Technical Report of the CAdES Remote Plugtests™ Event (June/July 2015)

ETSI

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

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

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

Reference

Keywords
Electronic Signature,

October 2015

Version 1.0

Author:

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

Editor:

Laurent Velez, ETSI laurent.velez@etsi.org

Abstract

This document is the technical report of the 2015 remote Plugtests event on CAdES Digital Signature. (CMS Advanced Electronic Signature ETSI TS 101 733 and EN 319 122), organized by ETSI' s Centre of Testing and Interoperability (CTI) conducted using the specifically designed ETSI portal which supports remote interoperability Plugtests.

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

Status of this Document

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

Contents

1 Introduction

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

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

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

The ETSI TS 119 124 part 1-5 "CAdES Testing Conformance & Interoperability" currently being prepared by the STF 459 is the basis of the testing proposed at the CAdES Plugtests 2015 interoperability event.

This Plugtests event is the 5th of the series of interoperability events scheduled to run for 2 years, as defined in the ETSI SR 003 186. This series of events will address interoperability and conformance needs for all the AdES signatures defined by ETSI.

ETSI has organized the remote Plugtests event on CAdES, held from Thursday 10th june to Friday 24th July 2015 This remote event aims to conduct conformance and interoperability testing on CAdES digital signatures. The testing will cover TS 101 733 but also the draft ETSI EN 319 122.

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

The CAdES specifications are in the process of becoming EN 319 122, but drafts are publicly available for review, so the participants were invited to take in account and to implement the new EN 319 122.

- 319 122-1 CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
- 319 122-2 CAdES digital signatures; Part 2: Extended CAdES signatures

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

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

The present document is the report from the 2015 remote Plugtests Event on CAdES Digital 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 Digital signatures, based on ETSI TS 119 124 "CAdES Testing Conformance& Interoperability

- The Remote Plugtests Event on CAdES was organized by ETSI and held from Thursday 11th June to Friday 24th July 2015.

In order to give participants time to prepare the testing, ETSI opened the portal to participants in "read-only" mode on 9th June, a couple of days before the official start date of the Plugtests event. An introduction web conference took place on Thursday 11th June to present the portal and the testing.

The event was initially planned to run until 10th July but it was extended to 24th July on request from the participants. The reason being that the amount of testing activities was extremely high within the initial scheduled period, due to the large number of participants.

The present document is organized as indicated below.

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

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

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

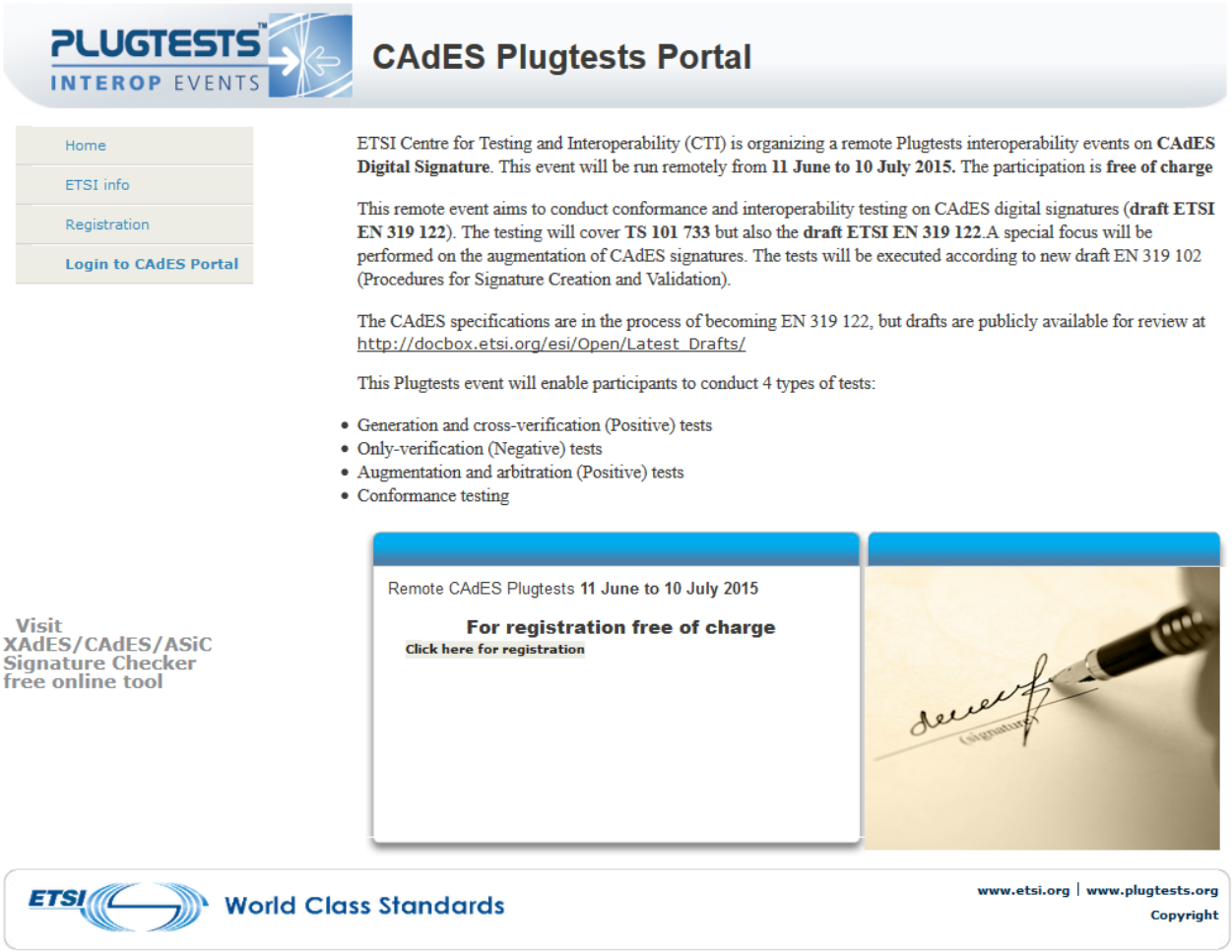
Section 5 provides details on a number of issues related to the CAdES specifications as identified by the participants. These issues have been raised to the ETSI TC ESI, with the recommendation that they are taken into consideration for future CAdES standardization activities, especially for the Draft EN 319 122.

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

2 Organization and contents of the portal

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

2.1 Public part of the portal



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

- The 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, PAdES, CAdES, 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 Interop 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") with different reasons. Each participant may, at his/her own discretion, try to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.

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

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

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

The test suite defined in Test Cases aims at representing a good coverage of the different CAdES specifications existing today, namely ETSI TS 101 733, ETSI TS 103 733, and the ETSI pre EN 319 122.

The CAdES signatures obtained by following the requirements of a good part of the test cases are in fact compliant, at the same time, with ETSI TS 103 173 and ETSI TS 101 733.

Also a part of the test cases lead to CAdES signatures that are compliant with pre EN 319 122.

Below follows the CAdES related specifications that will be addressed:

- ETSI pre EN 319 122. The test suite defined in Test Cases includes test cases for:
  - Part 1. CAdES Baseline signatures CAdES-B-B, CAdES-B-T, CAdES-B-LT, and CAdES-B-LTA levels.
- CAdES ETSI TS 103 173 (v2.2.1). The test suite defined in Test Cases includes test cases for the four conformance levels, identified within this document as CAdES-B conformance level, CAdES-T conformance level, CAdES-LT conformance level, and CAdES-LTA conformance level.
- CAdES ETSI TS 101 733. The test suite defined in Test Cases includes test cases for different CAdES forms.

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 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.

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

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

- **CA-related services**. This service provides issuance of certificates; generation of CRLs; publication of CRLs. Participants should use this service for getting their corresponding certificates for generating 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 have not to develop such a mechanisms in their tools.

2.2.1.4 Online PKI services access page

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

2.2.1.5 Online TSA services access page

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

2.2.1.6 Attribute certificate issuance page

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

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

2.2.1.7 Participants' List page

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

2.2.1.8 Meeting Support page

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

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

2.2.1.9 Mailing list

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

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

2.2.1.10 Chat page

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

2.2.1.11 Known issues pages

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

2.2.2 Contents of 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 a way to archive all the different uploads and keep a complete history of the interop testing of the event.

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

2.2.2.7 Download pages

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

These pages are also used for downloading the entire material generated by the participants at any precise moment during the event including all the 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 2015 CAdES remote Plugtests event.

There were **53 different organizations** and 84 people participating in the event.

#	COMPANY
1	ARhS
2	Ascertia Limited
3	Bit4id
4	Borica - Bankservice AD
5	BULL
6	Bundesnotarkammer
7	Certisign
8	Comfact AB
9	Cryptolog
10	Dignita. s.r.o.
11	Dirección de Impuestos y Aduanas - DIAN Colombia
12	Disig, a.s
13	ecsec GmbH
14	E-Government Innovationszentrum EGIZ
15	ELDOS CORPORATION LTD
16	Enigma S.O.I. Sp. z o.o.
17	ETDA
18	EVAL Tecnologia
19	EXPLAND UAB
20	FINA - Financijska agencija
21	Gemalto
22	Information Services Plc.
23	Insiel S.p.A.
24	Instituto Nacional de tecnologia da Informação
25	intarsys GmbH
26	Kale Yazilim A.S.
27	Lombardia Informatica
28	Microsec zrt
29	MIT-SOFT UAB
30	Národný bezpecnostný úrad
31	National security cabinet of Portugal
32	Noreg Ltd.
33	Nowina Solutions
34	Otip Office

35	Peculiar Ventures, Inc.
36	Polish Security Printing Works
37	Polysys Ltd
38	Safe Creative SL
39	Safelayer Secure Communications
40	SecCommerce Informationssysteme GmbH
41	secrypt GmbH
42	SEFIRA spol. s r.o.
43	SeguriData Privada, S. A. de C. V.
44	Software602 a.s.
45	TECSIDEL
46	Tessaris Integrated Security AG
47	Thales UK
48	Unimatica S.p.A.
49	Unizeto Technologies SA
50	Mentana-Claimsoft GmbH
51	UPC
52	InfoCert
53	IAIK

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 53 organizations from Europe, South America, Turkey and Japan participating, it would have been difficult to organise a face to face event.

4.2 Communication supporting technologies

The utilization of Web conference (GotoWebinar) has been very much appreciated by participants. It has allowed the participants to get very interactive conferences by sharing the same document or application. At the welcome meeting the team explained how to conduct84 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, 4 weeks of testing have been planned for this event, starting from 11th June to 10th July 2015.

In order to let participants read all the documentations and prepare the testing, ETSI has opened the portal on 9th June 2015, 2 days before the official beginning of the interoperability event.

Moreover, for this event, 53 companies were registered. As each company has to verify the signature of the others, the time needed increases with the number of companies and it was agreed that 4 weeks was definitely too short. For this reason the Plugtests team decided to extend the duration of the event until the 24th July 2015.

5 CAdES related Issues

5.1 Introduction

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

5.2 Usage of ‘issuerSerial' element in SigningCertificate/SigningCertificateV2

At the plugtest some participants discussed about the prohibition to use the 'issuerSerial' element of the SigningCertificate/SigningCertificateV2 as stated in CAdES Baseline EN 319 122-1 6.3. e), while including 'issuerSerial' is allowed in PAdES Baseline EN 319 142-1.
In the latest version of TS 102 853 Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies, is stated that the issuerSerial shall be ignored during the validation and so, to avoid having values that might give contradictory information (ignored during the validation), it was decided to recommend, in CAdES and XAdES, to not include issuerSerial element. In the baseline signatures, the signing certificate is included in the signature, thus the issuerSerial is not needed and it was decided to forbid it completely.
In PAdES Baseline EN 319 142-1 it's specified that the syntax of the attributes used to generate the DER-encoded SignedData object included as the PDF signature in the entry with the key Contents of the signature Dictionary shall be as defined in ETSI EN 319 122-1 clause 5. When there are no specific rules defined in PAdES specifications involving how to use the attributes defined in CAdES specifications the rules inherited from CAdES specifications themselves shall be applied. So there isn’t a contradiction between CAdES baseline signatures and PAdES baseline signatures specifications concerning issuerSerial element usage.

As a consequence of this issue was discussed if a PAdES baseline signature shall contain an underlying CAdES baseline signature.
In the table in clause 6.3 of EN 319 142-1, in the row concerning ESS signing certificate v2 there is the reference to EN 319 122-1 clause 5.2.2.3. This reference is intended to specify where the attribute is defined with its syntax.
The requirements for ESS signing certificate and ESS Signing Certificate v2 specify that "Generators shall use either the signing certificate or the signing-certificate v2 attribute, depending on the hash function using, in accordance with ETSI EN 319 122-1 [2]". There is no indication that in a PAdES baseline signature the underlying CAdES signature shall be a baseline one. Indeed the underlying CAdES signature is not a baseline one because it shall not include the signing time attribute.
Another consequence of this issue was the discussion between many participants concerning how to manage the usage of issuerSerial element when creating signatures conforming to TS 101 733 and TS 103 173.
It was stated that even if the future standard explicitly should state that the issuerSerial shall not be included, any signature generated according to TS 101 733 and/or TS 103 173 has to be fully aligned with these specifications.

5.3 Usage of OCSP responses

Some debate was devoted to the format of the OCSP response to be stored in the SignedData.crls.other attribute.

When the full set of revocation data contains OCSP responses, then the OCSP response values shall be included within SignedData.crls.other as specified in IETF RFC 5940.

RFC 5940 requires that:

To carry an OCSP response, the otherRevInfoFormat is set to

id-ri-ocsp-response, which has the following ASN.1 definition:

id-ri-ocsp-response OBJECT IDENTIFIER ::= { id-ri 2 }

In this case, otherRevInfo MUST carry the OCSP response using the OCSPResponse type defined in [OCSP]. The responseStatus field MUST be successful and the responseBytes field MUST be present.

ETSI TS 103 173 did not limit the type of OCSP responses that could be used (so both BasicOCSPResponse and OCSPResponse could be used). There could be some confusion about signatures already generated that used BasicOCSPResponses and it was wondering why baseline profiles don't maintain a backward compatibility.

It was stated that one of the issues of the previous CAdES plugtest was that it was not clear if OCSP responses should be added as OCSPResponse or as BasicOCSPResponse. As a reaction to this issue, the new baseline profile reduces the options making clearer what type of response shall be used. The goal of the baseline profile is to provide rules for generating signatures which are able to fulfil basic requirements, with as less options as possible to make interoperability easier. The decision to not have baseline requirements 100% backward compatible was done for having simpler and clearer profiles. The goal of the EN version is to have a profile as stable as possible.

5.4 ats-hash-index-v2 definition

Some debate was devoted to the format of the ats-hash-index-v2 attribute.

CMS allows to include more than one attribute value of the same type in one attribute. With the current implementation of ATSv3 adding new values into an already existing attribute is not possible. Since it is always possible to add a new attribute instead of adding a new value into an existing attribute, in order to minimize the changes in the current implementations, ESI meeting decided to keep the ats-hash-index-v2 as it is. A sentence stating that it is forbidden to add a new value to an existing attribute, but that instead a new attribute shall be added, should be included in EN 319 122 drafts before its definitive publication.

Peter Rybar proposed the following solutions.

- Creation of a new ats-hash-index-v3, whose rules will be compatible with the CMS signature, which fix a mistake.
- Updating the rules for the ats-hash-index-v2 to fix a mistake with CMS compatibility.
- Creation of a new ATSv4 with additional rules where will be fixed mistakes with CMS compatibility and where additional rules for the new ATSv4 fields will be included.

The second solution is compatible with the current definition in EN 319 122 drafts.

5.5 ats-hash-index-v2 calculation

There were some problems validating the ATSv2 hash for signatures containing ATSv2 and ATSv3, since there were different versions to compute the hash. So the participants discussed about the right way to calculate ats-has-index-v2.

There were different interpretations how to provide input to ats-has-index-v2 calculation. The different interpretations were outlined during discussion and corrected by the participants in their own implementations.

5.6 Signature policy syntax

Some participants complained about the right ASN.1 format for Signature Policies files provided in the plugtests. The main debates concerned about which data the hash value of the signature policy should be calculated and which format some fields should have. It was decided that this discussion was out of scope of the CAdES plugtest.

5.7 Timestamps verification

Some debate was devoted to the timestamps verification in a CAdES baseline T signature.

It was asked if, when validating TSA's certificate chain, it was correct checking that crl's ThisUpdate field was before TimestampToken's GenTime to make sure that the crl downloaded online was issued before the signature's content was time stamped.

It was stated that the timestamp generation time does not impact the validity of the TSA certificate. A TSA should be validated at any time using online objects provided the TSA certificate is not expired/revoked.

5.8 Time ordering in time stamps

There was some debate on the negative test case C-E_AN-1. In this signature the time in the SignatureTimeStamp was ulterior than the time in ArchiveTimeStamp and the participants discussed if a signature should be seen as invalid if it includes a signature time-stamp with date after the ArchiveTimeStamp.

In the proposed negative test case the hash of the ArchiveTimeStamp covered the signature time-stamp and so there was an error somewhere in the time ordering.

However, for TS 101 733 it would be possible first adding an ArchiveTimeStamp on a signature without signature time-stamp and just later on adding a signature time-stamp as unsigned attribute. While, in prEN 319 122-2, when creating a CAdES-E-A signature, we need the signature-time-stamp before adding the ArchiveTimeStamp.

6 CAdES Plugtests testing

6.1 Overall statistics

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

Tests	B-B	B-LT	B-LTA	B-T	E-A	UpdArb
Total	144	27	86	65	19	8

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

Tests	B-B	B-LT	B-LTA	B-T	E-A	UpdArb
Total	1285	171	470	647	85	28

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

Tests	B-BN	B-TN	B-LTAN	E-AN
Total	89	50	4	0

6.2 Generation and Verifications testcases

6.2.1 Test case CAdES-B-B form

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

- TESTCASE:C-B-B-1.xml:

This is the simplest CAdES-B-B signature test case. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. ContentType, MessageDigest and SigningTime attributes shall also be added to the signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

- TESTCASE:C-B-B-2.xml:

In this CAdES-B-B signature test case the signature contains an attributeCertificate of signer-attributes attribute (See 'TS 101 733 5.11.3') in addition to all mandatory attributes.

- TESTCASE:C-B-B-3.xml:

In this CAdES-B-B signature test case the signature contains a ClaimedAttribute of signer-attributes attribute (See 'TS 101 733 5.11.3') in addition to all mandatory attributes.

- TESTCASE:C-B-B-4.xml:

This test case tests a CAdES-B-B signature with multiple independent signatures. The input to this test is a CAdES-B-B signature as specified in C-B-B-1 test case.

- TESTCASE:C-B-B-5.xml:

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

- TESTCASE:C-B-B-6.xml:

This test case tests a CAdES-B-B signature that contains signer-location (See 'EN 319 122-1 5.3.5') and commitment-type-indication (See 'EN 319 122-1 5.3.3') attributes in addition to all mandatory attributes. The signer-location attribute contains at least the countryName and localityName attributes. The commitment-type-indication attribute could indicate "Proof of origin".

- TESTCASE:C-B-B-7.xml:

This test case tests a CAdES-B-B signature that contains a ContentTimeStamp attribute (See 'EN 319 122-1 5.3.8'), which provides time-stamp token of the signed data content before it is signed, in addition to all mandatory attributes.

- TESTCASE:C-B-B-8.xml:

This test case tests a CAdES-B-B signature with an explicit SignaturePolicyIdentifier attribute (See 'EN 319 122-1 5.3.9'). To calculate 'sigPolicyHash' field of 'SignaturePolicyIdentifier' attribute, the file '../../Data/TARGET-SIGPOL-ETSI1.der' shall be used as its input. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType, a MessageDigest and a SigningTime attributes shall also be added to the signature to respect CMS (See 'RFC 5652'). At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

- TESTCASE:C-B-B-9.xml:

This test case tests a CAdES-B-B signature in which digest algorithm SHA1 is used to digest data to be signed. ESSSigningCertificateV1 as specified by "Enhanced Security Services (ESS) RFC 2634" shall be used to reference signing certificate. ContentType, MessageDigest and SigningTime attributes shall also be added to the signature. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

- TESTCASE:C-EN_B-B-10.xml:

In this CAdES-B-B signature test case the signature contains an attributeCertificate of certifiedAttributesV2 of signer-attributes-v2 attribute (See 'EN 319 122-1 5.3.6.1') in addition to all mandatory attributes.

- TESTCASE:C-EN_B-B-11.xml:

In this CAdES-B-B signature test case the signature contains a ClaimedAttribute of signer-attributes-v2 attribute (See 'EN 319 122-1 5.3.6.1') in addition to all mandatory attributes.

- TESTCASE:C-B-B-12.xml:

This is the simplest CAdES-B-B signature test case. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. ContentType, MessageDigest and SigningTime attributes shall also be added to the signature. At

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

6.2.2 Test case CAdES-B-T form

The test cases in this section deal with the `CAdES Baseline level T` signatures.

- TESTCASE:C-B-T-1.xml:

This is the simplest CAdES-B-T signature test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute.

- TESTCASE:C-B-T-2.xml:

This test case tests the adding of an indipendent CAdES-B-T signature to an already signed document containing a CAdES-B-T signature. The input to this test is a CAdES-B-T signature as specified in C-B-T-1 test case.

- TESTCASE:C-B-T-3.xml:

This test case tests the adding of an indipendent CAdES-B-T signature to an already signed document containing a CAdES-B-B signature. The input to this test is a CAdES-B-B signature as specified in C-B-B-1 test case.

- TESTCASE:C-B-T-4.xml:

This is the simplest CAdES-B-T signature test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute.

6.2.3 Test cases for CAdES-B-LT signatures.

The test cases in this section deal with the `CAdES Baseline level LT` signatures.

- TESTCASE:C-B-LT-1.xml:

This is the simplest CAdES-B-LT signature test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES-B-B signatures 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.

- TESTCASE:C-B-LT-2.xml:

This is the simplest CAdES-B-LT signature test case. The signature ONLY CONTAINS the mandatory CAdES properties for CAdES-B-B signatures 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.

- TESTCASE:C-B-LT-3.xml:

This is a CAdES-B-LT signature test case. The signature contains the mandatory CAdES properties for CAdES-B-B signatures, 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.

- TESTCASE:C-B-LT-4.xml:

This is a CAdES-B-LT signature test case. The signature contains the mandatory CAdES properties for CAdES-B-B signatures, 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.

- TESTCASE:C-EN_B-LT-5.xml:

This is a CAdES-B-LT signature test case. The signature contains the mandatory CAdES properties for CAdES-B-B signatures, 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.

- TESTCASE:C-EN_B-LT-6.xml:

This is a CAdES-B-LT signature test case. The signature contains the mandatory CAdES properties for CAdES-B-B signatures, 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.

6.2.4 Test cases for CAdES-B-LTA signatures.

The test cases in this section deal with the CAdES-B-LTA signatures.

- TESTCASE:C-EN_B-LTA-1.xml:

This is the simplest CAdES-B-LTA signature test case. In this case there is one signed data object, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attribute. No attribute certificates are present. The revocation data used are CRLs.

- TESTCASE:C- EN_B-LTA-2.xml:

This is the simplest CAdES-B-LTA signature test case. In this case there is one signed data object, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attribute. No attribute certificates are present. The revocation data used are OCSP responses.

- TESTCASE:C- EN_B-LTA-3.xml:

A test case for testing CAdES-B-LTA signatures. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV2. Afterwards, the resulting long-term-validation signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV2 is included within time-stamp token itself by one of the following methods: (1) the TSU provides the information in the SignedData of the time-stamp token; (2) adding the certificate-values attribute and the revocation-values attribute of the TSP as an unsigned attribute within the time-stamp token. The revocation data used are CRLs.

- TESTCASE:C- EN_B-LTA-4.xml:

A test case for testing CAdES-B-LTA signatures. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV2. Afterwards, the resulting long-term-validation signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV2 is included within time-stamp token itself by one of the following methods: (1) the TSU provides the information in the SignedData of the time-stamp token; (2) adding the certificate-values attribute and the revocation-values attribute of the TSP as an unsigned attribute within the time-stamp token. The revocation data used are OCSP responses.

- TESTCASE:C- EN_B-LTA-5.xml:

A test case for testing CAdES-B-LTA signatures. 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.

- TESTCASE:C- EN_B-LTA-6.xml:

A test case for testing CAdES-B-LTA signatures. 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.

- TESTCASE:C-B-LTA-7.xml:

This is the simplest CAdES-B-LTA signature test case. In this case there is one signed data object, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attribute. No attribute certificates are present. The revocation data used are CRLs.

- TESTCASE:C-B-LTA-8.xml:

This is the simplest CAdES-B-LTA signature test case. In this case there is one signed data object, one SignatureTimeStamp, one Certificates, one Crls, and one ArchiveTimeStampV3 attribute. No attribute certificates are present. The revocation data used are OCSP responses.

- TESTCASE:C-B-LTA-9.xml:

A test case for testing CAdES-B-LTA signatures. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV2. Afterwards, the resulting long-term-validation signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV2 is included within time-stamp token itself by one of the following methods: (1) the TSU provides the information in the SignedData of the time-stamp token; (2) adding the certificate-values attribute and the revocation-values attribute of the TSP as an unsigned attribute within the time-stamp token. The revocation data used are CRLs.

- TESTCASE:C-B-LTA-10.xml:

A test case for testing CAdES-B-LTA signatures. In this case the LT-Level signature was time-stamped with an ArchiveTimeStampV2. Afterwards, the resulting long-term-validation signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV2 is included within time-stamp token itself by one of the following methods: (1) the TSU provides the information in the SignedData of the time-stamp token; (2) adding the certificate-values attribute and the revocation-values attribute of the TSP as an unsigned attribute within the time-stamp token. The revocation data used are OCSP responses.

- TESTCASE:C-B-LTA-11.xml:

A test case for testing CAdES-B-LTA signatures. 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.

- TESTCASE:C-B-LTA-12.xml:

A test case for testing CAdES-B-LTA signatures. 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.

6.2.5 Test cases for CAdES-E-A form.

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

- TESTCASE:C-E-A-1.xml:

This test case tests a CAdES-E-A with ATSv3 built on a CAdES-B-T signature as specified in C-B-T-1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are CRLs.

- TESTCASE:C-E-A-2.xml:

This test case tests a CAdES-E-A with ATSv3 built on a CAdES-B-T signature as specified in C-B-T-1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are OCSP responses.

- TESTCASE:C-E-A-3.xml:

This test case tests a CAdES-E-A with ATSv3 built on a CAdES-B-T signature as specified in C-B-T-1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are CRLs. A CAdES-C timestamp covering the signature, the signature timestamp, the complete-certificate-references attribute and complete-revocation-references attribute shall be included too.

- TESTCASE:C-E-A-4.xml:

This test case tests a CAdES-E-A with ATSv3 built on a CAdES-B-T signature as specified in C-B-T-1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are OCSP responses. A time-stamped-certs-crls-references attribute covering he complete-certificate-references attribute and complete-revocation-references attribute shall be included too.

6.3 Upgrade and Arbitration Test Cases

This section describes 'Upgrade and Arbitration" tests where the organizer acting as a participant (signer) generates a CAdES-B-T 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.

6.3.1 Test cases for upgrading to CAdES-B-LTA signatures.

The test cases in this section deal with the upgrading to CAdES-B-LTA signatures.

- TESTCASE:C-UpdArb-1.xml:

This test case tests a CAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.p7m and generate a CAdES-B-LTA based on archive-time-stamp-v3. Before adding the first archive-time-stamp-v3, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added. Before adding the second archive-time-stamp-v3, the validation material concerning the first archive-time-stamp-v3 shall be added. The validation material included in the certificates and crls entries in SignedData shall be certificates and CRLs.

- TESTCASE:C-UpdArb-2.xml:

This test case tests a CAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.p7m and generate a CAdES-B-LTA based on archive-time-stamp-v3. Before adding the first archive-time-stamp-v3, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added. Before adding the second archive-time-stamp-v3, the validation material concerning the first archive-time-stamp-v3 shall be added. The validation material included in the certificates and crls entries in SignedData shall be certificates and OCSP responses.

- TESTCASE:C-EN_UpdArb-3.xml:

This test case tests a CAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.p7m and generate a CAdES-B-LTA based on archive-time-stamp-v3. Before adding the

first archive-time-stamp-v3, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added. Before adding the second archive-time-stamp-v3, the validation material concerning the first archive-time-stamp-v3 shall be added. The validation material included in the certificates and crls entries in SignedData shall be certificates and CRLs.

- TESTCASE:C-EN_UpdArb-4.xml:

This test case tests a CAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.p7m and generate a CAdES-B-LTA based on archive-time-stamp-v3. Before adding the first archive-time-stamp-v3, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added. Before adding the second archive-time-stamp-v3, the validation material concerning the first archive-time-stamp-v3 shall be added. The validation material included in the certificates and crls entries in SignedData shall be certificates and OCSP responses.

6.4 Negative test cases for verification for CAdES

In the 'negative test' participants will do following:

1. A participating implementation must verify the CAdES signatures. Verification of the CAdES signatures shall be negative. That's why we say 'negative test' for this 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.

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

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

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

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

1. Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory SigningTime attribute
2. Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory SigningCertificate reference attribute
3. Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory ContentType attribute qualifying the signed data object
4. Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory certificates component into CMS signedData object
5. Verify a CAdES-B-B signature having a wrong signature (the hash that was signed isn't the hash computed on the content being signed together with the signed attributes)
6. Verify a document signed with an untrusted signing certificate
7. Verify a document signed with an expired signing certificate
8. Verify a document signed with a revoked/suspended signing certificate

9. Verify a document signed with a signing certificate generated by a CA whose certificate is revoked/suspended

10. Verify a signed document that includes a SignaturePolicyIdentifier attribute with explicit SignaturePolicyId. However its value of SignaturePolicyId.sigPolicyHash field *DOES NOT MATCH* to the hash value of signer policy file

11. Verify a signed document that includes a SignaturePolicyIdentifier attribute with explicit SignaturePolicyId. However its value of SignaturePolicyId.sigPolicyHash field is *NOT IDENTICAL* to the hash value which was calculated by the SignPolicyInfo without ASN.1 tag and length

12. 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

6.4.2 Negative test cases for CAdES-B-T signatures.

The following list summarizes negative test cases for CAdES Baseline level T signatures

1. 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

2. 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

3. Verify a CAdES-B-T signature in which the hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value of signerInfo

4. 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

5. 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

6. Verify a CAdES-B-T signature in which the timestamp signer certificate has been generated by an untrusted CA

7. Verify a CAdES-B-T signature in which the timestamp signer certificate has been generated by a CA whose certificate is revoked/suspended

6.4.3 Negative test cases for CAdES-B-LTA signatures.

1. 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

2. A negative test case for verifying ats-hash-index-v2 content. In this test case, the content in ats-hash-index-v2 element has not the right value related to the CAdES signature to which the ATSv3 has been applied

6.4.4 Negative test cases for CAdES-E-A signatures.

The following list summarizes negative test cases for CAdES-E-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-v2 element has not the right value related to the CAdES signature to which the ATSv3 has been applied

History

Document history		
v0.1	28 Aug 2015	Initial draft
v1.0	Oct 2015	Final version