**Technical Report of the
ASiC Remote Plugtests™ Event
(March-April 2014)**

ETSI

ETSI

May 2014

This version:

Author:

Andrea Caccia, Knowledge Work andrea.caccia@studiocaccia.com
Juan Carlos Cruellas, UPC cruellas@ac.upc.edu
Konrad Lanz, A-SIT Konrad.Lanz@iaik.tugraz.at
Laurent Velez, ETSI laurent.velez@etsi.org

Editor:

Laurent Velez, ETSI laurent.velez@etsi.org

Abstract

This document is the technical report of the 2014 Remote Plugtests Event on ASiC (Associate Signature Container ETSI TS 102 918), 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 .

.

Contents

1 Introduction

In reply to the Mandate M/460, phase 2 and within the Specialist Task Force (STF) 459, ETSI is working on the production of the whole set of technical specifications for testing interoperability and conformance of the main ETSI Advanced Electronic Signatures.

Additionally, ETSI aims to develop conformance testing tools for (X/C/P)AdES (and their baseline profiles) and ASiC containers (and its baseline profile). This valuable set of tools and test specifications will accelerate the deployment of Interoperable Electronic Signatures across Europe for the different formats.

However, the implementers need to be able to run interoperability and conformance testing to help to debug their products and to ensure that their understanding of the standards is correct. The more efficient and cost effective way to reach this goal is by participating to an interoperability event.

Running a Plugtest on ASiC was also a great opportunity to identify potential remaining issues in the drafts ETSI EN 319 162-1 and -2 before going to official EN review process

ETSI has organized the remote Plugtests event on ASiC, held from 24 March to 30 April 2014. This remote event aimed at conducting interoperability test cases on ASiC signatures (ETSI TS 102 918 V1.3.1 and draft ETSI EN 319 162-1) and also its associated ASiC Baseline Profile draft ETSI EN 319 162-2.
This testing provided full test coverage of the specifications including testing signatures evolution, simulating real life situations. It was based on the test specification ETSI TS 119 164-2 ASiC Interoperability testing" produced by ETSI STF459.

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

The present document is the report from the 2014 remote Plugtests Event on ASiC Signatures. 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 119 164-2 ASiC Interoperability testing

- The Remote Plugtests Event on ASIC was organized by ETSI and held from 24th March to 30th April 2014.

 In order to give participants time to prepare the testing, ETSI opened the portal to participants in "read-only" mode on 17th March, a week before the official start date of the Plugtests event. An introduction web conference took place on Tuesday 18th March to present the portal and the testing.

The event was initially planned to run until 11th April but it was extended to 30th April on request from the participants. The reason being that the amount of test proposed was very important and participants would need more time to complete their testing.

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 2014 ASiC Remote Plugtests Event.

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

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

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

2 Organization and contents of the portal

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

2.1 Public part of the portal

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

- The 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)

- 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 first page details the 3 types of tests provided at this Plugtests event:

☐ Generation and cross-verification (a.k.a. Positive) tests.
Each participant is invited to generate a certain set of 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.

☐ Only-verification (a.k.a. Negative) tests.
ETSI has generated a number of ASiC containeres 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 Plugtest defines test suites for testing ETSI TS 102 918 V1.3.1, draft ETSI prEN 319 162-1 (this one partially), which define the ASiC core specification, and ETSI TS 103 174 v2.2.1, and draft ETSI prEN 319 162-2 (this one partially), which define the ASiC Baseline Profile.

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

- ETSI ASiC Test Suite Specification for interoperability TS 119 164-2

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 Plugtest portal.

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

➢ The certificate for the Time-stamping server issued by Root_CA_OK. As above, this material will be published in the the LDAP server and in the HTTP server deployed in the plugtest portal.

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

Trust framework:

ETSI has defined a trust framework for this plugtest, within different scenarios are defined. ETSI will define groups of test cases (for instance a group defining different test cases for CAdES-BES signatures) for each scenario.

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

The trust framework has been defined as detailed below:

Trust framework. Root_CA_OK as Root CA. This framework will be used for conducting tests on CAdES signatures using time-stamp tokens issued by only one TSA. For this trust framework, one scenario has been defined:

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

Untrust framework:

ETSI has defined an untrusted framework too for this plugtest. The untrusted framework has been used for negative test cases only. In this framework an untrusted CA generating signature certificates and an untrusted TSA generating timestamp signing certificates are defined. The verifications of the signed and timestamped documents generated by using the above signature and timestamp signing certificates should fail.

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

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

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

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

2.2.1.3 Online PKI-related services page

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

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

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

- **CA-related services**. This service provides issuance of certificates; generation of CRLs; publication of CRLs. Participants should use this service for getting their corresponding certificates for generating 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^{TM}, was set up for supporting exchange of messages among them. This was the main medium for putting questions to the Plugtests^{TM} 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^{TM}.

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^{TM}.

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^{TM}, 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 2014 ASiC Remote Plugtests^{TM} Event.

There have been **35 different organizations** and 59 people participating in the event.

Company	Plugtest Acronym	Country
Agjencia Kombetare e Shoqerise se Informacionit	AKSI	Albania
Ardaco	ARD	Slovak Republic
Aktsiaselts Sertifitseerimiskesku	AS	Estonia
ARHS	ARHS	Luxemburg
Aron Szabo	SZA	Hungary
Ascertia	ASC	United Kingdom
ATM	ATM	Romania
Banco Lafise	BANCO	Costa Rica
Cross Borders Trust Services	CBTS	Estonia
Clizio Merli Consultant	CLI	Italy
COMFACT	COM	Sweden
Cryptotolog	CRY	France
DICTAO	DIC	France
Dignita	DIG	Czech Republic
Disig	DIS	Slovak Republic
e-Contract.be BVBA	ECON	Belgium
Eldos	ELD	United Kingdom
e-Sec Data Security	ESEC	Brazil
E-Val Tecnologia	EVAL	Brazil
IAIK	IAIK	Austria
Infoscope Kft.	INFO	Hungary
Knowledge Work	KW	Italy

Microsec	MIC	Hungary
MIT-SOFT	MIT	Lithuania
National Authority for Electronic Certification	NAEC	Albania
National Agency of Information Society	NAIS	Albania
National Security Authority	NSA	Slovak Republic
National Security Cabinet	NSC	Portugal
Noreg	NOR	Hungary
Polysys	POL	Hungary
Sistemas Informaticos Abiertos	SIA	Spain
Software602	SIX	Czech Republic
Tubitak Uekae	TUB	Turkey
Universitat Politècnica de Catalunya	UPC	Spain
Unizeto	UNI	Poland

4 Plugtests conclusions

4.1 Remote vs. Face to Face

With 35 companies/organizations from Europe and South America 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.

4 conference calls have been organized during the event, one kick off conf call to present the testing and 3 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, 3 weeks of testing have been planned for this event, starting from 24th Mars to 11th April 2014.

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, 35 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. 3 weeks were definitely too short.

For this reasons, the Plugtests team has decided to extend the duration of the event until the 30th April 2014.

5 ASiC Plugtests™ Statistics

5.1 Overall statistics

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

Tests	S_CS SC_C	S_CS SC_T	S_CS SC_X	S_ST V_C*	S_ST V_T	S_ST V_X*	E_CS SC_C	E_CS SC_T	E_CS SC_X	E_ST V_C*	E_ST V_T	E_ST V_X*
Total	61	38	48	110	4	86	52	36	53	80	2	70

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

Tests	S_CS SC_C	S_CS SC_T	S_CS SC_X	S_ST V_C*	S_ST V_T	S_ST V_X*	E_CS SC_C	E_CS SC_T	E_CS SC_X	E_ST V_C*	E_ST V_T	E_ST V_X*
Total	517	279	355	373	12	250	319	211	292	237	6	199

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

ORG	S_STV_C*N	S_STV_TN	S_STV_X*N	E_STV_C*N	E_STV_TN	E_STV_X*N
Total	8	1	12	10	2	20

6 ASiC PlugtestsTM Interoperability Testing

6.1 Positive test cases for generation and verification for ASiC

6.1.1 Test cases for `ASiC-S_CSSC_C` TestSet.

ASiC-S_CSSC_C-1.xml description: This test case tests if the container has an ".asics" extension and has a ZIP format extacting the content (TS 119 164-2 TC/ASiC-S/CS/1)

ASiC-S_CSSC_C-2.xml description: This test case tests if the container if the container format is identifiable using mimetype (TS 119 164-2 TC/ASiC-S/CS/2)

ASiC-S_CSSC_C-3.xml description: This test case tests if the ZIP comment, when used to identify the format, begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension (TS 119 164-2 TC/ASiC-S/CS/3)

ASiC-S_CSSC_C-4.xml description: This test case tests mimetype when set equal to the signed content mimetype (TS 119 164-2 TC/ASiC-S/CS/4)

ASiC-S_CSSC_C-5.xml description: This test case tests if A META-INF folder is present in the root folder containing signature.p7s (TS 119 164-2 TC/ASiC-S/CS/6 and TC/ASiC-S/SC/C1)

ASiC-S_CSSC_C-6.xml description: This test case tests if a single data object, in addition to the optional mimetype, is present in the root folder (TS 119 164-2 TC/ASiC-S/CS/7)

6.1.2 Test cases for ASiC-S_CSSC_T TestSet.

ASiC-S_CSSC_T-1.xml description: This test case tests if the container has a ZIP format and the content can be successfully extracted (TS 119 164-2 TC/ASiC-S/CS/1)

ASiC-S_CSSC_T-2.xml description: This test case tests if the container if the container format is identifiable using mimetype (TS 119 164-2 TC/ASiC-S/CS/2)

ASiC-S_CSSC_T-3.xml description: This test case tests if the ZIP comment, when used to identify the format, begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension (TS 119 164-2 TC/ASiC-S/CS/3)

ASiC-S_CSSC_T-4.xml description: This test case tests mimetype when set equal to the signed content mimetype (TS 119 164-2 TC/ASiC-S/CS/4)

ASiC-S_CSSC_T-5.xml description: This test case tests if A META-INF folder is present in the root folder containing timestamp.tst (TS 119 164-2 TC/ASiC-S/CS/6 and TC/ASiC-S/SC/T1)

ASiC-S_CSSC_T-6.xml description: This test case tests if a single data object, in addition to the optional mimetype, is present in the root folder (TS 119 164-2 TC/ASiC-S/CS/7)

ASiC-S_CSSC_T-7.xml description: This test case tests an ASiC-S with Time-stamp token container that includes 1 level of long term attributes i.e. a single ASiCArchiveManifest and an archive time-stamp that applies to it

6.1.3 Test cases for ASiC-S_CSSC_X TestSet.

ASiC-S_CSSC_X-1.xml description: This test case tests if the container has a ZIP format and the content can be successfully extracted (TS 119 164-2 TC/ASiC-S/CS/1)

ASiC-S_CSSC_X-2.xml description: This test case tests if the container if the container format is identifiable using mimetype (TS 119 164-2 TC/ASiC-S/CS/2)

ASiC-S_CSSC_X-3.xml description: This test case tests if the ZIP comment, when used to identify the format, begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension (TS 119 164-2 TC/ASiC-S/CS/3)

ASiC-S_CSSC_X-4.xml description: This test case tests mimetype when set equal to the signed content mimetype (TS 119 164-2 TC/ASiC-S/CS/4)

ASiC-S_CSSC_X-5.xml description: This test case tests if A META-INF folder is present in the root folder containing signatures.xml (TS 119 164-2 TC/ASiC-S/CS/6 and TC/ASiC-S/SC/X1)

ASiC-S_CSSC_X-6.xml description: This test case tests if a single data object, in addition to the optional mimetype, is present in the root folder (TS 119 164-2 TC/ASiC-S/CS/7)

6.1.4 Test cases for ASiC-S_STV_T TestSet.

ASiC-S-STV_T-1.xml description: This test case tests if META-INF/timestamp.tst contains a valid Time-stamp Token associated to the file specified in SignedData (TS 119 164-2 TC/ASiC-S/STV/T1)

ASiC-S-STV_T-2.xml description: This test case tests long term attributes (ASiCArchiveManifest and the related archive timestamp) added to ASiC-S-STV_T-1 test case

6.1.5 Test cases for ASiC-S_STV_C-A TestSet.

ASiC-S-C-A-EPES-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests a CAdES-A with ATSv3 built on CAdES-EPES signature as specified in C-EPES-1 test case. Validation data must be included in SignedData before applying archive-time-stamp-v3.

ASiC-S-C-A-C-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-C signature as specified in C-C-1 test case. Validation data must be included in SignedData before applying archive-time-stamp-v3.

ASiC-S-C-A-XL-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-XL Type1 signature as specified in C-XL-1 test case.

ASiC-S-C-A-T-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests a CAdES-A with ATSv3 built on a CAdES-T signature as specified in C-T-1 test case. Validation data must be included in SignedData before applying archive-time-stamp-v3.

ASiC-S-C-A-X-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-X Type1 signature as specified in C-X-1 test case. Validation data must be included in SignedData before applying archive-time-stamp-v3.

ASiC-S-C-A-BES-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-BES with SigningTime signature as specified in C-BES-2 test case. Validation data must be included in SignedData before applying archive-time-stamp-v3.

ASiC-S-C-A-XL-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-XL Type2 signature as specified in C-XL-2 test case.

ASiC-S-C-A-X-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-X Type2 signature as specified in C-X-2 test case. Validation data must be included in SignedData before applying archive-time-stamp-v3.

ASiC-S-C-A-ATSv2-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-A signature associated to the file specified in SignedDocument This test case tests the CAdES-A with ATSv3 built on a CAdES-A with ATSv2. Validation data related to ATSv2 must be included in CertificateValues and RevocationValues within time-stamp-token.

6.1.6 Test cases for ASiC-S_STV_C-BES TestSet.

ASiC-S-C-BES-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-BES signature associated to the file specified in SignedDocument This test case tests the simplest CAdES-BES *WITHOUT* SigningTime.

ASiC-S-C-BES-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-BES signature associated to the file specified in SignedDocument This test case tests the simplest CAdES-BES *WITH* SigningTime.

ASiC-S-C-BES-3.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-BES signature associated to the file specified in SignedDocument This test case tests CAdES-BES with a SignerAttributes containing a CertifiedAttribute.

ASiC-S-C-BES-4.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-BES signature associated to the file specified in SignedDocument This test case tests CAdES-BES with a ContentTimeStamp attribute.

ASiC-S-C-BES-6.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-BES signature associated to the file specified in SignedDocument This test case tests CAdES-BES with multiple independent signatures. The input to this test is a CAdES-BES signature as specified in C-BES-1 test case.

ASiC-S-C-BES-7.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-BES signature associated to the file specified in SignedDocument This test case tests CAdES-BES with following attributes at once: - MessageDigest - SigningTime - ESSSigningCertificateV2 - SignerLocation - SignerAttributes (only Claimed Attributes included) - ContentType - ContentHints - ContentIdentifier - CommitmentTypeIndication

6.1.7 Test cases for ASiC-S_STV_C-BpB TestSet.

ASiC-S-CBp-B-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level B test case. The signature ONLY CONTAINS the mandatory CAdES properties, namely: ContentType, SigningTime, SigningCertificate and ESSSigningCertificateV2.

ASiC-S-CBp-B-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile In this CAdES Baseline Profile conformance level B test case the signature contains a CertifiedAttribute in addition to all mandatory attributes.

ASiC-S-CBp-B-3.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile This test case tests a CAdES Baseline Profile conformance level B signature with CounterSignature attribute. The input to this test is a CAdES-BES signature as specified in CBp-B-1 test case.

ASiC-S-CBp-B-4.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile This test case tests CAdES Baseline Profile conformance level B with multiple independent signatures. The input to this test is a CAdES-BES signature as specified in CBp-B-1 test case.

6.1.8 Test cases for ASiC-S_STV_C-BpLT TestSet.

ASiC-S-CBp-LT-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level LT test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES Baseline Profile conformance level B and a SignatureTimeStamp 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.

ASiC-S-CBp-LT-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level LT test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES Baseline Profile conformance level B and a SignatureTimeStamp 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

ASiC-S-CBp-LT-3.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is a CAdES Baseline Profile conformance level LT test case. The signature contains the mandatory CAdES properties for CAdES Baseline Profile conformance level B, one attribute certificate and a SignatureTimeStamp 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.

ASiC-S-CBp-LT-4.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is a CAdES Baseline Profile conformance level LT test case. The signature contains the mandatory CAdES properties for CAdES Baseline Profile conformance level B, one attribute certificate and a SignatureTimeStamp 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

6.1.9 Test cases for ASiC-S_STV_C-BpLTA TestSet.

ASiC-S-CBp-LTA-1.xml : description: This test case tests the signature of an ASiC container claiming conformance to the LTA level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level LTA test case. In this case there is one signed data object, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attributes. No attribute certificates are present. The revocation data used are CRLs.

ASiC-S-CBp-LTA-2.xml : description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level LTA test case. In this case there is one signed data object, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attributes. No attribute certificates are present. The revocation data used are OCSP responses

ASiC-S-CBp-LTA-3.xml : description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile

A signature for testing CAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV3. Afterwards, the resulting LTA-Level signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV3 is included within time-stamp token itself. The revocation data used are CRLs.

ASiC-S-CBp-LTA-4.xml : description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile

A signature for testing CAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV3. Afterwards, the resulting LTA-Level signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV3 is included within time-stamp token itself. The revocation data used are OCSP responses

ASiC-S-CBp-LTA-5.xml : description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile

A signature for testing CAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV3. Afterwards, the resulting LTA-Level signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV3 is added in root SignedData. The revocation data used are CRLs.

ASiC-S-CBp-LTA-6.xml : description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile

A signature for testing CAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV3. Afterwards, the resulting LTA-Level signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV3 is added in root SignedData. The revocation data used are OCSP responses

6.1.10   Test cases for ASiC-S_STV_C-BpT TestSet.

ASiC-S-CBp-T-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the T level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level T test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES Baseline Profile conformance level B and a SignatureTimeStamp attribute

ASiC-S-CBp-T-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the T level of ASiC Baseline profile A CAdES Baseline Profile signature for testing conformance level T. This test case tests the adding of an indipendent CAdES Baseline Profile signature level T to an already signed document in CAdES Baseline Profile signature level T format. The input to this test is a CAdES-T signature as specified in CBp-T-1 test case.

6.1.11   Test cases for ASiC-S_STV_C-C TestSet.

ASiC-S-C-C-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-C signature associated to the file specified in SignedDocument This test case tests a CAdES-C format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only CRLListIDs must be included.

ASiC-S-C-C-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-C signature associated to the file specified in SignedDocument This test case tests a CAdES-C format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only OcspListIDs must be included. Every OcspListID must include the ocspIdentifier and the ocspRepHash elements.

6.1.12   Test cases for ASiC-S_STV_C-EPES TestSet.

ASiC-S-C-EPES-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-EPES signature associated to the file specified in SignedDocument This test case tests the simplest CAdES-EPES form. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI5.der' shall be used as its input.

ASiC-S-C-EPES-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-EPES signature associated to the file specified in SignedDocument This test case tests CAdES-EPES with following attributes at once: - MessageDigest - SigningTime - ESSSigningCertificateV2 - SignaturePolicyIdentifier - SignerLocation - ContentType - CommitmentTypeIndication. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI5.der' shall be used as its input.

ASiC-S-C-EPES-3.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-EPES signature associated to the file specified in SignedDocument This test case tests the CAdES-EPES form. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI5.der' shall be used as its input. The sigPolicyQualifiers must include the oid of sp-user-notice (1.2.840.113549.1.9.16.5.2) and a UTF8String as explicitText.

6.1.13   Test cases for ASiC-S_STV_C-T TestSet.

ASiC-S-C-T-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-T signature associated to the file specified in SignedDocument This test case tests the simplest CAdES-T format.

ASiC-S-C-T-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-T signature associated to the file specified in SignedDocument This test case tests the adding of an indipendent CAdES-T signature to an already signed document in CAdES-T format. The input to this test is a CAdES-T signature as specified in C-T-1 test case to which a new SignerInfo instance will be added containing the other CAdES-T signature

6.1.14   Test cases for ASiC-S_STV_C-X TestSet.

ASiC-S-C-X-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-X signature associated to the file specified in SignedDocument This test case tests a CAdES-X Type1 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only CRLListIDs must be included.

ASiC-S-C-X-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-X signature associated to the file specified in SignedDocument This test case tests a CAdES-X Type2 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only CRLListIDs must be included.

ASiC-S-C-X-3.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-X signature associated to the file specified in SignedDocument This test case tests a CAdES-X Type1 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only OcspListIDs must be included. Every OcspListID must include the ocspIdentifier and the ocspRepHash elements.

ASiC-S-C-X-4.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-X signature associated to the file specified in SignedDocument This test case tests a CAdES-X Type2 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only OcspListIDs must be included. Every OcspListID must include the ocspIdentifier and the ocspRepHash elements.

6.1.15   Test cases for ASiC-S_STV_C-XL TestSet.

ASiC-S-C-XL-1.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-XL signature associated to the file specified in SignedDocument This test case tests a CAdES-XL Type1 format. Its CompleteRevocationRefs must have only CRLListIDs and its RevocationValues must have only crlVals element.

ASiC-S-C-XL-2.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-XL signature associated to the file specified in SignedDocument This test case tests a CAdES-XL Type2 format. Its CompleteRevocationRefs must have only CRLListIDs and its RevocationValues must have only crlVals element.

ASiC-S-C-XL-3.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-XL signature associated to the file specified in SignedDocument This test case tests a CAdES-XL Type1 format. In the CompleteRevocationRefs only OcspListIDs must be included and RevocationValues must have only ocspVals element.

ASiC-S-C-XL-4.xml description: This test case tests if META-INF/signature.p7s contains a valid CAdES-XL signature associated to the file specified in SignedDocument This test case tests a CAdES-XL Type2 format. In the CompleteRevocationRefs only OcspListIDs must be included and RevocationValues must have only ocspVals element.

6.1.16   Test cases for ASiC-S_STV_X-A TestSet.

ASiC-S-X-A-1.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-2.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-3.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-4.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-5.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-6.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-7.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-8.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

ASiC-S-X-A-9.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-A signature associated to the file specified in SignedData.

6.1.17   Test cases for ASiC-S_STV_X-BES TestSet.

ASiC-S-X-BES-1.xml description: This test case tests an external SigningCertificate (i.e. the URI Attribute is referring to a certificate file outside the signature and the Certificate in the ds:KeyInfo shall be ignored).

ASiC-S-X-BES-2.xml description: This test case tests an external SigningCertificate and has the SigningTime property that lies within the validity of the certificate.

ASiC-S-X-BES-3.xml description: This test case tests an external SigningCertificate, no uri is given for the SigningCertificate any more. The SigningTime should be checked against the validity period of the certificates. A SignatureProductionPlace property is provided.

ASiC-S-X-BES-4.xml description: This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property. Now also the SignerRole with a ClaimedRole is added.

ASiC-S-X-BES-5.xml description: This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property. Now also the SignerRole with a CertifiedRole is added.

ASiC-S-X-BES-6.xml description: This is a test for DataObjectFormat. The DataObjectFormat should point to a ds:Reference whose URI attribute points to a simple text file outside of the document containing the signature. MimeType and Encoding do not have to be checked in this case.

ASiC-S-X-BES-7.xml description: This is a test for DataObjectFormat, the reference should point to a ds:Object that contains the MimeType and Encoding in a non contradicting way. To use #Reference-Id-6-4 is just a suggestion.

ASiC-S-X-BES-8.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-BES signature associated to the file specified in SignedData.

ASiC-S-X-BES-9.xml description: This is to test the IndividualDataObjectsTimeStamp.

ASiC-S-X-BES-10.xml description: This is to test the AllDataObjectsTimeStamp.

ASiC-S-X-BES-11.xml description: This is to test the CounterSignature, for simplicity it is signed by the same party.

ASiC-S-X-BES-15.xml description: This is to test all BES Properties, except CounterSignature.

6.1.18   Test cases for ASiC-S_STV_X-BpB TestSet.

ASiC-S-XBp-B-1.xml description: This is the simplest XAdES Baseline Profile conformance level B test case. The signature ONLY CONTAINS the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertifiateThe and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

ASiC-S-XBp-B-2.xml description: This is the simplest XAdES Baseline Profile conformance level B test case, with TWO signed data objects apart from the signed XAdES properties. This brings the presence of two xades:DataObjectFormat elements

ASiC-S-XBp-B-3.xml description: Signature for testing XAdES Baseline Profile conformance level B with ONE signed data object apart from the signed XAdES properties, the corresponding xades:DataObjectFormat, and one attribute certificate.

6.1.19   Test cases for ASiC-S_STV_X-BpLT TestSet.

ASiC-S-XBp-LT-1.xml description: A signature for testing the simpletst case of XAdES Baseline Profile conformance level LT. ONE signed data object, ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are CRLs.

ASiC-S-XBp-LT-2.xml description: A signature for testing the simpletst case of XAdES Baseline Profile conformance level LT. ONE signed data object, ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are OCSP responses.

ASiC-S-XBp-LT-3.xml description: A signature for testing XAdES Baseline Profile conformance level LT. One signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, and one xades:RevocationValues. The revocation material used are CRLs.

ASiC-S-XBp-LT-4.xml description: A signature for testing XAdES Baseline Profile conformance level LT. One signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, one xades:RevocationValues, and one xades:AttributeRevocationValues. The revocation material used are OCSP responses.

6.1.20   Test cases for ASiC-S_STV_X-BpLTA TestSet.

ASiC-S-XBp-LTA-1.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. Iin this case there is one signed data object, one xades:SignatureTimeStamp container, one xades:CertificateValues, one xades:RevocationValues, and one xades:ArchiveTimeStamp container. No attribute certificates are present. No xadesv141:ArchiveTimeStamp and no xadesv141:TimeStampValidationData elements. The revocation material used are CRLs.

ASiC-S-XBp-LTA-2.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again with a xades:ArchiveTimeStamp. The validation material corresponding to the first xades:ArchiveTimeStamp is included within time-stamp token itself. The revocation material used are CRLs.

ASiC-S-XBp-LTA-3.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are CRLs.

ASiC-S-XBp-LTA-4.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. Iin this case there is one signed data object, one xades:SignatureTimeStamp container, one xades:CertificateValues, one xades:RevocationValues, and one xades:ArchiveTimeStamp container. No attribute certificates are present. No xadesv141:ArchiveTimeStamp and no xadesv141:TimeStampValidationData elements. The revocation material used are OCSP responses.

ASiC-S-XBp-LTA-5.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again with a xades:ArchiveTimeStamp. The validation material corresponding to the first xades:ArchiveTimeStamp is included within time-stamp token itself. The revocation material used are OCSP responses.

ASiC-S-XBp-LTA-6.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are OCSP responses.

ASiC-S-XBp-LTA-7.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are both CRLs and OCSP responses depending on the certificates.

6.1.21   Test cases for ASiC-S_STV_X-BpT TestSet.

ASiC-S-XBp-T-1.xml description: A signature for testing the simpletst case of XAdES Baseline Profile conformance level T. ONE signed data object and ONE xades:SignatureTimeStamp container.

ASiC-S-XBp-T-2.xml description: A XAdES Baseline Profile signature for testing conformance level T. ONE signed data object and TWO xades:SignatureTimeStamp containers.

6.1.22   Test cases for ASiC-S_STV_X-C TestSet.

ASiC-S-X-C-1.xml description: This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefs and the corresponding CRLs in CompleteRevocationRefs.

ASiC-S-X-C-2.xml description: This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefs and the corresponding OCSP in CompleteRevocationRefs.

ASiC-S-X-C-3.xml description: This test case tests the use of AttributeCertificateRefs.

6.1.23 Test cases for ASiC-S_STV_X-EPES TestSet.

ASiC-S-X-EPES-1.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-EPES signature associated to the file specified in SignedData.

ASiC-S-X-EPES-2.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-EPES signature associated to the file specified in SignedData.

6.1.24 Test cases for ASiC-S_STV_X-T TestSet.

ASiC-S-X-T-1.xml description: This test case adds a SignatureTimeStamp.

6.1.25 Test cases for ASiC-S_STV_X-X TestSet.

ASiC-S-X-X-1.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-X signature associated to the file specified in SignedData.

ASiC-S-X-X-2.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-X signature associated to the file specified in SignedData.

ASiC-S-X-X-3.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-X signature associated to the file specified in SignedData.

ASiC-S-X-X-4.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-X signature associated to the file specified in SignedData.

6.1.26 Test cases for ASiC-S_STV_X-XL TestSet.

ASiC-S-X-XL-1.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-XL signature associated to the file specified in SignedData.

ASiC-S-X-XL-2.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-XL signature associated to the file specified in SignedData.

ASiC-S-X-XL-3.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-XL signature associated to the file specified in SignedData.

ASiC-S-X-XL-4.xml description: This test case tests if META-INF/signatures.xml contains a valid XAdES-XL signature associated to the file specified in SignedData.

6.1.27 Test cases for ASiC-E_CSSC_C TestSet.

ASiC-E_CSSC_C-1.xml description: This test case tests if the container has a ZIP format and the content can be successfully extracted (TS 119 164-2 TC/ASiC-E/CS/1)

ASiC-E_CSSC_C-2.xml description: This test case tests if the container if the container format is identifiable using mimetype (TS 119 164-2 TC/ASiC-E/CS/2)

ASiC-E_CSSC_C-3.xml description: This test case tests if the ZIP comment, when used to identify the format, begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension (TS 119 164-2 TC/ASiC-E/CS/3)

ASiC-E_CSSC_C-4.xml description: This test case tests mimetype when set to the signed content mime type (TS 119 164-2 TC/ASiC-E/CS/4)

ASiC-E_CSSC_C-5.xml description: This test case tests if A META-INF folder is present in the root folder containing ASiCManifest2.xml and signature2.p7s and that ASiCManifest2.xml conforms to TS 102 918 clause A.4 (TS 119 164-2 TC/ASiC-E/CS/5, TC/ASiC-E/SC/CT1 and TC/ASiC-E/SC/CT2)

ASiC-E_CSSC_C-6.xml description: This test case tests if the optional MimeType attributes of SigReference elements inside ASiCManifest are coherent to the referenced elements (TS 119 164-2 TC/ASiC-E/SC/CT3)

ASiC-E_CSSC_C-7.xml description: This test case tests an ASiC container including 1 level of long term attributes i.e. an ASiCArchiveManifest and a related Timestamp

ASiC-E_CSSC_C-8.xml description: This test case tests an ASiC container including 2 levels of long term attributes i.e. 2 ASiCArchiveManifests and related Timestamps

6.1.28   Test cases for ASiC-E_CSSC_T TestSet.

ASiC-E_CSSC_T-1.xml description: This test case tests if the container has a ZIP format and the content can be successfully extracted (TS 119 164-2 TC/ASiC-E/CS/1)

ASiC-E_CSSC_T-2.xml description: This test case tests if the container format is identifiable using mimetype (TS 119 164-2 TC/ASiC-E/CS/2)

ASiC-E_CSSC_T-3.xml description: This test case tests if the ZIP comment, when used to identify the format, begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension (TS 119 164-2 TC/ASiC-E/CS/3)

ASiC-E_CSSC_T-4.xml description: This test case tests mimetype when set to the signed content mime type (TS 119 164-2 TC/ASiC-E/CS/4)

ASiC-E_CSSC_T-5.xml description: This test case tests if A META-INF folder is present in the root folder containing ASiCManifest4.xml and timestamp4.tst and that ASiCManifest4.xml conforms to TS 102 918 clause A.4 (TS 119 164-2 TC/ASiC-E/CS/5, TC/ASiC-E/SC/CT1 and TC/ASiC-E/SC/CT2)

ASiC-E_CSSC_T-6.xml description: This test case tests if the optional MimeType attributes of SigReference elements inside ASiCManifest are coherent to the referenced elements (TS 119 164-2 TC/ASiC-E/SC/CT3)

6.1.29   Test cases for ASiC-E_CSSC_X TestSet.

ASiC-E_CSSC_X-1.xml description: This test case tests if the container has a ZIP format and the content can be successfully extracted (TS 119 164-2 TC/ASiC-E/CS/1)

ASiC-E_CSSC_X-2.xml description: This test case tests if the container if the container format is identifiable using mimetype (TS 119 164-2 TC/ASiC-E/CS/2)

ASiC-E_CSSC_X-3.xml description: This test case tests if the ZIP comment, when used to identify the format, begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension (TS 119 164-2 TC/ASiC-E/CS/3)

ASiC-E_CSSC_X-4.xml description: This test case tests mimetype when set to the signed content mime type (TS 119 164-2 TC/ASiC-E/CS/4)

ASiC-E_CSSC_X-5.xml description: This test case tests if A META-INF folder is present in the root folder containing signatures1.xml that conforms to TS 102 918 one of the items 3a, 3b or 3c of 6.2.2 (TS 119 164-2 TC/ASiC-E/CS/5, TC/ASiC-E/SC/X1)

ASiC-E_CSSC_X-6.xml description: This test case tests if container.xml is present in META-INF folder andd that conforms to TS 102 918 clause 6.2.2 point 4b (TS 119 164-2 TC/ASiC-E/CS/5, TC/ASiC-E/SC/X3, TC/ASiC-E/SC/X5)

ASiC-E_CSSC_X-7.xml description: This test case tests if manifest.xml is present in META-INF folder and that conforms to TS 102 918 clause 6.2.2 point 4b (TS 119 164-2 TC/ASiC-E/CS/5, TC/ASiC-E/SC/X3, TC/ASiC-E/SC/X4)

ASiC-E_CSSC_X-8.xml description: This test case tests if container.xml is present in META-INF folder and that conforms to TS 102 918 clause 6.2.2 point 4b (TS 119 164-2 TC/ASiC-E/CS/5, TC/ASiC-E/SC/X4, TC/ASiC-E/SC/X5)

ASiC-E_CSSC_X-9.xml description: This test case tests if All mime types present in manifest.xml metadata are coherent with referenced objects (TS 119 164-2 TC/ASiC-E/SC/X6)

6.1.30 Test cases for ASiC-E_STV_T TestSet.

ASiC-E_STV_T-1.xml description: This test case tests if the metadata timestamp1.tst contains a valid RFC3161 time-stamp token that is verified correctly on the ASiCManifest metadata. The references contained in ASiCManifest refer correctly the data objects and their hashes. (TS 119 164-2 TC/ASiC-E/STV/T1) Test cases for ASiC-E_STV_C-A TestSet.

6.1.31 Test cases for ASiC-E_STV_C-BES TestSet.

ASiC-E-C-BES-1.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests the simplest CAdES-BES *WITHOUT* SigningTime.

ASiC-E-C-BES-2.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests the simplest CAdES-BES *WITH* SigningTime.

ASiC-E-C-BES-3.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests CAdES-BES with a SignerAttributes containing a CertifiedAttribute.

ASiC-E-C-BES-4.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests CAdES-BES with a ContentTimeStamp attribute.

ASiC-E-C-BES-6.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests CAdES-BES with multiple independent signatures. The input to this test is a CAdES-BES signature as specified in C-BES-1 test case.

ASiC-E-C-BES-7.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests CAdES-BES with following attributes at once: - MessageDigest - SigningTime - ESSSigningCertificateV2 - SignerLocation - SignerAttributes (only Claimed Attributes included) - ContentType - ContentHints - ContentIdentifier - CommitmentTypeIndication

6.1.32 Test cases for ASiC-E_STV_C-BpB TestSet.

ASiC-E-CBp-B-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level B test case. The signature ONLY CONTAINS the mandatory CAdES properties, namely: ContentType, SigningTime, SigningCertificate and ESSSigningCertificateV2.

ASiC-E-CBp-B-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile In this CAdES Baseline Profile conformance level B test case the signature contains a CertifiedAttribute in addition to all mandatory attributes.

ASiC-E-CBp-B-3.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile This test case tests a CAdES Baseline Profile conformance level B signature with CounterSignature attribute. The input to this test is a CAdES-BES signature as specified in CBp-B-1 test case.

ASiC-E-CBp-B-4.xml description: This test case tests the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile This test case tests CAdES Baseline Profile conformance level B with multiple independent signatures. The input to this test is a CAdES-BES signature as specified in CBp-B-1 test case.

6.1.33 Test cases for ASiC-E_STV_C-BpLT TestSet.

ASiC-E-CBp-LT-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level LT test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES Baseline Profile conformance level B and a SignatureTimeStamp 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.

ASiC-E-CBp-LT-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level LT test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES Baseline Profile conformance level B and a SignatureTimeStamp 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

ASiC-E-CBp-LT-3.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is a CAdES Baseline Profile conformance level LT test case. The signature contains the mandatory CAdES properties for CAdES Baseline Profile conformance level B, one attribute certificate and a SignatureTimeStamp 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.

ASiC-E-CBp-LT-4.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LT level of ASiC Baseline profile This is a CAdES Baseline Profile conformance level LT test case. The signature contains the mandatory CAdES properties for CAdES Baseline Profile conformance level B, one attribute certificate and a SignatureTimeStamp 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

6.1.34 Test cases for ASiC-E_STV_C-BpLTA TestSet.

ASiC-E-CBp-LTA-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile This test case is based on ASiC-E-CBp-LT-1 Test Case adding Long Term attributes (ASiCArchiveManifest and the related archive time stamp)

ASiC-E-CBp-LTA-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile This test case is based on ASiC-E-CBp-LT-2 Test Case adding Long Term attributes (ASiCArchiveManifest and the related archive time stamp)

ASiC-E-CBp-LTA-3.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile This test case is based on ASiC-E-CBp-LT-3 Test Case adding Long Term attributes (ASiCArchiveManifest and the related archive time stamp)

ASiC-E-CBp-LTA-4.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile This test case is based on ASiC-E-CBp-LT-4 Test Case adding Long Term attributes (ASiCArchiveManifest and the related archive time stamp)

ASiC-E-CBp-LTA-5.xml description: This test case tests the signature of an ASiC container claiming conformnce to the LTA level of ASiC Baseline profile This test case is based on ASiC-E-CBp-LT-1 Test Case adding 2 levels Long Term attributes (2 ASiCArchiveManifests and the related archive time stamps)

6.1.35 Test cases for ASiC-E_STV_C-BpT TestSet.

ASiC-E-CBp-T-1.xml description: This test case tests the signature of an ASiC container claiming conformnce to the T level of ASiC Baseline profile This is the simplest CAdES Baseline Profile conformance level T test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES Baseline Profile conformance level B and a SignatureTimeStamp attribute

ASiC-E-CBp-T-2.xml description: This test case tests the signature of an ASiC container claiming conformnce to the T level of ASiC Baseline profile A CAdES Baseline Profile signature for testing conformance level T. This test case tests

the adding of an indipendent CAdES Baseline Profile signature level T to an already signed document in CAdES Baseline Profile signature level T format. The input to this test is a CAdES-T signature as specified in CBp-T-1 test case.

6.1.36 Test cases for ASiC-E_STV_C-C TestSet.

ASiC-E-C-C-1.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-C conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-C format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only CRLListIDs must be included.

ASiC-E-C-C-2.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-C conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-C format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only OcspListIDs must be included. Every OcspListID must include the ocspIdentifier and the ocspRepHash elements.

6.1.37 Test cases for ASiC-E_STV_C-EPES TestSet.

ASiC-E-C-EPES-1.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-EPES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests the simplest CAdES-EPES form. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI5.der' shall be used as its input.

ASiC-E-C-EPES-2.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-EPES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests CAdES-EPES with following attributes at once: - MessageDigest - SigningTime - ESSSigningCertificateV2 - SignaturePolicyIdentifier - SignerLocation - ContentType - CommitmentTypeIndication. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI5.der' shall be used as its input.

ASiC-E-C-EPES-3.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-EPES conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests the CAdES-EPES form. To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI5.der' shall be used as its input. The sigPolicyQualifiers must include the oid of sp-user-notice (1.2.840.113549.1.9.16.5.2) and a UTF8String as explicitText.

6.1.38 Test cases for ASiC-E_STV_C-T TestSet.

ASiC-E-C-T-1.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-T conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests the simplest CAdES-T format.

ASiC-E-C-T-2.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-T conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests the adding of an indipendent CAdES-T signature to an already signed document in CAdES-T format. The input to this test is a CAdES-T signature as specified in C-T-1 test case to which a new SignerInfo instance will be added containing the other CAdES-T signature

6.1.39 Test cases for ASiC-E_STV_C-X TestSet.

ASiC-E-C-X-1.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-X conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-X Type1 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only CRLListIDs must be included.

ASiC-E-C-X-2.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-X conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-X Type2 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only CRLListIDs must be included.

ASiC-E-C-X-3.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-X conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-X Type1 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only OcspListIDs must be included. Every OcspListID must include the ocspIdentifier and the ocspRepHash elements.

ASiC-E-C-X-4.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-X conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-X Type2 format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue must be included. In the CompleteRevocationRefs only OcspListIDs must be included. Every OcspListID must include the ocspIdentifier and the ocspRepHash elements.

6.1.40   Test cases for ASiC-E_STV_C-XL TestSet.

ASiC-E-C-XL-1.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-C conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-XL Type1 format. Its CompleteRevocationRefs must have only CRLListIDs and its RevocationValues must have only crlVals element.

ASiC-E-C-XL-2.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-C conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-XL Type2 format. Its CompleteRevocationRefs must have only CRLListIDs and its RevocationValues must have only crlVals element.

ASiC-E-C-XL-3.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-C conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-XL Type1 format. In the CompleteRevocationRefs only OcspListIDs must be included and RevocationValues must have only ocspVals element.

ASiC-E-C-XL-4.xml description: This test case tests if the metadata whose name matches signature1.p7s contains a valid CAdES-C conformant signature that is verified correctly on the related ASiCManifest1.xml metadata. This test case tests a CAdES-XL Type2 format. In the CompleteRevocationRefs only OcspListIDs must be included and RevocationValues must have only ocspVals element.

6.1.41   Test cases for ASiC-E_STV_X-A TestSet.

ASiC-E-X-A-1.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-2.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-3.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-4.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-5.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-6.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-7.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-8.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

ASiC-E-X-A-9.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-A signature that is verified correctly on the referenced data object

6.1.42 Test cases for ASiC-E_STV_X-BES TestSet.

ASiC-E-X-BES-1.xml description: This test case tests an external SigningCertificate (i.e. the URI Attribute is referring to a certificate file outside the signature and the Certificate in the ds:KeyInfo shall be ignored).

ASiC-E-X-BES-2.xml description: This test case tests an external SigningCertificate and has the SigningTime property that lies within the validity of the certificate.

ASiC-E-X-BES-3.xml description: This test case tests an external SigningCertificate, no uri is given for the SigningCertificate any more. The SigningTime should be checked against the validity period of the certificates. A SignatureProductionPlace property is provided.

ASiC-E-X-BES-4.xml description: This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property. Now also the SignerRole with a ClaimedRole is added.

ASiC-E-X-BES-5.xml description: This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property. Now also the SignerRole with a CertifiedRole is added.

ASiC-E-X-BES-6.xml description: This is a test for DataObjectFormat. The DataObjectFormat should point to a ds:Reference whose URI attribute points to a simple text file outside of the document containing the signature. MimeType and Encoding do not have to be checked in this case.

ASiC-E-X-BES-7.xml description: This is a test for DataObjectFormat, the reference should point to a ds:Object that contains the MimeType and Encoding in a non contradicting way. To use #Reference-Id-6-4 is just a suggestion.

ASiC-E-X-BES-8.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-BES signature that is verified correctly on the referenced data object

ASiC-E-X-BES-9.xml description: This is to test the IndividualDataObjectsTimeStamp.

ASiC-E-X-BES-10.xml description: This is to test the AllDataObjectsTimeStamp.

ASiC-E-X-BES-11.xml description: This is to test the CounterSignature, for simplicity it is signed by the same party.

ASiC-E-X-BES-15.xml description: This is to test all BES Properties, except CounterSignature.

6.1.43 Test cases for ASiC-E_STV_X-BpB TestSet.

ASiC-E-XBp-B-1.xml description: This is the simplest XAdES Baseline Profile conformance level B test case. The signature ONLY CONTAINS the mandatory XAdES properties, namely: xades:SigningTime, xades:SigningCertifiateThe and xades:DataObjectFormat. The signature only signs the XAdES signed properties and ONE document: a text file. The xades:DataObjectFormat should point to a ds:Reference whose URI attribute points to the signed simple text file.

ASiC-E-XBp-B-2.xml description: This is the simplest XAdES Baseline Profile conformance level B test case, with TWO signed data objects apart from the signed XAdES properties. This brings the presence of two xades:DataObjectFormat elements

ASiC-E-XBp-B-3.xml description: Signature for testing XAdES Baseline Profile conformance level B with ONE signed data object apart from the signed XAdES properties, the corresponding xades:DataObjectFormat, and one attribute certificate.

6.1.44 Test cases for ASiC-E_STV_X-BpLT TestSet.

ASiC-E-XBp-LT-1.xml description: A signature for testing the simpletst case of XAdES Baseline Profile conformance level LT. ONE signed data object, ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are CRLs.

ASiC-E-XBp-LT-2.xml description: A signature for testing the simpletst case of XAdES Baseline Profile conformance level LT. ONE signed data object, ONE xades:SignatureTimeStamp container, one xades:CertificateValues and one xades:RevocationValues. No attribute certificates are present. The revocation material used are OCSP responses.

ASiC-E-XBp-LT-3.xml description: A signature for testing XAdES Baseline Profile conformance level LT. One signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, and one xades:RevocationValues. The revocation material used are CRLs.

ASiC-E-XBp-LT-4.xml description: A signature for testing XAdES Baseline Profile conformance level LT. One signed data object, one attribute certificate, one xades:SignatureTimeStamp container, one xades:CertificateValues, one AttrAuthoritiesCertValues, one xades:RevocationValues, and one xades:AttributeRevocationValues. The revocation material used are OCSP responses.

6.1.45 Test cases for ASiC-E_STV_X-BpLTA TestSet.

ASiC-E-XBp-LTA-1.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. Iin this case there is one signed data object, one xades:SignatureTimeStamp container, one xades:CertificateValues, one xades:RevocationValues, and one xades:ArchiveTimeStamp container. No attribute certificates are present. No xadesv141:ArchiveTimeStamp and no xadesv141:TimeStampValidationData elements. The revocation material used are CRLs.

ASiC-E-XBp-LTA-2.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again with a xades:ArchiveTimeStamp. The validation material corresponding to the first xades:ArchiveTimeStamp is included within time-stamp token itself. The revocation material used are CRLs.

ASiC-E-XBp-LTA-3.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are CRLs.

ASiC-E-XBp-LTA-4.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. Iin this case there is one signed data object, one xades:SignatureTimeStamp container, one xades:CertificateValues, one xades:RevocationValues, and one xades:ArchiveTimeStamp container. No attribute certificates are present. No xadesv141:ArchiveTimeStamp and no xadesv141:TimeStampValidationData elements. The revocation material used are OCSP responses.

ASiC-E-XBp-LTA-5.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again with a xades:ArchiveTimeStamp. The validation material corresponding to the first xades:ArchiveTimeStamp is included within time-stamp token itself. The revocation material used are OCSP responses.

ASiC-E-XBp-LTA-6.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are OCSP responses.

ASiC-E-XBp-LTA-7.xml description: A signature for testing XAdES Baseline Profile conformance level LTA. In this case the LT-Level signature was time-stamped with a xades:ArchiveTimeStamp. Afterwards, the resulting LTA-Level signature is time-stamped again, but this time with a xadesv141:ArchiveTimeStamp. The validation material corresponding to the xades:ArchiveTimeStamp is included within a xadesv141:TimeStampValidationData. The revocation material used are both CRLs and OCSP responses depending on the certificates.

6.1.46 Test cases for ASiC-E_STV_X-BpT TestSet.

ASiC-E-XBp-T-1.xml description: A signature for testing the simpletst case of XAdES Baseline Profile conformance level T. ONE signed data object and ONE xades:SignatureTimeStamp container.

ASiC-E-XBp-T-2.xml description: A XAdES Baseline Profile signature for testing conformance level T. ONE signed data object and TWO xades:SignatureTimeStamp containers.

6.1.47   Test cases for ASiC-E_STV_X-C TestSet.

ASiC-E-X-C-1.xml description: This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefs and the corresponding CRLs in CompleteRevocationRefs.

ASiC-E-X-C-2.xml description: This test case has a SignatureTimeStamp and tests the use of CompleteCertificateRefs and the corresponding OCSP in CompleteRevocationRefs.

ASiC-E-X-C-3.xml description: This test case tests the use of AttributeCertificateRefs.

6.1.48   Test cases for ASiC-E_STV_X-EPES TestSet.

ASiC-E-X-EPES-1.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-EPES signature that is verified correctly on the referenced data object

ASiC-E-X-EPES-2.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-EPES signature that is verified correctly on the referenced data object

6.1.49   Test cases for ASiC-E_STV_X-T TestSet.

ASiC-E-X-T-1.xml description: This test case adds a SignatureTimeStamp.

6.1.50   Test cases for ASiC-E_STV_X-X TestSet.

ASiC-E-X-X-1.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-X signature that is verified correctly on the referenced data object

ASiC-E-X-X-2.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-X signature that is verified correctly on the referenced data object

ASiC-E-X-X-3.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-X signature that is verified correctly on the referenced data object

ASiC-E-X-X-4.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-X signature that is verified correctly on the referenced data object

6.1.51   Test cases for ASiC-E_STV_X-XL TestSet.

ASiC-E-X-XL-1.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-XL signature that is verified correctly on the referenced data object

ASiC-E-X-XL-2.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-XL signature that is verified correctly on the referenced data object

ASiC-E-X-XL-3.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-XL signature that is verified correctly on the referenced data object

ASiC-E-X-XL-4.xml description: This test case tests that the metadata signatures.xml contains a valid XAdES-XL signature that is verified correctly on the referenced data object

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.

Negative test cases files are in the 'NegativeTests' folder grouped by ASiC TestSet.

6.2.1 Negative test cases for ASiC-S_STV_C (TestSet ASiC-S_STV_CN).

ASiC-S_STV_CN-1.xml description: Negative test case with CAdES-BES One CAdES signature Correct signing cert. Signed document modified

ASiC-S_STV_CN-2.xml description: Negative test case with CAdES-BES Two parallel CAdES signatures First signature with correct signing cert. Second signature with revoked signing cert.

ASiC-S_STV_CN-3.xml description: Negative test case with CAdES-BES Two CAdES signatures First signature with correct signing cert. Second signature with revoked signing cert. First signature as in ASiC-S_STV_CN-1 test definition

6.2.2 Negative test cases for ASiC-S_STV_CBp (TestSet ASiC-S_STV_CBpN).

ASiC-S_STV_CBpN-1.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One CAdES signature. Signature with correct signing cert. Error source: the CAdES signature does not contain the mandatory attribute sigining-time.

ASiC-S_STV_CBpN-2.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One CAdES signature. Signature with signature-time-stamp unsigned attribute (T-conformance level) Signature with revoked signing cert.

6.2.3 Negative test cases for ASiC-S_STV_T (TestSet ASiC-S_STV_TN).

ASiC-S_STV_TN-1.xml description: This negative test case tests if META-INF/timestamp.tst contains a valid time-stamp token that does not apply to the file specified in

6.2.4 Negative test cases for ASiC-S_STV_X (TestSet ASiC-S_STV_XN).

ASiC-S_STV_XN-1.xml description: Negative test case with XAdES-BES Correct signing certificate. Signed document changed.

ASiC-S_STV_XN-2.xml description: Negative test case with XAdES-BES Two signatures. One with the correct signing certificate. The other with a revoked signing certificate.

ASiC-S_STV_XN-3.xml description: Negative test case with XAdES-BES Two signatures. One with the correct signing certificate (as in ASIC-S_STV_XN-1). The other with a signing certificate whose CA issuer has a revoked certificate. XML files specifying the signatures details: ASiC-S_STV-XN-3_1.xml and ASiC-S_STV-XN-3_2.xml

ASiC-S_STV_XN-4.xml description: Negative test case with XAdES-BES Two signatures. One with the correct signing certificate. The other with an expired signing certificate.

6.2.5 Negative test cases for ASiC-S_STV_XBp (TestSet ASiC-S_STV_XBpN).

ASiC-S_STV_XBpN-1.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature. Correct signing certificate. NO DataObjectFormat mandatory property.

ASiC-S_STV_XBpN-2.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature. NO DataObjectFormat mandatory property and revoked signing certificate. XAdES signature with SignatureTimeStamp.

ASiC-S_STV_XBpN-3.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature. XAdES signature with signature time-stamp, CertificateValues, and RevocationValues NO DataObjectFormat mandatory property and revoked signing certificate.

ASiC-S_STV_XBpN-4.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature. XAdES signature with signature time-stamp, CertificateValues, RevocationValues, and xades:ArchiveTimeStamp (this is also an error) NO DataObjectFormat mandatory property and revoked signing certificate.

6.2.6 Negative test cases for ASiC-E_STV_C (TestSet ASiC-E_STV_CN).

ASiC-E_STV_CN-1.xml description: Negative test case with CAdES-BES One CAdES signature Correct signing cert. The signature signs file ASiCManifest1.xml, and the file within the package is ASiCManifest1-modified.xml

ASiC-E_STV_CN-2.xml description: Negative test case with CAdES-BES Two parallel CAdES signature First signature with correct signing cert. Second signature with revoked signing cert. The signature signs file ASiCManifest2.xml, and the file within the package is ASiCManifest2.xml

ASiC-E_STV_CN-3.xml description: Negative test case with CAdES-BES Two CAdES signatures First signature with correct signing cert. Second signature with revoked signing cert. The signatures sign file ASiCManifest6.xml, and the file within the package is ASiCManifest6.xml First signature as in ASiC-S_STV_CN-1 test definition

ASiC-E_STV_CN-4.xml description: Negative test case with CAdES-BES Two CAdES signatures First signature with correct signing cert. Second signature with signing cert issued by a CA whose certificate is revoked. The second signature contains references to certificates in the cert path and to revocation lists. The signatures sign file ASiCManifest7.xml, and the file within the package is ASiCManifest7.xml First signature as in ASiC-S_STV_CN-1 test definition

6.2.7 Negative test cases for ASiC-E_STV_CBp (TestSet ASiC-E_STV_CNBp).

ASiC-E_STV_CBpN-1.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile. One CAdES signature. Signature with correct signing cert. Error source: the CAdES signature does not contain the mandatory attribute siging-time. The signatures sign file ASiCManifest2.xml, and the file within the package is ASiCManifest2.xml

ASiC-E_STV_CBpN-2.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile. One CAdES signature. Signature with signature-time-stamp unsigned attribute (T-conformance level) Signature with revoked signing cert. No mandatory attribute signing-time. The signature signs file ASiCManifest2.xml, and the file within the package is ASiCManifest2.xml

6.2.8 Negative test cases for ASiC-E_STV_T (TestSet ASiC-E_STV_TN).

ASiC-E_STV_TN-1.xml description: This test case tests if the metadata timestamp5.tst contains a valid RFC3161 time-stamp token that that fails verification on the ASiCManifest metadata. (TS 119 164-2 TC/ASiC-E/STV/NT1)

ASiC-E_STV_TN-2.xml description: This test case tests if the metadata timestamp5.tst contains a valid RFC3161 time-stamp token that is verified correctly on the ASiCManifest metadata but the verification fails on the modified data object. (TS 119 164-2 TC/ASiC-E/STV/NT2)

6.2.9 Negative test cases for ASiC-E_STV_X (TestSet ASiC-E_STV_XN).

ASiC-E_STV_XN-1.xml description: Negative test case with XAdES-BES Correct signing certificate. One of the two signed documents is changed.

ASiC-E_STV_XN-2.xml description: Negative test case with XAdES-BES Two signatures. One with the correct signing certificate. The other with a revoked signing certificate.

ASiC-E_STV_XN-3.xml description: Negative test case with XAdES-BES Two signatures. One with the correct signing certificate (as in ASIC-S_STV_XN-1). The other with a signing certificate whose CA issuer has a revoked certificate. XML files specifying the signatures details: ASiC-S_STV-XN-3_1.xml and ASiC-S_STV-XN-3_2.xml

ASiC-E_STV_XN-4.xml description: Negative test case with XAdES-BES Two signatures. One with the correct signing certificate. The other with an expired signing certificate.

6.2.10 Negative test cases for ASiC-E_STV_XBp (TestSet ASiC-E_STV_XBpN).

ASiC-E_STV_XBpN-1.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature on two data objects. Correct signing certificate. NO DataObjectFormat mandatory property.

ASiC-E_STV_XBpN-2.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature on two data objects. NO DataObjectFormat mandatory property and revoked signing certificate XAdES signature with SignatureTimeStamp.

ASiC-E_STV_XBpN-3.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature on two data objects. XAdES signature with signature time-stamp, CertificateValues, and RevocationValues NO DataObjectFormat mandatory property and revoked signing certificate.

ASiC-E_STV_XBpN-4.xml description: This is a negative test case to test the signature of an ASiC container claiming conformnce to the B level of ASiC Baseline profile One signature on two data objects. XAdES signature with signature time-stamp, CertificateValues, RevocationValues, and xades:ArchiveTimeStamp (this is also an error) NO DataObjectFormat mandatory property and revoked signing certificate.