Technical Report of the CAdES Remote Plugtests™ Event (Dec 2013)

ETSI

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

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

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

Reference

Keywords
Electronic Signature,

January 2014

Version 1.0

Author:

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

Editor:

Laurent Velez, ETSI laurent.velez@etsi.org

Abstract

This document is the technical report of the 2013 remote Plugtests event on CAdES (CMS Advanced Electronic Signature ETSI TS 101733), organized by ETSIs Centre of Testing and Interoperability (CTI) conducted using the specifically designed ETSI portal which supports remote interoperability Plugtests.

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

Status of this Document

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

.

Contents

1 Introduction

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

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

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

The ETSI TS 119 124 "CAdES Testing Conformance & Interoperability" currently being prepared by the STF 459 is the basis of the testing proposed at the CAdES Plugtests 2013 interoperability event.

This Plugtests event is the first 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 will address interoperability and conformance needs for all the AdES signatures defined by ETSI.

ETSI has organized the remote Plugtests event on CAdES, held from Monday 2nd December to Friday 20th December 2013. This remote event aims at conducting interoperability test cases on CAdES signatures (CMS Advanced Electronic Signature ETSI TS 101 733) V2.2.1 and also the CAdES Baseline Profile TS 103 173 V2.2.1. It takes into account the introduction of new Archive Time Stamp attribute V3.

This testing provides full test coverage of the specifications including testing signatures evolution, simulating real life situations

The present document is the report from the 2013 remote Plugtests Event on CAdES Signatures. It also provides details on the specification, design and implementation of the portal supporting remote Plugtests events on CAdES 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 CAdES Remote Plugtests.

The present report provides details on:

- Specification, design and implementation of those testcases description, including cross-verification and negative testcases for CAdES signatures, based on ETSI TS 119 124 "CAdES Testing Conformance& Interoperability
- The Remote Plugtests Event on CAdES was organized by ETSI and held from Monday 2nd November to Friday 20th December 2013.

In order to give participants time to prepare the testing, ETSI opened the portal to participants in "read-only" mode on 25th November, a week before the official start date of the Plugtests event. An introduction web conference took place on Monday 25th to present the portal and the testing.

The event was initially planned to run until 13th December but it was extended to 20th December on request from the participants. The reason being that the amount of testing activities was extremely high within the initial scheduled period, due to the large number of participants and the number of test descriptions proposed.

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 2013 CAdES Remote Plugtests Event.

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

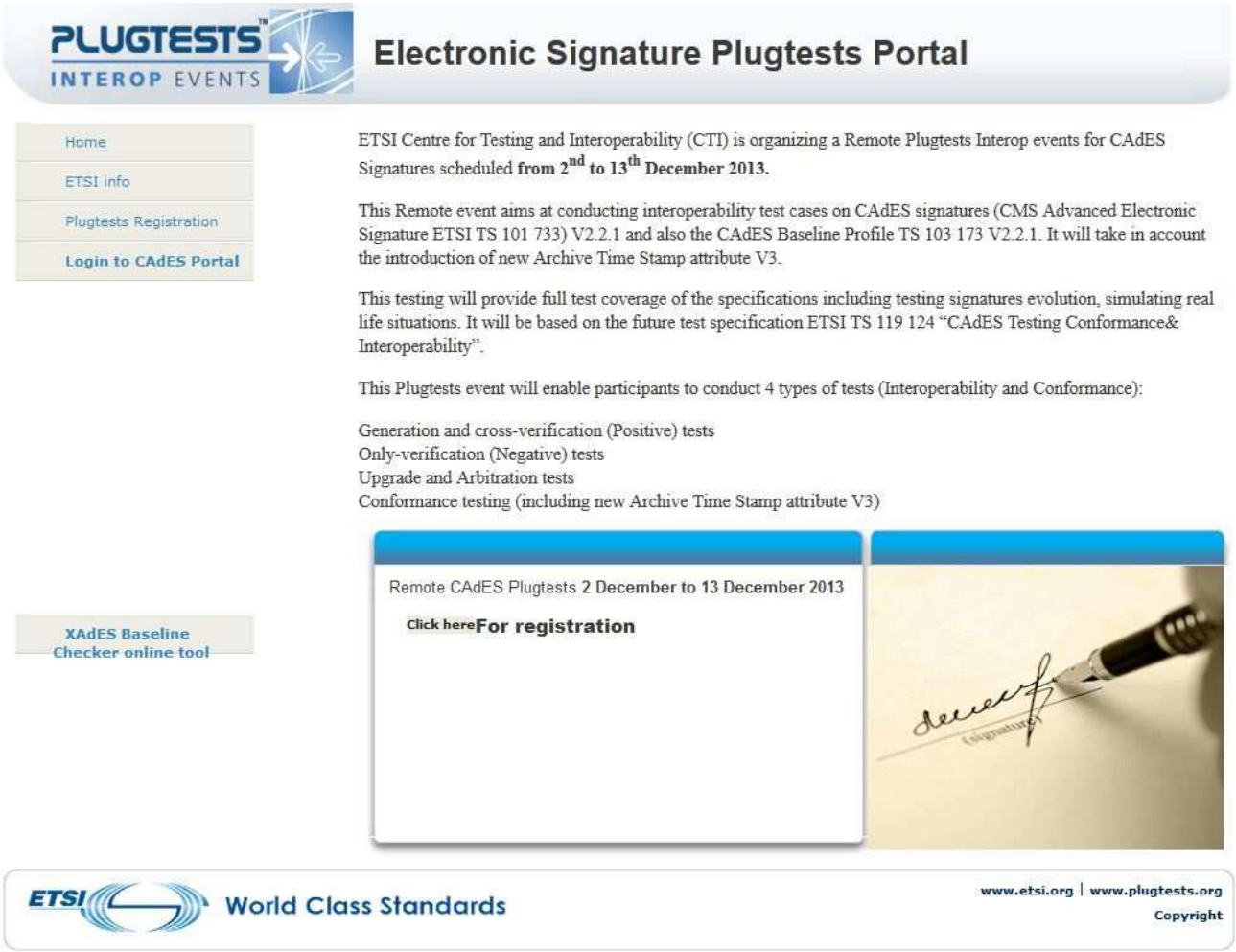
Section 5 provides details on a number of issues related to the CAdES specifications as identified by the participants. These issues have been raised to the ETSI TC ESI, with the recommendation that they are taken into consideration for future CAdES standardization activities.

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

2 Organization and contents of the portal

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

2.1 Public part of the portal



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

- The CAdES Plugtests page, providing some more details on the event itself, namely targeted specification, targeted audience, some general info on how to conduct such event, etc.

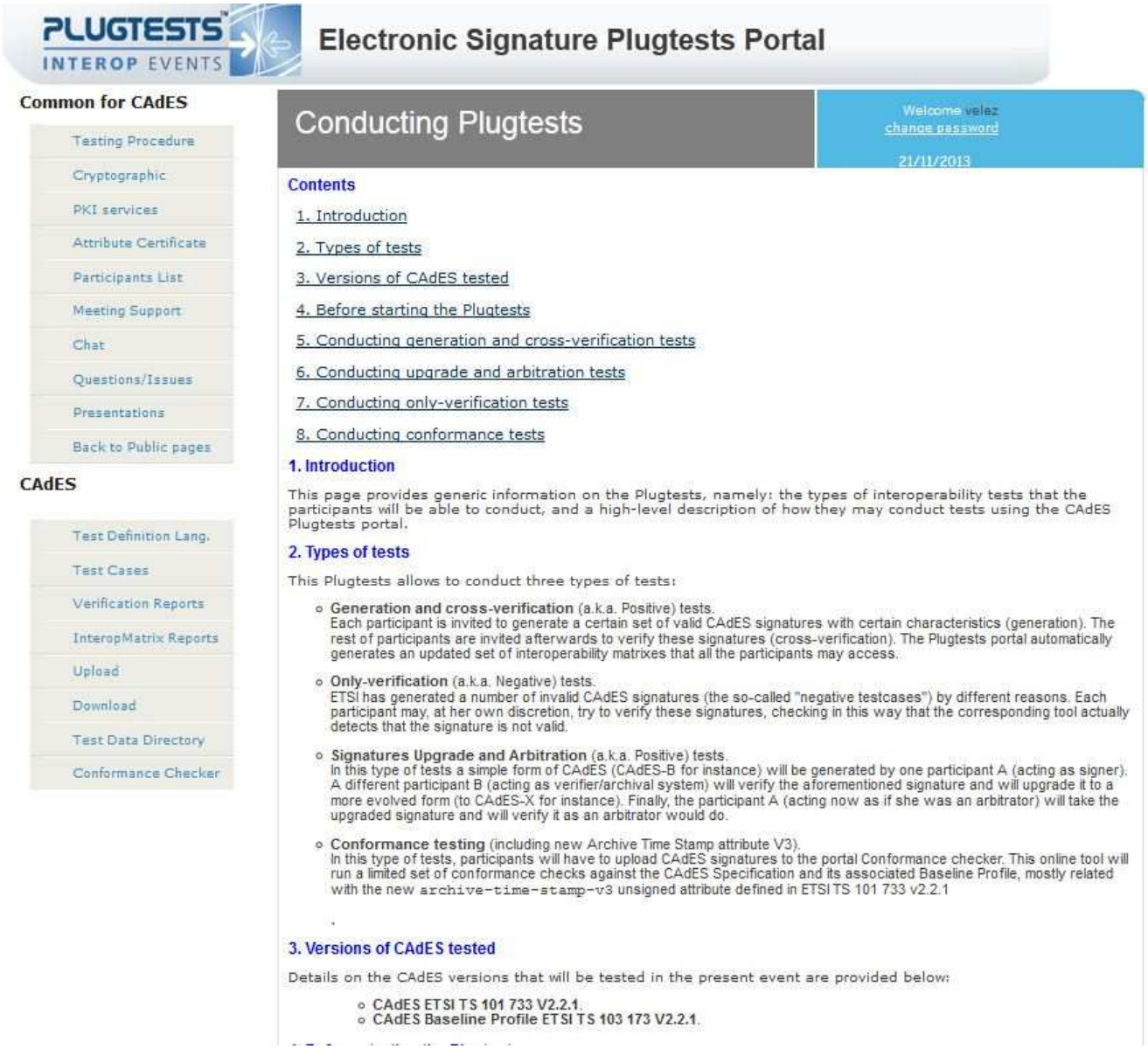
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating exchange of information.
- The Registration page, providing details on the Plugtests registration process.
- The Presentation of the Plugtests team.
- The Presentation of some past events (XAdES, CAdES, PAdES, ASiC)
- The **Login to Plugtests Area** page gives access to the **protected area** of the portal.

2.2 Private part of the portal

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

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

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



2.2.1 Contents of Common area of Private part

2.2.1.1 Conducting Plugtests information pages

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

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

- Generation and cross-verification (a.k.a. Positive) tests.

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

- Only-verification (a.k.a. Negative) tests.

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

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

 Conformance testing (including new Archive Time Stamp attribute V3).
In this type of tests, participants will have to upload CAdES signatures to the portal Conformance checker. This online tool will run a limited set of conformance checks against the CAdES Specification and its associated Baseline Profile, mostly related with the new archive-time-stamp-v3 unsigned attribute defined in ETSI TS 101 733 v2.2.1

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

- CAdES ETSI TS 101 733 V2.2.1.
- CAdES Baseline Profile ETSI TS 103 173 V2.2.1.

It also provides high level description of the steps that participants must perform for conducting the 4 different types of interoperability tests aforementioned and the Conformance checker tool.

The rest of pages of the set provide details on:

- How to download material from the portal for starting conducting the Plugtests (**Downloading material page**). This material is usually a zip file enclosing a well defined folder structure containing both signatures and verification reports on signatures.
- How to generate CAdES 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 CAdES 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.

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 CAdES signatures.
- **Time-stamp Authority server**. This server generates RFC 3161 time-stamp tokens as per request of the participants in the plugtest.
- **OCSP responders**, which are able to generate OCSP responses to OCSP requests submitted by the participants on the status of a certain certificate generated by the ETSI portal infrastructure. During this Plugtest, these OCSP responders will actually be the CAs issuing certificates (Direct Trust Model).

- **LDAP server**. This server acts as central repository for CA and TSA certificates, and CRLs.
- **Http server.** This server acts as alternative central repository for CA and TSA certificates, and CRLs.

This page also contains a link to a Java class implementing basic login/password authentication mechanism required for accessing these services, so that participants had not to develop such a mechanisms in their tools.

2.2.1.4 Online PKI services access page

The Online PKI Services access page allows to access to most of the on-line PKI-related services provided by the portal, namely: access to the CA software for requesting generation of a key-pair and the corresponding end-entity certificate for generating signatures, connection details for accessing the LDAP server where CRLs and CA certificates are stored, etc.

2.2.1.5 Online TSA services access page

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

2.2.1.6 Attribute certificate issuance page

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

Therefore the participants can issue their own attribute certificate for themselves by some security toolkits. However the Plugtests service can also issue the attribute certificate if required by the participants. The portal has integrated a tool allowing participants to upload their X509 certificates and generate the corresponding attribute certificates (‘Attribute Certificate Request’ section on the left menubar)

2.2.1.7 Participants’ List page

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

2.2.1.8 Meeting Support page

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

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

2.2.1.9 Mailing list

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

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

2.2.1.10 Chat page

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

2.2.1.11 Known issues pages

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

2.2.2 Contents of CAdES Interop Specific areas of Private part

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

2.2.2.1 Test Cases Definition Language

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

2.2.2.2 Test Cases pages

These are pages containing documents with the complete specification of the test cases for the CAdES 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 CAdES signature verified by each participant, process them and keep up to date the interoperability matrixes, which show what signatures of each participant have been verified by what other participants and the results of such verifications.

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

2.2.2.3 Individual verification reports

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

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

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

2.2.2.4 InteropMatrix reports

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

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

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

2.2.2.5 Statistics per signature form

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

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

2.2.2.6 Upload pages

This area contains a page that participants use for uploading their signatures and / or verification reports.

The Upload pages provide mechanisms for uploading new signatures, new verification reports or both.

Once uploaded, the portal re-builds a new downloading package in the CAdES area and makes it available for all the participants at the Download page. Within this package, participants will find all the signatures and verification reports generated up to that moment in the Plugtests. It is way to archive all the different uploads and keep a complete history of the interop testing of the event.

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

2.2.2.7 Download pages

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

These pages are also used for downloading the entire material generated by the participants at any precise moment during the event including all the CAdES signatures and verification reports generated thus far.

2.2.2.8 Test data directory pages

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

3 Participants list

The table below shows the details of all the organizations and people who have participated in the 2013 CAdES remote Plugtests event.

There were **62 different organizations** and 109 people participating in the event.

Company	Acronym	Name	Surname
ACTALIS S.p.A.	ACT	Mr. Simone	Baldini
ARDACO, a.s.	ARD	Ing. Juraj	Hájek
		Ing. Vladimír	Krajcovic
ARHS	ARHS	Mr. Yannick	Vincent
		Mr. Robert	Bielecki
Aruba Posta Elettronica Certificata S.p.A.	ARU	Mr. Simone	Baldini
Ascertia Limited	ASC	Mr. Yasir	Khan
Bit4id	BIT	Ing. Marco	Scognamiglio
		Fabrizio	Balsamo
		Daniele	Cinque
		Vincenzo	Del Gatto
Biznet Bilisim	BIZ	Mr. Fatih	Tuna
		Mr. Mehmet Onur	Atci
Bremen online services (bos)	BOS	Mr. Alexander	Funk
BULL S.A.S	BULL	Ms. Fanny	Puaud
CAOC	CAO	Mr. Daniel	Martínez
CERTSIGN S.A.	CERT	Mr. Mihai	Togan
Comfact AB	COM	Mr. Anders	Tornqvist
Cryptolog International	CRY	Dr. Moez	Ben Mbarka
		Miss Kahdija	Ferjani
		Dr. Andrea	Rock
DICTAO	DIC	Mr. Mehdi	Ben Abdallah
Disig a.s.	DISIG	Mr. Jaroslav	Ondriska
		Ing. Jaroslav	Imrich
		Ing. Tomas	Labuda
Ditec, a.s.	DIT	Ing. Peter	Obeda
		Ing. Marián	Major
		Ing. Michal	Pavlík
		Mr. Róbert	Vittek
e-Contract.be BVBA	ECON	Mr. Frank	Cornelis

E-imza Bilisim	EIMZ	Mr. Mustafa	Bayrak
ELDOS CORPORATION	ELD	Mr. Ken	Ivanov
e-Sec Data Security	ESEC	Mr. Luciano	Coelho
ETSI	ETSI	Laurent	Velez
European Commission	EC	Mrs. Anneli	Andresson
E-VAL Tecnologia em Informática Ltda	EVAL	Mr. Emerson	Tozette
		Miss Carolina	Santos
Gemalto s.r.o	GEM	Ing. Martin	David
Gabinete Nacional de Segurança - Portugal	GNS	Mr. Paulo	Balsinhas
Hellenic Ministry of Administrative Reform and e-Gov	HEL	Mr. Georgois	Katsikogiannis
IAIK	IAIK	Konrad	Lanz
I.T. Telecom S.r.l.	ITT	Ing. Gianluca	Tovo
IBM Slovakia, Ltd.	IBM	Mr. Attila	Szlovák
ICBPI S.p.A.	ICBPI	Ing. Fabio	Omenigrandi
ID Solutions Aps	IDS	Mr. Rune	Kock
IN.TE.S.A. S.p.A.	INT	Mr. Antonio	Raia
InfoCert s.p.a.	INF	Ing. Fabio	Capocasa
		Luigi	Rizzo
Intesa Sanpaolo S.p.A.	ISS	Mr. Stefano	Vercesi
		Ms. Laura	Cassinerio
		Marcello	Mazzoni
		Mr. Maurizio	Sisto
Intesi Group	INTESI	Mr. Giuseppe	Damiano
Izenpe S.A.	IZEN	Mr. Iñigo	Barreira
		Mrs. Isabel	Lumbreras
Keensoft	KEEN	Mr. Angel	Borroy
		Mr. Daniel Emilio	Fernández
		Mr. José Antonio	Matute
		Mr. Santiago	Navarro
Keeper Tech	KEEP	Mr. Jaime	Hablutzel
LangEdge,Inc.	LAN	Mr. Naoto	Miyachi
LEX PERSONA	LEX	Mr. Francois	Devoret

		Mr. Julien	Pasquier
Lombardia Informatica	LOMB	Dr. Luigi	Bongiorni
		Mrs. Doriana	Pepoli
Mentana - Claimsoft GmbH	MEN	Mr. Jürgen	Ludyga
Microsec Ltd	MIC	Ms. Balazs	Czekmany
MID	MID	Mr. Adrian	Aneci
MIT-SOFT UAB	MIT	Dr. Antanas	Mitasiunas
		Dr. Adomas	Birštunas
		Mr. Petras	Petkus
Namirial S.p.A.	NAM	Dr. Giuseppe	Benedetti
Národný bezpecnostný úrad (NSA)	NSA	Ms. Peter	Rybar
Noreg Ltd.	NOREG	Mr. László	Csaba
Polska Wytwórnia Papierów Wartosciowych S.A.	PWPW	Mr. Rafal	Jarosz
		Mr. Mariusz	Golaszewski
		Mr. Jacek	Kucharzewski
		Mr. Artur	Miekina
		Mr. Remigiusz	Swirkaitis
POLYSYS Ltd	POL	Miss Ágnes	Juhász
POSTECOM S.p.A	POST	Marco	Bongiovanni
PrimeKey Solutions AB	PRIM	Mr. Markus	Kilås
		Mr. Marcus	Lundblad
První certifikacní autorita, a.s.	PRV	Ing. Zdenek	Mihula
		Rostislav	Šaler
RENIEC	REN	Dr. Alvaro	Cuno
		Ing. Ricardo	Saavedra
		Mr. Fernando	Veliz
SECOM Co., Ltd.	SECOM	Mr. Masashi	Sato
SeguriData Privada	SEGU	Mr. Juan	Gonzalez
		Mr. Alejandro	Diaz
SIA, Sistemas Informáticos Abiertos	SIA	Mr. Juan Carlos	Moreno de Mingo
		Mr. Juan Carlos	Guerrero
Software602 a.s.	SIX	Mr. Jakub	Zemlicka

Transsped	TRAN	Mr. Adrian	Aneci
Tubitak Uekae	TUB	Mr. Ahmet	Yetgin
		Mr. Murat Yasin	Kubilay
		Mr. Suleyman	Uslu
		Mr. Beytullah	Yigit
UAB INVENTI	INV	Mr. Zilvinas	Kybartas
Unimatica S.p.A.	UNIM	Mr. Silvano	Ghedini
		Mr. Giacomo	Boccardo
		Mr. Fabio	Rubino
Universidad Politécnica de Cataluña	UPC	Mr. Juan Carlos	Cruellas
Unizeto Technologies SmartSign	UNIS	Mr. Robert	Hospodarysko
Unizeto Technologies Webnotarius	UNIW	Mr. Robert	Hospodarysko
Viafirma S.L.	VIA	Mr. Javier	Echeverría Usúa
		Mr. Alexis	Castilla
		Mr. Diego	Fajardo
		Mr. Benito	Galan

4 Plugtests conclusions

4.1 Remote vs. Face to Face

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

With 62 organizations from Europe, Japan, Central and South America participating, it would have been difficult to organise a face to face event

4.2 Communication supporting technologies

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

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

4.3 Event duration

Initially, 2 weeks of testing have been planned for this event, starting from 2nd December to 13th December 2013.

In order to let participants read all the documentations and prepare the testing, ETSI has opened the portal on 25th November, a week before the official beginning of the interoperability event.

Moreover, for this event, 62 companies were registered. As each company has to verify the signature of the others, the time needed increases with the number of companies and it was agreed that 2 weeks was definitely too short. For this reason the Plugtests team decided to extend the duration of the event until the 20th December 2013, however the portal remained accessible to participants until 6 January 2014.

5 CAdES related Issues

The present section lists some of the issues raised during the CAdES Plugtests event in December 2013. This technical report will be provided to ETSI TC ESI which is the technical working group in charge of the standardization of the CAdES Signature.

5.1 Usage of CompleteRevocationRefs

At the Plugtests many participants discussed the right number of CrlOcspRef fields that shall be included in CompleteRevocationRefs.

CAdES specification ETSI 101 733 V2.2.1 states:
The complete-certificate-references attribute is an unsigned attribute. It references the full set of CA certificates that have been used to validate an ES with Complete validation data up to (but not including) the signer's certificate. Only a single instance of this attribute shall occur with an electronic signature.

CompleteRevocationRefs attribute shall contain one CrlOcspRef field for the signing-certificate, followed by one for each OtherCertID in the CompleteCertificateRefs attribute. The second and subsequent CrlOcspRef fields shall be in the same order as the OtherCertID to which they relate. At least one of CRLListID or OcspListID or OtherRevRefs should be present for all but the "trusted" CA of the certificate path.

The question could be raised about the CrlOcspRef for the root CA if the root CA reference is included in the CompleteCertificateRefs attribute. Some Plugtests participants included an empty reference in the CrlOcspRef for the root CA while some other participants didn’t include any reference in the CrlOcspRef for the root CA. The clause "should be present for all but the trusted CA", means that it is required to put into revocation reference CRL/OCSP list for all certificates of the certificate path, but **without** revocation reference for trusted CA on the other hand the clause " followed by one for each OtherCertID in the CompleteCertificateRefs attribute" means that that it is required to put into revocation reference CRL/OCSP list for all certificates whose reference is included in the complete-certificate-references attribute.

5.2 Usage of OCSP responses

Some debate was devoted to which format of the OCSP response is preferable to be stored in the SignedData.OtherRevocationInfoFormat.

1. Identified by id-pkix-ocsp-basic of BasicOCSPResponse defined in clause 4.2.1of RFC 6960

2. Identified by id-ri-ocsp-response of OCSPResponse defined in clause 3 of RFC 5940 and in 4.2.1 of RFC 6960

When id-ri-ocsp-response is used then also some parts of OCSP protocol are included. Status from OCSP protocol is not protected and also not interesting in validation application. Only basic response as a signed object is important.

For that reason the first option id-pkix-ocsp-basic seems to be preferable.

A consequent/similar problem is that ETSI TS 101 733 does not specify what is the input for hash computation for the ocspRepHash field (complete-revocation-references attribute). Some participants used the entire OCSPResponse while other ones used only the BasicOCSPResponse. The same considerations reported above are still valid.

5.3 Usage of RevocationValues

Some participants asked about the correctness of including OCSP responses for TSA in RevocationValues. The problem relates to the correctness of including in RevocationValues any revocation material when the certificate to which it refers is not referenced in CompleteCertificateRefs.
A main conclusion of this topic is that RevocationValues holds the values of CRLs and OCSP referenced in the complete-revocation-references attribute and so revocation material for any certificate not referenced in CompleteCertificateRefs should not be included in RevocationValues (i.e. revocation material for TSA should be included in timestamptoken itself).

5.4 Encoding of ATSHashIndex

Some debate was devoted to which encoding shall be used for ATSHashIndex attribute. It seems that there is no clear requirement about ATSHashIndex BER or DER encoding in CAdES Mother Specification.

5.5 ASN.1 format for Signature Policies

Many participants discussed about the right ASN.1 format for Signature Policies. The main debate concerned from which data the hash value of the signature policy should be calculated. There were two main positions.

SignaturePolicy ::= SEQUENCE {

signPolicyHashAlg AlgorithmIdentifier,

signPolicyInfo SignPolicyInfo,

signPolicyHash SignPolicyHash OPTIONAL

}

The hash is calculated over the DER value of the SignaturePolicy field without the outer type and length fields, and without the optional signPolicyHash field.

1. It means the hash is calculated from the fields signPolicyHashAlg and signPolicyInfo and the hash value is included in field signPolicyHash. Hash is calculated without taking into account the outer type and length fields of SignaturePolicy ::= SEQUENCE {

2. It means the hash is calculated from the field signPolicyInfo and the hash value is included in field signPolicyHash. Hash is calculated without taking into account the outer type and length fields of SignPolicyInfo ::= SEQUENCE {

Related to this topic there was a general agreement in remarking that the ETSI specification on signature policies must be re-worked and updated.

5.6 Field's order of signing certificate's issuer DN

There was a wide debate regarding signature validation when the fields' order of the DN of the issuer in the signing certificate is different from the one declared in ESSSigningCertificateV2.IssuerAndSerialNumber.Name.

A Name is structured in hierarchical levels, each level (RelativeDistinguishedName) represented by a set, not ordered, of attributes and their values. A Name identifies a node of the tree of the directory (defined in X.501, which is interfaced using the LDAP protocol), each RelativeDistinguishedName is the name of a node; the position of the leaf node (Issuer / Subject) is the concatenation of the names of the nodes in the path from the root of directory to the leaf.

Two Name are equal if they identify the same node, so if the sequence of intermediate nodes is the same. To decide whether two intermediate nodes are equal one must compare the attributes that make their RelativeDistinguishedName: the attributes must be equal in number, type and corresponding value, no matter in what order they appear.

5.7 Signed attributes order

There were some discussions between participants regarding signature validation results if signed attributes (that shall be DER encoded) are not ordered (ascending lexicographic order of BER encoding). Shall the validation of the signature fail even if the signature is correct from the point of view of cryptographic calculation in such case?

Some participants relaxed their code to accept these signatures while other didn't consider them valid.

5.8 Syntax definition of ATSHashIndex

Some participants noticed that the syntax definition of ATSHashIndex seems to violate the ITU-T X.680 requirements for SEQUENCE type components.

5.9 Revocation material in ATSv3

One of the proposed test cases previewed that revocation material related to an ATSv3 should have been included within the token itself (when generated). It was suggested during the Plugtest that ATSv3 never contains revocation material. Revocation material for ATSv3 must always be included in the root SignedData only.

5.10 Evolution of CAdES Plugtests

The participants expressed an interest in an update of the mother specification including long term features and in holding another related Plugtests. An update of the CAdES mother specification with long term features is indeed in the ETSI TC ESI standardization roadmap and the possibility to have then new events will be duly considered.

6 CAdES Plugtests Interoperability matrixes

6.1 Statistics for Positive Test Cases

CAdES-BES

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-BES-1.xml	38	35	1179	1118	94,83	55	4,66	6	0,51
C-BES-2.xml	38	41	1379	1281	92,89	86	6,24	12	0,87
C-BES-3.xml	26	18	429	398	92,77	27	6,29	4	0,93
C-BES-4.xml	29	23	537	501	93,30	31	5,77	5	0,93
C-BES-5.xml	28	21	553	500	90,42	51	9,22	2	0,36
C-BES-6.xml	33	32	942	848	90,02	80	8,49	14	1,49
C-BES-7.xml	21	14	246	224	91,06	19	7,72	3	1,22

CAdES-EPES

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-EPES-1.xml	23	27	533	357	66,98	161	30,21	15	2,81
C-EPES-2.xml	21	18	314	218	69,43	84	26,75	12	3,82
C-EPES-3.xml	16	14	191	137	71,73	48	25,13	6	3,14

CAdES-T

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-T-1.xml	35	40	1255	1122	89,40	125	9,96	8	0,64
C-T-2.xml	28	30	789	667	84,54	112	14,20	10	1,27

CAdES-C

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-C-1.xml	23	24	503	391	77,73	71	14,12	41	8,15
C-C-2.xml	22	18	325	248	76,31	49	15,08	28	8,62

CAdES-X

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-X-1.xml	23	21	372	220	59,14	140	37,63	12	3,23
C-X-2.xml	20	19	319	197	61,76	113	35,42	9	2,82
C-X-3.xml	19	17	256	156	60,94	89	34,77	11	4,30
C-X-4.xml	18	16	238	143	60,08	85	35,71	10	4,20

CAdES-XL

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-XL-1.xml	23	25	461	293	63,56	151	32,75	17	3,69
C-XL-2.xml	21	21	368	227	61,68	128	34,78	13	3,53
C-XL-3.xml	20	18	287	163	56,79	109	37,98	15	5,23
C-XL-4.xml	19	17	271	156	57,56	103	38,01	12	4,43

CAdES-A

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-A-X-1.xml	9	8	53	31	58,49	19	35,85	3	5,66
C-A-C-1.xml	8	8	43	29	67,44	12	27,91	2	4,65
C-A-EPES-1.xml	11	9	70	48	68,57	20	28,57	2	2,86
C-A-BES-1.xml	12	10	90	50	55,56	39	43,33	1	1,11
C-A-T-1.xml	14	13	142	104	73,24	36	25,35	2	1,41
C-A-XL-1.xml	13	12	117	61	52,14	54	46,15	2	1,71
C-A-XL-2.xml	12	10	89	49	55,06	39	43,82	1	1,12

C-A-X-2.xml	9	7	37	23	62,16	12	32,43	2	5,41
C-A-ATSv2-1.xml	10	8	69	16	23,19	52	75,36	1	1,45

CAdES-BpB

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
CBp-B-1.xml	22	22	432	390	90,28	37	8,56	5	1,16
CBp-B-2.xml	17	11	165	137	83,03	24	14,55	4	2,42
CBp-B-3.xml	16	9	133	117	87,97	15	11,28	1	0,75
CBp-B-4.xml	19	17	282	256	90,78	21	7,45	5	1,77

CAdES-BpT

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
CBp-T-1.xml	21	22	418	375	89,71	37	8,85	6	1,44
CBp-T-2.xml	18	19	305	270	88,52	27	8,85	8	2,62

CAdES-BpLT

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
CBp-LT-1.xml	14	15	187	139	74,33	31	16,58	17	9,09
CBp-LT-2.xml	12	9	89	51	57,30	28	31,46	10	11,24
CBp-LT-3.xml	10	6	51	28	54,90	16	31,37	7	13,73
CBp-LT-4.xml	8	5	36	17	47,22	14	38,89	5	13,89

CAdES-BpLTA

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
CBp-LTA-1.xml	14	11	124	80	64,52	39	31,45	5	4,03
CBp-LTA-2.xml	10	7	58	28	48,28	28	48,28	2	3,45
CBp-LTA-3.xml	12	9	81	48	59,26	29	35,80	4	4,94
CBp-LTA-4.xml	9	5	35	21	60,00	12	34,29	2	5,71

CBp-LTA-5.xml	12	7	63	47	74,60	13	20,63	3	4,76
CBp-LTA-6.xml	8	6	36	20	55,56	15	41,67	1	2,78

6.2 Statistics for Negative Test Cases

CAdES-BESN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-BESN-1.xml	24	1	24	0	0,00	24	100,00	0	0,00
C-BESN-2.xml	24	1	24	0	0,00	24	100,00	0	0,00
C-BESN-3.xml	22	1	22	0	0,00	22	100,00	0	0,00
C-BESN-4.xml	23	1	23	1	4,35	22	95,65	0	0,00
C-BESN-5.xml	22	1	22	0	0,00	22	100,00	0	0,00
C-BESN-6.xml	17	1	17	0	0,00	16	94,12	1	5,88

CAdES-EPESN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-EPESN-1.xml	13	1	13	1	7,69	12	92,31	0	0,00
C-EPESN-2.xml	12	1	12	1	8,33	11	91,67	0	0,00

CAdES-TN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-TN-1.xml	23	1	23	0	0,00	23	100,00	0	0,00
C-TN-2.xml	21	1	21	0	0,00	21	100,00	0	0,00
C-TN-3.xml	19	1	19	0	0,00	19	100,00	0	0,00
C-TN-4.xml	18	1	18	0	0,00	18	100,00	0	0,00
C-TN-5.xml	19	1	19	1	5,26	18	94,74	0	0,00
C-TN-6.xml	14	1	14	0	0,00	13	92,86	1	7,14

CAdES-XN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-XN-1.xml	9	1	9	0	0,00	9	100,00	0	0,00
C-XN-2.xml	9	1	9	0	0,00	9	100,00	0	0,00
C-XN-3.xml	8	1	8	0	0,00	8	100,00	0	0,00

CAdES-XN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-XLN-1.xml	8	1	8	0	0,00	8	100,00	0	0,00
C-XLN-2.xml	8	1	8	0	0,00	8	100,00	0	0,00
C-XLN-3.xml	8	1	8	0	0,00	8	100,00	0	0,00
C-XLN-4.xml	8	1	8	0	0,00	8	100,00	0	0,00
C-XLN-5.xml	8	1	8	0	0,00	8	100,00	0	0,00
C-XLN-6.xml	8	1	8	0	0,00	8	100,00	0	0,00

CAdES-AN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-AN-1.xml	5	1	5	0	0,00	5	100,00	0	0,00
C-AN-2.xml	5	1	5	0	0,00	5	100,00	0	0,00
C-AN-3.xml	5	1	5	0	0,00	5	100,00	0	0,00
C-AN-4.xml	4	1	4	0	0,00	4	100,00	0	0,00

CAdES-BpBN

Signature	Number of Verifiers	Signatures generated by ETSI	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
CBp-BN-1.xml	9	1	9	1	11,11	8	88,89	0	0,00
CBp-BN-2.xml	12	1	12	0	0,00	12	100,00	0	0,00
CBp-BN-3.xml	12	1	12	1	8,33	11	91,67	0	0,00

CBp-BN-4.xml	11	1	11	0	0,00	11	100,00	0	0,00

6.3 Statistics for Upgrade and Arbitration Test Cases

Signature	Number of Verifiers	Generated Signatures	Total Verifications	Success		Failure		Incomplete	
				Absolute	%	Absolute	%	Absolute	%
C-A-BES-1-C-BES-2.xml	6	5	24	21	87,50	3	12,50	0	0,00
C-A-C-1-C-C-1.xml	5	5	19	15	78,95	3	15,79	1	5,26
C-A-T-1-C-T-1.xml	7	6	31	26	83,87	4	12,90	1	3,23
C-A-X-1-C-X-1.xml	5	5	18	14	77,78	3	16,67	1	5,56
C-A-XL-1-C-XL-1.xml	6	6	26	19	73,08	7	26,92	0	0,00
C-C-1-C-BES-2.xml	5	3	11	7	63,64	3	27,27	1	9,09
C-C-1-C-T-1.xml	5	3	11	7	63,64	3	27,27	1	9,09
C-X-1-C-BES-2.xml	5	3	11	6	54,55	5	45,45	0	0,00
C-X-1-C-C-1.xml	5	3	11	6	54,55	5	45,45	0	0,00
C-X-1-C-T-1.xml	5	3	11	6	54,55	5	45,45	0	0,00
C-XL-1-C-BES-2.xml	5	4	17	12	70,59	4	23,53	1	5,88
C-XL-1-C-C-1.xml	5	4	17	11	64,71	5	29,41	1	5,88
C-XL-1-C-T-1.xml	6	5	23	17	73,91	5	21,74	1	4,35

6.4 Positive test cases for generation and verification for CAdES

6.4.1 Test cases for CAdES-BES.

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

The following table shows which attributes are required to generate test CAdES-BES signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-BES.SCOK													
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS
C-BES-1.xml	*		*				*						
C-BES-2.xml	*	*	*				*						
C-BES-3.xml	*	*	*			*	*						
C-BES-4.xml	*	*	*				*					*	
C-BES-5.xml													*
C-BES-6.xml	*	*	*				*						
C-BES-7.xml	*	*	*		*	*	*	*	*		*	*	

All these tests should verify without any problems.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType

This test case tests the simplest CAdES-BES *WITHOUT* SigningTime.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

This test case tests the simplest CAdES-BES *WITH* SigningTime.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType

- CertifiedAttribute

This test case tests CAdES-BES with a SignerAttributes containing a CertifiedAttribute.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- ContentTimeStamp

This test case tests CAdES-BES with a ContentTimeStamp attribute.

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

- SignedDocument
- CounterSignature

This test case tests CAdES-BES with a CounterSignature attribute. The input to this test is a CAdES-BES signature as specified in C-BES-1 test case.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType

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.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- SignerLocation
- ClaimedAttribute
- ContentType
- ContentHints

- ContentIdentifier
- CommitmentTypeIndication
- ContentTimeStamp

This test case tests CAdES-BES with following attributes at once: - MessageDigest - SigningTime - ESSSigningCertificateV2 - SignerLocation - SignerAttributes (only Claimed Attributes included) - ContentType - ContentHints - ContentIdentifier - CommitmentTypeIndication

6.4.2 Test cases for CAdES-EPES form, positive test cases.

The test cases in this section deal with the CAdES-EPES form.

The following table shows which attributes are required to generate test CAdES-EPES signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-EPES.SCOK														
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI
C-EPES-1.xml	*	*	*				*							*
C-EPES-2.xml	*	*	*		*		*				*			*
C-EPES-3.xml	*	*	*				*							*

All these tests should verify without any problems.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- SignaturePolicyIdentifier
- ContentType

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.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- SignaturePolicyIdentifier

- SignerLocation
- ContentType
- CommitmentTypeIndication

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.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- SignaturePolicyIdentifier
- ContentType

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.

6.4.3 Test cases for CAdES-T form, positive test cases.

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

The following table shows which attributes are required to generate test CAdES-T signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-T.SCOK															
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS
C-T-1.xml	*	*	*				*								*
C-T-2.xml	*	*	*				*								*

All these tests should verify without any problems.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp

This test case tests the simplest CAdES-T format.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp

This test case tests the adding of an independent 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

6.4.4 Test cases for CAdES-C form, positive test cases.

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

The following table shows which attributes are required to generate test CAdES-C signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-C.SCOK																			
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR
C-C-1.xml	*	*	*				*								*	*	C		
C-C-2.xml	*	*	*				*								*	*	O		

All these tests should verify without any problems.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp

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.

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

- SignedDocument
- MessageDigest
- SigningTime

- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp

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.

6.4.5 Test cases for CAdES-X form, positive test cases.

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

The following table shows which attributes are required to generate test CAdES-X signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-X.SCOK																							
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR	ESCTS	TCCRL	CV	RV
C-X-1.xml	*	*	*				*								*	*	C			*			
C-X-2.xml	*	*	*				*								*	*	C				*		
C-X-3.xml	*	*	*				*								*	*	O			*			
C-X-4.xml	*	*	*				*								*	*	O				*		

All these tests should verify without any problems.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp

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.

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

- SignedDocument

- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- TimestampedCertsCRLs

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.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp

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.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- TimestampedCertsCRLs

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.

6.4.6 Test cases for CAdES-X Long form, positive test cases.

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

The following table shows which attributes are required to generate test CAdES-XL signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-XL.SCOK																							
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR	ESCTS	TCCRL	CV	RV
C-XL-1.xml	*	*	*				*								*	*	C			*		*	C
C-XL-2.xml	*	*	*				*								*	*	C				*	*	C
C-XL-3.xml	*	*	*				*								*	*	O			*		*	O
C-XL-4.xml	*	*	*				*								*	*	O				*	*	O

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp

This test case tests a CAdES-XL Type1 format. Its CompleteRevocationRefs must have only CRLListIDs and its RevocationValues must have only crlVals element.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- TimestampedCertsCRLs

This test case tests a CAdES-XL Type2 format. Its CompleteRevocationRefs must have only CRLListIDs and its RevocationValues must have only crlVals element.

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

- SignedDocument

- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp

This test case tests a CAdES-XL Type1 format. In the CompleteRevocationRefs only OcspListIDs must be included and RevocationValues must have only ocspVals element.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- TimestampedCertsCRLs

This test case tests a CAdES-XL Type2 format. In the CompleteRevocationRefs only OcspListIDs must be included and RevocationValues must have only ocspVals element.

6.4.7 Test cases for CAdES-A form, positive test cases.

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

The following table shows which attributes are required to generate test CAdES-A signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-A.SCOK																											
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR	ESCTS	TCCRL	CV	RV	ATS	ATSV2	ATSV3
C-A-X-1.xml	*	*	*				*								*	*	C			*				1		*
C-A-C-1.xml	*	*	*				*								*	*	C							1		*
C-A-EPES-1.xml	*	*	*				*							*										1		*
C-A-BES-1.xml	*	*	*				*																	1		*

C-A-T-1.xml	*	*	*				*							*								1		*
C-A-XL-1.xml	*	*	*				*							*	*	C			*		*	C	1		*
C-A-XL-2.xml	*	*	*				*							*	*	C				*	*	C	1		*
C-A-X-2.xml	*	*	*				*							*	*	C				*			1		*
C-A-ATSv2-1.xml	*	*	*				*							*	*	C			*		*	C	2	*	*

All these tests should verify without any problems.

C-A-BES-1.xml contains the following Properties:

- SignedDocument
- Crls
- Certificates
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- ArchiveTimeStampV3

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.

C-A-EPES-1.xml contains the following Properties:

- SignedDocument
- Crls
- Certificates
- MessageDigest
- ESSSigningCertificateV2
- SignaturePolicyIdentifier
- ContentType
- SigningTime
- ArchiveTimeStampV3

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.

C-A-T-1.xml contains the following Properties:

- SignedDocument
- Crls
- Certificates
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- ArchiveTimeStampV3

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.

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

- SignedDocument
- Crls
- Certificates
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ArchiveTimeStampV3

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.

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

- SignedDocument
- Crls
- Certificates
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp

- ArchiveTimeStampV3

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.

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

- SignedDocument
- Crls
- Certificates
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- TimestampedCertsCRLs
- ArchiveTimeStampV3

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.

C-A-XL-1.xml contains the following Properties:

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp
- ArchiveTimeStampV3

This test case tests the CAdES-A with ATSv3 built on a CAdES-XL Type1 signature as specified in C-XL-1 test case.

C-A-XL-2.xml contains the following Properties:

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp

- TimestampedCertsCRLs
- ArchiveTimeStampV3

This test case tests the CAdES-A with ATSv3 built on a CAdES-XL Type2 signature as specified in C-XL-2 test case.

C-A-ATSv2-1.xml contains the following Properties:

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp
- ArchiveTimeStampV2
- ArchiveTimeStampV3

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.

6.4.8 Test cases for CAdES Baseline profile level B form, positive test cases.

The test cases in this section deal with the CAdES Baseline profile level B form.

The following table shows which attributes are required to generate test CAdES Baseline profile level B signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-BpB.SCOK
Property → TestCase ↓
CBp-B-1.xml
CBp-B-2.xml
CBp-B-3.xml
CBp-B-4.xml

All these tests should verify without any problems.

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

CBp-B-2.xml contains the following Properties: In this CAdES Baseline Profile conformance level B test case the signature contains a CertifiedAttribute in addition to all mandatory attributes.

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

CBp-B-4.xml contains the following Properties: 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.

6.4.9 Test cases for CAdES Baseline profile level T form, positive test cases.

The test cases in this section deal with the CAdES Baseline profile level T form.

The following table shows which attributes are required to generate test CAdES Baseline profile level T signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-BpT.SCOK
Property → TestCase ↓
CBp-T-1.xml
CBp-T-2.xml

All these tests should verify without any problems.

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

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

6.4.10 Test cases for CAdES Baseline profile level LT form, positive test cases.

The test cases in this section deal with the CAdES Baseline profile level LT form.

The following table shows which attributes are required to generate test CAdES Baseline profile level LT signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-BpLT.SCOK
Property → TestCase ↓
CBp-LT-1.xml
CBp-LT-2.xml
CBp-LT-3.xml
CBp-LT-4.xml

All these tests should verify without any problems.

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

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

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

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

6.4.11 Test cases for CAdES Baseline profile level LTA form, positive test cases.

The test cases in this section deal with the CAdES Baseline profile level LTA form.

The following table shows which attributes are required to generate test CAdES Baseline profile level LTA signatures for each test case. Click a test case ID to see its test definition XML file.

CAdES-BpLTA.SCOK
Property → TestCase ↓
CBp-LTA-1.xml
CBp-LTA-2.xml
CBp-LTA-3.xml
CBp-LTA-4.xml
CBp-LTA-5.xml
CBp-LTA-6.xml

All these tests should verify without any problems.

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

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

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

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

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

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

6.5 Negative test cases for verification for CAdES

This section describes 'Negative Verification-Only' tests in which the test CAdES signatures shall be verified as invalid by participating implementations. In the negative test, participants do not need to generate signatures.

In the 'negative test' participants will do the following:

1. A participating implementation must verify the CAdES signatures. Verification of the CAdES signatures shall be negative. That's why it is called 'negative test'.
2. A participant will download CAdES signatures generated by the organizers.
3. Verify CAdES signatures.
4. Upload verification results as XML files.
5. See test result matrix.

Very Important Note: the EE and TSA certificates pre-generated for producing negative test cases signatures have a wrong CRL issuer attribute in CRLDP with http protocol. This wrong CRL Issuer attribute shall not be considered during validation operations. The signature validation should fail for the reason documented in xml files describing the negative test cases.

Negative test cases files are in the 'NegativeTests' folder grouped by CAdES Form.

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

6.5.1 Negative test cases for CAdES-BES form.

The following list summarizes negative test cases for CAdES-BES form

1. Verify a signed document having a wrong signature (the hash that was signed isn't the hash of the specified MessageDigest element)
2. Verify a document signed with an expired signing certificate
3. Verify a document signed with a revoked/suspended signing certificate
4. Verify a signed document in which the hash value of the signing certificate is different from the hash value in ESS signing certificate V2 attribute
5. Verify a signed document whos format is not CAdES-BES

6. Verify a document signed with an untrusted signing certificate

CAdES-BESN.SCOK													
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS
C-BESN-1.xml	*	*	*				*						
C-BESN-2.xml	*	*	*				*						
C-BESN-3.xml	*	*	*				*						
C-BESN-4.xml	*	*	*				*						
C-BESN-5.xml	*	*					*						

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

This is a negative test case for checking a wrong signature. This test data has a wrong signature because the hash that was signed isn't the hash of the specified MessageDigest element.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

This is a negative test case for checking an expired signer certificate. This test data has a signature created by a signer whose certificate is expired.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

This is a negative test case for checking a revoked signer certificate. This test data has a signature created by a signer whose certificate is revoked.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

This is a negative test case for checking ESSSigningCertificateV2. This test data has an ESSSigningCertificateV2 attribute whose value of certHash field does *NOT* match to the hash value of signer certificate.

C-BESN-5.xml contains the following Properties:

- SignedDocument
- MessageDigest
- ContentType
- SigningTime

This is a negative test case for checking CAdES-BES format. This test data is not a CAdES-BES signature.

CAdES-BESN.SCUN													
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS
C-BESN-6.xml	*	*	*				*						

C-BESN-6.xml contains the following Properties:

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

This is a negative test case for checking an untrusted signature. This test data has an untrusted signature because the anchor CA of the signing chain trust is unknown.

6.5.2 Negative test cases for CAdES-EPES form.

The following list summarizes negative test cases for CAdES-EPES form

1. Verify a signed document having the value of SignaturePolicyId.sigPolicyHash field that does *NOT* match to the hash value of signer policy file

2. Verify a signed document in which the sigPolicyHash field value of SignaturePolicyIdentifier attribute in the CAdES-EPES signature is identical to signPolicyHash field value of RFC 3125 ASN.1 signature policy file. However in the policy file, signPolicyHash is *NOT* identical to the hash value which was calculated by the SignPolicyInfo without ASN.1 tag and length

CAdES-EPESN.SCOK														
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI
C-EPESN-1.xml	*	*	*				*							*
C-EPESN-2.xml	*	*					*							*

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV2
- SignaturePolicyIdentifier
- ContentType

This is a negative test case for checking SignaturePolicyIdentifier. This test data has a SignaturePolicyIdentifier attribute with explicit SignaturePolicyId however its value of SignaturePolicyId.sigPolicyHash field does *NOT* match to the hash value of signer policy file.

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

- SignedDocument
- MessageDigest
- SigningTime
- ESSSigningCertificateV1orV2
- SignaturePolicyIdentifier
- ContentType

'C-EPESN-2' is a negative test case for checking 'RFC 3125 ASN.1 signature policy file'. In this test, the sigPolicyHash field value of SignaturePolicyIdentifier attribute in the CAdES-EPES signature is identical to signPolicyHash field value of RFC 3125 ASN.1 signature policy file. However in the policy file, signPolicyHash is *NOT* identical to the hash value which was calculated by the SignPolicyInfo without ASN.1 tag and length.

6.5.3 Negative test cases for CAdES-T form.

The following list summarizes negative test cases for CAdES-T form

1. Verify a signed document in which the signer certificate, at the time in SignatureTimeStamp, had been already expired
2. Verify a signed document in which the signer certificate, at the time in SignatureTimeStamp, had been already revoked
3. Verify a signed document in which the hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value of signerInfo
4. Verify a signed document in which the timestamp signer certificate, at the time in SignatureTimeStamp, had been already revoked
5. Verify a signed document in which the timestamp signer certificate, at the time in SignatureTimeStamp, had been already expired
6. Verify a signed and timestamped document in which the timestamp signer certificate is untrusted

CAdES-TN.SCOK															
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS
C-TN-1.xml	*	*	*				*								*
C-TN-2.xml	*	*	*				*								*
C-TN-3.xml	*	*	*				*								*
C-TN-4.xml	*	*	*				*								*
C-TN-5.xml	*	*	*				*								*

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp

This is a negative test case for verifying signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the signer certificate had been already expired. ETSI Invalid-Cert Expired SN:009BC934757604 21-Nov-2013 17:21:41Z - signer certificate expired SN:009BC934757604 02-Dec 2013 23:09:57Z - SignatureTimeStamp

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2

- ContentType
- SigningTime
- SignatureTimeStamp

This is a negative test case for verifying signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the signer certificate had been already revoked. ETSI Invalid-Cert Revoked SN:015FDBF4642F3E 20-Nov-2013 16:37:56Z - signer certificate revoked SN:015FDBF4642F3E 02-Dec 2013 23:10:16Z - SignatureTimeStamp

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp

This is a negative test case for SignatureTimeStamp. The hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value of signerInfo.

C-TN-4.xml contains the following Properties:

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp

This is a negative test case for verifying timestamp signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the timestamp signer certificate had been already revoked. ETSI Invalid-Cert Revoked SN:02BCCBFDA08E42 18-Nov-2013 15:22:07Z - timestamp signer certificate revoked SN:02BCCBFDA08E42 25-Nov 2013 09:45:51Z - SignatureTimeStamp

C-TN-5.xml contains the following Properties:

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp

This is a negative test case for verifying timestamp signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the timestamp signer certificate had been already expired. ETSI Invalid-Cert Expired SN:027A15B838E38E 17-Nov-2013 11:20:03Z - timestamp signer certificate expired SN:027A15B838E38E 25-Nov 2013 09:49:28Z - SignatureTimeStamp

CAdES-TN.SCUN															
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS
C-TN-6.xml	*	*	*				*								*

C-TN-6.xml contains the following Properties:

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp

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

6.5.4 Negative test cases for CAdES-X form.

The following list summarizes negative test cases for CAdES-X form

1. Verify a signed document in which the time in the SignatureTimeStamp is ulterior than the time in TimestampedCertsCRLs
2. Verify a signed document in which the time in the SignatureTimeStamp is ulterior than the time in ESCTimeStamp
3. Verify a signed document in which the hash value of messageImprint in TimestampedCertsCRLs does *NOT* match to the hash value of corresponding CompleteCertificateRefs and CompleteRevocationRefs

CAdES-XN.SCOK																					
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR	ESCTS	TCCRL
C-XN-1.xml	*	*	*				*								*	*	C				*
C-XN-2.xml	*	*	*				*								*	*	C			*	
C-XN-3.xml	*	*	*				*								*	*	C				*

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the SignatureTimeStamp is ulterior than the time in TimestampedCertsCRLs. ETSI Invalid-Sig Valid-Cert 11-Dec-2013 18:08:42Z - SignatureTimeStamp 10-Dec 2013 18:09:08Z - TimestampedCertsCRLs

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- ESCTimeStamp

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the SignatureTimeStamp is ulterior than the time in ESCTimeStamp. ETSI Invalid-Sig Valid-Cert 11-Dec-2013 18:13:15Z - SignatureTimeStamp 10-Dec-2013 18:13:47Z - ESCTimeStamp

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for TimestampedCertsCRLs. The hash value of messageImprint in TimestampedCertsCRLs does *NOT* match to the hash value of corresponding CompleteCertificateRefs and CompleteRevocationRefs. ETSI Invalid-Sig Valid-Cert 02-Dec-2013 23:06:46Z - SignatureTimeStamp 02-Dec-2013 23:06:49Z - TimestampedCertsCRLs

6.5.5 Negative test cases for CAdES-XL form.

The following list summarizes negative test cases for CAdES-XN form

1. Verify a signed document in which the crlIdentifier.issuedTime field does *NOT* match to the thisUpdate of corresponding CRL in the RevocationValues
2. Verify a signed document in which the crlIdentifier.crlNumber field does *NOT* match to the crlNumber extension of corresponding CRL in the RevocationValues
3. Verify a signed document in which the crlHash field does *NOT* match to the hash value of corresponding CRL in the RevocationValues
4. Verify a signed document in which the ocspIdentifier.responderID field does *NOT* match to the responderID field of corresponding BasicOCSPResponse in the RevocationValues
5. Verify a signed document in which the ocspIdentifier.producedAt field does *NOT* match to the producedAt field of corresponding BasicOCSPResponse in the RevocationValues
6. Verify a signed document in which the ocspRepHash field does *NOT* match to the hash value of corresponding BasicOCSPResponse in the RevocationValues

CAdES-XLN.SCOK																						
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR	ESCTS	TCCRL	CV	RV
C-XLN-1.xml	*	*	*				*								*	*	C				*	*	C
C-XLN-2.xml	*	*	*				*								*	*	C				*	*	C
C-XLN-3.xml	*	*	*				*								*	*	C				*	*	C
C-XLN-4.xml	*	*	*				*								*	*	O				*	*	O
C-XLN-5.xml	*	*	*				*								*	*	O				*	*	O
C-XLN-6.xml	*	*	*				*								*	*	O				*	*	O

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime

- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for matching between CompleteRevocationRefs and RevocationValues. In this test case, the crlIdentifier.issuedTime field does *NOT* match to the thisUpdate of corresponding CRL in the RevocationValues.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for matching between CompleteRevocationRefs and RevocationValues. In this test case, the crlIdentifier.crlNumber field does *NOT* match to the crlNumber extension of corresponding CRL in the RevocationValues.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for matching between CompleteRevocationRefs and RevocationValues. In this test case, the crlHash field does *NOT* match to the hash value of corresponding CRL in the RevocationValues.

C-XLN-4.xml contains the following Properties:

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for matching between CompleteRevocationRefs and RevocationValues. In this test case, the ocspIdentifier.responderID field does *NOT* match to the responderID field of corresponding BasicOCSPResponse in the RevocationValues.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for matching between CompleteRevocationRefs and RevocationValues. In this test case, the ocspIdentifier.producedAt field does *NOT* match to the producedAt field of corresponding BasicOCSPResponse in the RevocationValues.

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs

This is a negative test case for matching between CompleteRevocationRefs and RevocationValues. In this test case, the ocspRepHash field does *NOT* match to the hash value of corresponding BasicOCSPResponse in the RevocationValues.

6.5.6 Negative test cases for CAdES-A form.

The following list summarizes negative test cases for CAdES-A form

1. Verify a signed document in which the time in the SignatureTimeStamp is ulterior than the time in ArchiveTimeStamp
2. Verify a signed document in which the time in the TimestampedCertsCRLs is ulterior than the time in ArchiveTimeStamp
3. Verify a signed document in which the time in the ESCTimeStamp is ulterior than the time in ArchiveTimeStamp
4. Verify a signed document in which the content in ats-hash-index element has not the right value related to the CAdES signature to which the ATSv3 has been applied

CAdES-AN.SCOK																										
Property → TestCase ↓	MD	ST	ESSSCV2	OSC	SL	SA	CT	CH	CI	CR	CTI	CTS	CS	SPI	STS	CCR	CRR	ACR	ARR	ESCTS	TCCRL	CV	RV	ATS	ATSV2	ATSV3
C-AN-1.xml	*	*	*				*								*	*	C				*	*	C	1		*
C-AN-2.xml	*	*	*				*								*	*	C				*	*	C	1		*
C-AN-3.xml	*		*				*								*	*	C			*		*	C	1		*
C-AN-4.xml	*		*				*								*	*	C			*		*	C	1		*

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs
- ArchiveTimeStampV3

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the SignatureTimeStamp is ulterior than the time in ArchiveTimeStamp. ETSI Invalid-Sig Valid-Cert 11-Dec-2013 22:36:53Z - SignatureTimeStamp (*) 10-Dec-2013 22:37:06Z - TimestampedCertsCRLs 10-Dec-2013 22:37:11Z - ArchiveTimeStamp

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SigningTime
- SignatureTimeStamp
- TimestampedCertsCRLs
- ArchiveTimeStampV3

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the TimestampedCertsCRLs is ulterior than the time in ArchiveTimeStamp. ETSI Invalid-Sig Valid-Cert 10-Dec-2013 22:41:10Z - SignatureTimeStamp 11-Dec-2013 22:41:22Z - TimestampedCertsCRLs (*) 10-Dec-2013 22:41:32Z - ArchiveTimeStamp

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp
- ArchiveTimeStampV3

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the ESCTimeStamp is ulterior than the time in ArchiveTimeStamp. ETSI Invalid-Sig Valid-Cert 10-Dec-2013 22:45:12Z - SignatureTimeStamp 11-Dec-2013 22:45:26Z - ESCTimeStamp (*) 10-Dec-2013 22:45:35Z - ArchiveTimeStamp

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

- SignedDocument
- MessageDigest
- ESSSigningCertificateV2
- ContentType
- SignatureTimeStamp
- ESCTimeStamp
- ArchiveTimeStampV3

This is a negative test case for verifying ats-hash-index content. In this test case, the content in ats-hash-index element has not the right value related to the CAdES signature to which the ATSv3 has been applied.

6.5.7 Negative test cases for CAdES Baseline profile level B form.

The following list summarizes negative test cases for CAdES Baseline profile level B form

1. Verify a signed document in which the mandatory SigningTime attribute is not present
2. Verify a signed document in which the mandatory SigningCertificate in ESS attribute is not present
3. Verify a signed document in which the mandatory ContentType attribute is not present
4. Verify a signed document in which the mandatory SigningCertificate in CM signedData.certificates is not present

CAdES-BpBN.SCOK

Property → TestCase ↓
CBp-BN-1.xml
CBp-BN-2.xml
CBp-BN-3.xml
CBp-BN-4.xml

CBp-BN-1.xml contains the following Properties: The signature corresponding to this test case is not conformant against the CAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory SigningTime attribute.

CBp-BN-2.xml contains the following Properties: The signature corresponding to this test case is not conformant against the CAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory SigningCertificate attribute.

CBp-BN-3.xml contains the following Properties: The signature corresponding to this test case is not conformant against the CAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory ContentType attribute qualifying the signed data object.

CBp-BN-4.xml contains the following Properties: The signature corresponding to this test case is not conformant against the CAdES Baseline Profile conformance level B because it DOES NOT CONTAIN the mandatory certificates component into CMS signedData structure.

6.6 Upgrade and Arbitration Test Cases

This section describes 'Upgrade and Arbitration" tests where a participant (signer) generates a basic signature, a second participant (verifier) upgrades it after verifying to a more evolved form, and finally, a third participant (arbitrator) verifies the upgraded signature.

The following section contains upgrade test cases grouped by CAdES Form.

6.6.1 Test cases for upgrading to CAdES-C form.

The test cases in this section deal with the upgrading to `CAdES-C` form.

The following table shows a list of 2 upgrade to `CAdES-C` form and arbitration tests. Click a test case ID to see its test definition XML file.

CAdES-UpdArb.SCOK			
Property → TestCase ↓	U	O	UT
C-C-1-C-T-1.xml	*	*	*
C-C-1-C-BES-2.xml	*	*	*

All these tests should verify without any problems.

C-C-1-C-BES-2.xml contains the following Properties: This test case tests the upgrade of a CAdES-BES signature as specified in C-BES-2 test case to a CAdES-C signature as specified in C-C-1 test case.

C-C-1-C-T-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-T signature as specified in C-T-1 test case to a CAdES-C signature as specified in C-C-1 test case.

6.6.2 Test cases for upgrading to CAdES-X form.

The test cases in this section deal with the upgrading to CAdES-X form.

The following table shows a list of 3 upgrade to CAdES-X form and arbitration tests. Click a test case ID to see its test definition XML file.

CAdES-UpdArb.SCOK			
Property → TestCase ↓	U	O	UT
C-X-1-C-C-1.xml	*	*	*
C-X-1-C-T-1.xml	*	*	*
C-X-1-C-BES-2.xml	*	*	*

All these tests should verify without any problems.

C-X-1-C-BES-2.xml contains the following Properties: This test case tests the upgrade of a CAdES-BES signature as specified in C-BES-2 test case to a CAdES-X signature as specified in C-X-1 test case.

C-X-1-C-T-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-T signature as specified in C-T-1 test case to a CAdES-X signature as specified in C-X-1 test case.

C-X-1-C-C-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-C signature as specified in C-C-! test case to a CAdES-X signature as specified in C-X-1 test case.

6.6.3 Test cases for upgrading to CAdES-XL form.

The test cases in this section deal with the upgrading to CAdES-XL form.

The following table shows a list of 3 upgrade to CAdES-XL form and arbitration tests. Click a test case ID to see its test definition XML file.

CAdES-UpdArb.SCOK			
Property → TestCase ↓	U	O	UT
C-XL-1-C-C-1.xml	*	*	*
C-XL-1-C-T-1.xml	*	*	*
C-XL-1-C-BES-2.xml	*	*	*

All these tests should verify without any problems.

C-XL-1-C-BES-2.xml contains the following Properties: This test case tests the upgrade of a CAdES-BES signature as specified in C-BES-2 test case to a CAdES-XL signature as specified in C-XL-1 test case.

C-XL-1-C-T-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-C signature as specified in C-T-1 test case to a CAdES-XL signature as specified in C-XL-1 test case.

C-XL-1-C-C-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-C signature as specified in C-C-1 test case to a CAdES-XL signature as specified in C-XL-1 test case.

6.6.4 Test cases for upgrading to CAdES-A form.

The test cases in this section deal with the upgrading to CAdES-A form.

The following table shows a list of 5 upgrade to CAdES-A form and arbitration tests. Click a test case ID to see its test definition XML file.

CAdES-UpdArb.SCOK			
Property → TestCase ↓	U	O	UT
C-A-X-1-C-X-1.xml	*	*	*
C-A-T-1-C-T-1.xml	*	*	*
C-A-XL-1-C-XL-1.xml	*	*	*
C-A-C-1-C-C-1.xml	*	*	*
C-A-BES-1-C-BES-2.xml	*	*	*

All these tests should verify without any problems.

C-A-BES-1-C-BES-2.xml contains the following Properties: This test case tests the upgrade of a CAdES-BES signature as specified in C-BES-2 test case to a CAdES-A signature as specified in C-A-BES-1 test case.

C-A-T-1-C-T-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-T signature as specified in C-T-1 test case to a CAdES-A signature as specified in C-A-T-1 test case.

C-A-C-1-C-C-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-C signature as specified in C-C-1 test case to a CAdES-A signature as specified in C-A-C-1 test case.

C-A-X-1-C-X-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-X signature as specified in C-X-1 test case to a CAdES-A signature as specified in C-A-X-1 test case.

C-A-XL-1-C-XL-1.xml contains the following Properties: This test case tests the upgrade of a CAdES-BES signature as specified in C-XL-1 test case to a CAdES-A signature as specified in C-A-XL-1 test case.

History

Document history		
v0.1	20 December 2013	Initial draft
v0.2	6 January 2014	Added clause 5
v.1.0	14 January 2014	Final version
v.1.1	20 January 2014	Corrected some typos