Technical Report of the ASiC Remote Plugtests™ Event (Nov-Dec 2016)

Reference

Keywords
Electronic Signature,

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

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

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute yyyy.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Dec 2016

This version:

Author:

Andrea Caccia, Knowledge Work
Juan Carlos Cruellas, UPC
Konrad Lanz, GrEEV
Luigi Rizzo, InforCert
Laurent Velez, ETSI

Editor:

Laurent Velez, ETSI laurent.velez@etsi.org

Abstract

This document is the technical report of the 2016 Remote Plugtests Event on ASiC (Associate Signature Container ETSI EN 319 162), 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 shows the overall and anonymous statistics, without link to the company names.

Status of this Document

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

.

1 Introduction

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

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

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

The ETSI TS 119 164 parts 2 to 5 "ASiC Testing Conformance & Interoperability" prepared by the STF 459 is the basis of the testing proposed at the ASiC Plugtests 2016 interoperability event.

ETSI has organized the remote Plugtests event on ASiC, held from Monday 7th November to Monday 5th December 2016. This remote event aimed at conducting interoperability test cases on ASiC containers ETSI TS 103 174 but also ETSI EN 319 162-1 &-2.

- 319 162-1 Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers
- 319 162-2 Associated Signature Containers (ASiC); Part 2: Additional ASiC containers

The tests included creation and verification of signature and were executed according to new EN 319 102 (Procedures for Signature Creation and Validation).

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

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

The present document is the report from the 2016 remote Plugtests Event on ASIC Container. It also provides details on the specification, design and implementation of the portal supporting remote Plugtests events on ASiC 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 ASiC Remote Plugtests.

The present report provides details on:

Specification, design and implementation of those testcases description, including cross-verification and negative testcases for ASiC containers, based on ETSI TS 119 164. The Remote Plugtests Event on ASiC was organized by ETSI and held from Monday 7th November to Monday 5th December 2016.

An introduction web conference took place on Monday 7th November to present the portal and the testing.

The event was initially planned to run until 5th December but it was extended to 31st December on request from the participants. The reason being that the amount of testing activities was extremely high within the initial scheduled period, due to the large number of participants.

The present document is organized as indicated below.

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

Section 3 lists the participants to the 2016 ASiC Remote Plugtests Event.

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

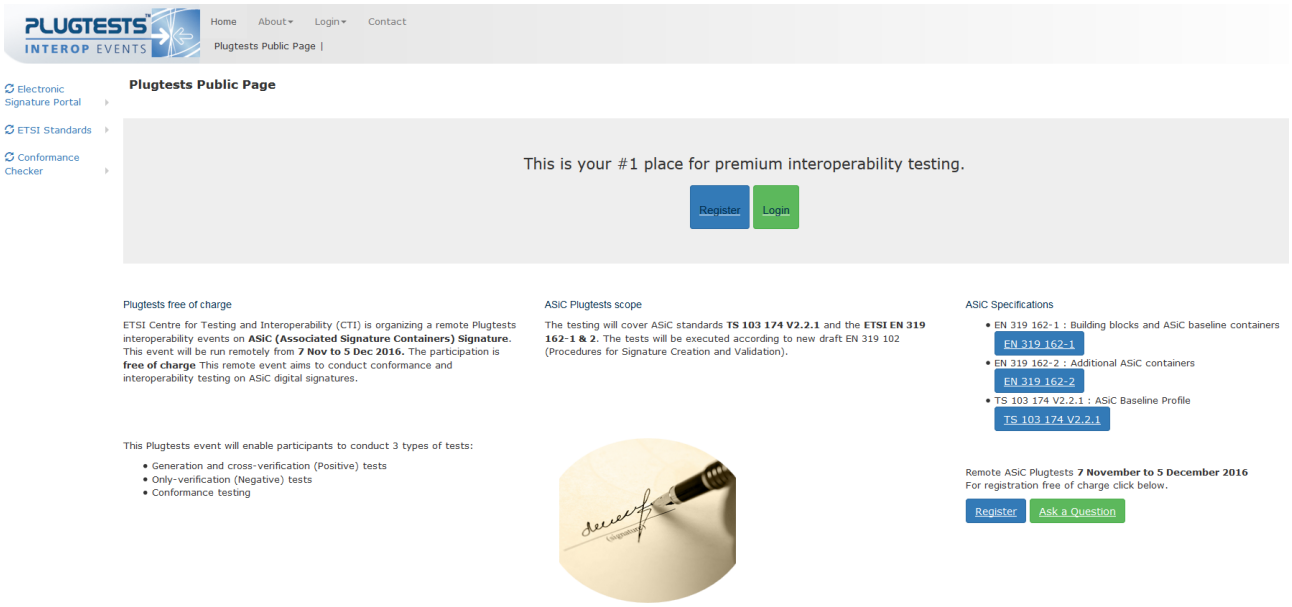
Section 5 provides details of ASiC issues raised at the Plugtest.

Section 6 provides details on the Interoperability testcases provided for the Plugtests event.

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

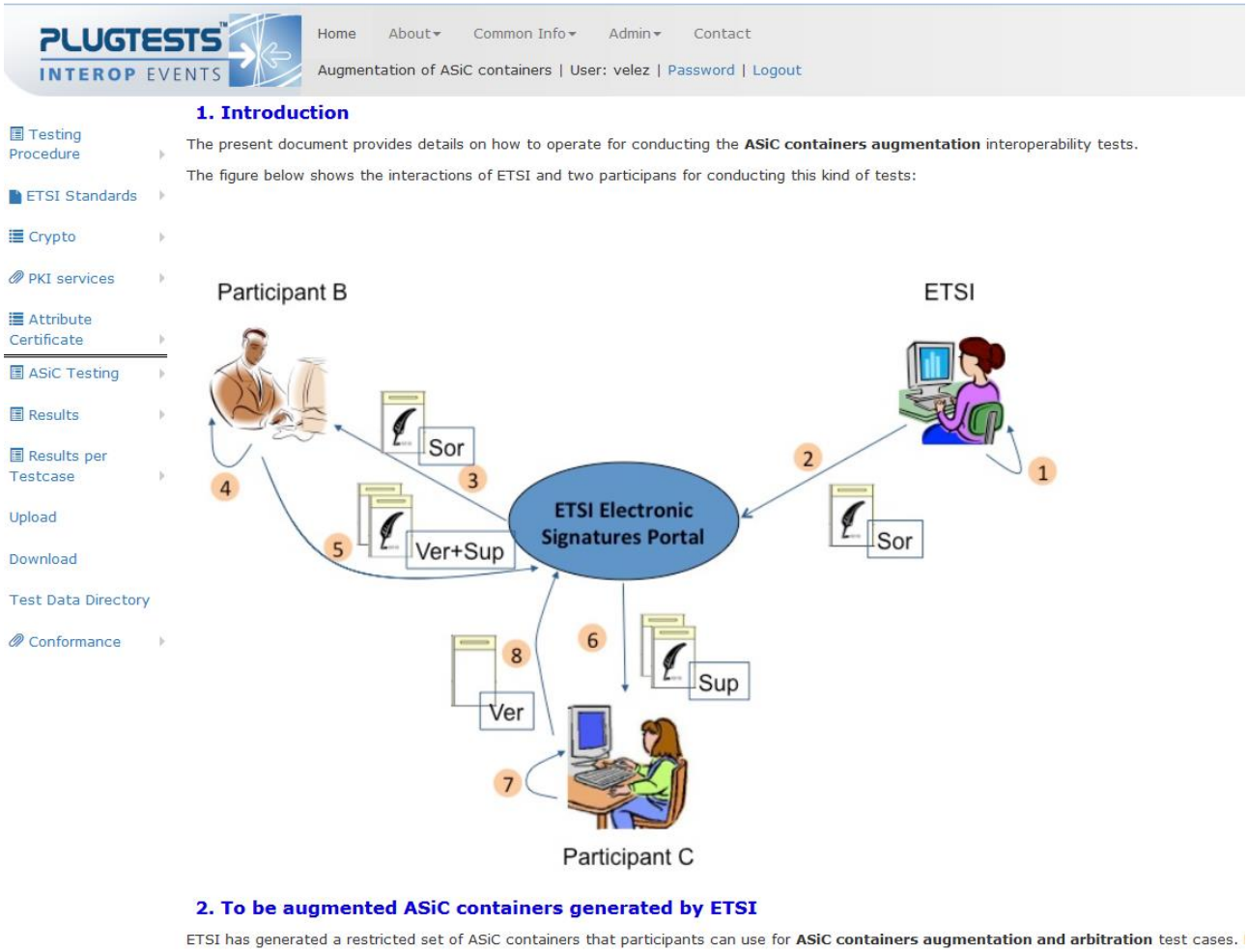
2.2 Private part of the portal

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

- **Common area**. This area contains a number of pages that provide generic information to the participants, which is relevant to participants of ASiC interoperability tests.

- **ASiC specific area**. This area contains a number of pages that support the interoperability tests on ASiC.

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 ASiC during this event.

This Plugtests event allows to conduct 4 types of tests:

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

- **Augmentation tests.**
  ETSI has generated a number of ASiC containers. For these test cases, one participant validates and augments them as specified; a second participant validates the augmented containers.

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

- **Conformance tests.**
  In this type of tests, participants will have to upload ASiC signatures to the portal Conformance checker. This online tool will run a limited set of conformance checks against the ASiC Specification and its associated Baseline Profile.

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

This Plugtests will target at testing ASiC containers as specified in the following documents:

- ETSI TS 103 174 v2.2.1
- ETSI EN 319 162-1 v1.1.1
- ETSI EN 319 162-2 v1.1.1 (partially)

This Plugtests event targets at testing both types of ASiC containers, namely the ASiC Simple Form (ASiC-S) and the ASiC Extended Form (ASiC-E).

It mainly targets at testing ASiC containers with CAdES signatures, with XAdES signatures, and with time-stamp tokens.

It also provides high level description of the steps that participants must perform for conducting the 2 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 ASiC 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 Plugtests portal.

- CRLs issued by the CAs operating in the Plugteststrust frameworks. These CRLs will be re-issued several times during the Plugtestswith 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 Plugtestsportal.

- 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 Plugtestsportal.

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

Trust framework:

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

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

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

1. **Scenario SCOK**. This scenario will include the first root CA (**RootCAOK**), one intermediate CA (**LevelACAOK**), one final CA, which issues certificates for end-entities (**LevelBCAOK**), and a Time Stamp Authority (**TSA1**), certified by **RootCAOK**. Participants will use its cryptographic material for both generating and verifying the signatures corresponding to the **generation and cross-verification**.In this scenario there are the certificates managed during the generation and verification of the signature, including the end-entities certificates issued by the CA deployed in the portal to the participants, that are valid. CAs within this scenario issuing certificates will issue the CRLs including references to the revoked certificate. CAs within this scenario will also generate OCSP responses reporting on the status of these certificates whenever it is requested by the participants. This scenario is intended to check implementations behavior when verifying signatures that will be provided by the other participants.

2. **Scenario SCUN**. This scenario will include the following services:

    1. **RootCAOK**, **LevelACAOK**, and **LevelBCAOK**.

    2. A CA, issuing certificates to end entities, whose certificate **shall be revoked** by the time the Plugtests will start (**LevelBCARev**, certified by **LevelACAOK**).

    3. A Time Stamp Authority, certified by **LevelBCARev**(**TSA2**).

    4. A Time Stamp Authority, certified by **RootCAOK**, whose certificate **shall be revoked** by the time the Plugtests will start (**TSA_Rev**).

    5. A Time Stamp Authority, certified by **RootCAOK**, whose certificate **shall be expired** by the time the Plugtests will start (**TSA_Exp**).

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

    1. One pre-generated signing certificate, issued by **LevelBCAOK**, which by the time the Plugtests will start **will be revoked**.

    2. One pre-generated signing certificate, issued by **LevelBCAOK**, which by the time the Plugtests will start **will be expired**.

        CAs within this scenario issuing the certificates will issue the CRLs including references to the revoked certificate. CAs within this scenario will also generate OCSP responses reporting on the status of these certificates whenever it is requested by the participants. ETSI will pre-generate one

XAdES signature using the revoked certificate and another one using the expired certificate. This scenario is intended to check implementations behavior when verifying not valid signatures.

2.2.1.3 Online PKI-related services page

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

The **Online PKI services details page** 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 ASiC 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.

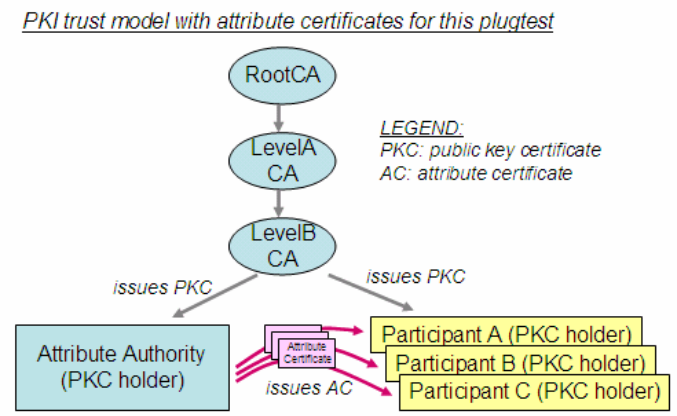
2.2.1.5 Online TSA services access page

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

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

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

After each upload of signatures or verifications, an email is sent to all participants via this mailing list to inform them. So the participants 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 ASiC Interop Specific areas of Private part

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

2.2.2.1 Test Cases Definition Language

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

2.2.2.2 Test Cases pages

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

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

- To browse the aforementioned test definition documents and to build pieces of text and tables corresponding to each test case within this document.
- To browse reports of verification (simple XML documents) of each single ASiC 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 ASiC 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 ASiC 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 ASiC 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 ASiC signatures generated and verified at each instant of the Plugtests™.

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

2.2.2.5 Upload pages

The ASiC 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 ASiC 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 ASiC 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 Plugtests™, including all the ASiC 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 ASiC 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.

3 Participants list

The table below shows the details of all the organizations and persons that have participated in the 2016 ASiC Remote Plugtests™ Event.

There have been **66 different organizations** and 99 people participating in the event.

Company	Country
5 P s.r.o.	Czech Republic
Agence Nationale de Certification Electronique	Tunisia
Agencija za komercijalnu djelatnost d.o.o.	Hungary
ALIS spol. s r.o.	Czech Republic
ApoloLab S.A.	Costa Rica
Ardaco	Slovakia
Artinpro	Germany
Aruba PEC	Italia
Ascertia Limited	UK
Asseco Data Systems	Poland
Asseco Poland SA	Poland
AULOCE	Spain

Company	Country
BIT4ID	Italia
Borica - Bankservice AD	Bulgaria
Certisign	Brazil
Comfact	Sweden
Connective NV	Belgium
Dignita	Czech Republic
Disig a.s.	Slovakia
Ditec, a.s.	Slovakia
Dokumenta a.s. Bratislava	Slovakia
E-Government Innovation Center	Austria
ELDOS CORPORATION LTD	UK
EUSO	Latvia
exceet Secure Solutions GmbH	Germany
eZprava.net s.r.o.	Czech Republic
Gordic spol	Czech Republic
Governikus GmbH & Co. KG	Germany
Hellenic Academic and Research Institutions Certification Authority	Greece
intarsys consulting GmbH	Germany
Intesi Group	Italia
Krajowa Izba Rozliczeniowa S.A	Poland
Lex Persona	Belgium
Lombardia Informatica S.p.A.	Italia
Mentana - Claimsoft GmbH	Germany
Microsec ltd.	Hungary
Ministero della Difesa - Comando C4 Difesa	Italia
Ministry of Finance and Public Administration	Spain
Minitry of interior	Serbia
MIT-SOFT UAB	Lithuania
Národný bezpecnostný úrad	Slovakia
National Security Cabinet	Portugal
Netlock Kft	Hungary
NG Technologies	Tunisia

Company	Country
NISZ Ltd.	Hungary
Nowina Solutions	Luxembourg
OpenLimit SignCubes GmbH	Germany
Otip Office	Japan
PDS	Czech Republic
Polysys Ltd	Hungary
První certifikacní autorita, a.s	Czech Republic
QuoVadis Trustlink	Netherlands
Real.not	France
Ricoh Spain IT Services	Spain
Riigi Infosüsteemi Amet	Estonia
SAFRAN IDENTITY & SECURITY	France
SecCommerce Informationssysteme	Germany
Secrypt GmbH	Germany
SEFIRA	Czech Republic
Sertifitseerimiskeskus AS	Estonia
Software602 a.s.	Czech Republic
Tesco SW	Czech Republic
Tessaris Integrated Security	Switzerland
UAB "BSS IT"	Lithuania
UPC	Spain
Viafirma SL	Spain

4 Plugtests conclusions

4.1 Remote vs. Face to Face

With 66 companies/organizations from Europe, but also Tunisia, Japan and Brazil and Costa Rica participating, 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.

3 conference calls have been organized during the event, one kick off conf call to present the testing and 2 other ones regularly to discuss the issues and answer to any technical questions.

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, 4 weeks of testing have been planned for this event, starting from 7th Nov to 5th Dec 2016.

In order to let participants read all the documentations and prepare the testing, ETSI has opened the portal on 17th March, a week before the official beginning of the interoperability event.

Moreover, for this event, 66 companies/organizations were registered, as each company has to verify the signature of the other ones, the time needed increases with the amount of companies. 4 weeks were definitely too short.

For this reasons, the Plugtests team has decided to extend the duration of the event until the 31h Dec 2016.

5 ASiC Plugtests related issues

5.0 Introduction

The present section lists some of the issues raised during the ASiC Plugtests event in November and December 2016. This technical report will be provided to ETSI TC ESI which is the technical working group in charge of the standardization of the ETSI Electronic Signatures, for possible action/input for further changes in standards.

5.1 Usage of deprecated qualifying properties in XAdES signatures

At the Plugtests it was discussed about the usage in XAdES signatures of the qualifying properties specified in ETSI TS 101 903 v1.4.2 that have been deprecated by ETSI EN 319 132-1 v1.1.0.

It was argued that the conformance testing specifications (ETSI TS 119 134) do not contain any check on the contemporary presence of the new and deprecated properties in the same signature. It was asked to add new assertions so to check that a signature cannot contain both one or more new qualifying properties and one or more deprecated qualifying properties at the same time. Consequently interoperability test specifications shall not require signatures containing contain both one or more new qualifying properties and one or more deprecated qualifying properties at the same time.

5.2 Usage of new attributes in CAdES signatures

At the Plugtests it was noticed that some participants validated positively the containers with CAdES signatures containing signer-attributes instead of signer-attributes-v2 attribute where the corresponding test case definition required to use signer-attributes-v2. It was confirmed that the validation should check that the signature incorporated in the ASiC container contains the attributes required in the test case definition.

5.3 XAdES signatures augmentation from LT to LTA level

At the Plugtests it was discussed about the augmentation of XAdES signatures incorporated in AsiC containers from LT to LTA level. The main issue concerned the doubt if it is needed having a XAdES-B-LT signature including all validation data before being able to augment it to a XAdES-B-LTA signature. It was confirmed tha a XAdES-B-LT signature shall contain all validation data needed to validate the incorporated signatures and timestamps. Another issue concerned how to incorporate TimestampValidationData elements. It was pointed out that it is not prohibited the URI attribute inclusion in a TimeStampValidationData element incorporated immediately after the respective electronic timestamp container element even if such inclusion should be avoided in these cases because this URI attribute is not needed and adding a wrong value that doesn't refer the correct timestamp container could create mistakes when validating the XAdES signature.

5.4 Invalid files in ASiC containers

At the Plugtests the following issues were noticed and reported to the involved companies.

- Some ASiC-E containers with CAdES signatures contained invalid ASiCManifest*.xml files because the namespace "http://uri.etsi.org/2918/v1.2.1#" was used instead of the correct "http://uri.etsi.org/02918/v1.2.1 namespace.
- Some ASiC-E containers with XAdES signatures contained invalid META-INF/manifest.xml files because
    - namespace prefixes for attributes were not used
    - or a wrong version was declared instead of the right version "1.2"
    - or the reference of the baseline ASiC-E container was missing.

.

5.5 Malformed XAdES signatures incorporated in ASiC containers

At the Plugtests the following issues concerning XAdES signatures incorporated in some ASiC containers were noticed and reported to the involved companies.

- The XAdES signatures contained invalid xades141:CompleteCertificateRefsV2 element because it had the child element xades132:CertRefs instead of the child element xades141:CertRefs.

- The XAdES signatures contained invalid xades141:SigningCertificateV2 element because it had the child element xades132:Cert which had the (optional) wrong child element xades132:IssuerSerial instead of the (optional even if not recommended) correct child element xades132:IssuerSerialV2.
- The XAdES signatures contained property DataObjectFormat placed directly within SignedProperties element instead of within SignedDataObjectProperties element.
- The XAdES signatures didn't contain the root element asic:XAdESSignatures as requested by ASiC requirements.
- The baseline XAdES signatures didn't contain the DataObjectFormat element.

5.6 xadesv141:ArchiveTimeStamp digest calculation

At the Plugtests it was raised a potential issue in xadesv141:ArchiveTimeStamp digest calculation as defined in ETSI EN 319 132-1.

During xadesv141:ArchiveTimeStamp digest calculation ETSI EN 319 132-1 requires to

- Process the retrieved ds:Reference element according to the reference processing model of XMLDSIG, clause 4.4.3.2.
- If the result is a XML node set, canonicalize it as specified in clause 4.5 (Managing canonicalization of XML nodesets); and
- Concatenate the resulting octets to those resulting from previously processed ds:Reference elements in ds:SignedInfo.

It was pointed out by some participants that it is not so clear, which canonicalization algorithm shall be used:

—the one presented in xades1.41:ArchiveTimeStamp element, or
—the one presented in ds:SignedInfo element

Some validations of baseline LTA ASiC containers with XAdES signatures returned an invalid result because of the different canonicalization algorithms used in signature creation and in signature validation applications.

The request to better clarify in ETSI EN 319 132-1 document the canonicalization algorithm to be used was raised by the participants.

5.7 Future Plugtests improvements about B-LTA signatures

During the Plugtests an issue, concerning definitions of B-LTA signatures creation and validation, was found out and it was asked to try to solve it in future Plugtests events.

While testing B-LTA signatures one of the most important validation checks involves the ArchiveTimeStamp.

Participants create B-LTA signatures using SignatureTimeStamps and ArchiveTimeStamps.

Participants use signing and timestamping certificates which, usually, are not expired during the Plugtests event.

So, if participants validate signatures using EN 319 102-1, SignatureTimeStamp and ArchiveTimeStamp attributes or elements validations are not be executed (at least if not explicitly forced in validation applications), since signing certificates are not expired (nor revoked) at validation time.

It means that some participants could omit main issues of test cases involving B-LTA signatures.

For the future Plugtests, it was suggested, to define more strictly how to validate B-LTA signatures during Plugtests events or to create more complex environments and test cases, so that B-LTA signatures shall contain expired signing and/or timestamping certificates.

5.8 ASiCArchiveManifest

In EN 319 162 -1 text:

The Clause 4.4.5 item 2) indicates that for long term availability (for ASiC-E containers with CAdES - time assertions) ASiCArchiveManifest (together with META-INF/*timestamp*.tst) may be used.

Inspite of this, in the clause 4.4.4.2 the file naming specified does not allow to have more than a single file and it was suggested to change the file name to "META-INF/*ASiCArchiveManifest*.xml" allowing multiple ASiCArchiveManifest files to be present in ASiC-E containers with CAdES - time assertions.

5.9 ASiCEvidenceRecordManifest

In EN 319 162 -1, in he clause 4.4.3.2. Item 4:

"4) One or more ASiCEvidenceRecordManifest files may be present. They

[...]:

[...]

c) be named:

- "evidencerecord.ers" if in ERS [8] format; or

- "evidencerecord.xml" if in XMLERS [9] format."

It is allowed to have several ASiCEvidenceRecordManifest files, and every file must refer to its own evicence record file.

But (according current text) evidence record file name is fixed "evidencerecord.ers" (or "evidencerecord.xml").

It should be "*evidencerecord*.ers" and "*evidencerecord*.xml" to allow the presence of multiple ASiCEvidenceRecordManifest files in the container.

5.10 EN 319 162-2 V1.1.1 various issues

1) It is written in the Annex A "ASiC part 1 [2], clause 4.4.2 item 3)", but 4.4.2 does not contain item 3.

2) Some participants reported it may not be clear enough if "META-INF/manifest.xml", "META-INF/container.xml", "META-INF/metadata.xml" and other files are allowed within ASiC-E CAdES additional and ASiC-E Time assertion additional container.

It is only mentioned in the informative annex A.

5.11 TS 103 174 V2.2.1 issues

In clause 7.3.1 a) (page 10) describes as follows:

The CAdES [1] signature specified above shall conform to the CAdES baseline profiles [3], clause 5 and all subclauses, except for subclause 5.1.1 where only the detached signature service shall be supported.

Its 8.4.1 b) (page 12) also describes likewise.

But in CAdES baseline profiles [3] (I referred to ETSI TS 103 173 V2.2.1 (2013-04)), there is no subclause 5.1.1.

the right clause to be referenced in ETSI TS 103 174 V2.2.1 document would have been the 6th instead of the 5th. So the subclause 5.1.1 should be changed to 6.1.1

5.12 General requests

One participant asked if ETSI has plans for making ASiC an ISO standard, to help ASiC becoming world-wide used, this will be discussed in the ETSI/ESI TC.

It was requested to extend the availability of the ETSI Plugtests portal and/or the mailing list to help the developer's community on a more stable basis, this will need further discussion.

6 ASiC Plugtests™ Interoperability Testing

6.1 Positive test cases for generation and verification for ASiC

In the 'positive test' participants will do following:

1. A partiticipating implementation may generate as many ASiC containers as the participant considers worth; the participan will do it as described in the test case definitions. Generated ASiC containers shall be valid. That's why we say 'positive test' for this test.
2. A participant will upload ASiC containers to the portal.
3. A participant will download ASiC containers generated by other participants.
4. Validate ASiC containers from other participants.
5. Upload verification results as XML files.
6. See test result matrix.

Signed Data and other files required as input for ASiC test container generation for any test case SHALL be as specified in the related test case definition and is available in the Data folder.

6.1.1 Test cases for ASiC-S-C.SCOK TestSet.

The test cases in this section deal with the `ASiC-S-C.SCOK` TestSet, i.e. test cases on ASiC Simple containers enclosing CAdES signatures. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AS-ENA-C-BES-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The signature is a valid CAdES-BES signature *WITHOUT* SigningTime, associated to the file specified in SignedDocument. Implementation shall add a ESSSigningCertificateV2, ContentType and MessageDigest attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AS-ENA-C-BES-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file

extension is ".asics". The signature is a valid CAdES-BES signature associated to the file specified in SignedDocument. Implementation shall add a ESSSigningCertificateV2, ContentType, SigningTime, MessageDigest and ContentTimeStamp attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AS-ENA-C-BES-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The signature is a valid CAdES-BES signature associated to the file specified in SignedDocument. Implementation shall the following attributes at once to generating signature: - MessageDigest - SigningTime - ESSSigningCertificateV2 - SignerLocation - ContentType - ContentHints - ContentIdentifier - CommitmentTypeIndication At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AS-ENB-C-B-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The signature is the simplest CAdES-B-B one. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. ContentType, MessageDigest and SigningTime attributes shall also be added to the signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AS-ENB-C-B-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-B signature contains an attributeCertificate in signer-attributes-v2 attribute (See 'EN 319 122-1 5.2.6.1') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AS-ENB-C-B-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades

- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-B signature contains a claimedAttribute in signer-attributes-v2 attribute (See 'EN 319 122-1 5.2.6.1') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AS-ENB-C-B-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes
- ++++SignaturePolicyIdentifier

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-B signature contains an explicit SignaturePolicyIdentifier attribute (See 'EN 319 122-1 5.2.9') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI1.der' shall be used as its input.

AS-ENB-C-B-5.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-B signature contains a CounterSignature unsigned attribute (See 'EN 319 122-1 5.2.7') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AS-ENB-C-B-6.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The signature is a valid CAdES-B-B signature with multiple independent signatures. The input to this test is a CAdES-B-B signature as specified in AS-ENB-C-B-1 test case. Implementation shall add a ESSSigningCertificateV2, ContentType, SigningTime and MessageDigest attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AS-ENB-C-T-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-T signature contains a SignatureTimeStamp unsigned attribute (See 'EN 319 122-1 5.3') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AS-ENB-C-T-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". In this test case an indipendent CAdES-B-T signature is added to another CAdES-B-T signature. The input to this test is a CAdES-B-T signature as specified in AS-ENB-C-T-1 test case.

AS-ENB-C-LT-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AS-ENB-C-LT-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

AS-ENB-C-LT-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures, an attributeCertificate in signer-attributes-v2 attribute (See 'EN 319 122-1 5.2.6.1') and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AS-ENB-C-LT-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures, an attributeCertificate in signer-attributes-v2 attribute (See 'EN 319 122-1 5.2.6.1') and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

AS-ENB-C-LTA-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LTA signature contains the mandatory CAdES attributes for CAdES-B-B signatures, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attributes. No attribute certificates are present. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AS-ENB-C-LTA-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades

- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attributes. No attribute certificates are present. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

AS-TSB-C-B-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-B signature contains a claimedAttribute in signer-attributes attribute (See 'TS 101 733 5.11.3') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AS-TSB-C-B-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-B signature contains an attributeCertificate in signer-attributes attribute (See 'TS 101 733 5.11.3') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AS-TSB-C-LT-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures, an attributeCertificate in signer-attributes attribute (See 'TS 101 733 5.11.3') and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AS-TSB-C-LT-2.xml

- +AsicSimpleContainer

- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures, an attributeCertificate in signer-attributes attribute (See 'TS 101 733 5.11.3') and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

AS-TSB-C-LTA-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LTA signature contains the mandatory CAdES attributes for CAdES-B-B signatures, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attributes. No attribute certificates are present. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AS-TSB-C-LTA-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedCades
- +++SignedAttributes

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asics". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attributes. No attribute certificates are present. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

6.1.2 Test cases for `ASiC-S-X.SCOK` TestSet.

The test cases in this section deal with the ASiC-S-X.SCOK TestSet, i.e. test cases on ASiC Simple containers enclosing XAdES signatures. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AS-ENA-X-BES-1.xml

- +AsicSimpleContainer
- ++AsicDataObject

- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to additional ASiC containers requirements, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-E-BES one containing the xades:SigningCertificateV2, and xades:DataObjectFormat properties. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENA-X-BES-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to additional ASiC containers requirements, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature CONTAINS the XAdES properties xades:SigningCertificateV2, and xades:DataObjectFormat. The signature signs the XAdES signed properties and the Manifest element referencing ONE document: a text file. The RenewedDigests properties CONTAINS the re-hash in SHA-256 algorithm of the signed document. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-B-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-B one containing the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertificateV2, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-B-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlaceV2. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-B-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:SignerRoleV2 containing one claimed role (XML encoded). The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-B-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:SignerRoleV2 containing one certified role within a X509 attribute certificate. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-B-5.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:CounterSignature. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-B-6.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades
- ++++xades:SignaturePolicyIdentifier

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B

signature containing the mandatory XAdES properties plus xades:SignatureProductionPlaceV2 and xades:SignaturePolicyIdentifier. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-T-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-T one containing the mandatory XAdES properties namely: xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat and xades:SignatureTimeStamp. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-T-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-T one containing the xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat and TWO xades:SignatureTimeStamp properties. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AS-ENB-X-LT-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat, xades:SignatureTimeStamp, xades:CertificateValues and xades:RevocationValues. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LT-2.xml

- +AsicSimpleContainer
- ++AsicDataObject

- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat, xades:SignatureTimeStamp, xades:CertificateValues and xades:RevocationValues. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LT-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one incorporating one attribute certificate, one xades:SignatureTimeStamp, one xades:CertificateValues, one xades:AttrAuthoritiesCertValues and one xades:RevocationValues. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LT-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one incorporating one attribute certificate, one xades:SignatureTimeStamp, one xades:CertificateValues, one xades:AttrAuthoritiesCertValues, one xades:RevocationValues, and one xades:AttributeRevocationValues. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LTA-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues and xadesv141:ArchiveTimeStamp. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LTA-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues and xadesv141:ArchiveTimeStamp. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LTA-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues, a first xadesv141:ArchiveTimeStamp, a xadesv141:TimeStampValidationData including the CRL reporting the status of the TSA's certificate (in real life, it could be different from the CRL present within RevocationValues property) and a second xadesv141:ArchiveTimeStamp. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-ENB-X-LTA-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificateV2, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues and a first xadesv141:ArchiveTimeStamp, a xadesv141:TimeStampValidationData including the OCSP response reporting the status of the TSA's certificate and a second xadesv141:ArchiveTimeStamp. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property.

AS-TSB-X-B-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-B one containing the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-B-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlace. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-B-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:SignerRole containing one claimed role (XML encoded). The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-B-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:SignerRole

containing one certified role within a X509 attribute certificate. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-B-5.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:CounterSignature. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-B-6.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades
- ++++xades:SignaturePolicyIdentifier

This test case tests an ASiC-S container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the a XAdES-B-B signature containing the mandatory XAdES properties plus xades:SignatureProductionPlace and xades:SignaturePolicyIdentifier. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-T-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-T one containing the mandatory XAdES properties namely: xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat and xades:SignatureTimeStamp. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-T-2.xml

- +AsicSimpleContainer

- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-T one containing the xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat and TWO xades:SignatureTimeStamp properties. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AS-TSB-X-LT-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat, xades:SignatureTimeStamp, xades:CertificateValues and xades:RevocationValues. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LT-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is the simplest XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat, xades:SignatureTimeStamp, xades:CertificateValues and xades:RevocationValues. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LT-3.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one incorporating one attribute certificate, one xades:SignatureTimeStamp, one xades:CertificateValues, one xades:AttrAuthoritiesCertValues and one xades:RevocationValues. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LT-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one incorporating one attribute certificate, one xades:SignatureTimeStamp, one xades:CertificateValues, one xades:AttrAuthoritiesCertValues, one xades:RevocationValues, and one xades:AttributeRevocationValues. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LTA-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues and xadesv141:ArchiveTimeStamp. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LTA-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues and xadesv141:ArchiveTimeStamp. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LTA-3.xml

- +AsicSimpleContainer

- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues, a first xadesv141:ArchiveTimeStamp, a xadesv141:TimeStampValidationData including the CRL reporting the status of the TSA's certificate (in real life, it could be different from the CRL present within RevocationValues property) and a second xadesv141:ArchiveTimeStamp. The revocation material used are CRLs. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

AS-TSB-X-LTA-4.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedXades

This test case tests an ASiC-S container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asics". The signature is a XAdES-B-LT one containing the XAdES properties xades:SigningTime, xades:SigningCertificate, xades:DataObjectFormat, xades:SignatureTimeStamp, xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP response issued by RootCAOK CA), xades:CertificateValues, xades:RevocationValues and a first xadesv141:ArchiveTimeStamp, a xadesv141:TimeStampValidationData including the OCSP response reporting the status of the TSA's certificate and a second xadesv141:ArchiveTimeStamp. The revocation material used are OCSP responses. 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. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property.

6.1.3 Test cases for ASiC-S-T.SCOK TestSet.

The test cases in this section deal with the ASiC-S-T.SCOK TestSet, i.e. test cases on ASiC Simple containers enclosing time assertions. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AS-ENA-T-T-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedTst

This test case tests that META-INF/timestamp.tst contains a valid Time-stamp Token associated to the file specified in AsicDataObject (EN 319 162-1 TC/ASiC-S/T1)

AS-ENA-T-T-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedTst

This test case tests long term attributes (ASiCArchiveManifest and the related archive timestamp) added to AS-ENA-T-T-1 test case

AS-ENA-E-T-1.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedTst

This test case tests that META-INF/evidencerecord.ers contains a valid evidence record in RFC 4998 format associated to the file specified in AsicDataObject (EN 319 162-1 TC/ASiC-S/T1)

AS-ENA-E-T-2.xml

- +AsicSimpleContainer
- ++AsicDataObject
- ++AsicAssociatedTst

This test case tests that META-INF/evidencerecord.xml contains a valid evidence record in RFC 6283 format associated to the file specified in AsicDataObject (EN 319 162-1 TC/ASiC-S/T1)

6.1.4 Test cases for ASiC-E-C.SCOK TestSet.

The test cases in this section deal with the ASiC-E-S.SCOK TestSet, i.e. test cases on ASiC Extended containers enclosing CAdES signatures. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AE-TSB-C-B-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The signature is the simplest CAdES-B-B one. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. ContentType, MessageDigest and SigningTime attributes shall also be added to the signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AE-TSB-C-B-2.xml

- +AsicExtendedContainer
- ++AsicDataObject

- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-B signature contains an attributeCertificate in signer-attributes attribute in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AE-TSB-C-B-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-B signature contains a claimedAttribute in signer-attributes attribute in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AE-TSB-C-B-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is

".asice". The signature is a valid CAdES-B-B signature with multiple independent signatures. The input to this test is a CAdES-B-B signature as specified in AE-TSB-C-B-1 test case. Implementation shall add a ESSSigningCertificateV2, ContentType, SigningTime and MessageDigest attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AE-TSB-C-B-5.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-B signature contains a CounterSignature unsigned attribute (See 'EN 319 122-1 5.2.7') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AE-TSB-C-B-6.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades
- ++++SignaturePolicyIdentifier

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-B signature contains an explicit SignaturePolicyIdentifier attribute (See 'EN 319 122-1 5.2.9') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI1.der' shall be used as its input.

AE-TSB-C-B-7.xml

- +AsicExtendedContainer
- ++AsicDataObject

- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing two ASiCManifest files and the requested CAdES signatures in "signature1.p7s" and "signature2.p7s" files. ASiC container file extension is ".asice". The signatures are the simplest CAdES-B-B ones. Implementation shall add a ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes to generating signatures. At least the signing certificate shall be included in the SignedData.certificates fields. All certificates needed for path building should be included too.

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AE-TSB-C-LT-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-LT signature contains the mandatory CAdES attributes for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

AE-TSB-C-T-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The CAdES-B-T signature contains a SignatureTimeStamp unsigned attribute (See 'EN 319 122-1 5.3') in addition to ESSSigningCertificateV2, ContentType, MessageDigest and SigningTime attributes.

AE-TSB-C-T-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". In this test case an indipendent CAdES-B-T signature is added to another CAdES-B-T signature. The input to this test is a CAdES-B-T signature as specified in AE-TSB-C-T-1 test case.

AE-ENA-C-A-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference

- +++DataObjectReference
- ++AsicAssociatedCades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file, the requested CAdES signature in a "signature.p7s" file, an ASiCArchiveManifest file and a timestamp token file. ASiC container file extension is ".asice". This test case is based on AE-TSB-LT-1 test case adding Long Term attributes (ASiCArchiveManifest and the related archive time stamp). The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AE-ENA-C-A-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file, the requested CAdES signature in a "signature.p7s" file, an ASiCArchiveManifest file and a timestamp token file. ASiC container file extension is ".asice". This test case is based on AE-TSB-LT-2 test case adding Long Term attributes (ASiCArchiveManifest and the related archive time stamp). The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.

AE-ENA-C-A-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference

- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file, the requested CAdES signature in a "signature.p7s" file, two ASiCArchiveManifest files and two timestamp token files. ASiC container file extension is ".asice". This test case is based on AE-TSB-LT-1 test case adding 2 levels Long Term attributes (2 ASiCArchiveManifests and the related archive time stamps). The full set of certificates that have been used to validate the signature and the first archive timestamp token is included. The revocation material that have been used in the validation of the signature and of the first archive timestamp token is included. The revocation data used are CRLs.

AE-ENA-C-A-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file, the requested CAdES signature in a "signature.p7s" file, an ASiCEvidenceRecordManifest file and an evidence record file. ASiC container file extension is ".asice". This

test case is based on AE-TSB-LT-1 test case adding Long Term attributes (ASiCEvidenceRecordManifest and the related archive evidence record). The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AE-ENA-C-A-5.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file, the requested CAdES signature in a "signature.p7s" file, an ASiCEvidenceRecordManifest file and an evidence record file. ASiC container file extension is ".asice". This test case is based on AE-TSB-LT-1 test case adding Long Term attributes (ASiCEvidenceRecordManifest and the related archive evidence record). The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.

AE-ENA-C-BES-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The signature is a valid CAdES-BES signature associated to the file specified in SignedDocument *WITHOUT* SigningTime. Implementation shall add a ESSSigningCertificateV2, ContentType and MessageDigest attributes to generating signature. At least the signing

certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AE-ENA-C-BES-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The signature is a valid CAdES-BES signature associated to the file specified in SignedDocument. Implementation shall add a ESSSigningCertificateV2, ContentType, SigningTime, MessageDigest and ContentTimeStamp attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AE-ENA-C-BES-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The signature is a valid CAdES-BES signature associated to the file specified in SignedDocument. Implementation shall add a ESSSigningCertificateV2, ContentType, SigningTime, MessageDigest and an attributeCertificate in signer-attributes-v2 attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

AE-ENA-C-BES-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject

- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedCades

This test case tests an ASiC-E container, including a mimetype file and a set of document files to be signed in the root folder and a META-INF folder containing an ASiCManifest file and the requested CAdES signature in a "signature.p7s" file. ASiC container file extension is ".asice". The signature is a valid CAdES-BES signature associated to the file specified in SignedDocument. Implementation shall add a ESSSigningCertificateV2, ContentType, SigningTime, MessageDigest and a claimedAttribute in signer-attributes-v2 attributes to generating signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

6.1.5 Test cases for ASiC-E-X.SCOK TestSet.

The test cases in this section deal with the ASiC-E-X.SCOK TestSet, i.e. test cases on ASiC Extended containers enclosing XAdES signatures. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AE-ENB-X-B-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature is the simplest XAdES-B-B one containing the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertificateV2, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificateV2 qualifying property. References to all certificates needed for path building should be included too.

AE-ENB-X-B-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and two document files to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. This brings the presence of two xades:DataObjectFormat elements. ASiC container file extension is ".asice". There are TWO signed data objects apart from the XAdES signed properties.

AE-ENB-X-B-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and two document files to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. This brings the presence of two xades:DataObjectFormat elements. ASiC container file extension is ".asice". There are TWO signed data objects apart from the XAdES signed properties and a xades:SignerRoleV2 containing one certified role within a X509 attribute certificate.

AE-ENB-X-T-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature only signs the XAdES signed properties and ONE document: a text file. The signature includes ONE xades:SignatureTimeStamp attribute.

AE-ENB-X-T-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature only signs the XAdES signed properties and ONE document: a text file. The signature includes TWO xades:SignatureTimeStamp attributes.

AE-ENB-X-LT-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature

contains 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.

AE-ENB-X-LT-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains 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.

AE-ENB-X-LT-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains 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.

AE-ENB-X-LT-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains 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 OCSP responses.

AE-ENB-X-LTA-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains ONE signed data object, ONE xades:SignatureTimeStamp, ONE xadesv141TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), ONE xades:CertificateValues, ONE xades:RevocationValues and ONE xadesv141:ArchiveTimeStamp. No attribute certificates are present. The revocation material used are CRLs.

AE-ENB-X-LTA-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains ONE signed data object, ONE xades:SignatureTimeStamp, ONE xadesv141:TimeStampValidationData (encapsulating the certificate of RootCAOK and the OCSP responses issued by RootCAOK CA), ONE xades:CertificateValues, ONE xades:RevocationValues and ONE xadesv141:ArchiveTimeStamp. No attribute certificates are present. The revocation material used are OCSP responses.

AE-ENB-X-LTA-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains ONE signed data object, ONE xades:SignatureTimeStamp, ONE xadesv141TimeStampValidationData, ONE xades:CertificateValues, ONE xades:RevocationValues, a first xadesv141:ArchiveTimeStamp, a xadesv141:TimeStampValidationData including the CRL reporting the status of the TSA's certificate (in real life, it could be different from the CRL present within RevocationValues property) and a second xadesv141:ArchiveTimeStamp. No attribute certificates are present. The revocation material used are CRLs.

AE-ENB-X-LTA-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains ONE signed data object, ONE xades:SignatureTimeStamp, ONE xadesv141TimeStampValidationData, ONE xades:CertificateValues, ONE xades:RevocationValues, a first xadesv141:ArchiveTimeStamp, a xadesv141:TimeStampValidationData including the OCSP response reporting the status of the TSA's certificate \and a second xadesv141:ArchiveTimeStamp. No attribute certificates are present. The revocation material used are OCSP responses.

AE-ENB-X-LTA-5.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container claiming conformance to the LTA level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains ONE signed data object, ONE xades:SignatureTimeStamp, ONE xadesv141TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), ONE xades:CertificateValues, ONE xades:RevocationValues and ONE xadesv141:ArchiveTimeStamp. No attribute certificates are present. The revocation material used are CRLs.

AE-TSB-X-B-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature is the simplest XAdES-B-B one containing the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertificate, and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file. At least the reference to the signing certificate shall be included in the SigningCertificate qualifying property. References to all certificates needed for path building should be included too.

AE-TSB-X-B-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and two document files to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. This brings the presence of two xades:DataObjectFormat elements. ASiC container file extension is ".asice". There are TWO signed data objects apart from the XAdES signed properties.

AE-TSB-X-B-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the B level of ASiC Baseline profile, including a mimetype file and two document files to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. This brings the presence of two xades:DataObjectFormat elements. ASiC container file extension is ".asice". There are TWO signed data objects apart from the XAdES signed properties and a xades:SignerRoleV2 containing one certified role within a X509 attribute certificate.

AE-TSB-X-T-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature only signs the XAdES signed properties and ONE document: a text file. The signature includes ONE xades:SignatureTimeStamp attribute.

AE-TSB-X-T-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the T level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature only signs the XAdES signed properties and ONE document: a text file. The signature includes TWO xades:SignatureTimeStamp attributes.

AE-TSB-X-LT-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature

contains 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.

AE-TSB-X-LT-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains 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.

AE-TSB-X-LT-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains 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.

AE-TSB-X-LT-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades

This test case tests an ASiC-E container claiming conformance to the LT level of ASiC Baseline profile, including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file and the requested XAdES signature in a "signature.xml" file. ASiC container file extension is ".asice". The signature contains 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 OCSP responses.

6.1.6 Test cases for ASiC-E-T.SCOK TestSet.

The test cases in this section deal with the ASiC-E-T.SCOK TestSet, i.e. test cases on ASiC Extended containers enclosing time assertions. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AE-ENA-T-T-1.xml

- +AsicExtendedContainer

- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedTst

This test case tests an ASiC-E container in which the META-INF/timestamp.tst contains a valid Time-stamp Token that is verified correctly on the ASiCManifest metadata. The references contained in ASiCManifest refer correctly the data objects and their hashes. ASiC container file extension is ".asice".

AE-ENA-T-T-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedTst
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container in which long term attributes (ASiCArchiveManifest and the related archive timestamp) are added to AE-ENA-T-T-1 test case. The full set of certificates that have been used to validate the first archive timestamp token is included. The revocation material that have been used in the validation of the first archive timestamp token is included. The revocation data used are CRLs. ASiC container file extension is ".asice".

AE-ENA-T-T-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference

- +++DataObjectReference
- ++AsicAssociatedTst
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container in which long term attributes (ASiCEvidenceRecordManifest and the related evidence record) are added to AE-ENA-T-T-1 test case. The full set of certificates that have been used to validate the first archive timestamp token is included. The revocation material that have been used in the validation of the first archive timestamp token is included. The revocation data used are CRLs. ASiC container file extension is ".asice".

AE-ENA-T-T-4.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedTst
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container in which long term attributes (ASiCEvidenceRecordManifest and the related evidence record) are added to AE-ENA-T-T-1 test case. The full set of certificates that have been used to validate the first archive timestamp token is included. The revocation material that have been used in the validation of the first archive timestamp token is included. The revocation data used are CRLs. ASiC container file extension is ".asice".

AE-ENA-E-T-1.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference

- ++AsicAssociatedTst

This test case tests an ASiC-E container in which the META-INF/evidencerecord.ers contains a valid evidence record in RFC 4998 format associated to the file specified in SignedDocument. The references contained in ASiCManifest refer correctly the data objects and their hashes. ASiC container file extension is ".asice".

AE-ENA-E-T-2.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicDataObject
- ++AsicManifest
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference
- ++AsicAssociatedTst

This test case tests an ASiC-E container in which the META-INF/evidencerecord.xml contains a valid evidence record in RFC 6283 format associated to the file specified in SignedDocument. The references contained in ASiCManifest refer correctly the data objects and their hashes. ASiC container file extension is ".asice".

AE-ENA-E-T-3.xml

- +AsicExtendedContainer
- ++AsicDataObject
- ++AsicMetaInfManifest
- ++AsicAssociatedXades
- +++SigReference
- +++DataObjectReference
- +++DataObjectReference

This test case tests an ASiC-E container including a mimetype file and a document file to be signed in the root folder and a META-INF folder containing a manifest.xml file, the requested XAdES signature in a "signature.xml" file, an ASiCEvidenceRecordManifest file and an evidence record file. ASiC container file extension is ".asice". The signature contains ONE signed data object, ONE xades:SignatureTimeStamp, ONE xadesv141TimeStampValidationData (encapsulating the certificate of RootCAOK and the CRL issued by RootCAOK CA), ONE xades:CertificateValues and ONE xades:RevocationValues. No attribute certificates are present. The revocation material used are CRLs.

6.2 Negative test cases for verification for ASiC

In the 'negative test' participants will do following:

1. A partiticipating implementation must verify the ASiC containers. Verification of the ASiC containers shall be negative. That's why we say 'negative test' for this test.
2. A participant will download ASiC containers generated by the organizers.
3. Verify ASiC containers.

4. Upload verification results as XML files.

5. See test result matrix.

6.2.1 Test cases for ASiC-S-CN.SCUN TestSet.

The test cases in this section deal with the ASiC-S-C.SCUN TestSet, i.e. test cases on ASiC Simple containers enclosing CAdES signatures. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AS-ENB-C-BN-1.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature DOES NOT CONTAIN the mandatory SigningTime attribute.

AS-ENB-C-BN-2.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature DOES NOT CONTAIN the mandatory SigningCertificate reference attribute.

AS-ENB-C-BN-3.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature DOES NOT CONTAIN the mandatory ContentType attribute qualifying the signed data object.

AS-ENB-C-BN-4.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature DOES NOT CONTAIN the mandatory certificates component into CMS signedData object.

AS-ENB-C-BN-5.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature has a wrong signature (the hash that was signed isn't the hash computed on the content being signed together with the signed attributes).

AS-ENB-C-BN-6.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature was created with an untrusted signing certificate.

AS-ENB-C-BN-7.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature was created with an expired signing certificate.

AS-ENB-C-BN-8.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature was created with a revoked/suspended signing certificate.

AS-ENB-C-BN-9.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature was created with a signing certificate generated by a CA whose certificate is revoked/suspended.

AS-ENB-C-BN-10.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature includes a SignaturePolicyIdentifier attribute with explicit

SignaturePolicyId. However its value of SignaturePolicyId.sigPolicyHash field does *NOT* match to the hash value of signer policy file (the signature policy file TARGET-SIGPOL-ETSI1.der is used): 0707070707070707070707070707070707070707070707070707070707070707 in SignaturePolicyIdentifier attribute (*WRONG HASH*) 969df17d712d3187646fbfd0812bf3d0ef25495b9277b2e5456fd54baaf67a3e in SignaturePolicy.signPolicyHash 969df17d712d3187646fbfd0812bf3d0ef25495b9277b2e5456fd54baaf67a3e calculated by SignaturePolicy.signPolicyInfo properly.

AS-ENB-C-BN-11.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. The included CAdES-B-B signature includes a SignaturePolicyIdentifier attribute with explicit SignaturePolicyId. The sigPolicyHash field value of SignaturePolicyIdentifier attribute in the CAdES-B-B signature is identical to signPolicyHash field value of ASN.1 signature policy file. However in the policy file (the signature policy file TARGET-SIGPOL-ETSI1Fake.der is used), signPolicyHash is *NOT* identical to the hash value which was calculated by the SignPolicyInfo without ASN.1 tag and length: 0909090909090909090909090909090909090909090909090909090909090909 in SignaturePolicyIdentifier attribute 0909090909090909090909090909090909090909090909090909090909090909 in SignaturePolicy.signPolicyHash 969df17d712d3187646fbfd0812bf3d0ef25495b9277b2e5456fd54baaf67a3e calculated by SignaturePolicy.signPolicyInfo properly

AS-ENB-C-BN-12.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with CAdES signatures. In the included CAdES-B-B signature the hash value of the signing certificate is different from the hash value in ESS signing certificate V2 attribute.

AS-ENB-C-TN-1.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. At the time in SignatureTimeStamp, the signer certificate had been already expired. ETSI Invalid-Cert Expired SN:01A4A73E344C7B 07-Nov-2016 22:06:29Z - signer certificate expired SN:01A4A73E344C7B 14-Nov 2016 15:15:17Z – SignatureTimeStamp

AS-ENB-C-TN-2.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. At the time in SignatureTimeStamp, the signer certificate had been already revoked. ETSI Invalid-Cert Revoked SN:009CFD50EF3DC7 06-Nov-2016 22:15:05Z - signer certificate revoked SN:009CFD50EF3DC7 14-Nov 2016 15:15:20Z – SignatureTimeStamp

AS-ENB-C-TN-3.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. The hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value of signerInfo.

AS-ENB-C-TN-4.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. At the time in SignatureTimeStamp, the timestamp signer certificate had been already revoked. ETSI Invalid-Cert Revoked SN:012535E3CE9266 29-Apr-2015 18:15:46Z - timestamp signer certificate revoked SN:012535E3CE9266 14-Nov 2016 15:15:26Z - SignatureTimeStamp

AS-ENB-C-TN-5.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. At the time in SignatureTimeStamp, the timestamp signer certificate had been already expired. ETSI Invalid-Cert Expired SN:01A6AD00B0238A 30-Apr-2015 18:54:37Z - timestamp signer certificate expired SN:01A6AD00B0238A 15-Nov 2016 15:15:29Z - SignatureTimeStamp

AS-ENB-C-TN-6.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. The timestamp signer certificate has been generated by an untrusted CA.

AS-ENB-C-TN-7.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with CAdES signatures. The timestamp signer certificate has been generated by a CA whose certificate is revoked/suspended.

AS-ENB-C-LTAN-1.xml

This negative test case tests an ASiC-S container claiming conformance to the LTA level of ASiC-S Baseline containers with CAdES signatures. In this test case, the time in the SignatureTimeStamp is ulterior than the time in ArchiveTimeStamp. ETSI Invalid-Sig Valid-Cert 06-Jul-2015 09:00:28Z - SignatureTimeStamp (*) 06-Jul-2015 09:00:02Z - ArchiveTimeStamp

AS-ENB-C-LTAN-2.xml

This negative test case tests an ASiC-S container claiming conformance to the LTA level of ASiC-S Baseline containers with CAdES signatures. In this test case, the content in ats-hash-index-v3 element has not the right value related to the CAdES signature to which the ATSv3 has been applied.

6.2.2 Test cases for `ASiC-S-XN.SCUN` TestSet.

AS-ENB-X-BN-1.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature DOES NOT CONTAIN the mandatory xades:SigningTime element.

AS-ENB-X-BN-2.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature DOES NOT CONTAIN the mandatory xades:SigningCertificate element.

AS-ENB-X-BN-3.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature DOES NOT CONTAIN the mandatory xades:DataObjectFormat element qualifying the signed data object.

AS-ENB-X-BN-4.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature has a wrong signature (the hash that was signed isn't the hash computed on the content being signed together with the signed properties).

AS-ENB-X-BN-5.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature has been created with an untrusted signing certificate.

AS-ENB-X-BN-6.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature has been created with an expired signing certificate.

AS-ENB-X-BN-7.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature has been created with a revoked/suspended signing certificate.

AS-ENB-X-BN-8.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature has been created with a signing certificate generated by a CA whose certificate is revoked/suspended.

AS-ENB-X-BN-9.xml

This negative test case tests an ASiC-S container claiming conformance to the B level of ASiC-S Baseline containers with XAdES signatures. The included XAdES-B-B signature contains a SigningCertificate property where digest does not match with the actual digest of the signer certificate.

AS-ENB-X-TN-1.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. At the time in xades:SignatureTimeStamp, the signer certificate had been already expired.

AS-ENB-X-TN-2.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. At the time in xades:SignatureTimeStamp, the signer certificate had been already revoked.

AS-ENB-X-TN-3.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. The hash value of messageImprint in xades:SignatureTimeStamp does *NOT* match to the hash value of the canonicalized ds:SignatureValue element.

AS-ENB-X-TN-4.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. At the time in xades:SignatureTimeStamp, the timestamp signer certificate had been already revoked.

AS-ENB-X-TN-5.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. At the time in xades:SignatureTimeStamp, the timestamp signer certificate had been already expired.

AS-ENB-X-TN-6.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. The timestamp signer certificate has been generated by an untrusted CA.

AS-ENB-X-TN-7.xml

This negative test case tests an ASiC-S container claiming conformance to the T level of ASiC-S Baseline containers with XAdES signatures. The timestamp signer certificate has been generated by a CA whose certificate is revoked/suspended.

AS-ENB-X-LTAN-1.xml

This negative test case tests an ASiC-S container claiming conformance to the LTA level of ASiC-S Baseline containers with XAdES signatures. In the XAdES-B-LTA signature the time in the SignatureTimeStamp is ulterior than the time in xadesv141ArchiveTimeStamp.

AS-ENB-X-LTAN-2.xml

This negative test case tests an ASiC-S container claiming conformance to the LTA level of ASiC-S Baseline containers with XAdES signatures. In the XAdES-B-LTA signature the hash value of messageImprint in xadesv141ArchiveTimeStamp element does *NOT* match to the hash value of all the time-stamped data objects.

6.2.3 Test cases for ASiC-E-TN.SCUN TestSet.

The test cases in this section deal with the ASiC-E-TN.SCUN TestSet, i.e. test cases on ASiC Extended containers enclosing time assertions. They include both ASiC baseline containers and ASiC additional containers, as specified within [EN_319162-1], [EN_319162-2] and [TS_103174].

AE-ENA-T-TN-1.xml

This negative test case tests an ASiC-E container in which the META-INF/timestamp.tst contains a valid time-stamp token that does not apply to the ASiCManifest file.

AE-ENA-T-TN-2.xml

This negative test case tests an ASiC-E container in which the META-INF/timestamp.tst contains a valid time-stamp token that applies on the ASiCManifest file but the verification fails on the data object referenced in the ASiCManifest file.

AE-ENA-E-TN-1.xml

This negative test case tests an ASiC-E container in which the META-INF/evidencerecord.ers contains a valid evidence record in RFC 4998 format that does not apply on the ASiCManifest file.

AE-ENA-E-TN-2.xml

This negative test case tests an ASiC-E container in which the META-INF/evidencerecord.xml contains a valid evidence record in RFC 6283 format that does not apply on the ASiCManifest file.