether the element mentioned was referring to the ds:CanonicalizationMethod child of ds:SignedInfo or the element present in the xadesv141:ArchiveTimeStamp.

2. A second comment related to this topic also identified the need to improve the wording and to fix the error in the name of the element for clause "7.3 The SignatureTimeStamp element".

3. Finally, it was also commented that in the case of the computation of the contribution to the messageImprint by a ds:Reference element within ds:SignedInfo, it would be useful some wording providing additional details on how and when the computation of the canonicalization has to be performed in the chain of steps leading to compute this contribution.

Indeed this should be and shall be clarified in the next version. A new wording is required.

5.6 Issues on XPath transformation followed by a canonicalization process

One of the test cases included in the test suite requested to generate a XAdES-EPES signature using an external fake XML signature policy document. It is the case, that the test case definition required to apply a XPath transformation to that XML file, and then canonicalize the result before computing the digest value to be inserted in the XAdES-EPES signature as digest value of the signature policy document.

Participants found two different results of the process of computing the sequence XPath/canonicalization to that XML file. Some of the participants were using their own tools and other were using open source tools. And even participants purportedly using the same open source tool for computing this sequence (apache XMLSig implementation) obtained different results!.

After a good number of exchanges and deep indagations of the causes it was concluded that different versions of the implementation of apache XMLSig open source tool, produced different results. This was due to a change in the source code.

After additional discussion, the group felt unaible to clearly opt for one result as the good one, and it was decided that a consultation would be raised to the XML Security Working Group in W3C and even a note would be sent to the implementers of apache XMLSig tool. It must be remarked though, that, strictly speaking, this is not a specific XAdES issue, but more a XMLSig or, even better, XPath/Canonicalization issue.

5.7 Usage of the ds:Manifest in XAdES Baseline Profile test cases

Some of the participants asked about the usage of ds:Manifest in the XAdES Baseline Profile.

At present XAdES Baseline Profile allows to use signed ds:Manifest. nevertheless, it must be remarked that ETSI ESI got comments firmly opposing to the usage of ds:Manifest in this way. The rationale for that being, among other things, the fact that XMLSIG itself is agnostic as how to deal with this in the sense that if the check of the ds:Reference fails how the validating application has to react, as this is left to the specific implementations; and this is seen as a problem for interoperability. On the other hand ETSI ESI heard from other countries taht were using ds:Manifest. In the end, the compromise reached was to leave the specification as it was and then, during some time, get comments and requirements on this specific issue, at relevant fora (experts group that generated a commission decission strongly related with what is now XAdES Bp Level-B is one of the most relevant) so that ESI could assess in the near future if the spec could be left as is or an additional restriction in the sense of banning the ds:Manifest would better satisfy requirements by relevant stakeholders.

There is an ad-hoc ESI team that is precisely dealing with this and other issues, and that will provide input to the next ESI meeting in October 2012 for adopting a final decision.

6 XAdES Plugtests© Interoperability matrixes

6.1 Summaries for Positive Test Cases

XAdES-BES

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete		Non Conformant	
					%		%		%		%		%
X-BES-1	21	23	399	347	86,97	48	12,03	0	0,00	4	1,00	0	0,00
X-BES-2	22	23	351	323	92,02	24	6,84	0	0,00	4	1,14	0	0,00
X-BES-3	20	22	363	332	91,46	28	7,71	0	0,00	3	0,83	1	1,09
X-BES-4	15	18	198	181	91,41	13	6,57	0	0,00	4	2,02	0	0,00
X-BES-5	10	18	116	106	91,38	7	6,03	1	0,86	2	1,72	0	0,00
X-BES-6	16	20	251	236	94,02	13	5,18	0	0,00	2	0,80	0	0,00
X-BES-7	14	19	191	181	94,76	8	4,19	0	0,00	2	1,05	0	0,00
X-BES-8	12	18	184	177	96,20	6	3,26	0	0,00	1	0,54	0	0,00
X-BES-9	10	14	119	119	100,00	0	0,00	0	0,00	0	0,00	0	0,00
X-BES-10	9	13	114	114	100,00	0	0,00	0	0,00	0	0,00	0	0,00
X-BES-11	11	15	135	109	80,74	16	11,85	0	0,00	10	7,41	0	0,00
X-BES-15	7	12	66	55	83,33	10	15,15	0	0,00	1	1,52	0	0,00
Total /Average	**167**	**215**	**2487**	**2280**	**91,86**	**173**	**6,57**	**1**	**0,07**	**33**	**1,50**	**1**	**0,09**

XAdES-EPES

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
X-EPES-1	14	13	102	62	60,78	29	28,43	1	0,98	10	9,80
X-EPES-2	4	6	22	12	54,55	10	45,45	0	0,00	0	0,00
Total /Average	**18**	**19**	**124**	**74**	**57,66**	**39**	**36,94**	**1**	**0,49**	**10**	**4,90**

XAdES-T

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
X-T-1	19	20	318	295	92,77	23	7,23	0	0,00	0	0,00
Total /Average	**19**	**20**	**318**	**295**	**92,77**	**23**	**7,23**	**0**	**0,00**	**0**	**0,00**

XAdES-C

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
X-C-1	11	13	134	128	95,52	6	4,48	0	0,00	0	0,00
X-C-2	12	12	131	120	91,60	11	8,40	0	0,00	0	0,00
X-C-3	2	7	14	14	100,00	0	0,00	0	0,00	0	0,00
Total /Average	**25**	**32**	**279**	**262**	**95,71**	**17**	**4,29**	**0**	**0,00**	**0**	**0,00**

XAdES-X

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
X-1	12	12	134	113	84,33	20	14,93	0	0,00	1	0,75
X-2	10	10	95	92	96,84	3	3,16	0	0,00	0	0,00
X-3	12	11	118	95	80,51	17	14,41	0	0,00	6	5,08
X-4	10	10	103	83	80,58	14	13,59	0	0,00	6	5,83
Total /Average	**44**	**43**	**450**	**383**	**85,57**	**54**	**11,52**	**0**	**0,00**	**13**	**2,91**

XAdES-XL

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
X-XL-1	14	13	165	140	84,85	24	14,55	0	0,00	1	0,61
X-XL-2	13	13	146	130	89,04	16	10,96	0	0,00	0	0,00
X-XL-3	14	14	169	141	83,43	22	13,02	0	0,00	6	3,55
X-XL-4	12	13	136	120	88,24	16	11,76	0	0,00	0	0,00
Total /Average	**53**	**53**	**616**	**531**	**86,39**	**78**	**12,57**	**0**	**0,00**	**7**	**1,04**

XAdES-A

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
X-A-1	12	12	132	114	86,36	15	11,36	0	0,00	3	2,27
X-A-2	10	12	108	98	90,74	6	5,56	0	0,00	4	3,70
X-A-3	12	13	131	108	82,44	17	12,98	0	0,00	6	4,58
X-A-4	10	12	108	90	83,33	13	12,04	0	0,00	5	4,63

X-A-5	10	12	106	92	86,79	9	8,49	0	0,00	5	4,72
X-A-6	9	11	95	82	86,32	9	9,47	0	0,00	4	4,21
X-A-7	12	12	121	110	90,91	9	7,44	0	0,00	2	1,65
X-A-8	11	11	107	93	86,92	8	7,48	5	4,67	1	0,93
X-A-9	9	10	79	69	87,34	7	8,86	0	0,00	3	3,80
Total /Average	**95**	**105**	**987**	**856**	**86,80**	**93**	**9,30**	**5**	**0,52**	**33**	**3,39**

XAdES-BES 141

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
141-BES-1	4	8	23	23	100,00	0	0,00	0	0,00	0	0,00
141 BES-2	4	8	28	28	100,00	0	0,00	0	0,00	0	0,00
Total /Average	**8**	**16**	**51**	**51**	**100,00**	**0**	**0,00**	**0**	**0,00**	**0**	**0,00**

XAdES-T 141

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
141-T	8	10	72	66	91,67	6	8,33	0	0,00	0	0,00
Total /Average	**8**	**10**	**72**	**66**	**91,67**	**6**	**8,33**	**0**	**0**	**0**	**0**

XAdES-X 141

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
141-X-2	5	8	34	33	97,06	1	2,94	0	0,00	0	0,00
141 X-3	6	8	42	36	85,71	1	2,38	0	0,00	5	11,90
Total /Average	**11**	**16**	**76**	**69**	**91,39**	**2**	**2,66**	**0**	**0,00**	**5**	**5,95**

XAdES-A 141

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
141 A-2	7	10	59	50	84,75	9	15,25	0	0,00	0	0,00
141 A-3	8	10	67	53	79,10	7	10,45	0	0,00	7	10,45
141 A-5	8	9	57	46	80,70	5	8,77	0	0,00	6	10,53

141 A-7	6	8	44	43	97,73	1	2,27	0	0,00	0	0,00
141 A-9	4	8	31	30	96,77	1	3,23	0	0,00	0	0,00

Total /Average	**33**	**45**	**258**	**222**	**87,81**	**23**	**7,99**	**0**	**0,00**	**13**	**4,19**

XBp-B

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete		Non Conformant	
					%		%		%		%		%
XBp-B-1	9	7	57	55	96,49	1	1,75	0	0,00	1	1,75		0,00
XBp-B-2	7	6	33	25	75,76	7	21,21	0	0,00	1	3,03	1	1,32
XBp-B-3	2	4	8	6	75,00	1	12,50	0	0,00	1	12,50		0,00

Total /Average	**18**	**17**	**98**	**86**	**82,42**	**9**	**11,82**	**0**	**0,00**	**3**	**5,76**	**1**	**0,44**

XBp-T

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
XBp-T-1	9	7	57	55	96,49	1	1,75	0	0,00	1	1,75
XBp-T-2	4	6	21	21	100,00	0	0,00	0	0,00	0	0,00

Total /Average	**13**	**13**	**78**	**76**	**98,25**	**1**	**0,88**	**0**	**0,00**	**1**	**0,88**

XBp-LT

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
XBp-LT-1	7	6	36	36	100,00	0	0,00	0	0,00	0	0,00
XBp-LT-2	6	6	31	30	96,77	1	3,23	0	0,00	0	0,00
XBp-LT-3	1	3	3	3	100,00		0,00		0,00		0,00
XBp-LT-4	1	3	3	3	100,00		0,00		0,00		0,00

Total /Average	**15**	**18**	**73**	**72**	**99,19**	**1**	**0,81**	**0**	**0,00**	**0**	**0,00**

XBp-LTA

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete	
					%		%		%		%
XBp-LTA-1	7	6	35	30	85,71	3	8,57	0	0,00	2	5,71
XBp-LTA-2	5	5	22	17	77,27	3	13,64	0	0,00	2	9,09
XBp-LTA-3	0	0	0	0		0		0		0	
XBp-LTA-4	6	6	28	23	82,14	4	14,29	0	0,00	1	3,57
XBp-LTA-5	4	5	17	12	70,59	4	23,53	0	0,00	1	5,88

XBp-LTA-6	1	3	3	2	66,67	0	0,00	0	0,00	1	33,33
XBp-LTA-7	0	0	0	0		0		0		0	

Total /Average	**23**	**25**	**105**	**84**	**76,48**	**14**	**12,00**	**0**	**0,00**	**7**	**11,52**

6.2 Summaries for Negative Test Cases

XAdES-BES N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
				%		%		%		%
X-BESN-1	1	5		0,00	5	100,00		0,00		0,00
X-BESN-2	1	4		0,00	4	100,00		0,00		0,00
X-BESN-3	1	4		0,00	4	100,00		0,00		0,00
X-BESN-4	1	8		0,00	8	100,00		0,00		0,00

Total /Average X-BES	**4**	**21**	**0**	**0,00**	**21**	**100,00**	**0**	**0,00**	**0**	**0,00**

XAdES-EPES N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
				%		%		%		%
X-EPESN-1	1	2		0,00	1	50,00	1	50,00		0,00

Total /Average EPESN	**1**	**2**	**0**	**0,00**	**1**	**50,00**	**1**	**50,00**	**0**	**0,00**

XAdES-T N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
				%		%		%		%
TN-3	1	4	0	0,00	4	100,00	0	0,00	0	0,00
TN-1 SC1	1	6	0	0,00	6	100,00	0	0,00	0	0,00
TN-2 SC1	1	6	0	0,00	6	100,00	0	0,00	0	0,00

Total /Average X-TN	**3**	**16**	**0**	**0,00**	**16**	**100,00**	**0**	**0,00**	**0**	**0,00**

XAdES-C N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
				%		%		%		%
X-CN-1	1	2		0,00	2	100,00	0	0,00		0,00

Total /Average X-CN	**1**	**2**	**0**	**0,00**	**2**	**100,00**	**0**	**0,00**	**0**	**0,00**

XAdES-X N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
				%		%		%		%
XN-1	1	2		0,00	2	100,00	0	0,00	0	0,00
XN-2	1	3		0,00	3	100,00	0	0,00	0	0,00
XN-3	1	2		0,00	2	100,00	0	0,00	0	0,00
XN-4	1	3		0,00	3	100,00	0	0,00	0	0,00
Total /Average X-T	**4**	**10**	**0**	**0,00**	**10**	**100,00**	**0**	**0,00**	**0**	**0,00**

XAdES-XL N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
				%		%		%		%
XL-1	1	3	1	33,33	2	66,67	0	0,00	0	0,00
XL-2	1	3	1	33,33	2	66,67	0	0,00	0	0,00
XL-3	1	2		0,00	2	100,00	0	0,00	0	0,00
XL-4	1	3	1	33,33	2	66,67	0	0,00		0,00
XL-5	1	3	1	33,33	2	66,67	0	0,00		0,00
XL-6	1	3	1	33,33	2	66,67	0	0,00		0,00
XL-7	1	3		0,00	3	100,00	0	0,00		0,00
XL-8	1	3		0,00	2	66,67	0	0,00	1	33,33
Total /Average XLN	**8**	**23**	**5**	**20,83**	**17**	**75,00**	**0**	**0,00**	**1**	**4,17**

XAdES-A N

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
			Absolute		Absolute		Absolute		Absolute	
AN-1	1	3		0,00	3	100,00	0	0,00		0,00
AN-2	1	3		0,00	3	100,00	0	0,00		0,00
AN-3	1	3		0,00	3	100,00	0	0,00		0,00
AN-4	1	2		0,00	2	100,00	0	0,00		0,00
AN-5	1	2		0,00	2	100,00	0	0,00		0,00
Total /Average X-AN	**5**	**13**	**0**	**0,00**	**13**	**100,00**	**0**	**0,00**	**0**	**0,00**

XBp-BN

Signature Negative Test Cases	Total Generated	Total Verifications	Success		Failure		Not Applicable		Incomplete	
XBp-BN-1	1	1	0	0,00	1	100,00	0	0,00		0,00
XBp-BN-2	1	1	0	0,00	1	100,00	0	0,00		0,00
XBp-BN-3	1	0	0		0		0			
Total /Average XBp-BN	**3**	**2**	**0**	**0,00**	**2**	**100,00**	**0**	**0,00**	**0**	**0,00**

6.3 Positive test cases for generation and verification for XAdES

6.3.1 Test cases for XAdES-BES form.

The following table shows the properties of the XAdES-BES form and wich test cases test them.

XAdES-BES.SCOK										
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD
X-BES-1.xml		*								
X-BES-2.xml	*	*								
X-BES-3.xml	*	*	*							
X-BES-4.xml	*	*	*			CR				
X-BES-5.xml	*	*	*			CfR				
X-BES-6.xml	*	*	*	*						
X-BES-7.xml	*	*	*	*						
X-BES-8.xml	*	*	*		*					
X-BES-9.xml	*	*	*				*			
X-BES-10.xml	*	*	*					*		
X-BES-11.xml	*	*	*						*	
X-BES-15.xml	*	*	*	*	*		*	*		

X-BES-1.xml contains the following Properties:

- SigningCertificate

This test case tests an external SigningCertificate (i.e. the URI Attribute is referring to a certificate file outside the signature and the Certificate in the ds:KeyInfo shall be ignored).

X-BES-2.xml contains the following Properties:

- SigningCertificate
- SigningTime

This test case tests an external SigningCertificate and has the SigningTime property that lies within the validity of the certificate.

X-BES-3.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace

This test case tests an external SigningCertificate, no uri is given for the SigningCertificate any more. The SigningTime should be checked against the validity period of the certificates. A SignatureProductionPlace property is provided.

X-BES-4.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- SignerRole

This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property. Now also the SignerRole with a ClaimedRole is added.

X-BES-5.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- SignerRole

This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property. Now also the SignerRole with a CertifiedRole is added.

X-BES-6.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- DataObjectFormat

This is a test for DataObjectFormat. The DataObjectFormat should point to a ds:Reference whose URI attribute points to a simple text file outside of the document containing the signature. MimeType and Encoding do not have to be checked in this case.

X-BES-7.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace

- DataObjectFormat
- DataObjectFormat

This is a test for DataObjectFormat, the reference should point to a ds:Object that contains the MimeType and Encoding in a non contradicting way. To use #Reference-Id-6-4 is just a suggestion.

X-BES-8.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- CommitmentTypeIndication

X-BES-9.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- IndividualDataObjectsTimeStamp

This is to test the IndividualDataObjectsTimeStamp.

X-BES-10.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- AllDataObjectsTimeStamp

This is to test the AllDataObjectsTimeStamp.

X-BES-11.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- CounterSignature

This is to test the CounterSignature, for simplicity it is signed by the same party.

X-BES-15.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- DataObjectFormat
- CommitmentTypeIndication
- AllDataObjectsTimeStamp
- IndividualDataObjectsTimeStamp

This is to test all BES Properties, except CounterSignature.

6.3.2 Test cases for the XAdES-EPES form.

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

XAdES-EPES.SCOK											
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI
X-EPES-1.xml	*	*									*
X-EPES-2.xml	*	*	*	*	*	CRCfR					*

X-EPES-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignaturePolicyIdentifier

X-EPES-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignaturePolicyIdentifier
- SignatureProductionPlace
- SignerRole
- DataObjectFormat
- DataObjectFormat
- DataObjectFormat
- DataObjectFormat
- CommitmentTypeIndication
- CommitmentTypeIndication
- CommitmentTypeIndication
- CommitmentTypeIndication

6.3.3 Test cases for XAdES-T form.

The test cases in this section deal with the `XAdES-T` form.

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

XAdES-T.SCOK												
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS
X-T-1.xml	*	*										*

X-T-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp

This test case adds a SignatureTimeStamp.

6.3.4 Test cases for XAdES-C form.

The test cases in this section deal with the `XAdES-C` form.

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

XAdES-C.SCOK																
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR
X-C-1.xml	*	*										*	*	C		
X-C-2.xml	*	*										*	*	O		
X-C-3.xml	*	*				CfR						*	*	O	*	

X-C-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs

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

X-C-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs

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

X-C-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignerRole
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- AttributeCertificateRefs

This test case tests the use of AttributeCertificateRefs.

6.3.5 Test cases for XAdES-X form.

The test cases in this section deal with the XAdES-X form.

The following table shows the properties of the XAdES-X form and wich test cases test them.

XAdES-X.SCOK																		
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS
X-X-1.xml	*	*										*	*	C			*	
X-X-2.xml	*	*										*	*	C				*
X-X-3.xml	*	*										*	*	O			*	
X-X-4.xml	*	*										*	*	O				*

X-X-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp

X-X-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp

X-X-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp

X-X-4.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp

6.3.6 Test cases for XAdES-XL form.

The test cases in this section deal with the XAdES-XL form.

The following table shows the properties of the XAdES-XL form and wich test cases test them.

XAdES-XL.SCOK																						
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS	CV	RV	AACV	ARV
X-XL-1.xml	*	*										*	*	C			*		*	C		
X-XL-2.xml	*	*										*	*	C				*	*	C		
X-XL-3.xml	*	*										*	*	O			*		*	O		
X-XL-4.xml	*	*										*	*	O				*	*	O		

X-XL-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

X-XL-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues

X-XL-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

X-XL-4.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues

6.3.7 Test cases for XAdES-A form.

The test cases in this section deal with the `XAdES-A` form.

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

XAdES-A.SCOK																							
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS	CV	RV	AACV	ARV	ATS
X-A-1.xml	*	*										*	*	C			*		*	C			1
X-A-2.xml	*	*										*	*	C				*	*	C			1
X-A-3.xml	*	*										*	*	O			*		*	O			1
X-A-4.xml	*	*										*	*	O				*	*	O			1
X-A-5.xml	*	*										*	*	O			*		*	O			2
X-A-6.xml	*	*										*	*	O				*	*	O			2
X-A-7.xml	*	*										*							*	C			1
X-A-8.xml	*	*										*							*	C			2
X-A-9.xml	*	*										*							*	O			1

X-A-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

X-A-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

X-A-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

X-A-4.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

X-A-5.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- ArchiveTimeStamp

X-A-6.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs

- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- ArchiveTimeStamp

X-A-7.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

X-A-8.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- ArchiveTimeStamp

X-A-9.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

6.4 Positive test cases for generation and verification for XAdES v1.4.1

The following section contains XAdES v1.4.1 version positive test cases grouped by XAdES Form.

6.4.1 Test cases for XAdES-BES form.

The test cases in this section deal with the XAdES-BES form.

The following table shows the properties of the XAdES-BES form and wich test cases test them.

XAdES-BES.SCOK										
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD
X141-BES-1.xml	*	*	*				*			*
X141-BES-2.xml	*	*	*					*		*

X141-BES-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- IndividualDataObjectsTimeStamp
- xadesv141TimeStampValidationData

This is to test the IndividualDataObjectsTimeStamp and TimeStampValidationData for this timestamp. TimeStampValidationData uses CRL values.

X141-BES-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureProductionPlace
- AllDataObjectsTimeStamp
- xadesv141TimeStampValidationData

This is to test the AllDataObjectsTimeStamp and TimeStampValidationData for this timestamp. TimeStampValidationData uses OCSP responses.

6.4.2 Test cases for XAdES-T form.

The test cases in this section deal with the `XAdES-T` form.

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

XAdES-T.SCOK												
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS
X141-T-1.xml	*	*								*		*

X141-T-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData

This test case adds a SignatureTimeStamp and TimeStampValidationData for this timestamp. TimeStampValidationData uses CRL values.

6.4.3 Test cases for XAdES-X form.

The test cases in this section deal with the `XAdES-X` form.

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

XAdES-X.SCOK																			
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS
X141-X-2.xml	*	*								*		*	*	C				*
X141-X-3.xml	*	*								*		*	*	O			*	

X141-X-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- xadesv141TimeStampValidationData

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

X141-X-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- xadesv141TimeStampValidationData

This test case tests Complete CertificteRefs and CompleteRevocationRefs based on OCSP responses. Also RefsOnlyTimeStamp and TimeStampValidationData for this timestamp. TimeStampValidationData uses CRL values.

6.4.4 Test cases for XAdES-A form.

The test cases in this section deal with the `XAdES-A` form.

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

XAdES-A.SCOK																						
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS	CV	RV	AACV	ARV	ATS
X141-A-2.xml	*	*								*		*	*	C				*	*	CCCC			1
X141-A-3.xml	*	*								*		*	*	O			*		*	OOOO			1
X141-A-5.xml	*	*								*		*	*	O			*		*	OOOOO			2
X141-A-7.xml	*	*								*		*							*	CCC			1

X141-A-9.xml	*	*								*		*						*	OOO			1

X141-A-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CertificateValues
- RevocationValues
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

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

X141-A-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CertificateValues
- RevocationValues
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

This test case tests xadesv141ArchiveTimeStamp with their corresponding TimeStampValidationData on SigAndRefsTimeStamp. TimeStampValidationData use OCSP responses.

X141-A-5.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues

- RevocationValues
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CertificateValues
- RevocationValues
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

This test case tests two xadesv141ArchiveTimeStamp with their corresponding xadesv141TimeStampValidationData. TimeStampValidationData use OCSP responses.

X141-A-7.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CertificateValues
- RevocationValues
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

This test case tests xadesv141ArchiveTimeStamp with their corresponding TimeStampValidationData without references. TimeStampValidationData use CRL values.

X141-A-9.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues
- CertificateValues
- RevocationValues
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

This test case tests xadesv141ArchiveTimeStamp with their corresponding TimeStampValidationData in a signature without any reference. TimeStampValidationData use OCSP responses.

6.5 Positive test cases for generation and cross-verification of XAdES Baseline Profile

The present section provides details of the generation and cross-verification XAdES Baseline Profile positive test cases.

The test cases are defined accordingly to the four conformance levels defined in [XAdESBp], namely: B-Level, T-Level, LT-Level and LTA-Level.

6.5.1 Test cases for XAdES Baseline Profile Conformance Level B

The present section provides details of the positive test cases for testing the simplest forms of XAdES Baseline Profile: those that are conformant to B-Level. XAdES signatures conformant to this level are XAdES-BES and XAdES-EPES suitably profiled.

The following table shows the properties within the XAdES signatures and wich test cases test them.

XAdES-BpB.SCOK									
Property → TestCase ↓	ST	SC	DOF	SPP	SR	ADOTS	IDOTS	CS	SPI
XBp-B-1.xml	*	*	*						
XBp-B-2.xml	*	*	*						
XBp-B-3.xml	*	*	*		CfR				

XBp-B-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat

This is the simplest XAdES Baseline Profile conformance level B test case. The signature ONLY CONTAINS the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertifiateThe 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.

XBp-B-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- DataObjectFormat

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

XBp-B-3.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignerRole

Signature for testing XAdES Baseline Profile conformance level B with ONE signed data object apart from the signed XAdES properties, the corresponding xades:DataObjectFormat, and one attribute certificate.

6.5.2 Test cases for XAdES Baseline Profile Conformance Level T

The present section provides details of the positive test cases for testing the simplest forms of XAdES Baseline Profile: those that are conformant to T-Level. XAdES signatures conformant to this level are XAdES-T signatures built on XAdES signatures conformant to B-Level.

The following table shows the properties within the XAdES signatures and wich test cases test them.

XAdES-BpT.SCOK										
Property → TestCase ↓	ST	SC	DOF	SPP	SR	ADOTS	IDOTS	CS	SPI	STS
XBp-T-1.xml	*	*	*							*
XBp-T-2.xml	*	*	*							*

XBp-T-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp

A signature for testing the simpletst case of XAdES Baseline Profile conformance level T. ONE signed data object and ONE xades:SignatureTimeStamp container.

XBp-T-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- SignatureTimeStamp

A XAdES Baseline Profile signature for testing conformance level T. ONE signed data object and TWO xades:SignatureTimeStamp containers.

6.5.3 Test cases for XAdES Baseline Profile Conformance Level LT

The present section provides details of the positive test cases for testing the simplest forms of XAdES Baseline Profile: those that are conformant to LT-Level. XAdES signatures conformant to this level build on XAdES signatures conformant to T-Level by adding XAdES properties containing certificate values and/or validation material values.

The following table shows the properties within the XAdES signatures and wich test cases test them.

XAdES-BpLT.SCOK															
Property → TestCase ↓	ST	SC	DOF	SPP	SR	ADOTS	IDOTS	CS	SPI	STS	CV	RV	AACV	ARV	141TSVD
XBp-LT-1.xml	*	*	*							*	*	C			
XBp-LT-2.xml	*	*	*							*	*	O			

XBp-LT-3.xml	*	*	*		CfR					*	*	C	*		
XBp-LT-4.xml	*	*	*		CfR					*	*	OO	*	*	

XBp-LT-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues

A signature for testing the simpletst 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 CRLs.

XBp-LT-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues

A signature for testing the simpletst 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.

XBp-LT-3.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignerRole
- SignatureTimeStamp
- CertificateValues
- AttrAuthoritiesCertValues
- RevocationValues

A signature for testing XAdES Baseline Profile conformance level LT. 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.

XBp-LT-4.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignerRole
- SignatureTimeStamp
- CertificateValues
- AttrAuthoritiesCertValues
- RevocationValues

- AttributeRevocationValues

A signature for testing XAdES Baseline Profile conformance level LT. 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.

6.5.4 Test cases for XAdES Baseline Profile Conformance Level LTA

The present section provides details of the positive test cases for testing the simplest forms of XAdES Baseline Profile: those that are conformant to LTA-Level. XAdES signatures conformant to this level build on XAdES signatures conformant to LT-Level by adding xades:ArchiveTimeStamp or xadesv141:ArchiveTimeStamp (and optionally xadesv141:TimeStampValidationData).

The following table shows the properties within the XAdES signatures and wich test cases test them.

XAdES-BpLTA.SCOK																	
Property → TestCase ↓	ST	SC	DOF	SPP	SR	ADOTS	IDOTS	CS	SPI	STS	CV	RV	AACV	ARV	141TSVD	ATS	141ATS
XBp-LTA-1.xml	*	*	*							*	*	C				1	
XBp-LTA-2.xml	*	*	*							*	*	C				2	
XBp-LTA-3.xml	*	*	*							*	*	CC			*	2	
XBp-LTA-4.xml	*	*	*							*	*	O				1	
XBp-LTA-5.xml	*	*	*							*	*	O				2	
XBp-LTA-6.xml	*	*	*							*	*	OO			*	2	
XBp-LTA-7.xml	*	*	*							*	*	OC			*	2	

XBp-LTA-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

A signature for testing XAdES Baseline Profile conformance level LTA. Iin this case there is one signed data object, one xades:SignatureTimeStamp container, one xades:CertificateValues, one xades:RevocationValues, and one xades:ArchiveTimeStamp container. No attribute certificates are present. No xadesv141:ArchiveTimeStamp and no xadesv141:TimeStampValidationData elements. The revocation material used are CRLs.

XBp-LTA-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp

- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- ArchiveTimeStamp

A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again with a xades:ArchiveTimeStamp. The validation material corresponding to the first xades:ArchiveTimeStamp is included within time-stamp token itself. The revocation material used are CRLs.

XBp-LTA-3.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are CRLs.

XBp-LTA-4.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

A signature for testing XAdES Baseline Profile conformance level LTA. Iin this case there is one signed data object, one xades:SignatureTimeStamp container, one xades:CertificateValues, one xades:RevocationValues, and one xades:ArchiveTimeStamp container. No attribute certificates are present. No xadesv141:ArchiveTimeStamp and no xadesv141:TimeStampValidationData elements. The revocation material used are OCSP responses.

XBp-LTA-5.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- ArchiveTimeStamp

A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again with a

xades:ArchiveTimeStamp. The validation material corresponding to the first xades:ArchiveTimeStamp is included within time-stamp token itself. The revocation material used are OCSP responses.

XBp-LTA-6.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are OCSP responses.

XBp-LTA-7.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp
- xadesv141TimeStampValidationData
- CertificateValues
- RevocationValues

A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are both CRLs and OCSP responses depending on the certificates.

6.6 Negative Test Cases (verification only)

The following section contains negative test cases grouped by XAdES Form.

6.6.1 XAdES-BES form, negative test cases.

The test cases in this section deal with the XAdES-BES form. 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-BES form and wich test cases test them.

XAdES-BESN.SCOK

Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD
X-BESN-1.xml	*			*						
X-BESN-2.xml	*	*		*						
X-BESN-3.xml	*	*		*						
X-BESN-4.xml	*	*								

X-BESN-1.xml contains the following Properties:

- SigningTime
- DataObjectFormat

One xades:DataObjectFormat does not reference any ds:Reference in the signature

X-BESN-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- DataObjectFormat

A signature with a ds:Reference element referenced by a xades:DataObjectFormat refers to a ds:Object whose MimeType is not equal to the one in xades:DataObjectFormat

X-BESN-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- DataObjectFormat

A signature with a ds:Reference element referenced by a xades:DataObjectFormat refers to a ds:Object whose Encoding attribute is not equal to the one in xades:DataObjectFormat

And results in the following Interop Matrix:

X-BESN-4.xml contains the following Properties:

- SigningCertificate
- SigningTime

A XAdES signature with a SigningCertificate property where digest does not match with the actual digest of the certificate.

6.6.2 XAdES-EPES form, negative test cases.

The following table shows the properties of the XAdES-EPES form and wich test cases test them.

XAdES-EPESN.SCOK											
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI
X-EPESN-1.xml	*	*									*

X-EPESN-1.xml contains the following Properties:

- SigningTime
- SignaturePolicyIdentifier
- SigningCertificate

The digest within xades:SignaturePolicyIdentifier property does not correspond with the digest computed on the document referenced by xades:SPURI

6.6.3 XAdES-T form, negative test cases.

The test cases in this section deal with the `XAdES-T` form.

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

XAdES-TN.SCOK												
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS
X-TN-3.xml	*	*										*

X-TN-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp

The time-stamp token within xades:SignatureTimeStamp is computed to not time-stamp the canonicalized ds:SignatureValue element but other object.

XAdES-TN.SC1												
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS
X-TN-1.xml	*											*
X-TN-2.xml	*											*

X-TN-1.xml contains the following Properties:

- SigningTime
- SignatureTimeStamp

The time in xades:SignatureTimeStamp is ulterior to the expiration time of the signing certificate

X-TN-2.xml contains the following Properties:

- SigningTime
- SignatureTimeStamp

The time in xades:SignatureTimeStamp is ulterior to the revocation time of the signing certificate

6.6.4 XAdES-C form, negative test cases.

The test cases in this section deal with the `XAdES-C` form.

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

XAdES-CN.SCOK																
Property → TestCase ↓	**ST**	**SC**	**SPP**	**DOF**	**CTI**	**SR**	**IDOTS**	**ADOTS**	**CS**	**141TSVD**	**SPI**	**STS**	**CCR**	**CRR**	**ACR**	**ARR**
X-CN-1.xml	*	*										*	*			

X-CN-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs

XAdES signatures with CompleteCertificateRefs such that the references do not reference a complete cert paht for signing certificate.

6.6.5 XAdES-X form, negative test cases.

The test cases in this section deal with the `XAdES-X` form.

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

XAdES-XN.SCOK																		
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS
X-XN-1.xml	*	*										*	*					*
X-XN-2.xml	*	*										*	*				*	
X-XN-3.xml	*	*										*	*					*
X-XN-4.xml	*	*										*	*				*	

X-XN-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs

- RefsOnlyTimeStamp

Time in xades:SignatureTimeStamp is ulterior to the time in xades:RefsOnlyTimeStamp

X-XN-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp

Time in xades:SignatureTimeStamp is ulterior to the time in xades:SigAndRefsTimeStamp

X-XN-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp

The time-stamp token in xades:RefsOnlyTimeStamp does not time-stamp the canonicalized xades:CompleteCertificateRefs and xades:CompleteRevocationRefs.

X-XN-4.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp

Time within xades:SignatureTimeStamp is ulterior to time within xades:SigAndRefsTimeStamp

6.6.6 XAdES-XL form, negative test cases.

The test cases in this section deal with the `XAdES-XL` form.

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

XAdES-XLN.SCOK																							
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS	CV	RV	AACV	ARV
X-XLN-1.xml	*	*										*	*					*	*			
X-XLN-2.xml	*	*										*	*					*	*			
X-XLN-3.xml	*	*										*	*					*	*			

X-XLN-4.xml	*	*										*	*				*		*			
X-XLN-5.xml	*	*										*	*				*		*			
X-XLN-6.xml	*	*										*	*				*		*			
X-XLN-7.xml	*	*										*	*				*		*			
X-XLN-8.xml	*	*										*	*				*		*			

X-XLN-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues

A signature with a xades:CompleteRevocationRefs that contains a CRL reference whose IssueTime element is not equal to the thisUpdate field of f the CRL identified by the Issuer and the crlNumber

X-XLN-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues

A signature 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 contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues

A signature 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 contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

A signature with a xades:CompleteRevocationRefs that contains an OCSP resp reference whose responderID element contains a name that is not equal to the responderID field of any of the OCSP responses in CertificateValues property

X-XLN-5.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

xades:CompleteRevocationRefs contains an oCSP resp reference whose ProducedAt element is not equal to the producedAt field of the OCSP responses generated by responderID

X-XLN-6.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

xades:CompleteRevocationRefs contains an oCSP resp reference whose digest element is not equal to the digest value computed on the OCSP responseidentified by the responderID and the ProducedAt elements

X-XLN-7.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

xades:CompleteRevocationValues does not contain all the CRLs referenced in xades:CompleteRevocationRefs

X-XLN-8.xml contains the following Properties:

- SigningTime

- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues

xades:CompleteRevocationValues does not contain all the OCSP responses referenced in xades:CompleteRevocationRefs

6.6.7 XAdES-A form, negative test cases.

The test cases in this section deal with the `XAdES-A` form.

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

XAdES-AN.SCOK																							
Property → TestCase ↓	ST	SC	SPP	DOF	CTI	SR	IDOTS	ADOTS	CS	141TSVD	SPI	STS	CCR	CRR	ACR	ARR	SARTS	ROTS	CV	RV	AACV	ARV	ATS
X-AN-1.xml	*	*										*	*				*		*				1
X-AN-2.xml	*	*										*	*					*	*				1
X-AN-3.xml	*	*										*	*				*		*				1
X-AN-4.xml		*										*											1
X-AN-5.xml		*										*							*				1

X-AN-1.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

Time in xades:SignatureTimeStamp is ulterior to the time in xades:ArchiveTimeStamp

X-AN-2.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs

- RefsOnlyTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

Time in xades:RefsOnlyTimeStamp is ulterior to the time in xades:ArchiveTimeStamp

X-AN-3.xml contains the following Properties:

- SigningTime
- SigningCertificate
- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

Time within xades:SigAndRefsTimeStamp is ulterior to time within xades:ArchiveTimeStamp.

X-AN-4.xml contains the following Properties:

- SigningCertificate
- SignatureTimeStamp
- RevocationValues
- ArchiveTimeStamp

No property xades:CertificateValues is present.

X-AN-5.xml contains the following Properties:

- SigningCertificate
- SignatureTimeStamp
- CertificateValues
- ArchiveTimeStamp

No property xades:RevocationValues is present.

6.7 Negative Test Cases (verification only) for XAdES Baseline Profile

The following sub-clauses specify negative test cases for XAdES Baseline Profile.

Participants will find at the portal a number of XAdES signatures that are non-compliant with the specifications of XAdES Baseline Profile for the indicated conformance levels.

6.7.1 XAdES Baseline Profile Conformance Level B negative test cases

The test cases in this section deal with the details of sigantures that are non conformant against XAdES Baseline Profile level B.

The following table shows the properties of the XAdES signatures and wich test cases test them.

XAdES-BpBN.SCOK									
Property → TestCase ↓	ST	SC	DOF	SPP	SR	ADOTS	IDOTS	CS	SPI
XBp-BN-1.xml		*	*						
XBp-BN-2.xml	*		*						
XBp-BN-3.xml	*	*							

XBp-BN-1.xml contains the following Properties:

- SigningCertificate
- DataObjectFormat

The signature corresponding to this test case is not conformat against the XAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory xades:SigningTime element.

XBp-BN-2.xml contains the following Properties:

- SigningTime
- DataObjectFormat

The signature corresponding to this test case is not conformat against the XAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory xades:SigninCertificate element.

XBp-BN-3.xml contains the following Properties:

- SigningCertificate
- SigningTime

The signature corresponding to this test case is not conformat against the XAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory xades:DataObjectFormat element qualifying the signed data object.

6.7.2 XAdES Baseline Profile Conformance Level LT negative test cases

The test cases in this section deal with the details of sigantures that are non conformant against XAdES Baseline Profile level LT.

The following table shows the properties of the XAdES signatures and wich test cases test them.

XAdES-BpLTN.SCOK															
Property → TestCase ↓	ST	SC	DOF	SPP	SR	ADOTS	IDOTS	CS	SPI	STS	CV	RV	AACV	ARV	141TSVD
XBp-LTN-1.xml	*	*	*							*	*	C			
XBp-LTN-2.xml	*	*	*							*	*	C			

XBp-LTN-1.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat

- SignatureTimeStamp
- CertificateValues
- RevocationValues

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

XBp-LTN-2.xml contains the following Properties:

- SigningCertificate
- SigningTime
- DataObjectFormat
- SignatureTimeStamp
- CertificateValues
- RevocationValues

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

6.8 Positive test cases for upgrade and arbitration

The present section provides details of the upgrade and arbitration XAdES positive test cases.

These test cases are built on tuples of already defined test cases, namely [upgradedForm, basicForm] and these tuples serve for fully specifying them.

The following subsections provide the full list of upgrade and arbitration test cases organized by the upgraded form.

In these sections, each test case is defined in a file whose name follows the pattern [UpgradedForm]~[BasicForm], where [BasicForm] identifies the code of the test case definition file that contains the details of the initial signature to be upgraded; [UpgradedForm identifies the test case definition file that contains the details of the upgraded signature itself. Both test case definition files are files already used in the generation and verification test suite.

6.8.1 Test cases for upgrading to XAdES-C form.

Among all the upgrade and arbitration testcases proposed, the following types of testcases have been performed by the participants :

- Upgrade to XAdES-C-1 from XAdES-T-1 signature : **X-C-1~X-T-1.xml**

6.8.2 Test cases for upgrading to XAdES-X form.

Among all the upgrade and arbitration testcases proposed, the following types of testcases have been performed by the participants :

- Upgrade to XAdES-X-1 from XAdES-T-1 signature : **X-X-1~X-T-1.xml**
- Upgrade to XAdES-X-1 from XAdES-C-1 signature : **X-X-1~X-C-1.xml**

6.8.3 Test cases for upgrading to XAdES-XL form.

Among all the upgrade and arbitration testcases proposed, no testcase for this type has been performed by the participants .

6.8.4 Test cases for upgrading to XAdES-A form.

Among all the upgrade and arbitration testcases proposed, the following types of testcases have been performed by the participants :

- Upgrade to XAdES-A-1 from XAdES-T-1 signature : **X-A-1~X-T-1.xml**
- Upgrade to XAdES-A-1 from XAdES-C-1 signature : **X-A-1~X-C-1.xml**
- Upgrade to XAdES-A-7 from XAdES-T-1 signature : **X-A-7~X-T-1.xml**
- Upgrade to XAdES-A-7 from XAdES-C-1 signature : **X-A-7~X-C-1.xml**

Annex A: Time stamp revocation data inclusion into the signature according XAdES 1.4.2

This annex gathers the technical input provided by Adomas Birstunas to the participants during the Plugtests.

Time stamps in the XAdES signature form ordered sequence of time stamps:

1) TS_1 (i.e., SignatureTimeStamp),
2) TS_2 (i.e., SigAndRefsTimeStamp or RefsOnlyTimeStamp),
3) TS_3 (i.e., first xades141:ArchiveTimeStamp or ArchiveTimeStamp),
4) TS_4 (i.e., second xades141:ArchiveTimeStamp or ArchiveTimeStamp),
…
n) TS_N.

A.1) During time stamp validation, revocation data for the time stamp signing certificates (TSA certificate revocation data) must be collected and stored in xades141:TimeStampValidationData element. Revocation data must be collected at the right time, since the old revocation data is unreliable. Verifier 1 who upgrades signature format (and creates a new time stamp) must validate the last (and all previous) time stamp placed in the signature. The last time stamp must be valid at current time. The Verifier 1 cannot rely on the revocation data (for the last time stamp) placed in the signature, since it is the old data, and signature may be fake (for details see example bellow). Therefore, Verifier 1 must collect new revocation data (for the last time stamp) at validation (current) time.

Conclusion 1: There is no sense to create last time stamp together with its revocation data (in xades141:TimeStampValidationData element). Revocation data for the last time stamp (if it is presented) will be ignored by verifier in any case.

Conclusion 2: Verifier must add new revocation data about the TS_N time stamp, when TS_(N+1) timestamp is created.

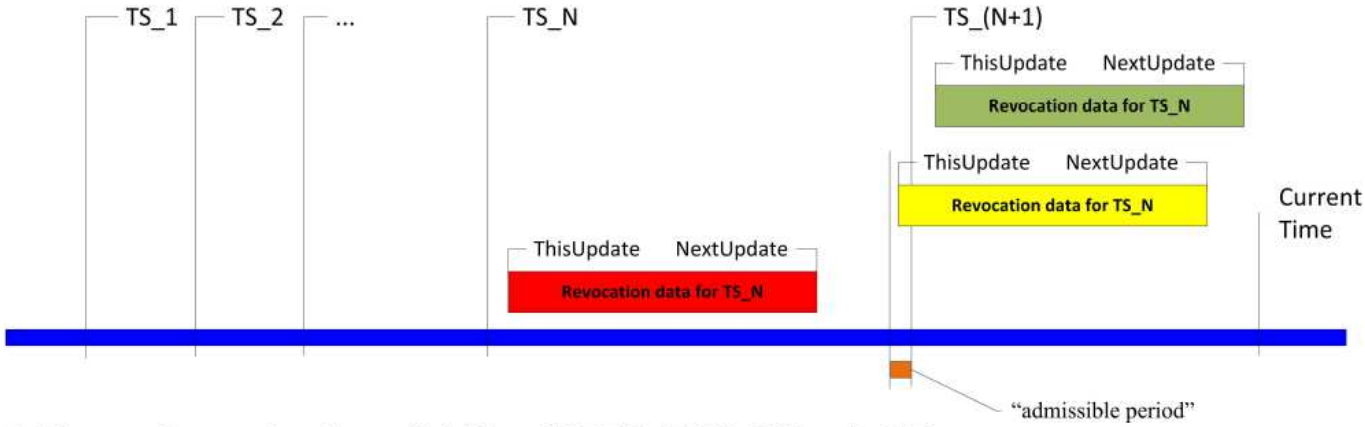
A.2) Suppose that Verifier 1 upgrades signature (containing TS_1, TS_2, …, TS_N) and adds a new timestamp (TS_(N+1)). Verifier 1 collects new revocation data about TS_N and includes it into the signature (in order the next Verifier 2 do not need to collect it for the second time). Verifier 1 wants to ensure the next Verifier 2, that revocation data included in the signature is reliable (collected NOT BEFORE time declared in TS_(N+1)).

Verifier 2 validates TS_N according time declared in TS_(N+1). Verifier 2 founds revocation data (about TS_N) in the signature (included by Verifier 1). There are several possible cases:

a) GREEN case: Revocation data (about TS_N) has ThisUpdate > TS_(N+1), then Verifier 2 knows that this data was collected at the right time and it is 100% reliable.

b) YELLOW case: Revocation data (about TS_N) has ThisUpdate < TS_(N+1), but ThisUpdate > TS_(N+1) – "admissible period" (it may be 1 hour or 1 day), then Verifier 2 knows that this data was created JUST BEFORE creating TS_(N+1). So, data is NOT 100% reliable, but there is a rather big possibility, that data was collected at the same time as TS_(N+1) was created.

c) RED cas: Revocation data (about TS_N) has ThisUpdate < TS_(N+1) – "admissible period" (created in some earlier time, months or even years ago) , then Verifier 2 knows that this data is TOO OLD and it is indeed unreliable.



1. Picture. Revocation data reliability: GREEN, YELLOW and RED cases.

XAdES 1.4.2 does not define at which time revocation data must be collected, or which revocation data must be treated as reliable. It describes XML fields used to store this data.
Nevertheless, requirements listed in XAdES 1.4.2 do not allow to create XAdES-A signature which contains 100% reliable revocation data about time stamps signing certificates.

According XAdES 1.4.2 (section 8.1.1), xades141:TimeStampValidationData element containing revocation data about TS_N, MUST be included as the NEXT element after TS_N element. Therefore, TS_(N+1) must be added after TS_N element and AFTER xades141:TimeStampValidationData element (containing revocation data about TS_N).

xades141:ArchiveTimeStamp covers all elements placed BEFORE it (section 8.2.1). So, TS_(N+1) time stamp also covers xades141:TimeStampValidationData element (containing revocation data about TS_N). Therefore, xades141:TimeStampValidationData element was created BEFORE TS_(N+1) and revocation data placed in it was created and collected BEFORE time declared in

TS_(N+1). And revocation data about the TS_N can not be 100% reliable.

Conclusion 3: Using XAdES 1.4.2 we cannot create signature, which contains time stamp TS_N and 100% reliable revocation data about it. So:

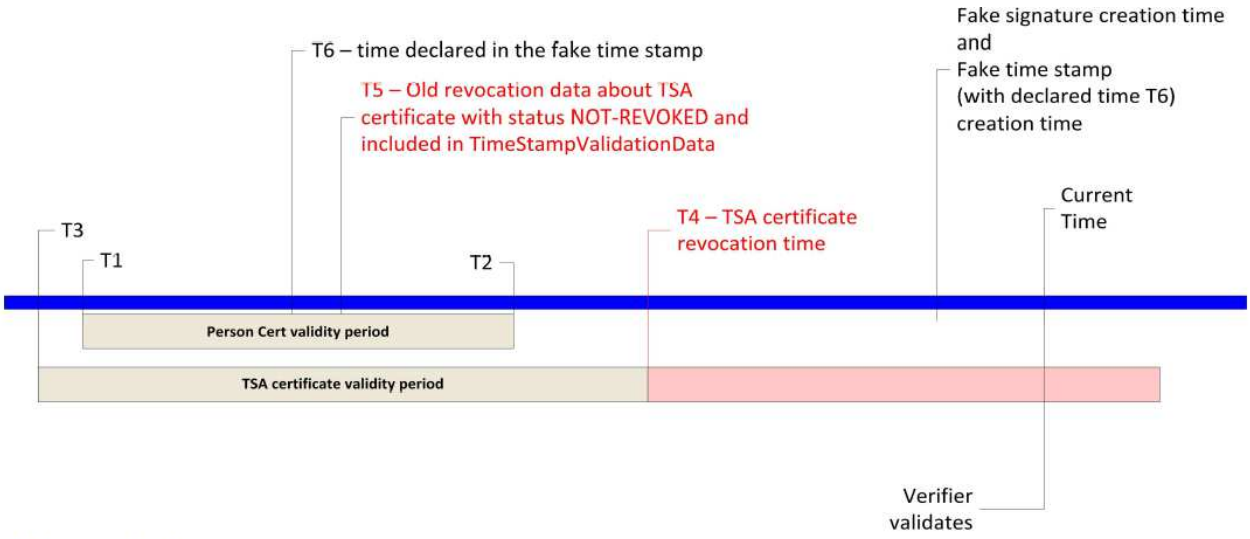
- Green case is impossible.
- Yellow case is possible at the best.
- Red case is possible and, unfortunately, it is the usual case, since revocation data about TS_N is included just after TS_N creation.

Conclusion 4: If Verifier 1 wants to include reliable revocation data about TS_N, it can do this only in such a way:
a) Do not include xades141:TimeStampValidationData after TS_N,
b) Create TS_(N+1),
c) Wait until the newest revocation data (having ThisUpdate > TS_(N+1)) about TS_N is created,
d) Create xades141:TimeStampValidationData element with revocation data about TS_N and include it as validation data for the TS_(N+1),
e) Hope, that the Verifier 2 will take revocation data from the xades141:TimeStampValidationData element associated with TS_(N+1), but apply it to validate TS_N.

In fact, we do not think, that ETSI expected such a scenario. Therefore, we have implemented yellow case. Now we have the other problem – how long must be the "admissible period"?

Fake signature creation example
(case then verifier relies on old revocation data):
Suppose, we have:

- Person's certificate those validity period is from T1 until T2 (T1, T2 < current time).
- TSA certificate which was valid from T3 until it was revoked at T4 (T3 < T1 and T2 < T4 < current time).
- Old revocation data (with NOT REVOKED status) for TSA certificate generated at T5 (and T1 < T5 < T2).
- Private key of the revoked TSA certificate (we have stolen it at time T4, and, therefore, it was revoked at that time).



2. Picture. Fake signature generation.

Fake signature generation:
a) Create signature at current time using expired person certificate.
b) Using TSA private key, create a fake time stamp with declared time T6 (and T1 < T6 < T5 < T2).
c) Add this fake time stamp into the signature, and after add xades141:TimeStampValidationData containing old revocation data (collected at the time T5).

If Verifier ignores revocation data contained inside the signature xades141:TimeStampValidationData) and collects new revocation data at the current time - he will realize, that time stamp is invalid, and, therefore, signature is NOT VALID.

If Verifier validates time-stamp using data contained inside the signature
(xades141:TimeStampValidationData) – he will treat time stamp valid, and signature will be treated as VALID as well.

Conclusion:
The Verifier SHALL NOT RELY on TSA certificate revocation data included
(in xades141:TimeStampValidationData) just after time stamp creation.

Therefore, there is no reason to add such a revocation data together with generated time stamp (it become unreliable after several hours).

In the good case, revocation data about time stamp 1 must be collected (and generated) after time stamp 2 was created.
Unfortunately, XAdES 1.4.2 requires to include it before time stamp 2.
So the only more or less secure way to create signature with xades141:TimeStampValidationData (about time stamp 1) is to collect and include it into the signature just before creating time stamp 2.

History

Document history		
v0.1	13 April 2012	Creation of the document
v0.2	23 May 2012	Editorial changes
v.1.0	26 July 2012	Final version
v.1.1	27 August 2012	Editorial changes