Technical Report of the PAdES Remote Plugtests™ Event (May 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,

June 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 PAdES (PDF Advanced Electronic Signature ETSI TS 102 778), 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 119 144 "PAdES Testing Conformance & Interoperability" currently being prepared by the STF 459 is the basis of the testing proposed at the PAdES Plugtests 2015 interoperability event.

This Plugtests event is the 4th 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 PAdES, held from Monday 4th May to Friday 5th June 2015. This remote event aimed at conducting interoperability test cases on PAdES signatures ETSI TS 102 778 but also ETSI Draft EN 319 142. A special focus was performed on the augmentation of PAdES signatures and on the usage of some new attributes defined in CAdES and XAdES 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 PAdES specifications are in the process of becoming EN 319 142, but drafts are publicly available for review, so the participants were invited to take in account and to implement the new EN 319 142.

- 319 142-1 PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- 319 142-2 PAdES digital signatures; Part 2: Additional PAdES signatures profiles

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 PAdES Signatures. It also provides details on the specification, design and implementation of the portal supporting remote Plugtests events on PAdES 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 PAdES Remote Plugtests.

The present report provides details on:

- Specification, design and implementation of those testcases description, including cross-verification and negative testcases for PAdES signatures, based on ETSI TS 119 144 "PAdES Testing Conformance& Interoperability

- The Remote Plugtests Event on PAdES was organized by ETSI and held from Monday 4th May to Friday 5th June 2015.

In order to give participants time to prepare the testing, ETSI opened the portal to participants in "read-only" mode on 30 April , few days before the official start date of the Plugtests event. An introduction web conference took place on Monday 4th May to present the portal and the testing.

The event was initially planned to run until 29th May but it was extended to 5th June 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 PAdES Remote Plugtests Event.

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

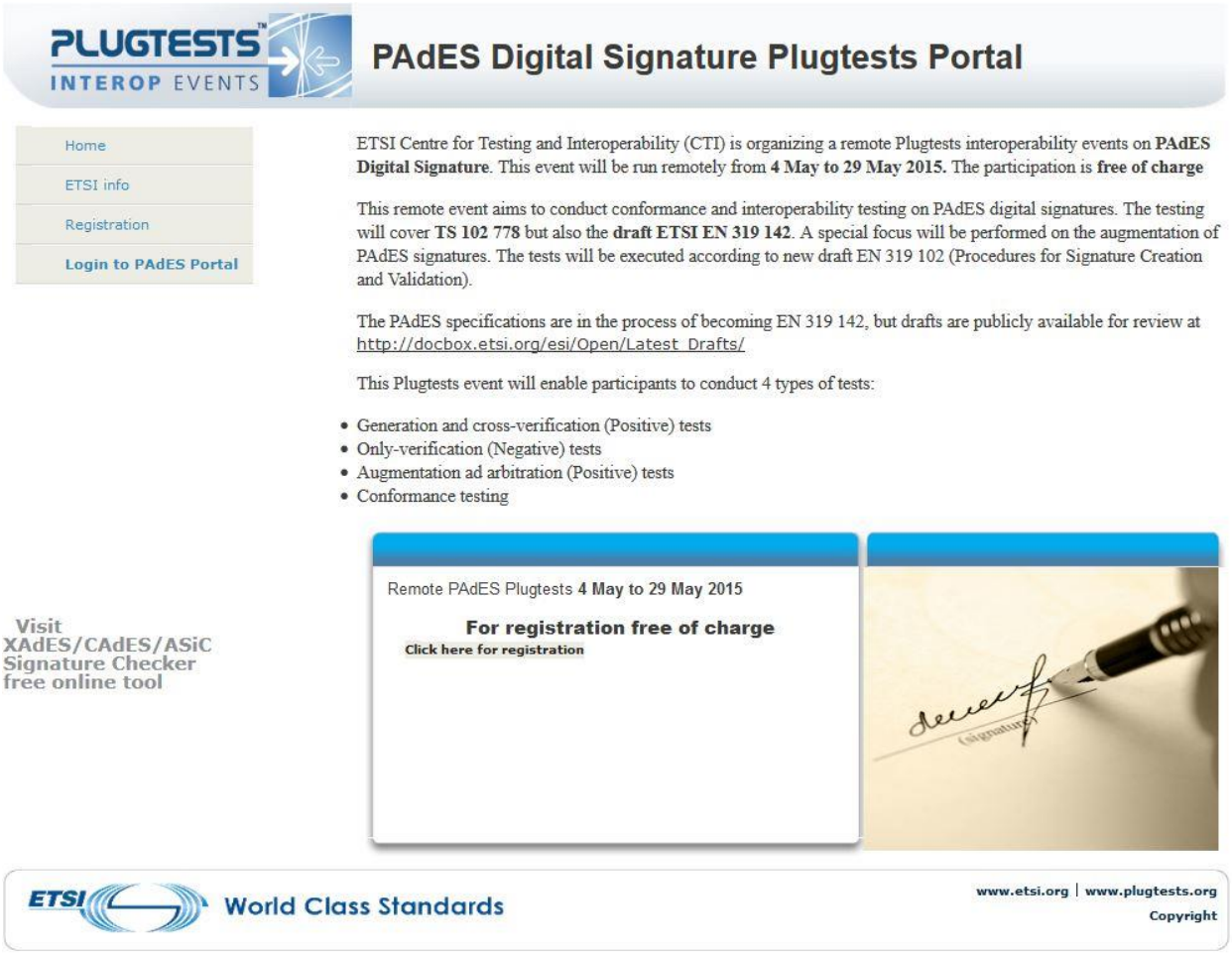
Section 5 provides details on a number of issues related to the PAdES specifications as identified by the participants. These issues have been raised to the ETSI TC ESI, with the recommendation that they are taken into consideration for future PAdES standardization activities, especially for the Draft EN 319 142.

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:

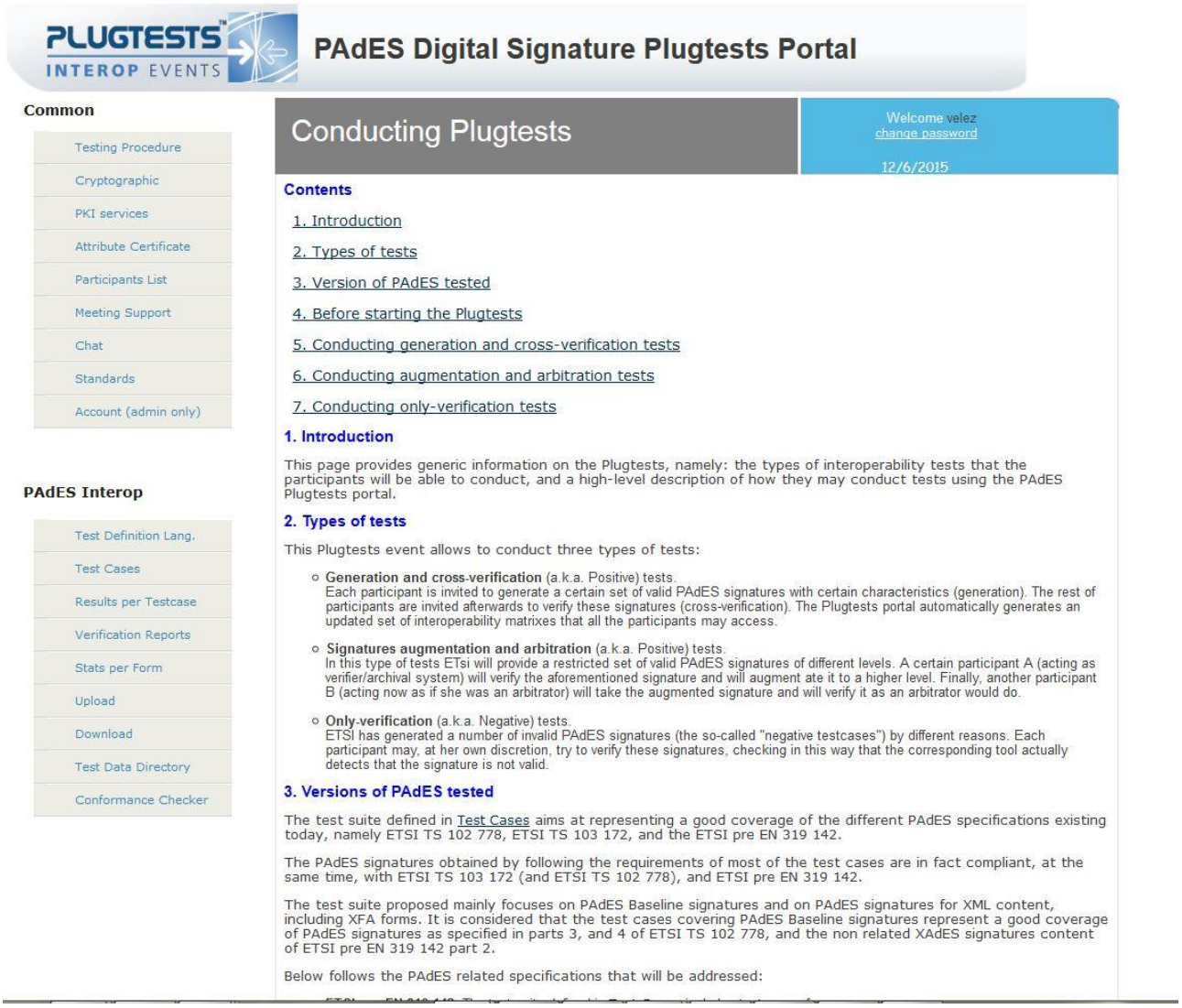
- The PAdES Plugtests page, providing some more details on the event itself, namely targeted specification, targeted audience, some general info on how to conduct such event, etc.
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating 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 PAdES interoperability tests.
- **PAdES specific area**. This area contains a number of pages that support the interoperability tests on PAdES.

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 PAdES 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 PAdES 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 PAdES 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 PAdES (PAdES-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 PAdES-X 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 PAdES signatures to the portal Conformance checker.

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

- ETSI pre EN 319 142. The test suite defined in Test Cases includes test cases for:
  - Part 1. PAdES Baseline signatures PAdES-B-B, PAdES-B-T, PAdES-B-LT, and PAdES-B-LTA levels.
  - Part 2. PAdES-XML signatures.
- PAdES ETSI TS 103 172 (v2.2.2). The test suite defined in Test Cases includes test cases for the four conformance levels, identified within this document as PAdES-B conformance level, PAdES-T conformance level, PAdES-LT conformance level, and PAdES-LTA conformance level.
- **PAdES ETSI TS 102 778.** The test suite defined in Test Cases includes test cases for:
  3. Part 2: "PAdES Basic – Profile based on ISO 32000-1"; (V 1.2.1)
  4. Part 5: "PAdES for XML Content – Profiles for XAdES signatures"; (V 1.1.2). This includes also signatures on XFA 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 PAdES 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, where different scenarios are defined. ETSI defined groups of test cases (for instance a group defining different test cases for PAdES-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 PAdES 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 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 PAdES 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 PAdES 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 PAdES Interop Specific areas of Private part

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

2.2.2.1 Test Cases Definition Language

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

2.2.2.2 Test Cases pages

These are pages containing documents with the complete specification of the test cases for the PAdES 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 PAdES 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 PAdES 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 PAdES signatures generated and verified at each moment of the Plugtests.

The tables show how many signatures of a certain PAdES 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 PAdES 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 PAdES 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 PAdES 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 PAdES remote Plugtests event.

There were **63 different organizations** and 101 people participating in the event.

#	COMPANY
1	e-Contract.be BVBA
2	Certisign
3	Unimatica S.p.A
4	Registro Nacional de identificacin y Estado Civil
5	Consorci AOC
6	Cryptolog
7	Kale Yazilim A.S.
8	Ardaco A.S.
9	Disig A.S.
10	EVAL Tecnologia
11	Noreg Ltd.
12	SEFIRA A.S.
13	Ulicka - Cancelled
14	BULL
15	Software602
16	InfoCert
17	E-Government Innovation Centre
18	ARhS
19	Secrypt GmbH
20	ELDOS CORPORATION LTD
21	Polysys Ltd
22	SIA
23	SecCommerce Informationssysteme GmbH
24	Crux Consultores - Cancelled
25	LangEdge,Inc.

26	Safelayer Secure Communications, S.A.
27	PrimeKey Solutions AB
28	EXPLAND UAB
29	Lombardia Informatica
30	Biznet Bilisim Sistemleri ve Danismanlik Sanayi Ticaret A.S.
31	EUSO
32	MIT-SOFT UAB
33	GEMALTO
34	INTARSYS GmbH
35	Deutsche Rentenversicherung Bund
36	Adobe Systems
37	Governikus KG
38	Seiko Solutions Inc.
39	ARX (Algorithmic Research)
40	AMANO Business Solutions Corporation
41	První certifikacní autorita, a.s.
42	Národný bezpecnostný úrad (National Security Authority)
43	PDFlib GmbH
44	Enigma
45	nSymphony - Cancelled
46	SECOM
47	Nowina Solutions
48	System Art, Inc
49	HyperGEAR, Inc.
50	Morpho
51	Communication & Systèmes
52	Digital Agenda Agency for Romania
53	Peculiar Ventures, Inc.
54	Ascertia Limited
55	Seguridata Privada
56	SIGNificant Signature Solutions GmbH
57	Skaitmeninio sertifikavimo centras (SSC)
58	IT Alkaid Consulting S.A.
59	Microsec ltd.
60	Logalty - Cancelled
61	Unizeto
62	BORICA BANKSERVICE AD
63	NORTAL AS

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 63 organizations from Europe, Turkey, Japan, and Brazil 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, 4 weeks of testing have been planned for this event, starting from 4th May to 29th May 2015.

In order to let participants read all the documentations and prepare the testing, ETSI has opened the portal on 30th April 2015, few days before the official beginning of the interoperability event.

Moreover, for this event, 63 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 5th June 2015.

5 PAdES related Issues

5.1 Introduction

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

5.2 Timestamp definition references

At the Plugtest some participants discussed about the timestamp definition references.

- RFC 3161 requires use of the ESSCertID identifier in the SigningCertificate attribute. This implies the use of SHA-1 hashing algorithm.
- RFC 5816 allows the use of ESSCertIDv2 (inside a SigningCertificateV2 attribute) which supports the use of other hash functions.

At the moment only the reference to RFC3161 is included in ISO 32000-1, the 2014-10 draft of ISO 32000-2, ETSI TS 102 778 and draft EN 319 142. This means that time-stamp tokens that only contain ESSCertIDv2 do not conform to ISO 32000, ETSI TS 102 778 and EN 319 142.

The format documents ETSI EN 319 1x2 have been modified for referencing RFC 5816 too.

5.3 Extensions Dictionary for DSS and DTS validation data and ETSI.CAdES.detached SubFilter

At the Plugtest some participants noticed that in EN 319 142-1 the entry defining the extensions dictionary for ETSI.CAdES.detached SubFilter usage was dropped.

At the Plugtest some participants asked which extensions dictionary shall be used concerning DSS and DTS validation data or ETSI.CAdES.detached SubFilter usage.

5.4 ByteRange for DTS dictionary

At the Plugtest some participants noticed that both in ISO 32000 and ETSI TS and EN specifications it wasn't clearly stated that the ByteRange for DTS dictionary shall cover the entire file including the signature dictionary but excluding the PDF Signature (clearly stated, on the contrary, in the case of Signature Dictionary).

5.5 PKCS#1 and PKCS#7 signatures

It was pointed out that in TS 102 778-3 "Requirements specified in ISO 32000-1 [1], clauses 12.8.3.2 (PKCS#1) and 12.8.3.3 (PKCS#7) signatures as used in ISO 32000-1 [1] do not apply." This requirement is stated in EN 319 142-1 but not in EN 319 142-2. So in PAdES-BES the attribute adbe-revocationInfoArchival could be used. It's better to specify when this attribute can be used (only when SubFilter is "adbe.pkcs7.detached" or both values).

A main conclusion of this topic is that the attribute adbe-revocationInfoArchival may be used only when SubFilter is "adbe.pkcs7.detached".

Moreover, the phrase "Requirements specified in ISO 32000-1 [1], clauses 12.8.3.2 (PKCS#1) and 12.8.3.3 (PKCS#7) signatures as used in ISO 32000-1 [1] do not apply." could be intended that a signature creation application is not obligated to apply the requirements defined in ISO 32000-1 [1], clauses 12.8.3.2 (PKCS#1) and 12.8.3.3 (PKCS#7) but it could make use of what is defined in the above clause while the right intention is to mandate not to use at all what is defined in ISO 32000-1 [1], clauses 12.8.3.2 (PKCS#1) and 12.8.3.3 (PKCS#7).

5.6 Validation data included in SignedData.crls

At the Plugtest some participants asked to have the possibility to include validation in SignedData.crls attribute instead of having to include validation data in DSS and VRI dictionaries only when SubFilter is “ETSI.CAdES.detached“.

A main conclusion of this topic is that validation shall be included only in DSS and VRI dictionaries when SubFilter is “ETSI.CAdES.detached“.

5.7 Management of multiple DSS dictionaries

At the Plugtest some participants asked for a clarification about using several DSS. Considering the way PDF usually works, when you add a "new" DSS, you have to keep all the references (on validation objects) of the first DSS object ***and*** add the new needed references (rather than to add only the new objects and to "forget" the old one).
By this way, a PDF reader uses the same mechanism as usual to parse a PDF, i.e. check the last cross-reference table to find the last PDF catalog, and find a "unique" DSS reference.

It could be possible to find the previous DSS offsets by parsing all the PDF cross-reference tables but this is not the way to do in PDF. Then, a validation algorithm shall check if the offset of this object is included inside one byte-range or another to determine by which signature this object is protected.

The main conclusion of this topic is that when you add a "new" DSS, you have to keep all the references (on validation objects) of the first DSS object ***and*** add the new needed references.

5.8 VRI dictionary purpose

At the Plugtest some participants were wondering about the VRI dictionary purpose. All validation data is stored in the DSS itself and so it seems that VRI dictionary is redundant.

A main conclusion to this topic was that the original purpose for the VRI dictionary was for optimization. Its entries point to the collaterals needed for this specific signature, and it gives the signature validator ability to parse only those collateral items that pertain to the signature being validated and not all collaterals in DSS. In some cases this may improve performance, especially when you have many signatures in the same document that chain up to different roots and contain many CRLs, only small number of which pertain to the signature being validated.

6 PAdES Plugtests testing

6.1 Overall statistics

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

Tests	B-B	B-LT	B-LTA	B-T	PK7	XFA	XML	LTV	BES
Total	91	36	42	45	52	1	7	33	14

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

Tests	B-B	B-LT	B-LTA	B-T	PK7	XFA	XML	LTV	BES
Total	1067	236	423	480	379	0	7	237	65

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

Tests	B-BN	B-TN	PK7N
Total	60	45	61

6.2 Generation and Verifications testcases

6.2.1 Test case PAdES-PK7 form

The test cases in this section deal with the PAdES-PK7 form (PAdES Basic, based on ISO 32000-1).

A byte range digest shall be computed over a range of bytes in the file, that shall be indicated by the ByteRange entry in the signature dictionary. This range shall be the entire file, including the signature dictionary but excluding the signature value itself (the Contents entry). The signature is encoded in CMS defined by PKCS #7 1.5 (RFC 2315), placed into the Contents entry of the signature dictionary and at minimum contains the signer's X.509 signing certificate. The signature dictionary shall not contain a Cert entry.

TESTCASE:P-PK7-1.xml description:

This test case tests the simplest PADES Basic form with SigningTime entry in signature dictionary by using sha256 as hashing algorithm. Implementation shall add a adbe.pkcs7.detached subfilter key and a Contents key in signature dictionary.

TESTCASE:P-PK7-2.xml description:

This test case tests a PADES Basic signature with signature time stamp attribute which ensures the time of signing, Location attribute which describes where the data was signed (CPU host name or physical location), Reason attribute that describes the reason for the signing, ContactInfo attribute that provides information to enable a recipient to contact the signer to verify the signature. Implementation may insert any value in Location, Reason and ContactInfo keys as far as respecting PAdES.

TESTCASE:P-PK7-3.xml description:

This test case tests a PADES Basic signature with SigningTime entry in signature dictionary and adbe Revocation Information attribute, by using sha256 as hashing algorithm. Implementation shall add a certificate revocation list, described in RFC 5280, as a Revocation Information attribute.

TESTCASE:P-PK7-4.xml description:

This test case tests a PADES Basic signature with SigningTime entry in signature dictionary and adbe Revocation Information attribute, by using sha256 as hashing algorithm. Implementation shall add an OCSP response, described in RFC 6960, as a Revocation Information attribute.

And results in the following Interop Matrix:

TESTCASE:P-PK7-5.xml description:

This test case tests a PADES Basic certification signature with SigningTime entry in signature dictionary and LegalContentAttestation attributes.

TESTCASE:P-PK7-6.xml description:

This test case tests a PADES serial signature. Implementation shall create a signed document adding a adbe.pkcs7.detached subfilter attribute, a Content attribute and a SigningTime entry in signature dictionary by using sha256 as hashing algorithm and then add to the above document a serial signature by using the same attributes and hashing algorithm used in the first signature operation.

6.2.2 Test cases for PAdES-B-B signatures.

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

A byte range digest shall be computed over a range of bytes in the file, that shall be indicated by the ByteRange entry in the signature dictionary. This range shall be the entire file, including the signature dictionary but excluding the signature value itself (the Contents entry). A DER-encoded SignedData object as specified in CMS (RFC 3852) shall be included as the PDF signature in the entry with the key Content of the signature dictionary. The signature dictionary shall contain a value of ETSI.CAdES.detached for the key SubFilter. The signature dictionary shall not contain a Cert entry.

TESTCASE:P-B-B-1.xml description:

This test case tests the simplest PAdES-B-B signature with SigningTime entry in signature dictionary. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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:P-B-B-2.xml description:

This test case tests a PAdES-B-B signature with SigningTime, Location, Reason of signature and ContactInfo entries in signature dictionary. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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:P-EN_B-B-3.xml description:

This test case tests a PAdES-B-B signature with a ClaimedAttribute of signer-attributes-v2 attribute (See 'EN 319 122-1 5.3.6.1') which describes the signer's claimed attribute. Implementation may add any value of a ClaimedAttribute as far

as respecting PAdES and CAdES. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

TESTCASE:P-EN_B-B-4.xml description:

This test case tests a PAdES-B-B signature with attributeCertificate of certifiedAttributesV2 of signer-attributes-v2 attribute (See 'EN 319 122-1 5.3.6.1') which describes the signer's attribute. In the attributeCertificate, your X.509 V2 attribute certificate assigned to your public key certificate shall be included. At least the signing certificate shall be included in the SignedData.certificates field. All certificates needed for path building should be included too.

TESTCASE:P-B-B-5.xml description:

This test case tests a PAdES-B-B signature with 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. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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 can be included too.

TESTCASE:P-B-B-6.xml description:

This test case tests a PAdES-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 and a MessageDigest 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 can be included too.

TESTCASE:P-B-B-7.xml description:

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

6.2.3 Test cases for the PAdES-B-T signatures.

TESTCASE:P-B-T-1.xml description:

This test case tests the simplest PAdES-B-T signature with signature-time-stamp attribute which is the most common optional attribute in CMS SignedData and describes trusted time when the data was signed. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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 can be included too.

TESTCASE:P-EN_B-T-2.xml description:

This test case tests a PAdES-B-T signature with ClaimedAttribute of signer-attributes-v2 attribute (See 'EN 319 122-1 5.3.6.1') which describes the signer's claimed attribute. Implementation may add any value of a ClaimedAttribute as far as respecting PAdES and CAdES. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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 can be included too.

TESTCASE:P-B-T-3.xml description:

This test case tests a PAdES-B-T 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 and a MessageDigest 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 can be included too.

TESTCASE:P-B-T-4.xml description:

This test case tests a PAdES-B-T signature with 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. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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 can be included too.

6.2.4 Test cases for PAdES-B-LT signatures.

The test cases in this section deal with the PAdES-B-LT signatures.

For the purpose to verify the signatures of a signed PDF document long after their creation, in particular after the signing certificates have expired, because the original validation data (such as CA certificates, CRLs, OCSP) may no longer be available (the cryptographic protection afforded by the signature could not be guaranteed after the certificate has expired too), some extensions to ISO 32000-1 can be used.

1. Document Security Store (DSS) that is able to carry validation data necessary to validate a signature, optionally with Validation Related Information (VRI) which relates the validation data to a specific signature.

The B-LT format adds validation stuff to a signed PDF so possible input is P-B-T-1 (with Signature Time Stamp)

TESTCASE:P-B-LT-1.xml description:

This test case tests a PAdES-B-LT signature. Participating implementations generate and verify P-B-T-1 signature and a subsequent PAdES-B-LT based on DSS with Certs and CRLs. DSSCerts and DSSCRLs entries shall contain references to certificates and CRLs needed to validate the signature.

TESTCASE:P-B-LT-2.xml description:

This test case tests a PAdES-B-LT signature. Participating implementations generate and verify P-B-T-1 signature and a subsequent PAdES-B-LT based on DSS with Certs and OCSPs. DSSCerts and DSSOCSPs entries must contain references to certificates and OCSP responses needed to validate the signature.

TESTCASE:P-B-LT-3.xml description:

This test case tests a PAdES-B-LT signature. Participating implementations verify the P-B-T-1 ETSI signature, generate and verify a second signature as described in P-B-T-1 test cases itself and a subsequent PAdES-B-LT based on DSS with Certs and CRLs and VRI with Cert and CRL. DSSCerts and DSSCRLs entries shall contain references to certificates and CRLs needed to validate the signatures. VRICert and VRICRL entries must contain references to certificates and CRLs needed to validate the second signature present in the document.

TESTCASE:P-B-LT-4.xml description:

This test case tests a PAdES-B-LT signature. Participating implementations verify the P-B-T-1 ETSI signature, generate and verify a second signature as described in P-B-T-1 test cases itself and a subsequent PAdES-B-LT based on DSS with Certs and OCSPs and VRI with Cert and OCSP. DSSCerts and DSSOCSPs entries shall contain references to certificates and OCSP responses needed to validate the signatures. VRICert and VRIOCSP entries must contain references to certificates and OCSP responses needed to validate the second signature present in the document.

6.2.5 Test cases for PAdES-B-LTA signatures.

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

For the purpose to verify the signatures of a signed PDF document long after their creation, in particular after the signing certificates have expired, because the original validation data (such as CA certificates, CRLs, OCSP) may no longer be available (the cryptographic protection afforded by the signature could not be guaranteed after the certificate has expired too), some extensions to ISO 32000-1 can be used.

1. Document Security Store (DSS) that is able to carry validation data necessary to validate a signature, optionally with Validation Related Information (VRI) which relates the validation data to a specific signature.
2. Document Time Stamp that is able to extend document life-time.

The B-LTA format adds validation stuff to a signed PDF so possible input is P-B-T-1 (with Signature Time Stamp)

TESTCASE:P-B-LTA-1.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations verify P-B-LT-1 signature and generate a subsequent PAdES-B-LTA based on DTS. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-B-LTA-2.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations verify P-B-LT-2 signature and generate a subsequent PAdES-B-LTA based on DTS. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-B-LTA-3.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations verify P-B-LT-3 signature and generate a subsequent PAdES-B-LTA based on DTS. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-B-LTA-4.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations verify P-B-LT-4 signature and generate a subsequent PAdES-B-LTA based on DTS. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

6.2.6 Test cases for PAdES-LTV form.

The test cases in this section deal with the PAdES-LTV form.

For the purpose to verify the signatures of a signed PDF document long after their creation, in particular after the signing certificates have expired, because the original validation data (such as CA certificates, CRLs, OCSP) may no longer be available (the cryptographic protection afforded by the signature could not be guaranteed after the certificate has expired too), some extensions to ISO 32000-1 can be used.

1. Document Security Store (DSS) that is able to carry validation data necessary to validate a signature, optionally with Validation Related Information (VRI) which relates the validation data to a specific signature.
2. Document Time Stamp that is able to extend document life-time.

The LTV format adds validation stuff to a signed PDF so possible input is P-B-T-1 (with Signature Time Stamp)

TESTCASE:P-LTV-1.xml description:

This test case tests a PAdES-LTV signature. Participating implementations generate and verify a PAdES signature including a timestamp (i.e. P-PK7-2 or P-B-T-1 signature) and generate a subsequent PAdES-LTV based on DSS and DTS. DSSCerts and DSSCRLs entries shall contain references to certificates and CRLs needed to validate the signature. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-LTV-2.xml description:

This test case tests a PAdES-LTV signature. Participating implementations generate and verify a PAdES signature including a timestamp (i.e. P-PK7-2 or P-B-T-1 signature) and generate a subsequent PAdES-LTV based on DSS and DTS. DSSCerts and DSSOCSPs entries must contain references to certificates and OCSP responses needed to validate the signature. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-LTV-3.xml description:

This test case tests a PAdES LTV format. Participating implementations apply a Document time-stamp and verifies on unsigned pdf document. Only one Document TimeStamp is necessary.

TESTCASE:P-LTV-4.xml description:

This test case tests a PAdES LTV format. Participating implementations apply a Document time-stamp and verifies on unsigned pdf document (that's the output of P-LTV-3 test case), then apply DSS based on VRI with Certificates and CRL responses. VRICert and VRICRL entries must contain references to certificates and CRLs needed to validate the first timestamp, and then apply and verify another Document time-stamp. Two Document TimeStamps are needed.

6.2.7 Test cases for PAdES-XML form.

The test cases in this section deal with the PAdES-XML form.

1st Profile: XML signed document that is embedded within a PDF file

An XML document created and signed with XAdES (forms XAdES-B-B, XAdES-B-T) out of PDF framework can be embedded within a PDF container and transported within it.

For the purpose to verify the signatures of an XML document signed with XAdES and embedded within a PDF container long after their creation, a verifier may extracts the XML document, verify the XAdES signature, upgrade the XAdES signature itself (to more evolved forms) and embeds again the modified XML document within the PDF container.

The xades;SigningCertificate or the ds:KeyInfo element must be used to secure the signing certificate.

TESTCASE:P-XML-1.xml description:

This test case tests a XADES-B-B signature with the signed properties “SignedSignatureProperties” containing the SigningTime, SigningCertificate, SignatureProductionPlace, SignerRole attributes.

TESTCASE:P-XML-2.xml description:

This test case tests a XADES-B-T signature with the signed properties “SignedDataObjectProperties” and unsigned properties SignatureTimeStamp. The DataObjectFormat, CommitmentTypeIndication, AllDataObjectsTimeStamp, “SignedDataObjectProperties” have to be used.

TESTCASE:P-XML-3.xml description:

This test case tests a CounterSignature. The XML file is XADES-B-B signature. For simplicity the CounterSignature can be from the same previous signer.

TESTCASE:P-XML-4.xml description:

This test case tests a XADES-B-LTA signature containing the following properties: SignatureTimeStamp, CertificateValues, RevocationValues, ArchiveTimeStamp.

6.2.8 Test cases for PAdES-XFA form.

The test cases in this section deal with the PAdES-XFA form.

2nd Profile: XADES signatures for signing dynamic XFA forms

The XAdES signature will be able to sign XFA data only or any XML content from XFA allowed by XFA specification, Signature is encoded as XAdES-B-B and XAdES-B-T forms.

The xades:SigningCertificate or the ds:KeyInfo element must be used to secure the signing certificate.

For long-term validation XAdES signatures on XFA the LTV technology (XAdES-B-LT or XAdES-B-LTA signatures) can be used.

TESTCASE:P-XFA-1.xml description:

This test case tests a XADES-B-T signature. The XFA signed file is a XADES-B-T signature with the signed properties SigningCertificate, SignatureProductionPlace, SigningTime and SignerRole, and a SignatureTimeStamp.

TESTCASE:P-XFA-2.xml description:

This test case tests a CounterSignature. The XFA signed file is XADES-B-B signature with an enveloped CounterSignature

TESTCASE:P-XFA-3.xml description:

This test case tests PAdES-B-LTA signature. Its VRICert and VRICRL entries must contain references to certificates and CRLs needed to validate the XADES signature inserted in the document in XFA forms. Participating implementation generates and verifies one P-XFA-1 signature and a subsequent PAdES-LTV based on VRI with Certificates and CRLs. This signature has a Document time-stamp.

6.2.9 Test cases for PAdES-BES form.

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

A byte range digest shall be computed over a range of bytes in the file, that shall be indicated by the ByteRange entry in the signature dictionary. This range shall be the entire file, including the signature dictionary but excluding the signature value itself (the Contents entry). A DER-encoded SignedData object as specified in CMS (RFC 5652) shall be included as the PDF signature in the entry with the key Contents of the signature dictionary. The signature dictionary shall contain a value of ETSI.CAdES.detached for the key SubFilter. The signature dictionary shall not contain a Cert entry.

TESTCASE:P-BES-1.xml description:

This test case tests a PADES-BES signature with SigningTime entry in signature dictionary and adbe Revocation Information attribute, by using sha256 as hashing algorithm. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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. Implementation shall add a certificate revocation list, described in RFC 5280, as a Revocation Information attribute.

TESTCASE:P-BES-2.xml description:

This test case tests a PADES-BES signature with SigningTime entry in signature dictionary and adbe Revocation Information attribute, by using sha256 as hashing algorithm. Implementation shall add a ESSSigningCertificateV2 attribute to generating signature. A ContentType and a MessageDigest 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. Implementation shall add an OCSP response, described in RFC 6960, as a Revocation Information attribute.

6.3 Upgrade and Arbitration Test Cases

This section describes 'Upgrade and Arbitration" tests where ETSI (signer) generates a basic signature, a second participant (verifier) upgrades it after verifying, by using EU TL, 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 PAdES-B-LTA signatures.

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

TESTCASE:P-UpdArb-1.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.pdf and generate a PAdES-B-LTA based on DSS and DTS. DSS will include Certs and CRLs entries. DSSCerts and DSSCRLs entries shall contain references to certificates and CRLs needed to validate the signature. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-UpdArb-2.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.pdf and generate a PAdES-B-LTA based on DSS and DTS. DSS will include Certs and OCSPs entries. DSSCerts and DSSOCSPs entries must contain references to certificates and OCSP responses needed to validate the signature. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-UpdArb-3.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.pdf, generate a PAdES-B-LTA based on DSS and DTS, add a new signature as in P-B-T-1 test case and generate a PAdES-B-LTA based and DSS and DTS. DSS will include Certs and CRLs entries. DSSCerts and DSSCRLs entries shall contain references to certificates and CRLs needed to validate the signature. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

TESTCASE:P-UpdArb-4.xml description:

This test case tests a PAdES-B-LTA signature. Participating implementations, by using EU TL, verify the signed file Signed_TimeStamped_EU_TL.pdf, generate a PAdES-B-LTA based on DSS and DTS, add a new signature as in P-B-T-1 test case and generate a PAdES-B-LTA based and DSS and DTS. DSS will include Certs and OCSPs entries. DSSCerts and DSSOCSPs entries must contain references to certificates and OCSP responses needed to validate the signature. DTSType shall be valued DocTimeStamp. DTSSubFilter shall be valued ETSI.RFC3161.

6.4 Negative test cases for verification for PAdES

In the 'negative test' participants will do following:

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

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

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

6.4.1 Negative test cases for PAdES-PK7 form.

1. Verify a signed pdf document having a wrong signature (the hash that was signed isn't the hash of the specified byte range)
2. Verify a pdf document signed with an untrusted signing certificate
3. Verify a pdf document signed with an expired signing certificate
4. Verify a pdf document signed with a revoked/suspended signing certificate
5. Verify a signed pdf document containing an untrusted signature timestamp
6. Verify a signed pdf document containing an expired signature timestamp
7. Verify a signed pdf document containing a revoked signature timestamp
8. Verify a signed pdf document having a wrong byte range

6.4.2 Negative test cases for PAdES-B-B signatures.

1. Verify a signed pdf document having a wrong signature (the hash that was signed isn't the hash of the specified byte range)
2. Verify a pdf document signed with an untrusted signing certificate
3. Verify a pdf document signed with an expired signing certificate
4. Verify a pdf document signed with a revoked/suspended signing certificate
5. Verify a pdf document signed with a signing certificate generated by a CA whose certificate is revoked/suspended

6.4.3 Negative test cases for PAdES-B-T signatures.

1. Verify a signed pdf document having a wrong time stamp signature (the signature that was timestamped is not pdf document signature)

2. Verify a signed pdf document containing an untrusted signature timestamp
3. Verify a signed pdf document containing an expired signature timestamp
4. Verify a signed pdf document containing a revoked signature timestamp
5. Verify a signed pdf document containing a signature timestamp signed by a certificate generated by a CA whose certificate is revoked/suspended

History

Document history		
v0.1	12 June 2015	Initial draft
v1.0	15 July 2015	Final version