Technical Report of the eSignature Validation Remote Plugtests Nov-Dec 2014

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,
Plugtests

January 2015
Version 1.0
Author:
Robert Bielecki, ARHS
Juan Carlos Cruellas, UPC
Laurent Velez, ETSI

Editor:
Laurent Velez, ETSI laurent.velez@etsi.org

Abstract

This document is the technical report of the 2014 remote Plugtests event on eSignature Validation (ETSI TS 102 853), organized by ETSI 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 5
2 Organization and contents of the portal 6
2.1 Public part of the portal 6
2.2 Private part of the portal 7
2.2.1 Contents of the Common area in the Private part 8
2.2.1.1 Conducting Plugtests information pages 8
2.2.1.2 Participants' List page 8
2.2.1.3 Meeting Support page 8
2.2.1.4 Mailing list 9
2.2.1.5 Chat page 9
2.2.1.6 Technical Discussions pages 9
2.2.2 Contents of eSignature Validation Interop Specific areas of Private part 9
2.2.2.1 Upload "new" Signature page 9
2.2.2.2 Upload Verification pages 10
2.2.2.3 Verification reports 10
2.2.2.4 Download pages 10
2.2.2.5 Test data directory pages 10
3 Signature Generation 11
3.1 Types of signatures to be generated 11
3.2 Certificates 11
3.3 Signatures details per format 11
3.3.1 CAdES signatures 11
3.3.2 PAdES signatures 11
3.3.3 XAdES signatures 12
3.3.4 ASiC Containers 12
3.3.5 File names convention 12
4 Participants list 14
5 Plugtests conclusions 16
5.1 Remote vs. Face to Face 16
5.2 Communication supporting technologies 16
5.3 Event duration 16
6 eSignature Validation related Issues 17
6.1 Presence/absence of the POE in case of a revoked or expired certificate 17
6.2 Weak algorithm 17
6.3 Mandatory signed properties 17
6.4 Claimed signing time 17
6.5 Multiple signatures 18
6.6 PAdES SubFilter 18
6.7 Trust anchor 18
6.8 TSL issues 18
6.9 CRL and critical extensions 18
6.10 Timestamp without the trust anchor defined as TSP 18
6.11 PDF and CMS signing-time 18
6.12 CAdES: BasicOCSPResponse or OCSPResponse 19
6.13 Expired or revoked certificate in the TSL 19
6.14 ASiC: Value of the manifest:version attribute 19
History 20

1 Introduction

Under the Services Directive a couple of legal and practical measures have been taken by the European Commission to facilitate the use of e-signatures across borders. The Member States who ask for e-signatures in the context of their administrative procedures should allow the use of e-signatures originating from the other Member States and put in place technical solutions to be able to process as a minimum the common formats of e-signatures as described in Decision 2011/130/EU1, as amended by the Implementing Decision 2014/148/EU2.

In order to ensure the cross-border dimension, it is necessary to assess which problems arise in practice for cross-border validation of e-signatures via mutually checking the Member States' signatures against their existing e-signature validation applications. In order to support cross-border interoperability, an e-signature validation Plugtest has been organized by ETSI in cooperation with the European Commission from 3 November to 12 December 2014.

The aim of this Plugtest was twofold. First, it tried to take stock of what the Member States currently have as e-signatures used for their e-government purposes and to test whether these can be validated in other Member States. Second, it aimed at detecting possible issues in different validation processes and identifying possible divergencies in the validation applications for the same signature used.

A number of Member States had already submitted signatures to the Commission before the Plugtest which were taken over and stored on the portal to be validated by the Plugtest participants. In addition to e-signatures already submitted, there was a need to have additional e-signatures that would on the one hand allow testing certain features of the Trusted Lists and also validating e-signatures created according to the ETSI AdES baseline profiles. For the latter reason participants had the possibility to upload new/additional signatures that fulfilled the defined criteria.

The testing provided test coverage of the specification ETSI TS 102 853 (Signature verification procedures and policies) and covered the validation of the 4 main eSignature formats (XAdES, CAdES, PAdES and ASiC)

The present document is the report from the 2014 remote Plugtests Event on eSignature Validation. It also provides details on the specification, design and implementation of the portal supporting remote Plugtests events , including an overview of the contents of the portal .The present report provides details on:

- Specification, design and implementation of those test descriptions, including cross-verification and negative tests for signatures validation, based on ETSI TS 102 853.
- The Remote Plugtests Event on eSignature Validation organized by ETSI with the support of European Commission, and held from Monday 3rd November to Friday 12th December 2014.

In order to give participants time to prepare for the testing, ETSI opened the portal to participants in "read-only" mode on 27th October, a week before the official start date of the Plugtest event. An introduction web conference took place on Monday 3rd November to present the portal and the testing.

The event was initially planned to run until 21st of November but it was extended to 12th of December 2014, on the request from the participants. The reason behind was the amount of testing activities which was extremely high within the initial scheduled period, due to the large number of participants and the number of proposed signatures to validate.

The present document is divided into the following sections:

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

Section 3 provides an overview of the requirements and guidance given for the generation of new signatures during the Plugtest.

Section 4 lists the participants to the 2014 eSignature Validation Remote Plugtests Event.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1412147852707&uri=CELEX:32011D0130
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014D0148

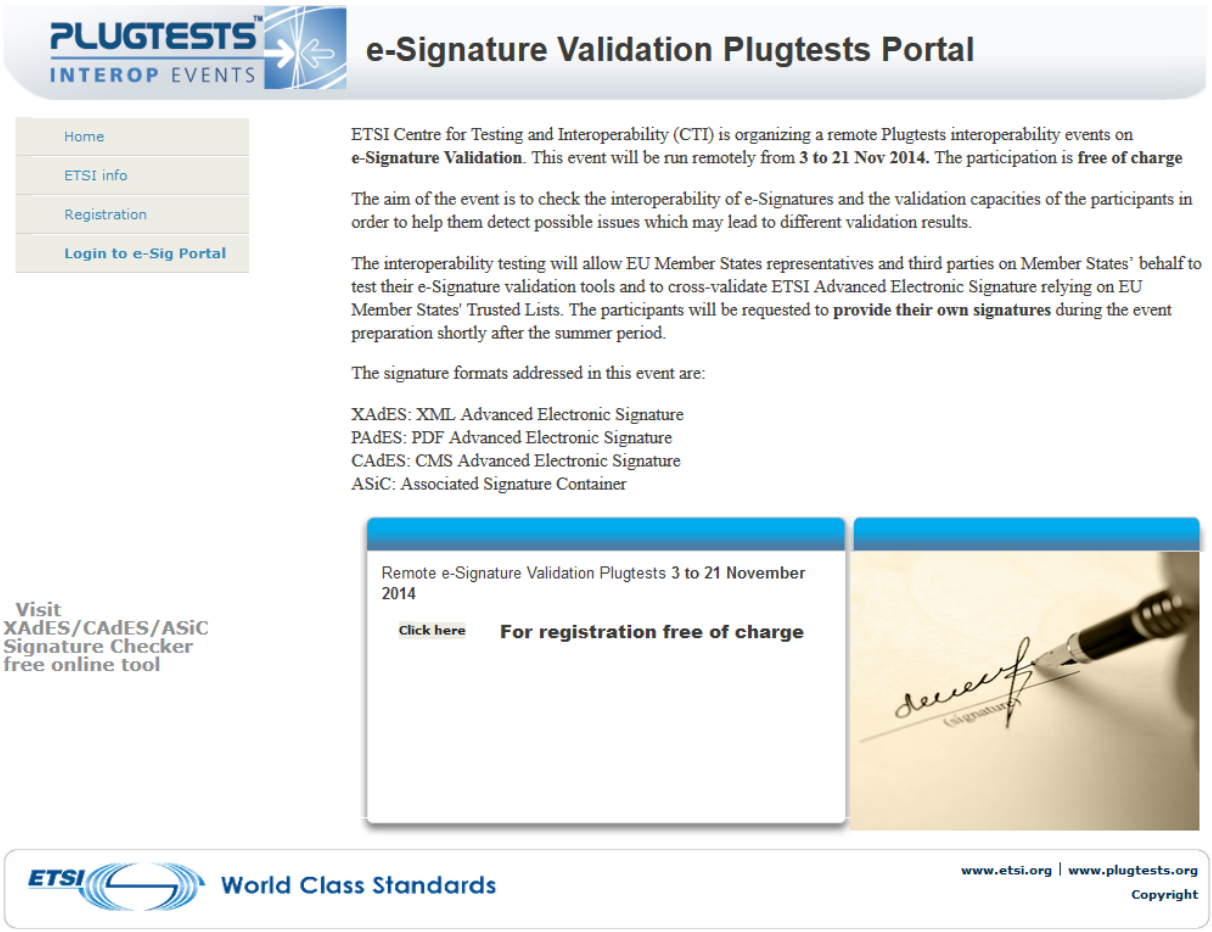
Section 5 provides a summary of the most important results and conclusions of the Plugtests.

Section 6 provides details on a number of issues related to the specifications as identified by the participants. These issues will be raised to the ETSI TC ESI, with the recommendation that they are taken into consideration for future standardization activities.

2 Organization and contents of the portal

The portal had two different parts, namely the public part, that anybody could 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 remained as it was for previous events. It includes the following contents:

- The Plugtests page, providing some more details on the event itself, namely targeted specification, targeted audience, some general info on how to conduct such event, etc.
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating exchange of information.
- The Registration page, providing details on the Plugtests registration process.
- The Presentation of the Plugtests team.

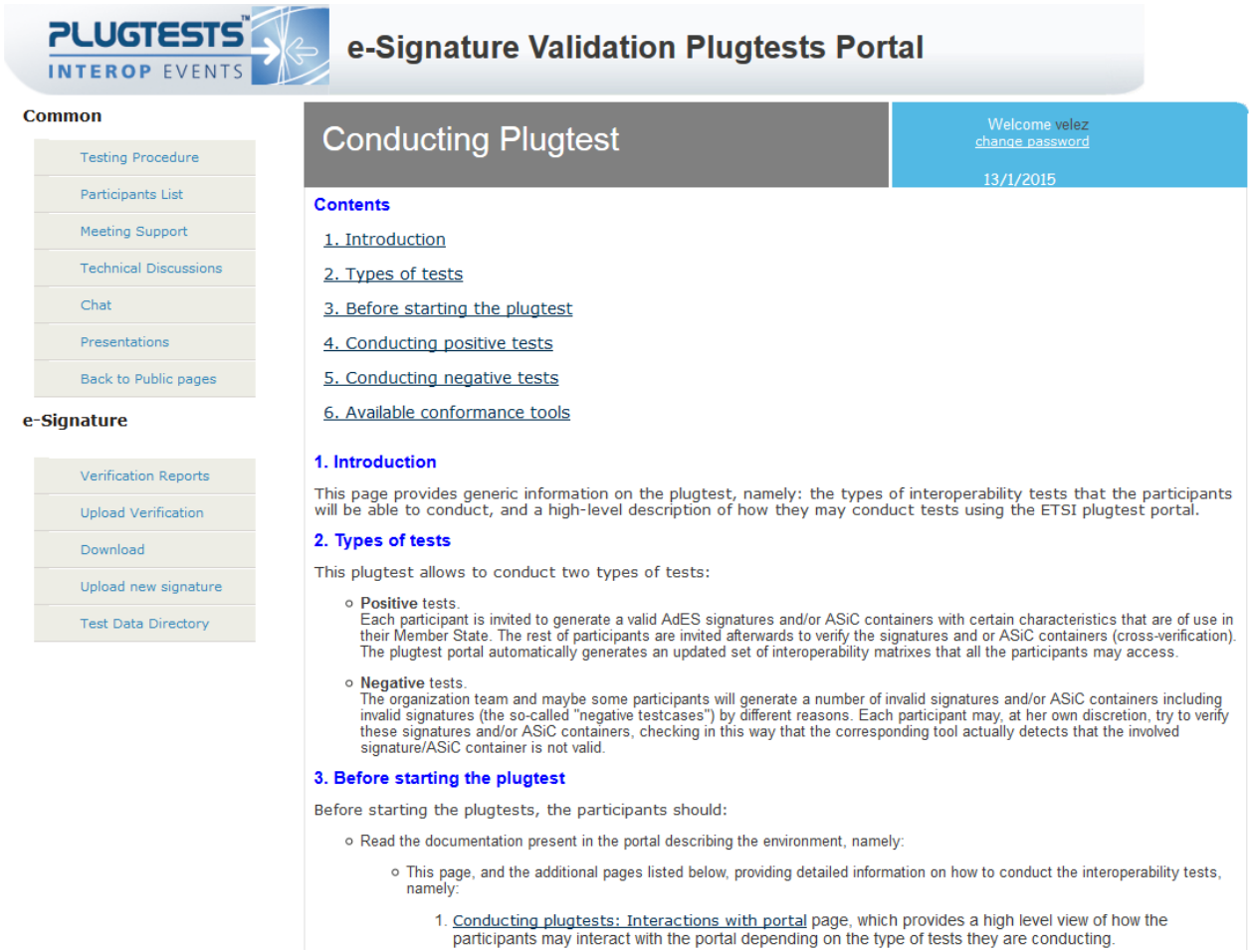
- The Presentation of some past events (XAdES, CAdES, PAdES, ASiC)
- The **Login to Plugtests Area** page gives access to the **protected area** of the portal.

2.2 Private part of the portal

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

- **Common area**. This area contained a number of pages that provided generic information to the participants, which was relevant to the participants of the interoperability event.
- **E-Signature specific area**. This area contained a number of pages that supported the interoperability tests on eSignature Validation.

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



2.2.1 Contents of the Common area in the Private part

2.2.1.1 Conducting Plugtests information pages

The Conducting Plugtests page was the first of a set of 7 pages providing detailed explanations on how to conduct tests during the event.

This first page detailed the 2 types of tests provided at this Plugtests event:

- **Positive** tests.
  Each participant was invited to generate some valid AdES signatures and/or ASiC containers with certain characteristics that are of use in their Member State. The rest of participants were invited afterwards to verify the signatures and or ASiC containers (cross-verification). The plugtest portal automatically generated an updated set of interoperability matrixes that all the participants could access.

- **Negative** tests**.**
  The organization team and some participants were expected to generate a number of invalid signatures and/or ASiC containers including invalid signatures (the so-called "negative testcases") , where the invalidity would have different causes. Each participant could, at their own discretion, try to verify these signatures and/or ASiC containers, checking in this way that the corresponding tool actually detected that the involved signature/ASiC container was invalid.

An access to Conformance testing tools was provided to the participants on a dedicated portal.

These online tools perform numerous checks in order to verify the conformity of the ETSI Advanced Electronic Signatures.

The tool performs conformance tests on:

- XAdES Baseline Profile ETSI TS 103 171
- CAdES signatures (CMS Advanced Electronic Signature ETSI TS 101 733)
- ASiC signatures (Associated Signature Container ETSI TS 102 918)

The rest of the pages of the set provided 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 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 Participants' List page

This page listed the details of all the companies and people that participated in the Plugtests, as well as their login names.

2.2.1.3 Meeting Support page

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

- Introductory presentation which was made available before the start of the Plugtests, and 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.

2.2.1.4 Mailing list

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

After each upload of signatures or verification reports, an email was sent to all participants via this mailing list to make them aware that a company had performed an upload with the related content.

2.2.1.5 Chat page

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

2.2.1.6 Technical Discussions pages

This page listed all the technical issues initiated at the regular conf calls and in the mailing list.

2.2.2 Contents of eSignature Validation Interop Specific areas of Private part

Within the private area of the portal there was a specific area for the eSignature Validation that was tested during this event.

2.2.2.1 Upload “new” Signature page

This area contained a page that the participants used for uploading their signatures.

The “Upload new signature” page provided mechanisms for uploading new signatures.

Once uploaded, the portal re-built a new downloading package and made it available for all the participants at the Download page. Within this package, participants could find all the signatures and verification reports generated up to that moment in the Plugtests. It was 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 had the immediate effect of updating the corresponding verification report matrix within the related area.

2.2.2.2 Upload Verification pages

This area contained a page that participants used for uploading their verification reports.

The Upload Verification page provided mechanisms for uploading verification reports.

Once uploaded, the portal re-built a new downloading package and made it available for all the participants at the Download page. Within this package, participants could find all the signatures and verification reports generated up to that moment in the Plugtests. It was 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 had the immediate effect of updating the verification reports within the related area.

2.2.2.3 Verification reports

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

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

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

In addition to the signatures uploaded by the Plugtests participants, a full set of "existing" signatures (of 4 formats) produced by some Member States was provided by European Commission.

2.2.2.4 Download pages

This area contained a page that participants used for downloading the signatures and verification reports generated. These pages were also used for downloading the entire material generated by the participants at any precise moment during the event including all the signatures and verification reports generated thus far.

2.2.2.5 Test data directory pages

The page was used by the participants for browsing the folders structure where the portal stored the "pre-existing" and new signatures and the verification files generated by all the participants. This allowed a detailed inspection of the files uploaded to the portal at any moment during the event.

3 Signature Generation

In addition to the existing signatures provided by the Commission, the participants were invited to follow the below recommendations when generating new signatures and containers for the e-signature validation Plugtest.

3.1 Types of signatures to be generated

For each AdES format, i.e., CAdES, PAdES, and XAdES, the highest priority was to generate at least one signature for every different conformance level defined in the corresponding ETSI Technical Specifications, as indicated below:

- (C/P/X)AdES signatures claiming B-Level (Basic level) conformance.
- (C/P/X)AdES signatures claiming T-Level (Trusted time for signature existence level) conformance.
- (C/P/X)AdES signatures claiming LT-Level (Long Term level) conformance.
- (C/P/X)AdES signatures claiming LTA-Level (Long Term with Archive time-stamps level) conformance.

For ASiC containers, the highest priority was also to generate ASiC-S containers with CAdES and XAdES with at least one signature for every different level of CAdES/XAdES Baseline Profile, as indicated below:

- CAdES and XAdES based ASiC-S/ASiC-E containers claiming B-Level (Basic level) conformance.
- CAdES and XAdES based ASiC-S/ASiC-E containers claiming T-Level (Trusted time for signature existence level) conformance.

- CAdES and XAdES based ASiC-S/ASiC-E containers claiming LT-Level (Long Term level) conformance.
- CAdES and XAdES based ASiC-S/ASiC-E containers claiming LTA-Level (Long Term with Archive time-stamps level) conformance.

Participants were kindly requested to also generate some signatures supported by revoked certificates for using them as negative test cases, and some ASiC containers containing signatures supported by revoked certificates.

3.2 Certificates

The signing certificates to be used in signature operations had to be generated by CAs whose certificates are contained in one of the EU member state TLs.

3.3 Signatures details per format

This clause provided further recommendations on signatures and containers that participants were suggested to generate.

3.3.1 CAdES signatures

The recommended data to be signed is a simple text file which consists of ASCII string 'toBeSigned'. As for signed content, enveloping signature' is strongly RECOMMENDED. 'Internal signature' is also called as 'attached signature' or 'embedded signature'. In this case, the signed data content will consist in encapContentInfo.eContent field of CMS SignedData.

3.3.2 PAdES signatures

The recommended data to be signed is a simple pdf file which consists of the text 'toBeSigned'. When a Signed XML form file is submitted our tool require that the input is a pdf file provided by the organizers at the url ..
During the signature operation a byte range digest will be computed over a range of bytes in the file, that will be indicated by the ByteRange entry in the signature dictionary. This range should 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) will be included as the PDF signature in the entry with the key Content of the signature dictionary. The signature dictionary will not contain a Cert entry.

3.3.3 XAdES signatures

If the signature is created from the scratch and participants do not have a special preference, it is recommended to generate enveloping XAdES signatures, and that the data to be signed is a simple text file which consists of ASCII string 'toBeSigned'.
Participants may however, if they consider it worth, to bring XAdES signatures that do not match the characteristics aforementioned, more specifically:

- Enveloping signatures signing one or more different data object(s) than the one mentioned before.
- Enveloped signatures within a XML document, signing this document or part(s) of it, in which case this XML document, enveloping the signature, should be provided.
- Detached signatures. Two cases can be distinguished here:
    - The signature and the signed data object(s) share an ancestor (i.e. the signature and the signed data object(s) are part of the same XML document but the signature is disjoint from all the signed data object(s)), in which case, the XML document containing them should be provided.
    - The signature and the signed data object(s) do not share an ancestor (i.e. the signature is in one file and the signed data object(s) is(are) in another one usually in a web server and referenced by URI(s)). Given the fact that the signed data object(s) should be likely available in remote websites fully accessible to all the Plugtests participants, and that there could be access problems to them, participants envisaging to submit this kind of signatures are kindly requested to make any effort in ensuring that the signed data objects are effectively accessible from outside, explicitly notify this fact to the Plugtests organization team, and enumerate the reasons for their interest in them, so that the Plugtests organization team may perform initial checks on accessibility to the signed data object(s) and assess the worthiness of their incorporation to the test suites.

3.3.4 ASiC Containers

The recommended data object file to be signed by signatures in Simple ASiC containers is a simple text file named “tobesigned.txt” containing the ASCII string 'toBeSigned'.

3.3.5 File names convention

Participants were kindly requested to name the signatures and containers files as proposed in the present clause.
The names of the files containing the signatures or ASiC containers should be created chaining the following strings:

1. 2 characters defining the iso country code of the Member State followed by a hyphen character ‘-‘
2. A sequence of characters [XXX] indicating the type of signature or the container followed by a hyphen character ‘-‘. The sequence of characters should be selected as indicated afterwards.
3. The “Bp” string, indicating “Baseline Profile”
4. a string defining the level of Baseline Profile to which the signature is claiming conformance. This value will take one of the following values:
    - ‘B’ in case of B-Level conformance
    - ‘T’ in case of T-Level conformance
    - “LT” in case of LT-Level conformance
    - “LTA” in case of LTA-Level conformance
5. A hyphen character ‘-‘
6. A character defining the validity of the signing certificate whose value can be one the following
    - ‘V‘ in case of a valid certificate
    - ‘R’ in case of a revoked certificate

7. A hyphen character '-'

8. An increasing number, starting from 1, numbering different signatures generated for every Baseline Profile level

9. A sequence of characters [YYY], which will depend of the type of signature / container generated.

The sequence of characters [XXX] shall be:

- 'C' for files containing CAdES signatures.
- 'P' for files containing PAdES signatures.
- 'X' for files containing XAdES signatures.
- A sequence of three characters for ASiC containers, as indicated below:

  1) the 'A' character followed by
  2) the character 'S' if the container is simple or 'E' if the container is extended, followed by
  3) the character 'C' if the container contains CAdES signature(s) or 'X' if the container contains XAdES signature(s)

The sequence of characters [YYY] shall be:

- ".txt.p7m" for files containing CAdES signatures.
- ".pdf" for files containing PAdES signatures.
- ".xml" for files containing XAdES signatures.
- ".asics" if the container is simple or ".asice" if the container is extended.

For **detached signatures**, the extensions files could be:

- ".xml.zip" for the zipped files containing XAdES signatures and the associated material.
- ".txt.p7m.zip" for the zipped files containing CAdES signatures and the associated material.

Some examples are shown below:

1. The name "IT-C-BpB-V-1.txt.p7m" would identify the first CAdES signature; this signature claims conformance to B-Level and has been generated by an Italian participant using a valid signing certificate.

2. The name "IT-P-BpB-V-1.pdf" would identify the first PAdES signature; it claims conformance to B-Level and has been generated by an Italian participant using a valid signing certificate.

3. The name "IT-X-BpB-V-1.xml" would identify the first XAdES signature; it claims conformance to B-Level and has been generated by an Italian participant while using a valid signing certificate.

4. The name "IT-ASC-BpB-V-1.asics" would identify the first ASiC simple container with CAdES signature; this container claims conformance to B-Level and has been generated by an Italian participant while using a valid signing certificate.

5. The name "IT-AEX-BpB-V-1.asice" would identify the first ASiC extended container with XAdES signatures; this container claims conformance to B-Level and has been generated by an Italian participant while using a valid signing certificate.

4 Participants list

The table below shows the details of all the organizations and people who have participated in the 2014 eSignature Validation remote Plugtests event.

There were **65 different organizations** and 100 people participating in the event.

Country	Company
AT	A-SIT
BE	Connective N.V.
BE	e-Contract.be BVBA
BG	Borica Bankservice AD
BG	Information Services Plc.
BG	System for Electronic Payments Bulgaria
CH	Tessaris Integrated Security AG
CZ	DIGNITA, s.r.o.
CZ	SEFIRA spol. s r.o.
CZ	Software602 a.s.
DE	Bundesdruckerei GmbH
DE	Bundesnotarkammer
DE	Secrypt GmbH
DE	bwild@intarsys.de
DE	SecCommerce Informationssysteme GmbH
DE	Secunet Security Networks AG
DK	ID Solutions ApS
EU	Knowledge Works srl
EU	InfoCert s.p.a
EU	Universitat Politecnica De Catalunya
EU	IAIK
EU	ETSI
EU	European Commission
EE	AS Sertifitseerimiskeskus
EE	Cross Borders Trust Services
EL	Ministry of Administrative Reform and eGov
ES	Ministerio de Hacienda y Admin Públicas
ES	SIA
ES	Smart Access
FR	BULL
FR	Cryptolog
FR	DICTAO
FR	Gemalto
FR	Real.not
FR	OPENTRUST
HR	ANADA d.o.o

Country	Company
HR	Fina
HU	Microsec ltd.
HU	Netlock Ltd
HU	NISZ - National Infocommunications Service
HU	Polysys Ltd
HU	Aron Szabo
IT	Adobe System
IT	BIT4ID
IT	Ministero della Difesa - Comando C4 Difesa
IT	InfoCert S.p.A.
IT	Insiel S.p.A.
IT	Lombardia Informatica SPA
IT	Namirial S.p.A.
IT	Notartel S.p.A
LT	UAB Estina
LT	UAB MIT-SOFT
LV	EUSO
PL	EuroCert Sp. z o.o.
PL	Krajowa Izba Rozliczeniowa S.A.
PL	Polish Security Printing Works
PL	Unizeto Technologies
PT	Gabinete Nacional de Seguranca
PT	MULTICERT - Servios de Certificao Electrnica
RO	Digital Agenda Agency for Romania
RO	Transped
SE	3xA Security
SI	Ministry of Interior, Slovenia
SK	Ardaco, a.s.
SK	Disig, a.s.
SK	Ditec, a.s.
SK	Národný bezpecnostný úrad
UK	ELDOS CORPORATION LTD

5 Plugtests conclusions

5.1 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 65 organizations participating, it would have been difficult to organize a face to face event.

5.2 Communication supporting technologies

The utilization of Web conference (GotoWebinar) 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 Plugtest by carrying out a demonstration of the portal utilization.

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

5.3 Event duration

Initially, 3 weeks of testing had been planned for this event, starting from 3rd November to 12th December 2014.

In order to allow the participants to read all the documentation and prepare for the testing, ETSI opened the portal on 27th October, a week before the official beginning of the interoperability event.

Moreover, for this event, 65 companies were registered. As each company had to verify the signatures of other participants and also the existing signatures provided by European Commission, it was agreed that 3 weeks were definitely too short. At the request of participants, the Plugtests team decided to extend the duration of the event until the 12th December 2014, however the portal remained accessible to participants in read only until 5 January 2015.

6 eSignature Validation related Issues

The present section lists some of the issues raised during the eSignature Validation Plugtests event in November-December 2014. This technical report will be provided to ETSI TC ESI which is the technical working group in charge of the standardization of the ETSI Electronic Signatures, for further action/input for further changes in standards.

6.1 Presence/absence of the POE in case of a revoked or expired certificate

➔Issue: How should the validation process behave in case of a signature with a revoked or expired signing certificate?

Reply given at Plugtests: Following the ETSI TS 102 853 standard the POE must be provided to obtain VALID indication in an automated manner;

Where the signature contained no POE the majority of the participants validated the signing certificates at current time.

6.2 Weak algorithm

➔Is a signature using a weak algorithm (notably SHA-1) valid?

Reply given at the Plugtests: All algorithms should be accepted during the Plugtests. In case you run into any problems one of the following indications/sub-indications should be used:

- INVALID.CRYPTO_CONSTRAINTS_FAILURE

The signature is considered invalid because at least one of the algorithms that have been used in a material (e.g. the signature value, a certificate...) involved in validating the signature or the size of the keys used with such an algorithm is no longer considered reliable and the Signature Validation Algorithm can ascertain that this material was produced after the time up to which this algorithm was considered secure.

- INDETERMINATE.CRYPTO_CONSTRAINTS_FAILURE_NO_POE

At least one of the algorithms that have been used in a material (e.g. the signature value, a certificate...) involved in validating the signature or the size of the keys used with such an algorithm is no longer considered reliable at the validation date/time. However, the Signature Validation Algorithm cannot ascertain that the concerned material has been produced before or after the algorithm or the size of the keys have been considered not reliable.

- ERROR + text “Not supported algorithm”

The validation tool is not able to deal with a specific algorithm or crypto suite.

6.3 Mandatory signed properties

➔Must the signed reference to the signing certificate be present within the signature?

Reply given at the Plugtests: Following ETSI TS 102 853, an *INVALID.FORMAT_FAILURE* should be returned (non-compliance with the core specifications)

6.4 Claimed signing time

➔Must the signed property “claimed signing time” be present within the signature?

Reply given at the Plugtests: The baselines require the presence of the signing time. If no claimed signing time is present, non-conformance to the baseline is to be expressed via a warning indicating the format failure.

6.5 Multiple signatures

➔How to cope with the validation of multiple signature/countersignatures?

Reply given at the Plugtests: Currently the portal does not display directly the result of the validation for each of the multiple signatures. This would require a preliminary analysis of the files which is not easy. Therefore if the individual results are different then INDETERMINATE indication with INCONSISTENT_MULTIPLE_ELEMENTS_VALIDATION sub-indication should be used. The details regarding each signature, countersignature should be provided with in the detailed report.

6.6 PAdES SubFilter

➔Can the SubFilter value in the case of a PDF document lead to the invalidity of the signature?

Reply given at the Plugtests: The baseline profiles should be followed. Like above, signatures may still be valid even if non conformant to PAdES baseline profiles (in this case because they do not use the required SubFilter indication). This non-conformance is again to be expressed via a warning indicating the format failure

6.7 Trust anchor

➔Does the trust anchor have to be in the TSL?

Reply given at the Plugtests: To obtain a VALID result it must be possible to build the certificate chain till the trust anchor from one of the MS TSLs.

Each certificate within the chain till the trust anchor must be valid at the time of the validation (not always the current time).

Suggested indication / sub-indication:

INDETERMINATE.NO_CERTIFICATE_CHAIN_FOUND

6.8 TSL issues

Some specific issues with MS trusted lists were discovered during the Plugtests and reported to them bilaterally. Solved by now.

6.9 CRL and critical extensions

➔How do the critical extensions within the CRL influence the validation process?

Reply given at the Plugtests: When a critical extension is encountered and the validation application is not able to handle it then the CRL must be rejected

6.10 Timestamp without the trust anchor defined as TSP

➔Is a timestamp without the trust anchor defined as TSP valid?

Reply given at the Plugtests: In the European, cross-border context the validation of the timestamp does not require that the trust anchor is defined as time-stamping generation service within the TSL. The timestamp cannot be rejected because the certificate chain cannot be built till the TSL. The absence of the trust anchor is to be expressed via a warning.

6.11 PDF and CMS signing-time

➔Does the presence of the CMS signing-time invalidate the signature?

Reply given at the Plugtests: The presence of the CMS signing-time within the signature should not invalidate the signature. The non-conformance to the PAdES baseline is to be expressed via a warning indicating the format failure.

6.12 CAdES: BasicOCSPResponse or OCSPResponse

➔Are the two types of OCSP responses valid?

Reply given at the Plugtests: Both of these types can be used.

6.13 Expired or revoked certificate in the TSL

➔Should the certificates present within the TSL be validated?

Reply given at the Plugtests: The trusted lists are to be seen as sources of trust anchors for validating certificates supporting electronic signatures/seals based on public key cryptographic digital signatures, or other types of trust services based elements like time-stamps, electronic delivery evidences, etc. According to RFC 5280, a trust anchor is identified by the public key of the CA, the CA's name. In the trusted lists, the certificates that are associated to any listed service are there purely as a convenient container for such CA public key and name information and in conformance to RFC 5280, the validation of those certificates is not part of the certificate path validation algorithm. They can simply be ignored and the signature stays VALID even if this certificate is expired or revoked. Only the public key and the associated subject name are needed as Trust Anchor information.

6.14 ASiC: Value of the manifest:version attribute

➔Does the manifest version attribute value influence the validation process?

Reply given at the Plugtests: The inconsistency in the structure of the manifest file (in general in the meta-data) is not the reason to invalidate the signature. This issue can be notified by error or warning system.

The ASiC baseline profile will clarify the version of the manifest to be used.

History

Document history		
V0.1	13 January 2014	Initial draft
V1.0	30 January 2015	Final version