Technical Report of the eSignature Validation Plugtests May-July 2022

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

Aug 2022
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 2022 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 CTI 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 has 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) 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.

In order to ensure that the cross-border dimension is working in practice, testing needs to be done to mutually check Member States' signatures against their existing Digital Signature validation applications. To allow such testing to happen, ETSI has organized regularly some eSignature validation Plugtests.

The current document is a report of the 4th eSignature validation Plugtests run remotely from 16th May to 15th July 2022.
The aim of this Plugtests was twofold:

- First, it would allow to take stock of what Member States currently have as Digital 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 Digital Signatures based on qualified certificates and/or qualified signatures without additional requirements.

The clauses below explain how the Plugtests has been organized and what was expected from the participants to make the Plugtests as useful as possible.
The interoperability testing allowed participants to test their digital signature validation tools and to cross-validate ETSI Digital Signatures relying on EU Member States' Trusted Lists (based on TS 119 612 and TS 119 615).

Each participant was invited to generate some valid digital signatures with certain characteristics that are of use in their Member State. The rest of participants were invited afterwards to verify the signatures (cross-verification) and generate a standardized ETSI validation report. The Plugtests portal automatically generated an updated set of interoperability matrixes that all the participants could access. After each upload of signatures or the verification reports, all the participants were notified using a dedicated mailing list.

The testing provided covered the validation of the 5 main Digital Signature formats (XAdES, CAdES, PAdES, ASiC and JAdES) according to the following standards:

- EN 319 102-1 Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

- TS 119 102-2 Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report

- TS 119 172-4 Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists

The present document is divided into the following clauses:

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

Clause 3 provides an overview on how to conduct the Plugtests.

Clause 4 lists the companies participating to the 2022 eSignature Validation Remote Plugtests Event.

Clause 5 provides the conclusions of the Plugtests.

[1] OJ L 257, 28.8.2014, p. 73–114.

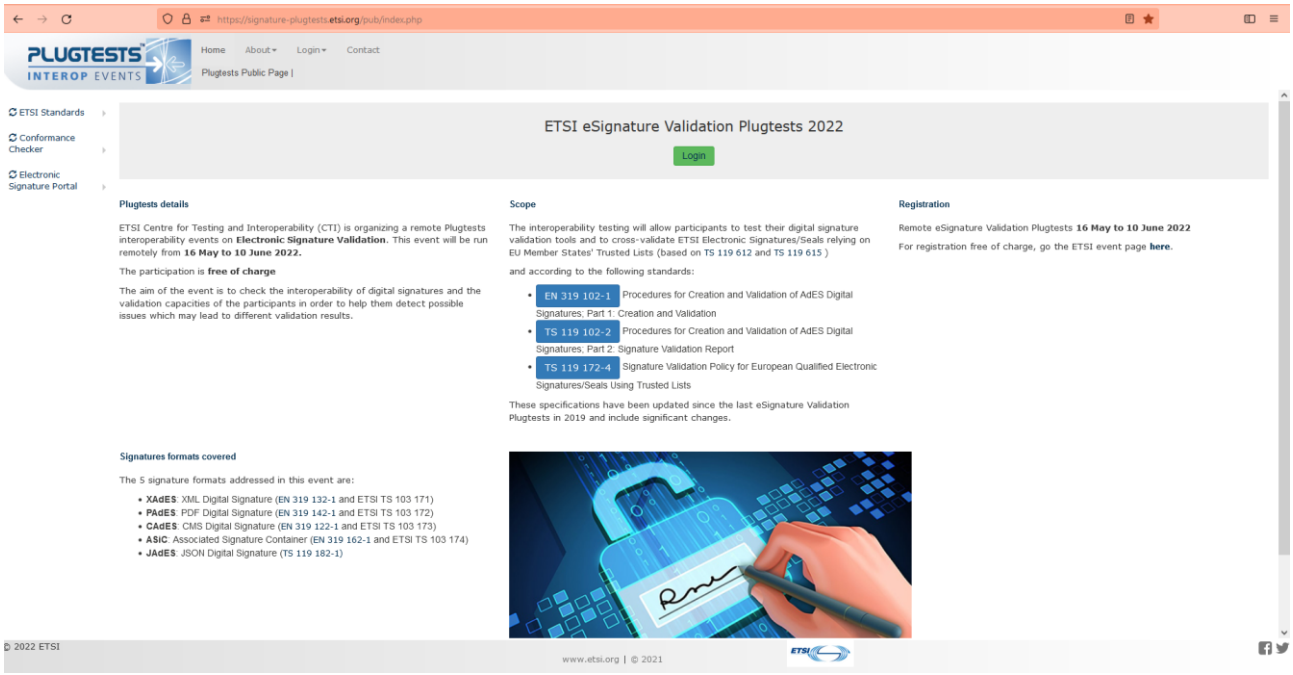
Clause 6 provides the overall results.

Clause 7 provides details on some issues related to the specifications, identified by the support team and the participants. These issues are intended to be presented and discussed with the ETSI TC ESI, with the recommendation that they are taken into consideration for future standardization activities.

2 Presentation of the Plugtests 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 list of ETSI standards covered by the Testing
- Link to the ETSI Signature Conformance Checker
- 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.
- **eSignature 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.

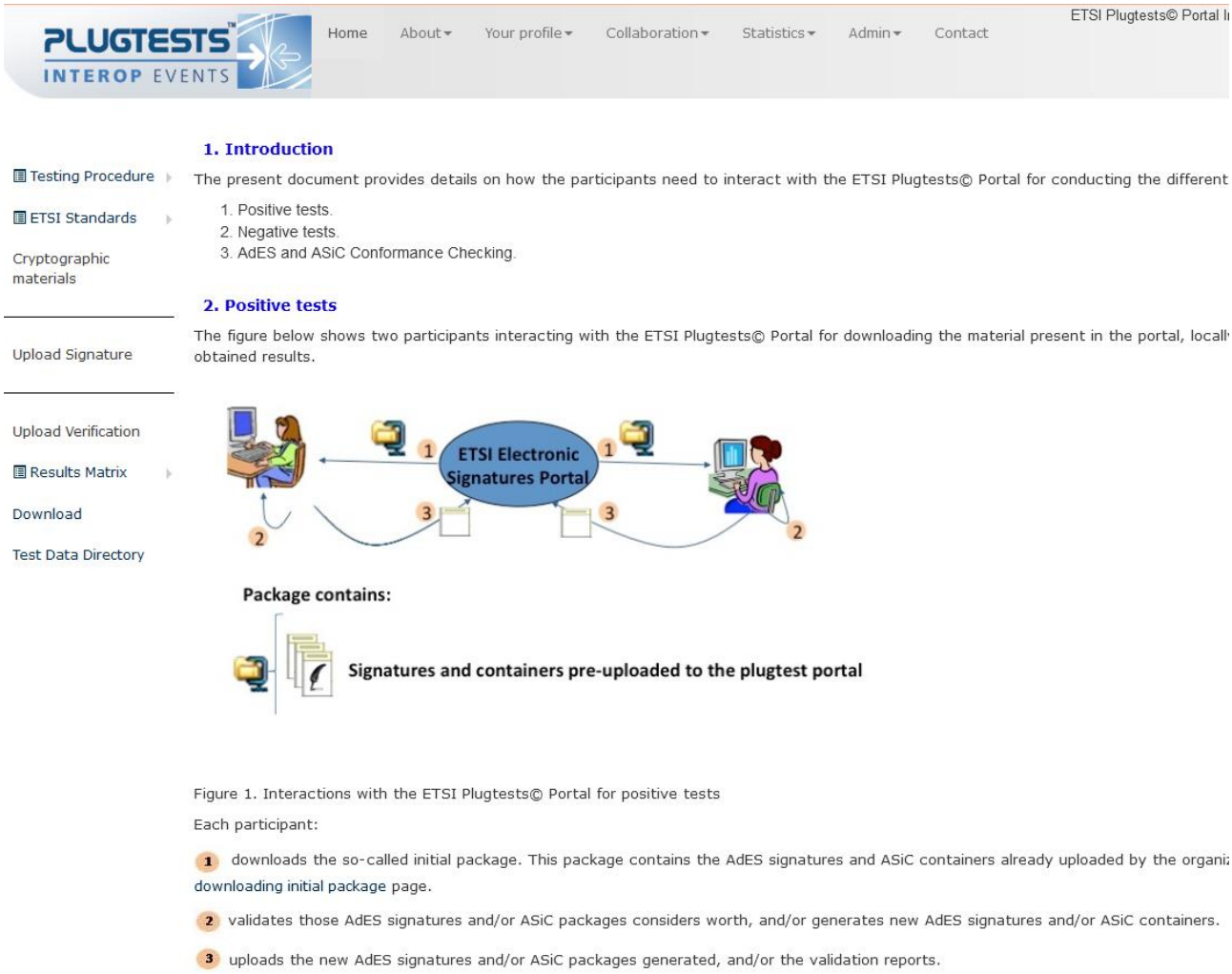


Figure 1. Interactions with the ETSI Plugtests© Portal for positive tests

Each participant:

1. downloads the so-called initial package. This package contains the AdES signatures and ASiC containers already uploaded by the organi
downloading initial package page.
2. validates those AdES signatures and/or ASiC packages considers worth, and/or generates new AdES signatures and/or ASiC containers.
3. uploads the new AdES signatures and/or ASiC packages generated, and/or the validation reports.

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 pages providing detailed explanations on how to conduct tests during the event.

2 types of tests were provided at this Plugtests event:

- **Positive** tests.
  Each participant was invited to generate some valid AdES signatures and/or ASiC containers. The rest of participants were invited afterwards to verify the signatures/containers (cross-verification).

- **Negative** tests**.**
  The organization team has generated a number of invalid signatures and/or ASiC containers including invalid signatures where the invalidity would have different causes. The participants were invited to verify the signatures/containers (only-verification).

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 a signature to the ETSI Advanced Electronic Signatures standards.

The 5 signature formats addressed in this event were:

- **XAdES:** XML Digital Signature (EN 319 132-1 and ETSI TS 103 171)
- **PAdES**: PDF Digital Signature (EN 319 142-1 and ETSI TS 103 172)
- **CAdES**: CMS Digital Signature (EN 319 122-1 and ETSI TS 103 173)
- **ASiC**: Associated Signature Container (EN 319 162-1 and ETSI TS 103 174)
- **JAdES**: JSON Digital Signature (TS 119 182-1)

The rest of the pages of the set provided details on:

- How to download material from the portal for 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 the 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 and their associated company acronym.

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
- The video record of the kick-off meeting, including a full demo on how to use the portal and how to upload signatures and verification reports.

2.2.1.4 Mailing list

2 Mailing lists were set up, restricted to the participants only:

- ESIG2022_UPLOADS@list.etsi.org : used by the Plugtests portal to automatically notify the participants after each upload of signatures or verification reports.

- ESIG2022_PARTICIPANTS@list.etsi.org : used to contact the participants and exchanges information. It was used for fruitful technical discussions and to raise some issues.

2.2.1.5 Slack

In order to allow better exchanges between participants, a slack channel was set up at :
https://esig2022-Plugtests.slack.com

Each participant was invited to create an account and use slack discussion forum.
In complement of the mailing list, it was an excellent way for the participants to raise technical discussions and to share experience, information and best practices.

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 signature had the immediate effect of updating the corresponding verification report matrix within the related area.

2.2.2.2 Upload Verification page

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 verification reports package had the immediate effect of updating the verification reports matrix within the related area.

2.2.2.3 Verification reports

This area contained a page where each participant could 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.

2.2.2.4 Download page

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 page

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 Lists.

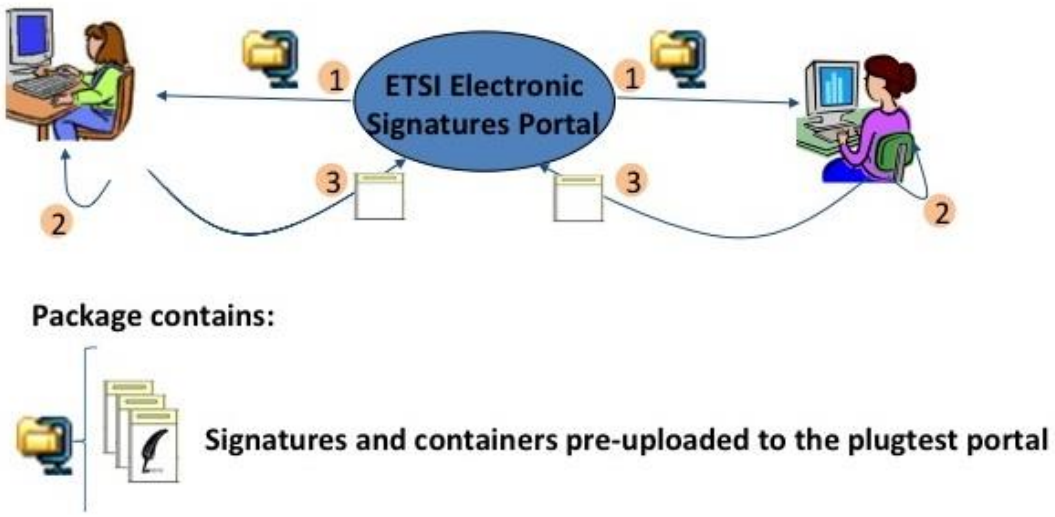
2.2.2.6 Cryptographic materials pages

This area contained a page where participants could fill a form to obtain by email a signing credentials in PKCS #12 format.

3 Conducting Testing

3.1 Generation and Cross-validation

The figure below shows two participants interacting with the portal for downloading the material present in the portal, locally performing the required operations for signature generation and cross-validation Plugtests type, and uploading to the portal the obtained results.



For the Plugtests, the participants should follow the following steps:

1) Download the so-called initial package. This package contains the AdES signatures and ASiC containers already uploaded by the organization team, distributed in a folders tree whose structure is explained in detail in the ETSI portal documentation pages.

2) Generate the signatures and/or ASiC containers and upload them to the portal

3) Participants are invited to validate other participants' signatures and/or ASiC containers, that considers worth to validate and upload the corresponding validation reports to the portal.

➔Each time a participant uploads a signature/ASiC containers and/or validation reports to the portal, the interoperability matrixes are updated reflecting the status of the testing.

3.2 Signature Generation

- **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 Plugtests portal automatically generated an updated set of interoperability matrixes that all the participants could access.

- **Negative** tests**:**
  The organization team had generated a number of invalid signatures and/or ASiC containers including invalid signatures (the so-called "negative testcases") , where the invalidity had 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.

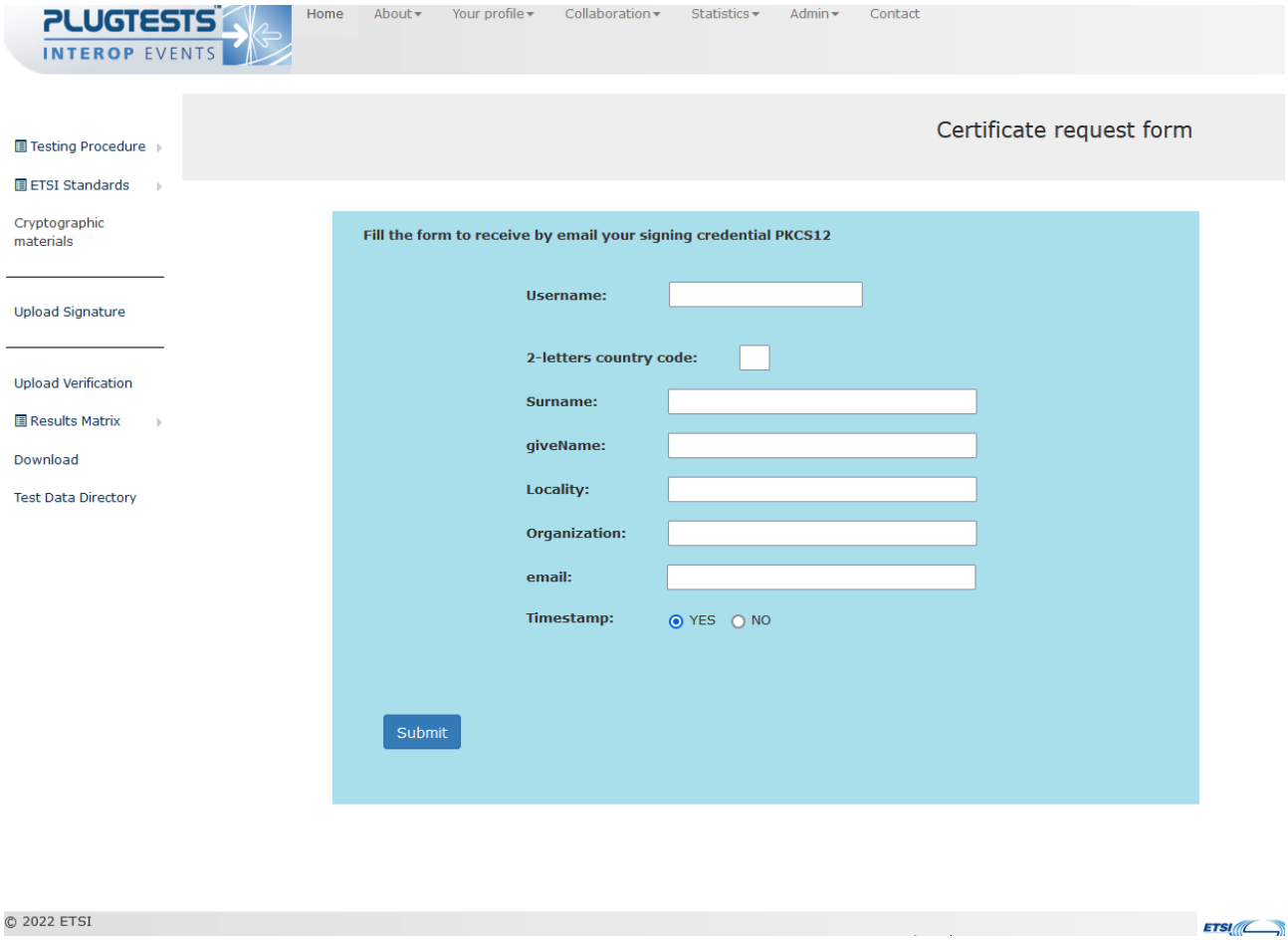
3.3 Certificates

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

It was also offered the possibility to obtain “Test” certificates produced by InfoCert, to be used for the Plugtests duration. Companies had to fill an online form with details to receive the corresponding signing credentials in PKCS #12 format.



3.4 Signature Validation Reports

The following formats for validation reports were admitted by the portal at this Plugtests event:

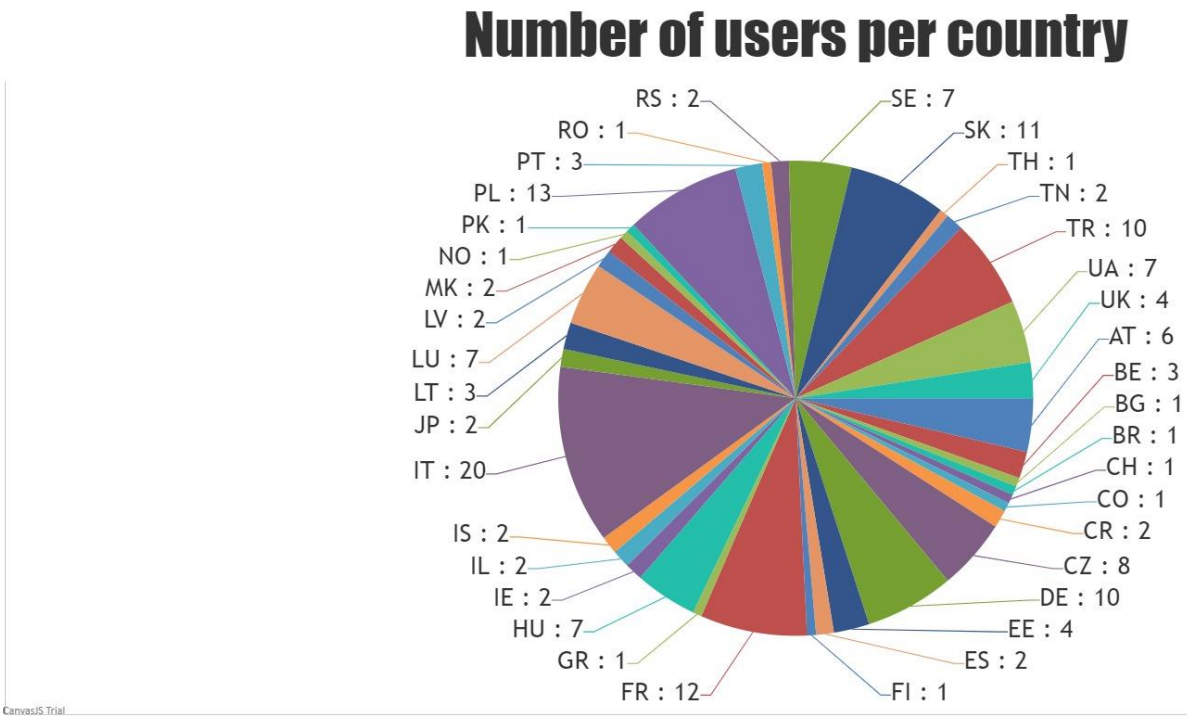
1. A validation report conformant to ETSI Draft TS 119 102-2 v1.2.2: Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report.

2. An ad-hoc validation report as the one used in former Plugtests.

4 Participants list

The table below shows the details of all the organizations and people who have participated in the 2022 eSignature Validation remote Plugtests event.

There were **111 different organizations** from **37 countries**, and **165 people** involved in the event.



Code	Country	Nb of users
AT	Austria	6
BE	Belgium	3
BG	Bulgaria	1
BR	Brazil	1
CH	Switzerland	1
CO	Colombia	1
CR	Costa Rica	2
CZ	Czech Republic	8
DE	Germany	10
EE	Estonia	4
ES	Spain	2
FI	Finland	1
FR	France	12
GR	Greece	1
HU	Hungary	7
IE	Ireland	2
IL	Israel	2
IS	Iceland	2
IT	Italy	20
JP	Japan	2
LT	Lithuania	3

Code	Country	Nb of users
LU	Luxembourg	7
LV	Latvia	2
MK	North Macedonia	2
NO	Norway	1
PK	Pakistan	1
PL	Poland	13
PT	Portugal	3
RO	Romania	1
RS	Serbia	2
SE	Sweden	7
SK	Slovakia	11
TH	Thailand	1
TN	Tunisia	2
TR	Turkey	10
UA	Ukraine	7
UK	United Kingdom	4

Total = 165

Country	Company
AT	GrEEV.com KG
	Rundfunk und Telekom Regulierungs - GmbH
	rit edv-consulting GmbH
	SignD Identity GmbH
	TU Graz (Graz University of Technology)
BE	Colruyt Group Services
	FPS Justice
BG	BORICA AD

Country	Company
BR	Certisign
CH	Swisscom Trust Servcies AG
CO	DIAN, Impuestos y Aduanas de Colombia
CR	BIS (Business Integrators Systems)
	Hermes Soluciones de Internet
CZ	ALIS spol. s r.o.
	Gordic spol. s r. o.
	I.CA (První certifikační autorita, a.s.)
	MONET+,a.s.
	RELSIE spol. s r.o.
	SEFIRA spol. s r.o.
	Software602 a.s.
DE	DIaLOGIKa GmbH
	Fujitsu Services GmbH
	Governikus GmbH & Co. KG
	intarsys GmbH
	SecCommerce Informations. GmbH
	Secrypt GmbH
	Segusoft GmbH
EE	Andri Möll
	eID Easy
	State Information System Authority (RIA)
ES	DAC-UPC
	Validated ID
FI	Methics Oy
FR	ADSN
	Bull SAS
	COPYRIGHT SAS
	DOCAPOSTE Trust & Sign
	ESMA (European Securities and Markets Authority)
	Gli services
	Universign
GR	QMSCERT Ltd
HU	Microsec Ltd
	MobilSign Ltd. (RoE+NDA signed by MobilSign Kft)
	Noreg Ltd.
	POLYSYS Ltd.
	TechTeamer Kft.
IE	Adobe Systems Software Ireland Limited
IL	Comsign Ltd
	Elbit Systems C4l and Cyber Ltd
IS	Advania Ísland ehf.
	University of Iceland
IT	ARIA S.p.A.
	Aruba PEC S.p.A

Country	Company
	Bit4id
	CINECA
	Entaksi Solutions SpA
	IN.TE.S.A. S.P.A.
	InfoCert S.p.A.
	INTESI GROUP S.p.A.
	IPZS
	Sanmarco Informatica S.p.A.
	Lang Edge
JP	Otip Office
	MIT-SOFT UAB
LT	SSC (Skaitmeninio sertifikavimo centras)
	Jemmic s.a r.l.
	LuxTrust S.A
	Nowina Solutions
LU	RCDevs Security
	Cobalt
LV	EUSO
MK	Nextsense
NO	Nets Branch Norway
PK	eTugra
	Asseco Data Systems S.A
	Enigma SOI Sp z o.o.
	ESYSCO Sp. z o.o.
	EuroCert Sp. z o.o.
	KIR (Krajowa Izba Rozliczeniowa S.A.)
	Madkom SA
	Regionalna Dyrekcja Lasów Państwowych w Szczecinie (Lasy Państwowe)
	Target Global ONE Ltd
PL	TIMT
	Devise Futures - IT Solutions, Lda
PT	Multicert S.A.
RO	certSIGN S.A
RS	Chamber of Commerce and Industry of Serbia
	3xA Security AB
	Comfact AB
	Idsec Solutions
	Telia Company AB
SE	TellusTalk AB
	Ardaco, a.s.
	Archimetes, s.r.o
	Disig a.s.
	DITEC, a.s.
	Narodna banka Slovenska (Nbs)
SK	NASES

Country	Company
	National Security Authority
TH	ETDA
TN	ANCE (AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE)
	NG Technologies
TR	Cyberwise (Cyberwise Siber Güvenlik ve Tic. A.S)
	Duru Bilişim
	Techsign
	Tubitak Uekae
UA	EGA
	State Enterprise "DIIA"
UK	Allied Bits Ltd
	Ascertia Limited
	Lyquidity Solutions Limited

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 111 organizations gathering 165 participants, 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 Plugtests by carrying out a demonstration of the portal utilization.

The utilization of Slack platform has also been very important for the participants to write their questions or requests and to record meeting minutes.

2 Mailing lists were set up:

- ESIG2022_UPLOADS@list.etsi.org : used by the Plugtests portal to automatically notify the participants after each upload of signatures or verification reports
- ESIG2022_PARTICIPANTS@list.etsi.org : used to contact the participants and exchanges information. It was used for fruitful technical discussions and to raise some issues.

5.3 Event duration

Initially, 4 weeks of testing had been planned for this event, starting from 16th May to 10th June 2022.

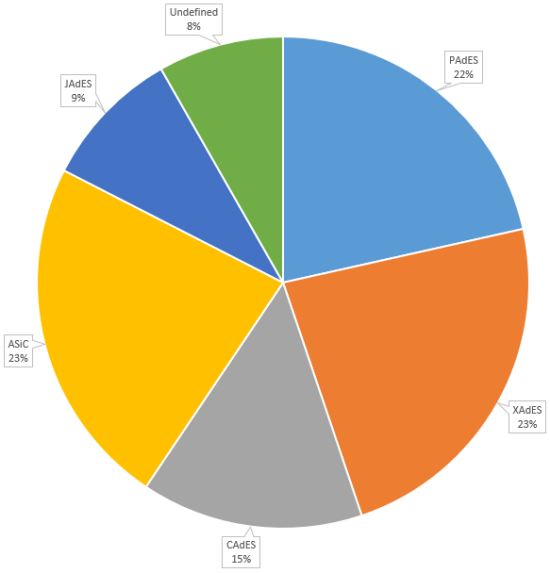
ETSI opened the portal on 15th May few hours before the Kick off meeting on 16th May in the afternoon CEST

Moreover, for this event, 165 participants were registered. As each company had to verify the signatures of other participants, the testing activity was very dense. It was therefore requested to extent the event twice, first until the 1st July 2022 and finally until the 15th July 2022.

6 Overall results

6.1 Signature uploads

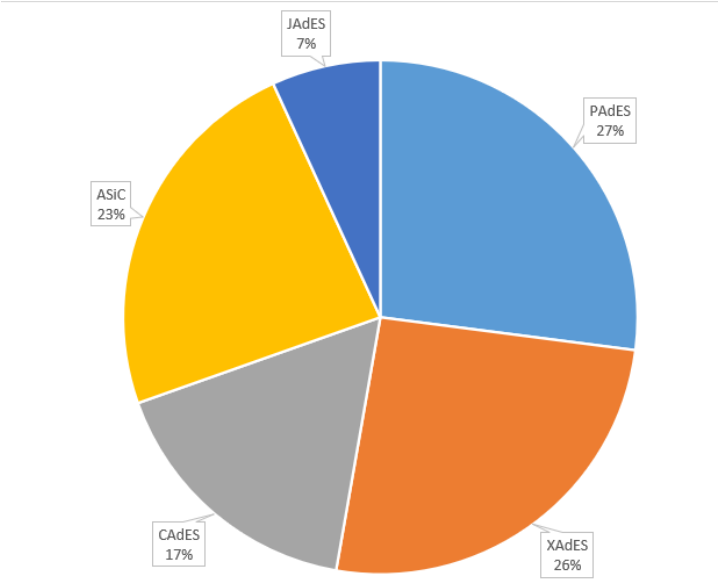
Format	Nb of signatures
PAdES	224
XAdES	243
CAdES	152
ASiC	241
JAdES	96
Undefined	86
Total	1042



6.2 Signatures validation report uploads

In total, **36 179** Verification reports have been produced and uploaded to the portal.

Verified Format	Verifications
PAdES	9931
XAdES	9440
CAdES	6179
ASiC	8656
JAdES	2513
Total	36 719



7 eSignature Validation related Issues

This clause lists some of the issues raised during the eSignature Validation Plugtests event. This list with the present technical report has been 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 CAdES signed attributes order

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

According to DER rules, defined in the "ITU-T X.690 International Standard 8825-1", the encoding of values within a set-of component shall appear in ascending order, in a way the encodings being compared as octet strings with the shorter components being padded at their trailing end with 0-octets (see "11.6 Set-of components").

Some participants relaxed their code to accept these signatures while other did not consider them valid.
A validation application should fail in "Cryptographic Verification" ETSI EN 319 102 building block, as the calculated message digest (with sorted values) does not match the one used to calculate the Signature Value.

7.2 Spoofing PDF Signatures

At the Plugtests the participants discussed about the possibility to create forged PDF signatures. The proposed attack works by duplicating a valid signature, in particular re-using its ByteRange and Contents value. It thus signs the same PDF contents as the original signature. However, due to being placed within a new signature dictionary in a new incremental update, the PDF signed properties in the new signature dictionary can be replaced, because they are not covered by the signature anymore. This includes PDF signed properties like Reason, Location, ContactInfo, Name, and the claimed signing time (M).

The forged signature in the sample PDF file specifies a forged Reason, Location, and ContactInfo, and specifies a claimed signing time one day earlier than the original time. Some existing validation software does not detect the forgery and produces a validation report claiming that the signature is valid, and listing the forged signed property values as being genuine.

This relates to the topic regarding what constitutes a valid byte range according to the PAdES specification. In particular, the PAdES specification is silent on what constitutes a valid byte range in the presence of incremental updates, e.g. when there are multiple signatures and or LT/LTA augmentations. Clearly in such case not every signature can sign the whole PDF.

It could be advisable considering the content of the above attack in order to check if some modifications to PAdES and/or AdES digital signatures validation specifications can mitigate the effects of this attack.

7.3 Revocation information for expired certificates

At the Plugtests some participants reported different opinions about the provision of revocation information for expired certificates.
Some participants think that the requirements stated in clause 6.3.10 in ETSI EN 319 411-2 allow QTSPs to provide revocation information for expired certificates in different ways other than in CRLs and/or in OCSP responses, therefore in some proprietary (non interoperable) ways while other participants think that, according to what stated in the above cited clause, revocation information of expired certificates shall be provided at least in CRLs and/or OCSP responses. It is asked to clarify this issue in the clause 6.3.10 in ETSI EN 319 411-2.

7.4 SignersDocument definition in SignatureValidationReportType

At the Plugtests one participant reported an issue in ETSI TS 119 102-2 V1.3.1 (2021-09):
Section 4.3.2 about Signature validation report XML element structure:

```
<xs:complexType name="SignatureValidationReportType">
<xs:sequence>
  <xs:element name="SignatureIdentifier"
type="vr:SignatureIdentifierType" minOccurs="0"/>
  <xs:element name="ValidationConstraintsEvaluationReport"
type="vr:ValidationConstraintsEvaluationReportType" minOccurs="0"/>
  <xs:element name="ValidationTimeInfo"
type="vr:ValidationTimeInfoType" minOccurs="0"/>
  <xs:element name="SignersDocument" type="vr:SignersDocumentType"
minOccurs="0"/>
  [...]
</xs:sequence>
</xs:complexType>
```

This definition allows only single <SignersDocument> element to be used and this is a problem in cases where the signature signs several files as in ASiC-E with several data files. It was requested to fix this issue in ETSI TS 119 102-2 V1.3.1.

7.5 Wrong definition in Annex A of ETSI TS 119 102-2 V1.3.1

At the Plugtests one participant reported that the sentence “A PAdES signature signs the whole document and consequently has only one pair of integers in the ByteRange child”, that appears in
Annex A Section 34.3 of ETSI TS 119 102-2 V1.3.1 (2021-09), is incorrect, since there shall be 2 pairs of integers in the ByteRange field of the Signature Dictionary because the whole PDF file except the Signature Dictionary field Contents is signed. The Signature Dictionary (and its Contents field) will be somewhere in the middle of the PDF file and, therefore, there is the need of a first pair of integers to locate the bytes up to the Contents field, and a second pair of integers to locate the bytes after Contents field. It was requested to fix this issue in ETSI TS 119 102-2 V1.3.1.

7.6 Wrong ASiC-E containers according to ODF 1.2 specifications

At the Plugtests it was noted that some ASiC-E containers included a META-INF/manifest.xml file not aligned with ASiC specifications.
In the ASiC standard in clause “4.4.3 Detailed format for ASiC-E with XAdES” it is clearly specified that "manifest.xml", if present, shall be as specified in OASIS: "Open Document Format for Office Applications (OpenDocument) Version 1.2; Part 3: Packages" 29 September 2011. Therefore

- the tag manifest:version shall be included in "manifest.xml" file with fixed value "1.2"
- attributes shall be used with namespaces, i.e. manifest:media-type="text/plain" shall be used instead of media-type="text/plain".

It was requested to check if some clarifications should be added to ASiC specifications about this topic.

7.7 Wrong ASiC-E containers with CAdES signatures

At the Plugtests it was noted that some ASiC-E containers with CAdES signatures included a META-INF/manifest.xml file and this inclusion seems not be allowed by ASiC specifications.
It was requested to include some clarifications in ASiC specifications about this topic.

7.8 TSA/QTST Sdi specifications in ETSI TS 119 612

At the Plugtests there were discussions between some participants because there are different interpretations concerning the possibility to specify a CA/TSA X.509 certificate as Sdi of a TSA/QTST Sti in a trusted list. Some participants interpret that only a TSU X.509 certificate shall be specified as Sdi of a TSA/QTST Sti in a trusted list while other participants interpret that also a CA/TSA X.509 certificate may be specified as Sdi of a TSA/QTST Sti in a trusted list.
It was requested to clarify this topic in TS 119 612 because, generally speaking, there shall not be different interpretations in what stated in a standard.

7.9 When gathering validation data for AdES-LT signatures

At the Plugtests there were long discussions concerning when the validation data needed to create AdES-LT signatures shall/may be collected.

There are different interpretations concerning the usage and possible values of the maximum accepted revocation freshness. Shall it be positive, or may it be negative too? When the revocation data is considered fresh and the signing certificate is valid, according to such revocation data, shall the signing certificate be considered valid or, if available, fresher revocation data shall be checked in any case? Are big values of revocation freshness a serious security issue? Shall the validation data included in AdES-LT signatures always have an issuance time after signature timestamp issuance time? What about if validation data issuance time is before signature timestamp issuance time or if validation data and/or signature timestamp is invalid in AdES-LT/LTA signatures (shall the signatures be considered AdES-B signatures or AdES-T signatures?)?

There are different interpretations concerning if when checking a CRL the value thisUpdate shall be considered trusted or a POE demonstrating the existence of the CRL at certain time is needed when validating an AdES-LT signature. It would be very appropriate clarifying such misinterpretations in ETSI EN 310 102-1.

7.10 OCSP certificate missing id-pkix-ocsp-nocheck extension

At the Plugtests it was noted that some OCSP responder certificates, involved in the signatures uploaded to the Plugtests portal, don't include the id-pkix-ocsp-nocheck extension. In many cases, when checking such OCSP responder certificates validity, an OCSP response signed by themselves (that's the same OCSP responder certificates) is returned but there is no sense/security in such OCSP responses where the OCSP signing certificate claims that it is not revoked by itself. Therefore, CRLs have to be used in such cases and it means OCSP service exists, but is completely useless. Of course, the id-pkix-ocsp-nocheck extension is not mandatory, but what is the sense of such an OCSP responder? Some recommendations in order to avoid above mentioned situations are suggested by the Plugtests participants.

7.11 Suggested fields to be added to the validation report

At the Plugtests some participants proposed certain indications/information/fields to be added to the validation report definition in order to improve its usefulness.

- An indication of the prospective lifetime of the signature under the current validation policy, which would also serve to indicate the latest time at which the signature should be further augmented to extend its lifetime.
- An information about signature Level: B, T, LT, LTA.
- An indication to declare, which validation data used to complete the signature validation is external (that's collected during signature validation) and which data is internal (included within signature itself).
- A placeholder for human-readable error messages.

7.12 Revocation data validation

At the Plugtests some participants reported that in ETSI EN 319 102-1 the revocation data validation process is not clearly and precisely specified. Some more detailed specifications were requested.

7.13 Validation of expired trust anchor TSU certificates

At the Plugtests one participant uploaded signatures including signature timestamps that were signed with TSU certificates listed in the member state TL as a TSA/QTST service that expired during the Plugtests period. Some validations performed after the TSU certificates expiration have not successfully validated such signature timestamps while some other ones have successfully validated such signature timestamps. The participants wondered if the above mentioned signature timestamps should be considered valid if the corresponding TSU certificates are still in the TL, therefore they are trust anchors, despite such certificates were expired. Should their status in the TL be changed? Indeed at least some validations of the following signature were completed with main indication total-passed considering valid such timestamps signed with expired TSU certificates because they are trust anchors in a member state TL.
The signature should be not valid (INDETERMINATE),

- since signing certificates of the first 2 timestamps were already expired,
- and the last time stamp (3-rd) was created after previous time stamp signing certificate expiration,
- therefore, there is no proof-of-existence for SignatureValue and the signing certificate was expired at current (validation) time too.

Signature contains an old OCSP response, which was also non-reliable due to missing valid timestamps. This OCSP response was signed using non-reliable algorithm (RSA-SHA1) - another reason to reject this revocation data.

But the following validation process according to ETSI EN 319 102-1 concluded with a total-passed main indication for one participant.

1. The signing certificate for the signature has expired at validation time, therefore we report OUT_OF_BOUNDS_NO_POE within “x509CertificateValidation” block;
2. The OCSP response for the signing certificate has been signed with rsa-sha1 algorithm, that is not reliable at the validation time, therefore CRYPTO_CONSTRAINTS_FAILURE_NO_POE indication is returned at validation time;
3. Moreover, the issuer certificate of the OCSP response has also expired at validation time, that produces OUT_OF_BOUNDS_NO_POE subIndication for the OCSP response as well;
4. As the revocation data is not reliable, we request a new OCSP response and provide it to the validation process;
5. The new OCSP response can be used even for an expired certificate, as it contains ArchiveCutoff property with a time before expiration of the validating certificate;
6. As the timestamps are produced by a directly trusted certificate (I do not 100% agree about that processing, but that behavior has been confirmed a while ago by ETSI), we effectively skip their validation and retrospectively valid the signing-certificate of the signature with regards to the available POE(s).

Formal clarifications from TC ESI have been requested by the participants.

7.14 XAdES revocationValues property

At the Plugtests there were some discussions about the limitation that a XAdES signature may include at most one single revocationValues property. Some participants believe that it should be allowed including more than one revocationValues property in a XAdES signature or alternatively, it should be allowed adding such new revocation information as instances of TimeStampValidationData. A reason is that the accepted revocation values may depend on the validation policy, and thus it makes sense adding more/different revocation values for the original signature even after an archive timestamp has been added (and thus an existing RevocationValues element can't be changed without removing the archive timestamp), to make the signature valid for different/new validation policies.

Formal clarifications from TC ESI have been requested by the participants.

7.15 Trusted list issues

7.15.1 Duplicated Sdi with same Sti in trusted lists

At the Plugtests it was reported that some trusted lists (specific examples are IE and BE) violates the requirement stated in ETSI TS 119 612 V2.2.1 (2016-04) "5.5.3 Service digital identity" specifying that the same public key (and hence the same certificate representing this public key) shall not appear more than once in the trusted list for the same type of service. Are there any possibilities to report this issue to the member states SBs?

7.15.2 Incorrectly formatted OID in trusted lists

At the Plugtests it was reported that some trusted lists contain wrong values in the PolicyIdentifier nodes.
Some examples:

```
<ns5:PolicyIdentifier>
    <ns4:Identifier>1.3.6.1.4.1.7597.2.</ns4:Identifier>
</ns5:PolicyIdentifier>

<ns5:PolicyIdentifier>
    <ns4:Identifier Qualifier="OIDAsURI">http://www.fineid.fi/cps33/</ns4:Identifier>
</ns5:PolicyIdentifier>
```

Encoding an OID as a URN according to RFC 3061 (as specified in ETSI EN 319 132-1) requires the prefix "urn:oid:" (cf. https://datatracker.ietf.org/doc/html/rfc3061#section-3).

Encoding an OID as a URI that is not a URN still requires some scheme prefix (cf. https://datatracker.ietf.org/doc/html/rfc3986#section-3). A string without a scheme is not a URI.

A plain OID like "1.3.6.1.4.1.7597.2" is therefore NOT a valid value for the Identifier element.
Many TL entries specify OIDs without the "urn:oid:" prefix, and without the required Qualifier attribute, in violation of the specification.
Are there any possibilities to report this issue to the member states SBs?

7.16 OCSP values in DSS dictionary

At the Plugtests there were some discussions about the DSS dictionary specifications defined in PAdES format. It was indicated that PAdES specifications are not entirely clear about what shall be included in the OCSPs array in the DSS dictionary: an OCSPResponse, a BasicOCSPResponse or just one of them. ETSI EN 319 142-1, indeed, specifies that it shall be a “DER-encoded Online Certificate Status Protocol (OCSP) response (that shall be as defined in IETF RFC 6960 [5])” without explicitly mentioning either the OCSPResponse or the BasicOCSPResponse ASN.1 type (which are both defined in RFC 6960).
To ensure proper interoperability, it would be desirable to clarify in PAdES which ASN.1 types are specifically allowed for the elements of the OCSPs array. Note that OCSPResponse and BasicOCSPResponse values are in principle easily distinguished by the ASN.1 tag of the first sub-element, so there would be little overhead in supporting both.
Formal clarifications from TC ESI would be appreciated by the participants.

History

Document history		
V1.0	30 Aug 2022	First version