Technical Report of the eSignature Validation Remote Plugtests April-May 2016

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

June 2016

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 2016 remote Plugtests event on eSignature Validation (ETSI EN 319 102), 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

European Union Member States need to put in place the necessary technical means allowing them to process electronically signed documents that are required when using an online service offered by, or on behalf of, a public sector body.
Regulation (EU) No 910/2014[1] (eIDAS Regulation) which will apply as of 1 July 2016 in relation to trust services provides for Member States requiring an advanced electronic signature or seal for the use of an online service offered by, or on behalf of, a public sector body, to recognize advanced electronic signatures and seals, advanced electronic signatures and seals based on a qualified certificate and qualified electronic signatures and seals in specific formats, or alternative formats validated pursuant to specific reference methods[2].

Commission Implementing Decision 2014/148/EU[3], amending Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC[4], has defined a number of the most common advanced electronic signature formats to be supported technically by the Member States, where advanced electronic signatures are required for an online administrative procedure. Establishing the reference formats aims at facilitating the cross-border validation of electronic signatures and at improving the cross-border interoperability of electronic procedures.

Commission Implementing Decision (EU) 2015/1506[5], which becomes applicable as of 1 July 2016 together with the eIDAS Regulation, lists the same standards for formats of advanced electronic signatures, notably excluding standards detailing long-term archiving due to the ongoing revision by the standardization bodies of the long term archival forms of the referenced formats.

The testing of e-signature validation solutions is mainly done at Member States' level based on their national tools (eID cards, secure signature creation devices), solutions, policy options (signature validation policies). In order to ensure that the cross-border dimension is working in practice, more testing needs to be done to mutually check Member States' signatures against their existing e-signature validation applications.

To allow such testing to happen, **a second e-signature validation Plugtest** was organized by ETSI in cooperation with the Commission. It **has run remotely from 6th April to 30th May 2016**.

The Plugtest was **open to all** but particularly targets participants who are either governmental entities, have a link to the e-government solutions of Member States (like outsourced private solution providers), or are recognized by Member States' public services when it comes to signatures and their validation results.

The aim of this Plugtest was twofold. First, it would allow to take stock of what Member States currently have as e-signatures used for their public online services purposes and to test whether these can be validated in other Member States.
Second, it would allow to detect possible issues in different validation processes and to see whether there are differences in the validation applications for the same signature used. The latter would be a good basis to better understand the problems faced by validation applications and where some further clarifications, be it at the level of standards or policy/legislation, may be needed to ensure the same results for the same signature are achieved in the same context, notably where Member States are obliged to accept advanced e-signatures based on qualified certificates and/or qualified signatures without additional requirements.

The clauses below explain how the Plugtest has been organized and what was expected from the participants to make the Plugtest as useful as possible.

[1] OJ L 257, 28.8.2014, p. 73–114.
[2] To be noted that where a qualified electronic signature is required, all qualified electronic signatures will have to be recognised regardless the formats of the underpinning advanced electronic signature (combination of articles 25 and 27 of the eIDAS Regulation)
[3] OJ L 80, 19.3.2014, p. 7–9.
[4] OJ L 376, 27.12.2006, p. 36–68.
[5] OJ L 235, 9.9.2015, p. 37–41.

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 EN 319 102 (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 2016 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 EN 319 102.
- The Remote Plugtests Event on eSignature Validation organized by ETSI with the support of European Commission, and held from Wednesday 6th April to Monday 30th May 2016.

In order to give participants time to prepare for the testing, ETSI opened the portal to participants in "read-only" mode on 4th April, before the official start date of the Plugtest event. An introduction web conference took place on Wednesday 6th April to present the portal and the testing.

The event was initially planned to run until 29th April 2016 but it was extended to 30th May 2016, 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 (193) and the corresponding number of proposed signatures to validate.

The present document is divided into the following sections:

Section 2 provides details on the organization of the portal.

Section 3 provides details on how the material of the portal was organized and the services it provided to the participants of the Plugtests Events.

Section 4 provides an overview of the requirements and guidance given for the generation of new signatures during the Plugtest.

Section 5 lists the participants to the 2016 eSignature Validation Remote Plugtests Event.

Section 6 provides a summary of the most important results and conclusions of the Plugtests.

Section 7 provides details on a number of issues related to the specifications as identified by the participants. These issues will be provided as feedback to the ETSI TC ESI, with the recommendation that they are taken into consideration for future standardization activities.

2 Organization of the Plugtest

The interoperability testing has allowed the participants to test their e-signature validation tools to cross-validate ETSI e-signatures in whatever format these may be, relying on Member States' Trusted Lists and according to new European Standard EN 319 102 (Procedures for Creation and Validation of AdES Digital Signatures).

ETSI has published the first of a series of European Standards to support the European Regulation on electronic identification and trust services for electronic transactions in the internal market, or eIDAS (Regulation (EU) 910/2014). The proposed date for this Plugtest event, April 2016, has been chosen to allow sufficient time to Member States implementations to fulfil the requirements of new EN on ETSI AdES Signatures, as well as the EN 319 102. This Plugtest was a good way for Member States to test their compliance/prepare their compliance to the implementing acts

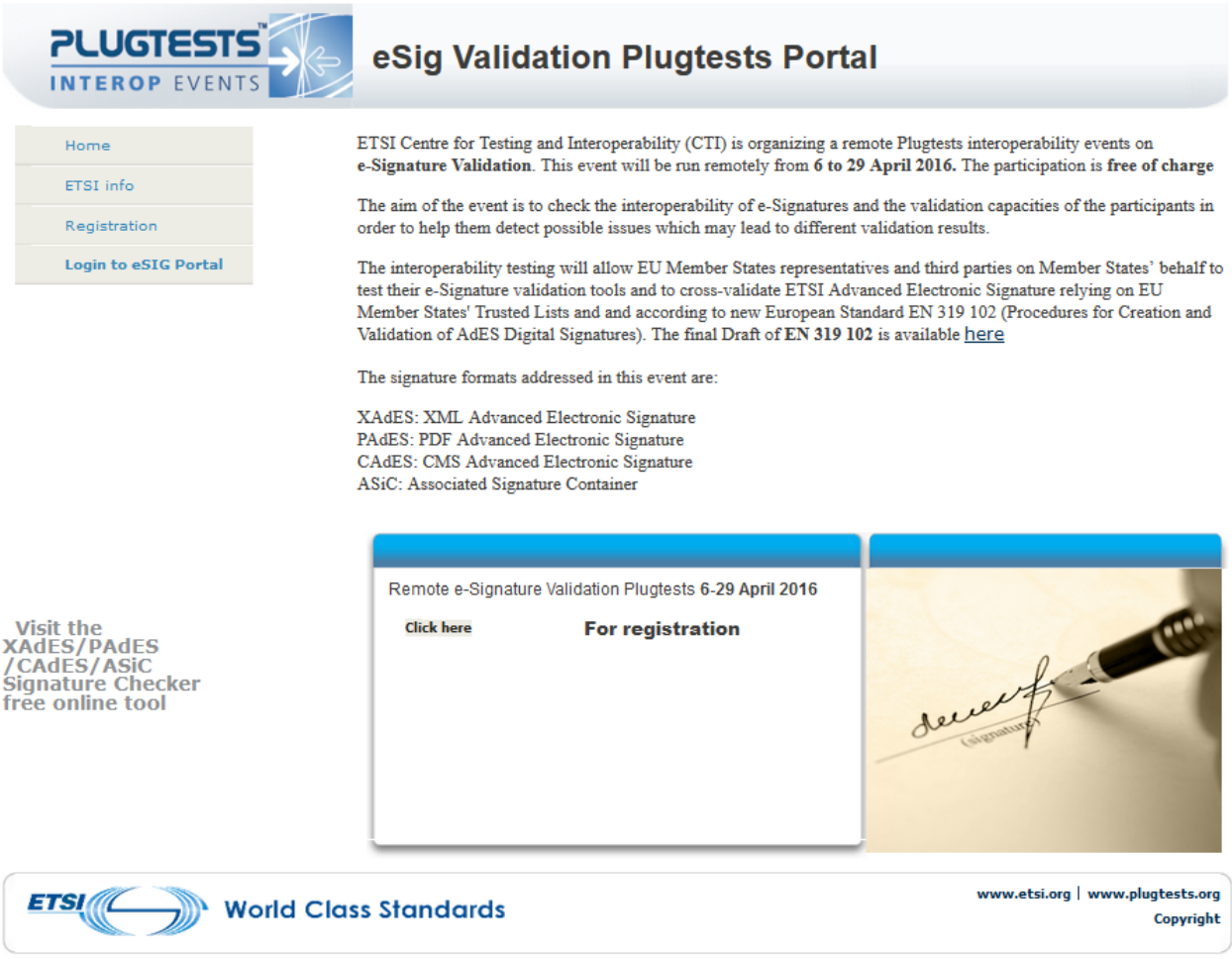
requirements, still several months before the date of application of the implementing acts under eIDAS (i.e. 1 July 2016).
The signature formats addressed in this remote Plugtests event are:

- XAdES: XML Advanced Electronic Signature
- PAdES: PDF Advanced Electronic Signature
- CAdES: CMS Advanced Electronic Signature
- ASiC: Associated Signature Container

3 Presentation of the Plugtest 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.

3.1 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.

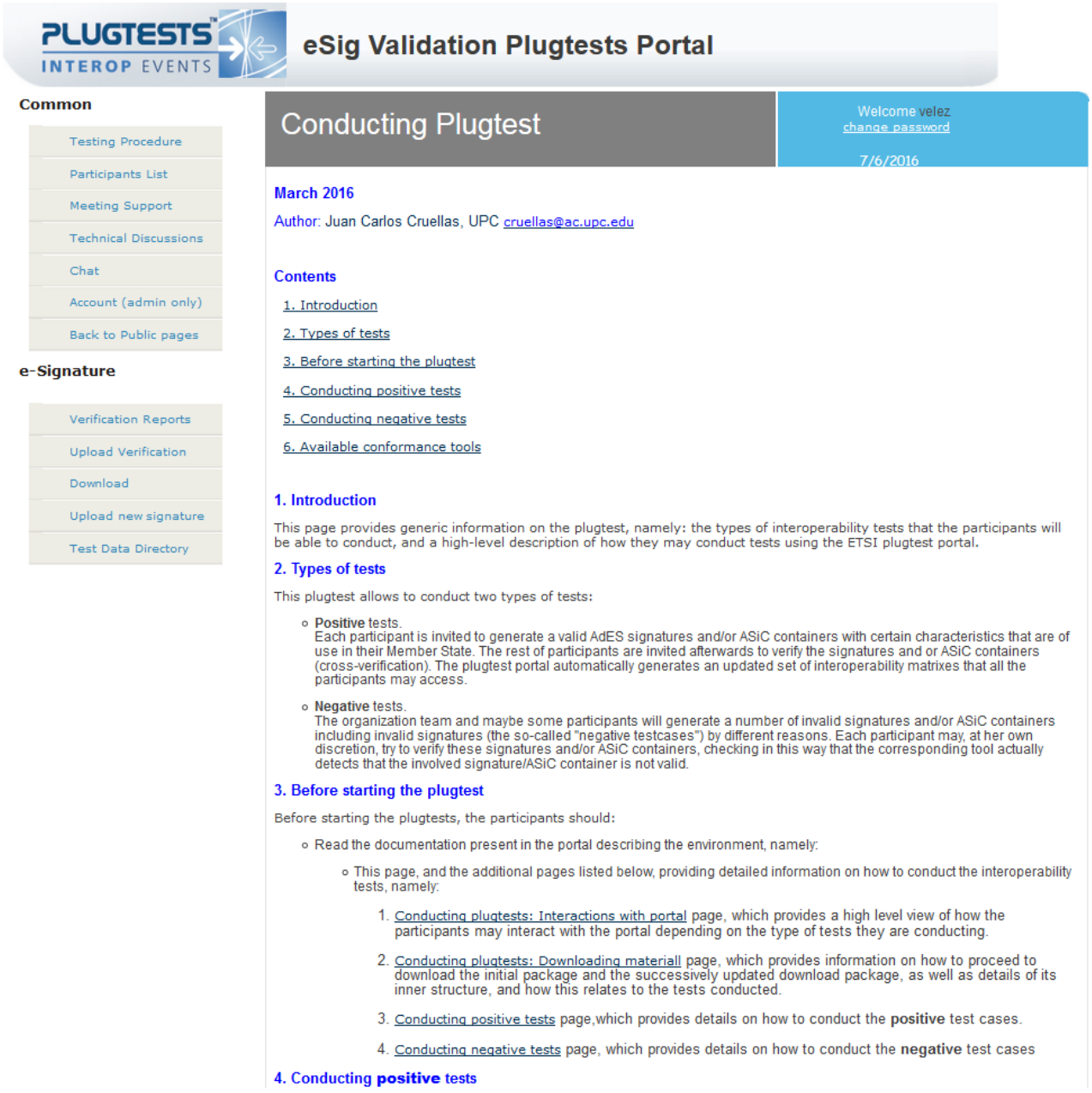
- The Registration page, providing details on the Plugtests registration process.
- The Presentation of the Plugtests team.
- The Presentation of some past events (XAdES, CAdES, PAdES, ASiC)
- The **Login to Plugtests Area** page gives access to the **protected area** of the portal.

3.2 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.



3.2.1 Contents of the Common area in the Private part

3.2.2.1 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 http://signatures-conformance-checker.etsi.org/

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 (XML Advanced Electronic Signature ETSI 101 903, TS 103 171 and EN 319 132-1&2)
- CAdES (CMS Advanced Electronic Signature ETSI TS 101 733)
- ASiC (Associated Signature Container ETSI TS 102 918)
- PAdES (PDF Advanced Electronic Signature ETSI TS 102 778)

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**).

3.2.2.2 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.

3.2.2.3 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.

3.2.2.4 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.

3.2.2.5 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.

3.2.2.6 Technical Discussions pages

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

3.2.3 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.

3.2.3.1 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.

3.2.3.2 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.

3.2.3.3 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.

3.2.3.4 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.

3.2.3.5 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.

It was also the location of a CA store that contained Root and Intermediate certificates provided by participants. It was requested to validate signatures from non-european countries, or at least for the ones created with CA certificates not present in the European Trusted List.

4 Signature Generation

To the extent possible, the participants were invited to follow the below recommendations when generating signatures and containers for the e-signature validation Plugtest.

4.1 Types of signatures and containers to be generated

For each AdES format, i.e., CAdES, PAdES, and XAdES, the highest priority is to generate at least one baseline signature for each 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 is 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 based ASiC-S containers claiming B-Level (Basic level) conformance.
- CAdES ASiC-S containers claiming T-Level (Trusted time for signature existence level) conformance.
- CAdES based ASiC-S containers claiming LT-Level (Long Term level) conformance.
- CAdES based ASiC-S containers claiming LT-Level (Long Term level) conformance.
- XAdES based ASiC-S/ASiC-E containers claiming B-Level (Basic level) conformance.
- XAdES based ASiC-S/ASiC-E containers claiming T-Level (Trusted time for signature existence level) conformance.
- XAdES based ASiC-S/ASiC-E containers claiming LT-Level (Long Term level) conformance.
- XAdES based ASiC-S/ASiC-E containers claiming LTA-Level (Long Term with Archive time-stamps level) conformance.

Participants are 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.

4.2 Certificates

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

As some participants were from out of Europe, It was requested to validate signatures from non-european countries, or at least for the ones created with CA certificates not present in the European Trusted List.

The Plugtest team has created a CA store into the portal that includes the Root or Intermediate CA certificates from these companies.

4.3 Signatures details per format

This clause provides further recommendations on signatures and containers that participants are suggested to generate.

4.3.1 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.

4.3.2 PAdES signatures

The recommended data to be signed is a simple pdf file which consists of the text 'toBeSigned'.
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 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) 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.

4.3.3 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 Plugtest 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 Plugtest organization team, and enumerate the reasons for their interest in them, so that the Plugtest 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.

4.3.4 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'.

4.4 File names convention

Participants are 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 optional string “EN-“ indicating that the signature/container is compliant against one of the ETSI ENs that specifies the signature/container formats (ETSI EN 319 122, ETSI EN 319 132, ETSI EN 319 142, and ETSI EN 319 162). Absence of this string indicates that the signature/container is compliant with the ETSI TS that specifies the signature/container formats (ETSI TS 103 171, ETSI TS 103 172, ETSI TS 103 173, and ETSI TS 103 174).

4) The 'B' character, indicating "Baseline signature/container", followed by a hyphen character '-'.

5) a string defining the Baseline level to which the signature/container is claiming conformance. This value will take one of the following values:

- o 'B' in case of B-B level conformance
- o 'T' in case of B-T level conformance
- o "LT" in case of B-LT level conformance
- o "LTA" in case of B-LTA level conformance

6) A hyphen character '-'

7) A character defining the validity of the signing certificate whose value can be one the following

- o 'V' in case of a valid certificate
- o 'R' in case of a revoked certificate

8) A hyphen character '-'

9) An increasing number, starting from 1, numbering different signatures/containers generated for every Baseline level.

10) 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:

- ".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.

Some examples are shown below:

1. The name "IT-C-B-B-V-1.p7m" would identify the first CAdES signature; this signature claims conformance to B-B level as specified in ETSI TS 103 173, and has been generated by an Italian participant using a valid signing certificate.

2. The name "IT-P-B-B-V-1.pdf" would identify the first PAdES signature; it claims conformance to B-B level as specified in ETSI TS 103 172, and has been generated by an Italian participant using a valid signing certificate.

3. The name "IT-X-B-B-V-1.xml" would identify the first XAdES signature; it claims conformance to B-B level as specified in ETSI TS 103 171, and has been generated by an Italian participant while using a valid signing certificate.

4. The name "IT-ASC-B-B-V-1.asics" would identify the first ASiC simple container with CAdES signature; this container claims conformance to B-B level as specified in ETSI TS 103 174, and has been generated by an Italian participant while using a valid signing certificate.

5. The name "IT-AEX-B-B-V-1.asice" would identify the first ASiC extended container with XAdES signatures; this container claims conformance to B-B level as specified in ETSI TS 103 174, and has been generated by an Italian participant while using a valid signing certificate.

6. The name "IT-AEX-EN-B-B-V-1.asice" would identify the first ASiC extended container with XAdES signatures; this container claims conformance to B-B level as specified in ETSI EN 319 162 part 1, and has been generated by an Italian participant while using a valid signing certificate

5 Participants list

The table below shows the details of all the organizations and people who have participated in the 2016 eSignature Validation remote Plugtests event.

There were **98 different organizations** and 193 people participating in the event.

Country	Company
Austria	Secure Information and Communication Technologies
Austria	A-SIT Zentrum für sichere Informationstechnologie Austria
Austria	eGovernment Innovation Center (EGIZ)
Austria	GrEEV.com KG
Belgium	e-Contract.be BVBA
Belgium	ZETES
Belgium	Connective N.V.
Brazil	Certisign
Brazil	e-Sec Digital Security
Brazil	E-val Tecnologia
Bulgaria	BORICA BANKSERVICE AD
Bulgaria	Information Services
Canada	Silanis Technology Inc.
Croatia	Elis Missoni
Czech Republic	SEFIRA spol. s r.o.
Czech Republic	TECHNISERV IT, spol. s r.o.
Czech Republic	Dignita
Czech Republic	Software602
Czech Republic	První certifikacní autorita,a.s.
Czech Republic	Exon
Czech Republic	Gordic spol. s r. o.
Czech Republic	ICZ
Czech Republic	ALIS spol. s r.o.
Czech Republic	Singularita s.r.o.
Estonia	Sertifitseerimiskeskus AS
Estonia	Estonian Information System Authority
France	Cryptolog

Country	Company
France	CS Systèmes d'Information
France	Real.not
France	Trustcorp
France	Lex Persona
France	Bull Atos technologies
France	SAFRAN MORPHO
Germany	Mentana-Claimsoft GmbH
Germany	Secrypt
Germany	SecCommerce Informationssysteme GmbH
Germany	T-Systems International GmbH
Germany	exceet Secure Solutions AG
Germany	Governikus GmbH & Co. KG
Germany	PDFlib
Germany	intarsys consulting
Germany	ecsec GmbH
Hungary	NISZ
Hungary	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Kft
Hungary	Polysys Ltd
Hungary	Microsec ltd
Hungary	Noreg
Italy	Intesi
Italy	Adobe Systems
Italy	Unimatica S.p.A.
Italy	Lombardia Informatica S.p.A.
Italy	BIT4ID
Italy	Ministero dell Difesa - Comando C4 Difesa
Italy	Intesa Sanpaolo S.p.A.
Italy	Intesa S.p.A.
Italy	Infocert
Italy	Namirial SpA
Italy	Elaide S.r.l.
Italy	ICBPI - Istituto Centrale delle Banche Popolari S.p.A.
Italy	Postecom s.p.a
Japan	LangEdge,Inc.
Japan	AMANO Business Solutions Corporation
Japan	Otip Office
Japan	System Art
Latvia	Autentica, SIA
Latvia	EUSO
Liechtenstein	Amt für Informatik
Lithuania	EXPLAND UAB
Lithuania	UAB INVENTI
Lithuania	MIT-SOFT UAB
Lithuania	BSS IT, UAB

Country	Company
Lithuania	Estina
Luxembourg	EC DIGIT
Luxembourg	Nowina Solutions
Mexico	SEGURIDATA PRIVADA SA DE CV
Peru	RENIEC (Registro Nacional de Identificacion de Peru)
Poland	Asseco Data Systems S.A
Poland	Krajowa Izba Rozliczeniowa S.A.
Romania	TRANSSPED
Slovakia	Disig, a.s.
Slovakia	National Security Authority - Slovakia
Slovakia	Ditec, a.s.
Slovenia	Halcom CA
Slovenia	SETCCE
Spain	IZENPE S.A
Spain	Ivnosys Soluciones S.L.
Spain	Ricoh Spain IT Services
Spain	MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (MINHAP)
Spain	Safelayer Secure Communications, S.A.
Spain	Universidad Politecnica de Cataluna
Sweden	Comfact AB
Tunisia	NGSign
Turkey	Kale Yazilim
United Kingdom	Thales UK
United Kingdom	Ascertia Limited.
United Kingdom	ELDOS CORPORATION LTD
USA	Peculiar Ventures, Inc.
USA	Microsoft Corporation

6 Plugtests conclusions

6.1 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 98 organizations participating, it would have been difficult to organize a face to face event.

6.2 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.

6.3 Event duration

Initially, 4 weeks of testing had been planned for this event, starting from 6th April to 29th April 2016.

In order to allow the participants to read all the documentation and prepare for the testing, ETSI opened the portal on 4nd April before the official beginning of the interoperability event.

Moreover, for this event, 98 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 4 weeks were definitely too short. At the request of participants, the Plugtests team decided to extend twice the duration of the event that has led to finish on 30 May, 2 months after the beginning of the event.

7 eSignature Validation related Issues

The present section lists some of the issues raised during the eSignature Validation Plugtests event in April and May 2016. 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 possible action/input for further changes in standards.

7.1 The archive timestamp purpose in AdES-LTA signatures

At the Plugtest it was discussed about the purpose of archive timestamp in AdES-LTA signatures.
It was agreed that the main purpose of archive timestamp is to extend the validity of signature timestamps and/or OCSP responses and CRLs after their signing certificates expiration and/or to protect the signatures against algorithms weaknesses over time (because the archive timestamp can protect the signatures with a stronger cryptographic algorithm).

7.2 Management of multiple DSS dictionaries

At the Plugtest some participants asked for a clarification about using several DSS. Considering the way PDF 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).
The main conclusion of this topic is that when you add a "new" DSS, you should keep all the references (on validation objects) of the first DSS object ***and*** add the new needed references, as clearly stated in clause 5.4.1 of ETSI EN 319 142-1 "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures" version 1.1.1.

7.3 Historical validation of signing certificates that have been in “on hold” state

At the Plugtest the participants discussed about the way to manage the validation of signing certificates that have been in on hold state during their lifetime.
Some participants stated that when validating AdES-T or AdES-LT signatures the periods in which the signing certificates have been on hold should be taken into account in the signing certificates validation and that this validation should be performed at the declared signing time.
Other participants stated that declared signing time is not a reliable time and so it shall not be used during validation and that there is no reason to invalidate the signatures created during the hold period if the signing certificates have been removed from hold and turned valid. Therefore the latest available revocation information is sufficient to validate the signing certificate provided that signing certificate was not expired at the revocation information generation time.

7.4 Provision of validation data after certificates expiration

At the Plugtest there were some discussions concerning the need that the CAs provide validation status information after certificates expiration. At the moment many CAs return OCSP response with status GOOD for the revoked certificates if they are already expired because such certificates are removed from CRLs at their expiration time. It shall be considered that the regulation states in Article 24 item 4 "With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient".

7.5 Revocation freshness

At the Plugtest it was discussed what stated in clause 5.2.5 Revocation freshness checker of ETSI EN 319 102 "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation". Some participants criticized the algorithm described in the above clause because it leaves to the driving application the responsibility to choose which revocation freshness shall be used during signing certificates validation.

7.6 META-INF/manifest.xml in ASiC-E with XAdES signatures

At the Plugtest it was discussed about the need to use the META-INF/manifest.xml in ASiC-E containers even with XAdES baseline signatures because not all the ASiC-E container data shall be signed. META-INF/manifest.xml can be used to define mime-types of unsigned files.

7.7 ds:X509IssuerName in xades:SigningCertificate in Bulgarian TSL

During the Plugtest it was noticed an issue, concerning certificate that signed the Bulgarian TSL, because the ds:X509IssuerName element in xades:SigningCertificate signature property was inconsistent with the issuer DN specified in the certificate.
It was pointed out that TS 102 853 v1.2.1 (2014-12) inside clause 1.2.1 states "When IssuerSerial element is additionally present in xades:SigningCertificate, the details of the issuer's name and the serial number of the IssuerSerial element may be compared with those indicated in the signer's certificate: if they do not match, an additional warning shall be returned with the output". Therefore such issue cannot be a valid reason to invalidate the TSL signature even if it would be better that the SigningCertificateProperty IssuerSerial matches the actual signing certificate.

7.8 Bad encoded PL certificate in LOTL

During the Plugtest it was noticed that in LOTL TSLSequenceNumber 134 there was a bad encoded PL certificate. The issue was solved by publication of LOTL TSLSequenceNumber 135.

7.9 Sdi associated to trust services having different Sti

At the Plugtest some participants noticed that in the HR TSL there are some cases in which the same public key appear more than once in the trusted list associated to trust services, qualified and not qualified, having different Service type identifier values making difficult to conclude if a certificate issued by such public keys is qualified or not qualified.

7.10 Invalid OCSP responders

At the Plugtest it was noticed that an OCSP responder from a TSP was violating the requirements stated both in RFC2560 and in RFC6960 for the OCSP signing certificates.
The OCSP signing certificate shall meet at least one of the following criteria:
1. Matches a local configuration of OCSP signing authority for the certificate in question, or
2. Is the certificate of the CA that issued the certificate in question, or
3. Includes a value of id-kp-OCSPSigning in an extended key usage extension and is issued by the CA that issued the certificate in question as stated above.
This issue can occur when a TSP service is listed in TSL with status "supervisionincessation" and is "TakenOver" by another TSP and the latter TSP includes the trusted OCSP service that provides the status information for certificates in signer certificate chain.

7.11 Signatures validation after signing certificates revocation

At the Plugtest there were some discussions concerning the reason for not successfully validating qualified electronic signatures without POE after signing certificates revocation, being such qualified electronic signatures equivalent to handwritten signatures which very rarely need a proof of existence (i.e. from a notary). It was explained that, unlike what happens with handwritten signatures, the signing certificates creating qualified electronic signatures can be revoked, and such certificates should not be trusted after the revocation date, since certificates keys can no longer be considered secure after the certificates have been revoked.

7.12 ASiC container containing multiple files with the same name

At the Plugtest it was stated that ASiC containers that contain multiple files with the same path and name should not pass container structure validation because signed data objects in the container should be uniquely identifiable with the ds:Reference URI attribute.

History

Document history		
V1.0	07 June 2016	Final version