Technical Report of the LTA Signature Augmentation & Validation Plugtests Oct-Dec 2023

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

February 2024
Version 1.1
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 2023 remote Plugtests event on Long-Term Archive (LTA) Signature Augmentation and Validation, 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 1st LTA Signature Augmentation and Validation Plugtests run remotely from **23rd October to 22nd December 2023**.

The aim of the event was to check the interoperability of digital signatures augmentation to LTA (Long-Term Archive) level and validation capacities of LTA level signatures of the participants to help them detect possible issues which may lead to different augmentation and/or validation results.

The interoperability testing allowed participants to test their digital signature validation tools and to cross-validate ETSI Electronic Signatures/Seals relying on EU Member States' Trusted Lists (based on TS 119 612 and TS 119 615) and 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
- TS 119 312 Cryptographic Suites

The signature formats addressed in this event were the following :

- XAdES: XML Digital Signature (EN 319 132-1/-2 and ETSI TS 103 171)
- PAdES: PDF Digital Signature (EN 319 142-1/-2 and ETSI TS 103 172)
- CAdES: CMS Digital Signature (EN 319 122-1/-2 and ETSI TS 103 173)
- ASiC: Associated Signature Container (EN 319 162-1/-2 and ETSI TS 103 174)
- JAdES: JSON Digital Signature (TS 119 182-1)
- Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES (TS 119 122-3)
- Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES (TS 119 132-3)

For the participants, the benefits of attending are

- 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.

[1] OJ L 257, 28.8.2014, p. 73–114.

Each participant was invited to generate some valid digital signatures with certain characteristics that are of use in their Member State. The rest of the participants were then invited to augment these signatures to LTA or ERS level.

All participants were invited afterwards to verify the signatures and the augmented ones (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, augmentations or the validation reports, all the participants were notified using a dedicated mailing list.

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 2023 LTA Signature Augmentation and Validation Remote Plugtests Event.

Clause 5 provides the conclusions of the Plugtests.

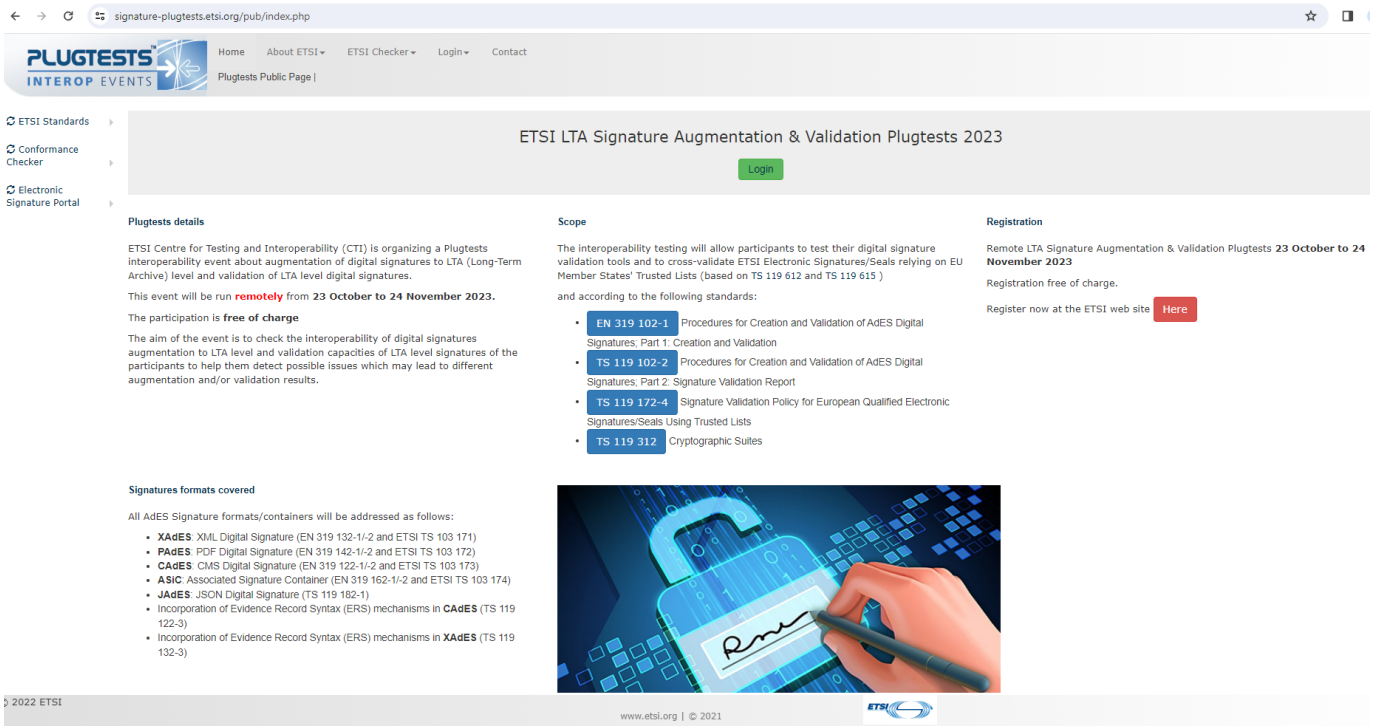
Clause 6 provides the overall results.

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.

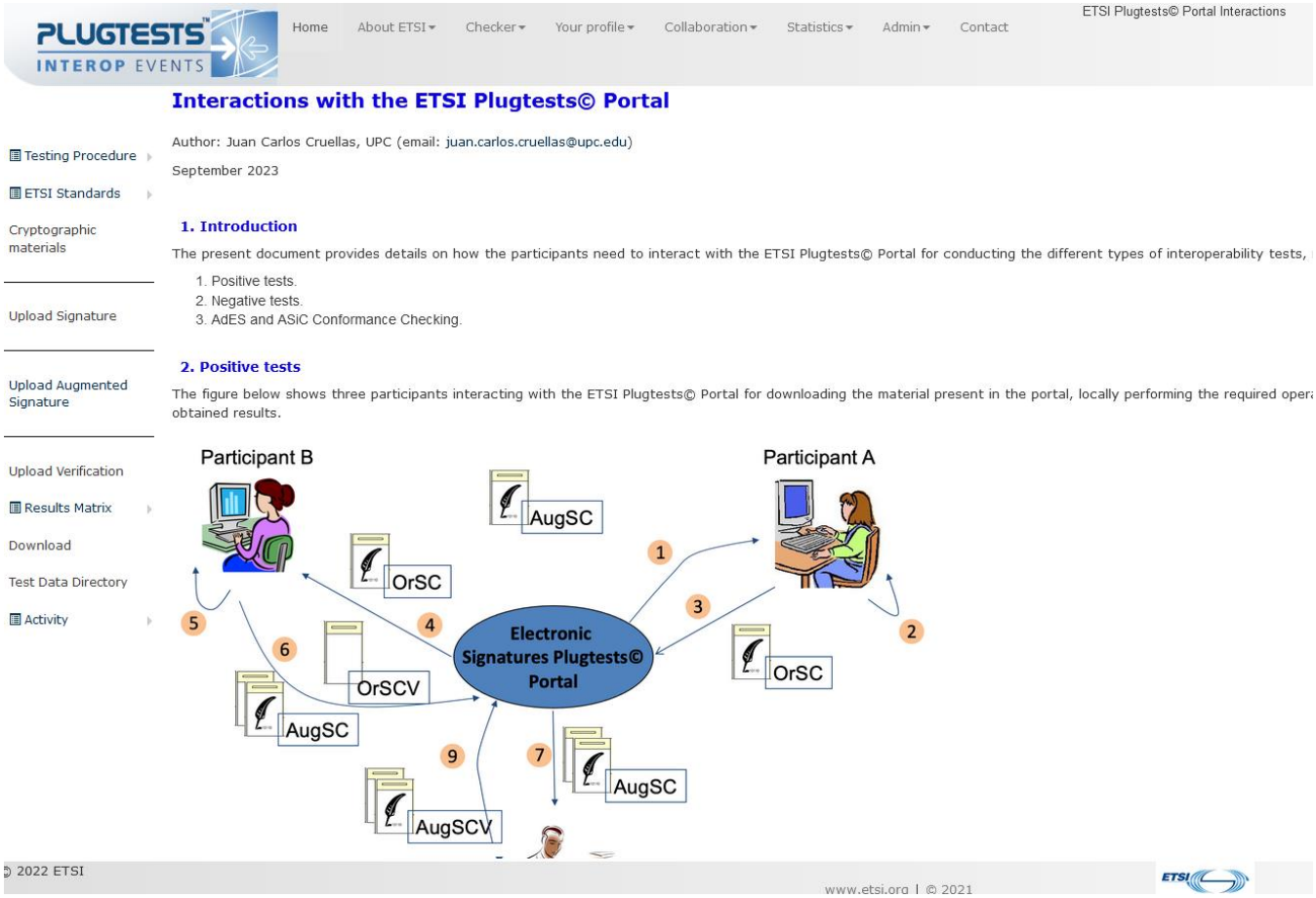
2.2 Private part of the portal

2.2.1 Overview

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 LTA Signature Augmentation and Validation.

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



2.2.2 Contents of the Common area in the Private part

- **Conducting Plugtests information pages**

The documentation is gathered in a set of pages providing detailed explanations on how to conduct tests during the event.

- **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.

- **Meeting Support page**

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

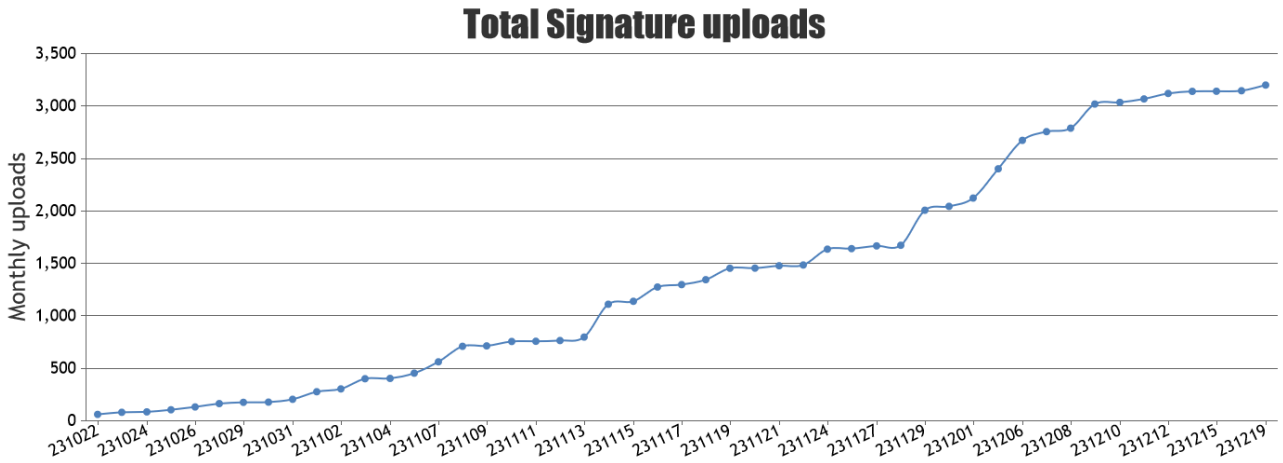
  - Introductory presentation which was made available before the start of the Plugtests, and provides the most relevant information on the event, including structure of the portal, relevant URLs, rules to be followed during the participation, etc
  - The video record of the kick-off meeting, including a full demo on how to use the portal and how to upload signatures and verification reports.

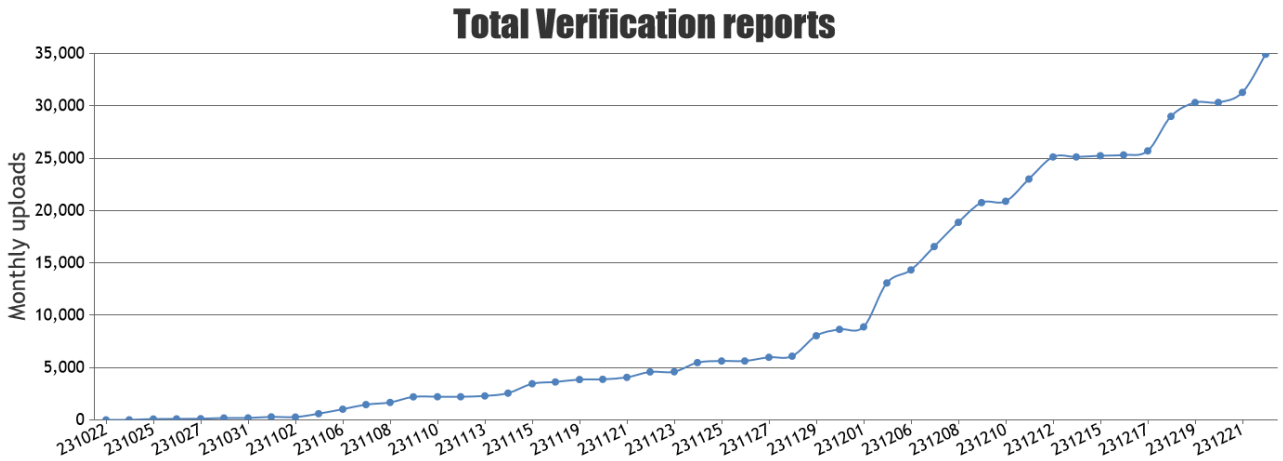
- **Cryptographic materials pages**

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

- **Statistics**

This page contained some data and statistics on the total number of signatures and validation reports uploaded per day and per signature format, and the daily upload activity for each signature format.





2.2.3 Contents of LTA augmentation and Validation Specific areas

- **Upload "new" Signature page**

The "Upload new signature" page provided mechanisms for uploading new signatures.
Participants are invited to upload only those signature format: X, P, C, J , AEX, AEC, ASX, ASC
The signature type must be B-B, B-T, B-LT or B-LTA.

- **Upload "Augmented Signature" page**

Participants are invited to augment the signature already uploaded by other participants and upload the new augmented signatures in order to be validated by other participants.
The signatures are augmented to LTA or ERS level.

- **Upload Validation reports page**

The participant can also upload the validation report obtained after validating the initial signature/container, OR the augmented signatures.

- **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 and augmentations

These matrixes included links to the signature files and to the validation report files as well as an indication of the validation 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 validation reports pages of the other participants.

In addition to the matrix, the list of uploaded signatures and the Validation reports (with result) is provided on several tables but also a downloadable excel file.

- **Download page**

This area contained a page that participants used for downloading the signatures and validation 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.

- **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.

- **Activity page**

Tables and downloadable excel files for all the upload activity for:

- Signatures
- Augmentations
- Validation report

2.3 Communications

2.3.1 Web conferences

2 web conferences were done,

- Kick-off of the Plugtests on 23 Oct 2023. To Introduce the event. The team explained how to conduct the testing and carrying out a demonstration of the portal utilization.

- A follow-up conference on 10 Nov 2023 to make a first debrief on the status of the testing and where participants had the possibility to put question on the testing but also to raise technical discussions.

The utilization of Web conference (GotoWebinar) has allowed the participants to get very interactive conferences by sharing the same document or application.

2.3.2 Mailing list

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

- LTA2023_UPLOADS@list.etsi.org : used by the Plugtests portal to automatically notify the participants after each upload of signatures, augmentations or validation reports

- LTA2023_PLUGTESTS@list.etsi.org : used to contact the participants and exchanges information. It was used for fruitful technical discussions and to raise some issues.

2.3.3 Slack

In order to allow better exchanges between participants, a slack channel was set up at :
https://ltasignaturep-try4386.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.

3 Conducting B-LTA and E-ERS Augmentation and Validation Plugtests

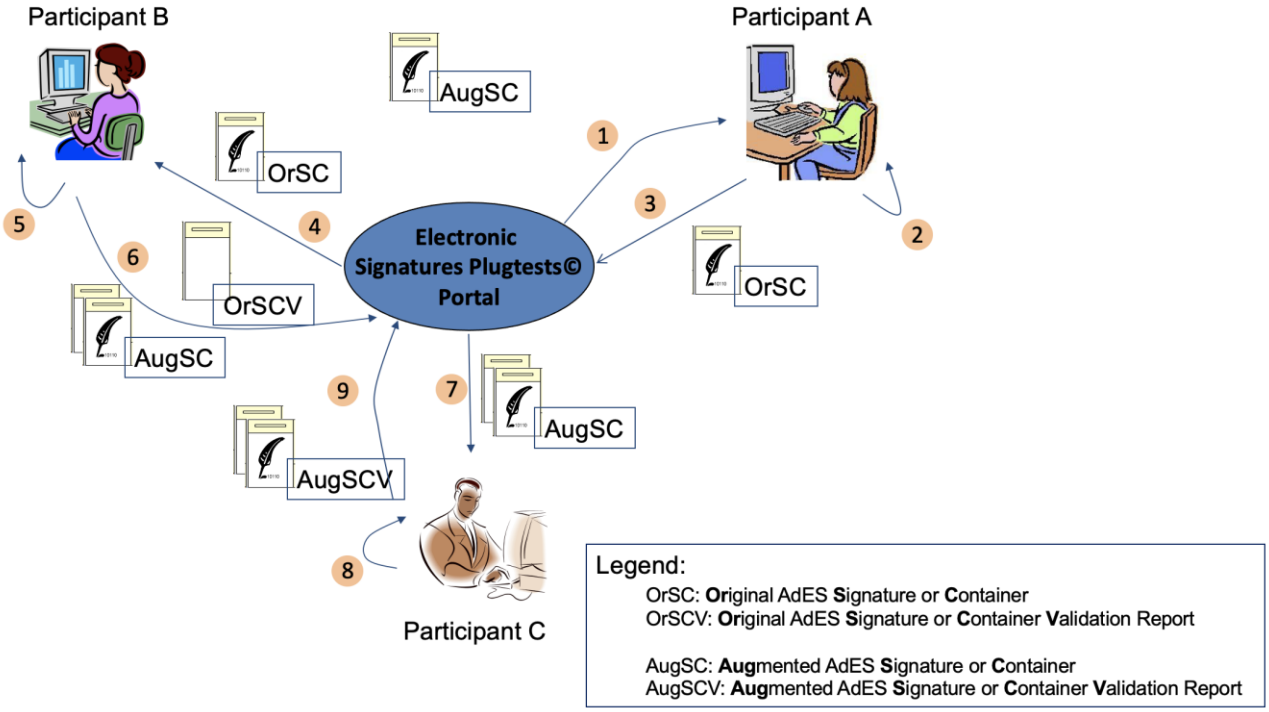
3.1 Generation , Augmentation & Cross-validation

3.1.1 Augmentation-positive tests:

Each participant is invited to generate a valid AdES signatures and/or ASiC containers with certain characteristics that are of use in their Member State. After that, each participant may either:

1. Take a signature/ASiC container (initial signature/container) uploaded by other participant, validate it, augment it to B-LTA or E-ERS level, and upload it to the ETSI Plugtests Portal so that the rest of participants can try to validate them, testing interoperability of B-LTA or E-ERS signatures/containers. The participant can also upload the verification report obtained after validating the initial signature/container, OR

2. Take an augmented signature/ASiC that another participant has uploaded after following the process indicated in the previous bullet, validate it (for checking interoperability) and upload the verification report to the ETSI Plugtests Portal



1. Participant A downloads the so-called initial package. This package contains the AdES signatures and ASiC containers already uploaded by the organization team (which may also include AdES signatures and ASiC containers delivered by other participants before the start of the Plugtests) distributed in a folders tree whose structure is explained in detail in the documentation.

2. Participant A generates an AdES signature or an ASiC container (**OrSC**).

3. Participant A uploads the AdES signature or ASiC container to the ETSI Plugtests© Portal.

4. Participant B downloads the AdES signature or ASiC container generated by Participant A.

5. Participant B validates the AdES signature or ASiC container generated by Participant A; generates a validation report (**OrSCV**), and **augments** the AdES signature or ASiC container generated by Participant A to **B-LTA** or/and **E-ERS** level (**AugOrSC**).

6. Participant B uploads the augmented signature (**AugOrSC**), and optionally the validation report (**OrSCV**) to the ETSI Plugtests© Portal.

7. Participant C downloads the augmented AdES signature or ASiC container generated by Participant B.

8. Participant C validates the augmented AdES signature or ASiC container and generates a validation report (**AugSCV**).

9. Participant C uploads the the validation report (**AugSCV**) to the ETSI Plugtests Portal

In general, each participant, once downloaded the initial package, may perform one, some, or all the following tasks:

- To validate those signatures and/or ASiC packages within the package that the participant considers worth.
- To augment to B-LTA and/or E-ERS levels some (or all) of the signatures and/ASiC packages previously validated.
- To validate some signature/ASiC container that has been previously augmented to B-LTA and/or E-ERS levels by other participants.

Therefore, a participant uploads to the ETSI Plugtests© Portal one, some, or all the following objects:

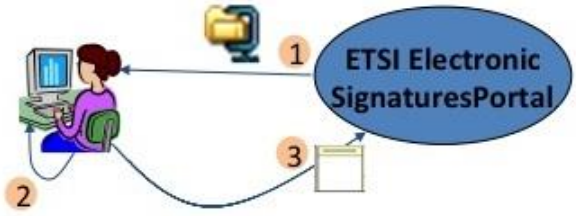
- Validation reports of signatures (not augmented) generated by other participants, resulting from the validation processes performed as for step 2.1.
- The augmented signatures/ASiC packages that the participant has generated augmenting signatures/ASiC containers generated by other participants to B-LTA and/or E-ERS levels, resulting from the augmentation processes performed as for step 5 above.
- Validation reports of augmented signatures/ASiC packages of B-LTA and/or E-ERS levels, whose augmentation has been performed by other participants, resulting from the validation processes performed as for step 5 above.

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

3.1.2 Negative tests:

The organization team and maybe some participants will generate a number of invalid signatures and/or ASiC containers including invalid signatures (the so-called "negative testcases") by different reasons.

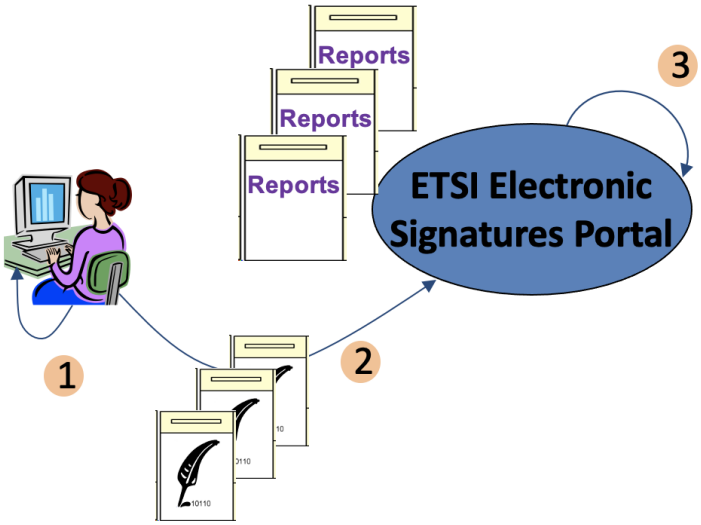
Each participant may, at her own discretion, try to verify these signatures and/or ASiC containers, checking in this way that the corresponding tool actually detects that the involved signature/ASiC container is not valid, which will prevent their augmentation.



Each participant:

- downloads the initial package.
- locally validates the AdES signatures and ASiC packages corresponding to the negative tests.
- uploads the verification reports obtained in the former step to the ETSI Plugtests Portal.

3.1.3 AdES and ASiC Conformance Checkers



- Participant generates a AdES signature or ASiC container purportedly conformant to its corresponding ETSI EN or TS.
- Participant requests conformance test to the ETSI Plugtests Portal. This is done signing in to the Conformance Checkers site and uploading the signature to the corresponding Conformance Checker.
- The corresponding Conformance Checker tool tests the signature and generates set of HTML reports that are shown to the participant.

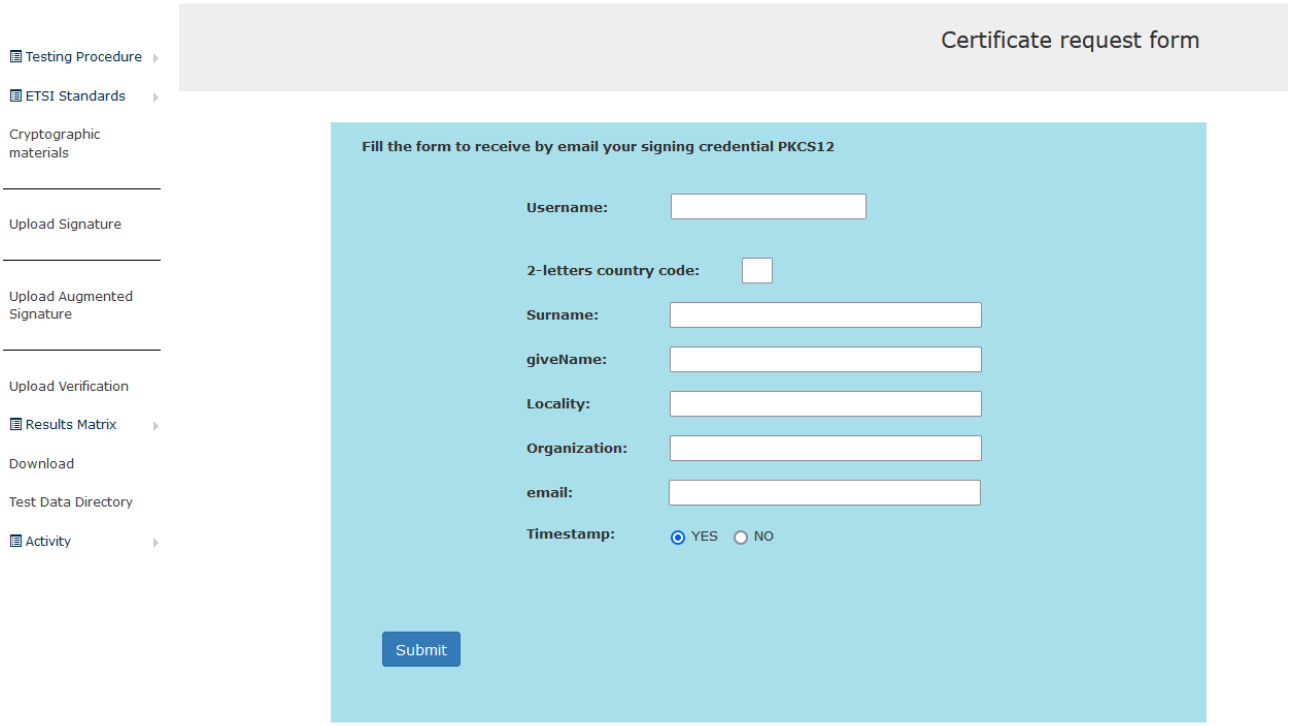
3.2 Certificates

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 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.



3.3 Signature Validation Reports

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

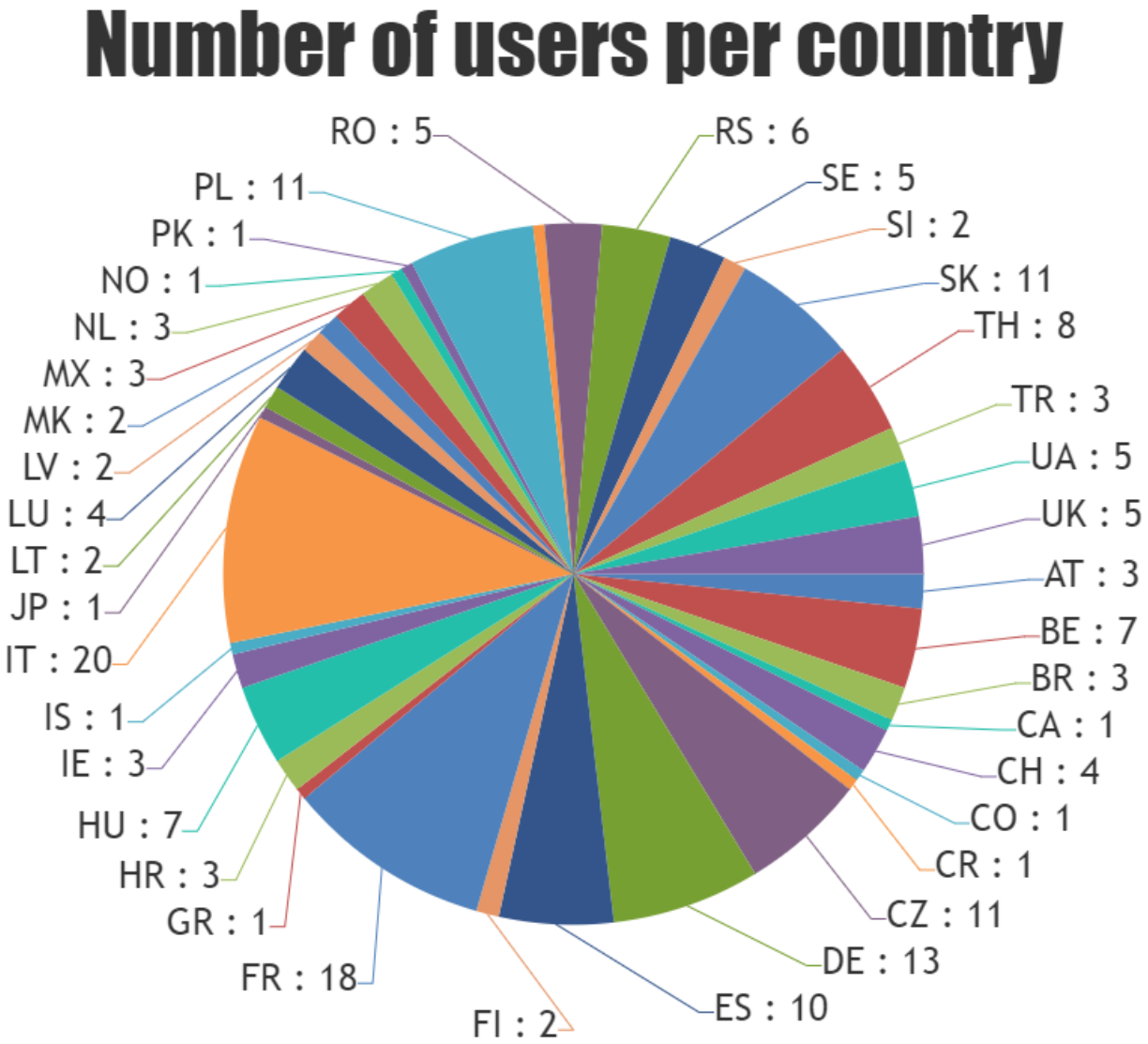
1. A validation report conformant to ETSI TS 119 102-2: Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report.

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 2023 LTA Signature Augmentation and Validation remote Plugtests event.

There were **122 different organizations** from **38 countries**, and **190 people** involved in the event.


Number of users per country
RO : 5
RS : 6
PL : 11
SE : 5
PK : 1
SI : 2
NO : 1
SK : 11
NL : 3
TH : 8
MX : 3
TR : 3
MK : 2
UA : 5
LV : 2
UK : 5
LU : 4
AT : 3
LT : 2
BE : 7
JP : 1
BR : 3
IT : 20
CA : 1
IS : 1
CH : 4
IE : 3
CO : 1
HU : 7
CR : 1
HR : 3
CZ : 11
GR : 1
DE : 13
FR : 18
ES : 10
FI : 2

Code	Country	Nb of users
AT	Austria	3
BE	Belgium	7
BR	Brazil	3
CA	Canada	1
CH	Switzerland	4
CO	Colombia	1
CR	Costa Rica	1
CZ	Czech Republic	11
DE	Germany	13
ES	Spain	10
FI	Finland	2
FR	France	18
GR	Greece	1
HR	Croatia	3
HU	Hungary	7
IE	Ireland	3
IS	Iceland	1
IT	Italy	20
JP	Japan	1
LT	Lithuania	2
LU	Luxembourg	4

Code	Country	Nb of users
LT	Lithuania	2
LU	Luxembourg	4
LV	Latvia	2
MK	Republic Of North Macedonia	2
MX	Mexico	3
NL	Netherlands	3
NO	Norway	1
PK	Pakistan	1
PL	Poland	11
PT	Portugal	1
RO	Romania	5
RS	Serbia	6
SE	Sweden	5
SI	Slovenia	2
SK	Slovakia	11
TH	Thailand	8
TR	Turkey	3
UA	Ukraine	5
UK	United Kingdom	5

Country	Company
AT	Danube Tech
	GREEV.com KG
	Namirial GmbH
BE	Apryse Group NV
	Federal Public Service Justice of Belgium
	Matthias Valvekens (Independent sole proprietor)

BR	Autentique LTDA
	Certisign
	e-Sec Digital Security
CA	Notarius
CH	Skribble AG
	Swiss Cyber Com SA
	Swisscom Trust Services AG
CO	Persona Digital
CR	Business Integrators Systems (BIS)
CZ	3Key Company s.r.o.
	ALIS spol. s r.o.
	eZprava.net s.r.o.
	Gordic spol. s r.o.
	MONET+,a.s.
	PDS s.r.o.
	První certifikační autorita, a.s. (I.CA)
	SEFIRA spol. s r.o.
	Software602 a.s.
DE	DiaLOGIKa GmbH
	ecsec GmbH
	Fujitsu Services GmbH
	Governikus GmbH & Co. KG
	intarsys GmbH
	Michael Klink (IT Consultant self-employed)
	Msg systems ag
	Procilon GmbH
	SecCommerce Informationssysteme GmbH
	secrypt GmbH
	Tomasz Kusber (independent)
	Ulrike Korte (Independent)
ES	ANF AC
	Autoritat Portuaria de Barcelona
	Coteco
	Departamento de Arquitectura de Computadores de la Universidad Politecnica de Cataluna (DAC-UPC)
	Docuten S.L.
	Entrust EU, S.L.
	NGS Software
	Servicios de MailCertificado - Codicert
	University of Vic - Central University of Catalonia (UVic)
FI	Methics Oy
	Studyo Oy
FR	ADSN
	AeonX AI
	Docaposte Arkhineo
	Docaposte Trust & Sign

	DTACCEL
	European Telecommunications Standards Institute
	GLI Services
	TLedger
GR	Ministry of Digital Governance
HR	Privredna banka Zagreb (PBZ d.d.)
	yottabyte j.d.o.o.
HU	Microsec Ltd
	MobilSign Ltd.
	NISZ Zrt.
	Noreg Ltd.
	POLYSYS Ltd.
IE	Adobe Inc
IS	UniDoc ehf
IT	AbleTech S.r.l.
	ARIA S.p.A.
	Aruba PEC S.p.A.
	Bit4id SRL
	Ecocerved SCARL
	Entaksi Solutions SpA
	InfoCert S.p.A.
	INTESI GROUP S.p.A.
JP	Otip Office
LT	MIT-SOFT UAB
LT	Skaitmeninio sertifikavimo centras (SSC)
LU	Jemmic
	LuxTrust S.A.
	Nowina Solutions
	RCDevs Security
LV	EUSO Ltd.
MK	KIBS AD Skopje
MX	SeguriData Privada, SA de CV
NL	Kadaster
	SecuMailer
	Zynyo
NO	Nets Norway
PK	TERASIGN GLOBAL PVT LIMITED
PL	Asseco Data Systems S.A.
	Enigma SOI Sp. z o.o.
	EuroCert Sp. z o.o.
	Krajowa Izba Rozliczeniowa S.A. (KIR)
	Madkom SA
PT	Devise Futures - IT Solutions, LDA
RO	AlfaTrust
	certSIGN
	ISSM CONSULTING

	Special Telecommunications Service (STS)
RS	Chamber of Commerce and Industry of Serbia
	E-Smart Systems d.o.o.
	Post of Serbia
SE	Comfact AB
	DIGG - Agency for Digital Government
	Revoltera Labs
	ZealiD
SI	SETCCE d.o.o.
SK	Archimetes
	Ardaco, a.s.
	Disig a.s.
	DITEC, a.s.
	Národná banka Slovenska (NBS) - National Bank of Slovakia
	NASES
	National Security Authority
TH	ETDA
TR	Duru Bilişim
	Ilerian Technology Ltd.
	Techsign
UA	CIPHER PRO, LLC
	eGA
	JSC Institute of Information Technologies
UK	Allied Bits Ltd.
	Ascertia

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 122 organizations gathering 190 participants, it would have been difficult to organize a face-to-face event.

5.2 Event duration

Initially, 5 weeks of testing had been planned for this event, starting from 23rd October to 24th November 2023.

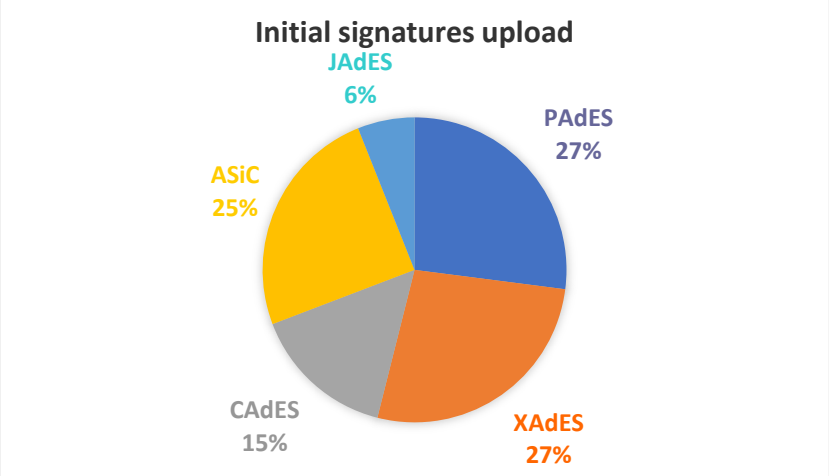
Due to intense testing and on the request of the participants, the event has been extended until 22nd December 2023, for a total duration of 9 weeks.

6 Overall results

6.1 Initial Signatures

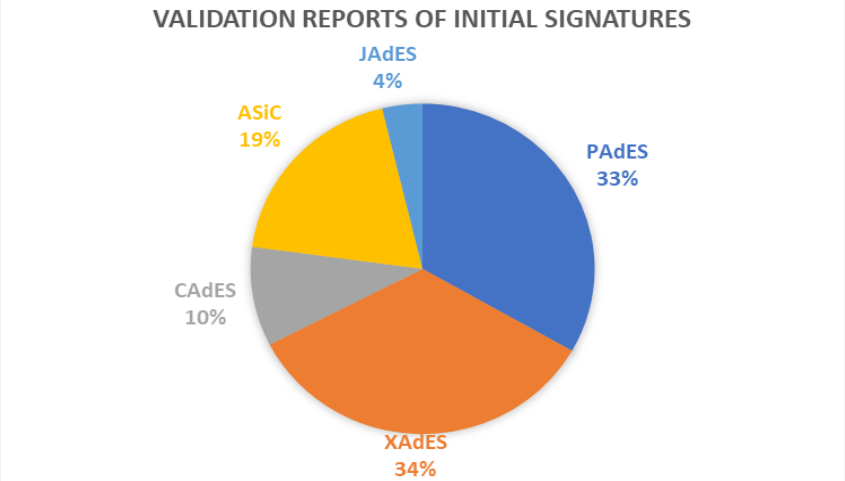
6.1.1 Signatures Uploads

Format	Nb of signatures uploads
PAdES	223
XAdES	222
CAdES	126
ASiC	204
JAdES	50
Total	825



6.1.2 Validation reports uploads

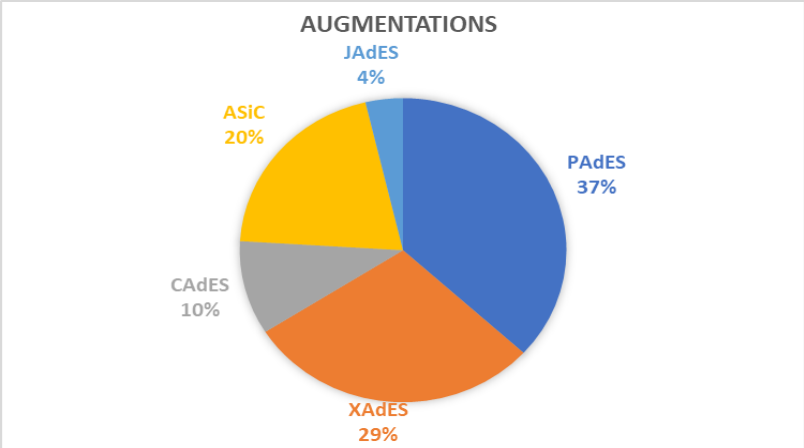
Format	Nb of signatures uploads
PAdES	3635
XAdES	3734
CAdES	1061
ASiC	2086
JAdES	413
Total	10929



6.2 Augmentations uploads

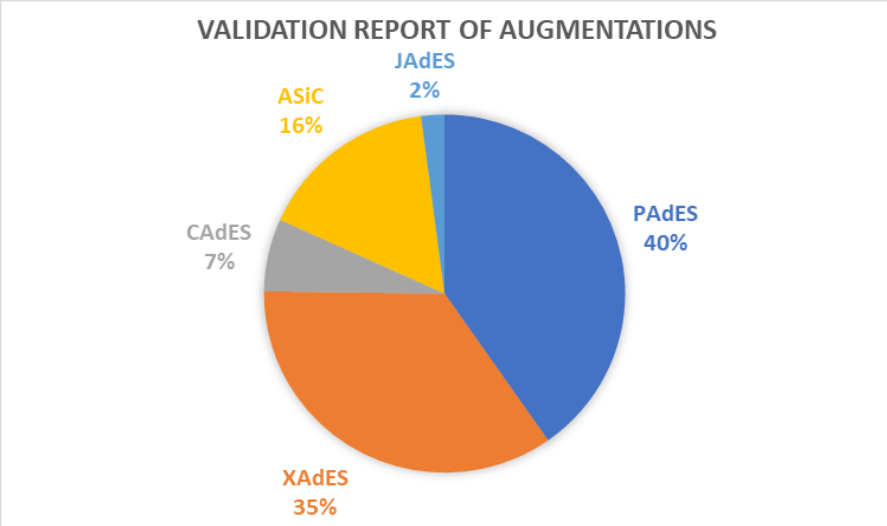
6.2.1 Augmentation Uploads

Format	Nb of augmentations
PAdES	874
XAdES	693
CAdES	237
ASiC	483
JAdES	88
Total	2375



6.2.2 Validation reports of Augmentations

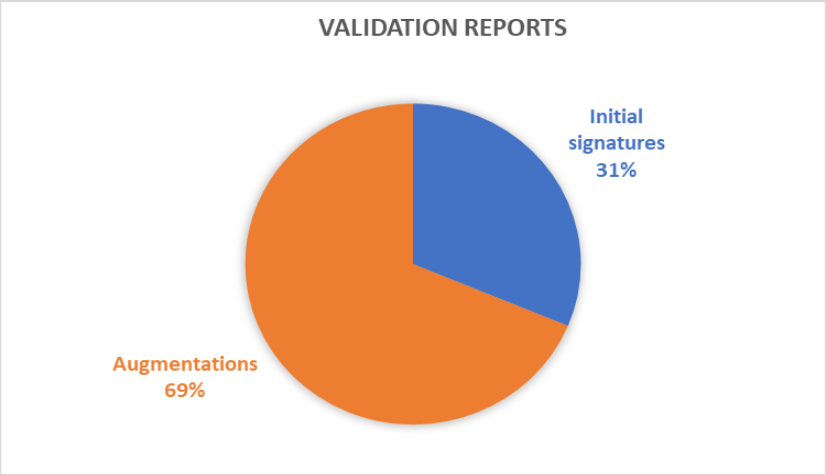
Verified Format	Validations
PAdES	9667
XAdES	8380
CAdES	1570
ASiC	3878
JAdES	501
Total	24296



6.3 Total Validation report uploads

In total, **35 225** Validation reports have been produced and uploaded to the portal.

Validated signatures	Validation reports
Initial signatures	10 929
Augmentations	24 296
Total	35 225



7 LTA Signature Augmentation & Validation related Issues

7.0 Introduction

This clause lists some of the issues raised during the LTA Signature Augmentation & 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 LTA level signatures freshness

At the Plugtests it was reported that if the signature timestamp signing certificate is not present in a member state trusted list, that's the case in which the TSU certificate is issued by a TSA being present in a member state trusted list, it is impossible to create LTA level signatures using freshness <= 0.
The reason is:

- having a signature timestamp generated at time T1, and
- revocation data included at time T2

archive timestamp will be included at time T3 (archive timestamp shall cover revocation data) and, necessarily, T1 <= T2 <= T3.

Signature timestamp signing certificate should be validated at time T3 (according to sliding process). Therefore, we should have OCSP.thisUpdate >= T3 - FRESHNESS (OCSP response for signature timestamp signing certificate). On the other hand, OCSP response validating signature timestamp signing certificate is included in the LTA level signature at time T2 <= T3. Therefore, OCPS.thisUpdate <= T3.

In such case LTA level signature creation and validation are possible if and only if FRESHNESS >= 0

Could such limitation be noted/clarified in EN 319 102-1?
Some proposals, in the case of LTA level signatures:

- FRESHNESS shall not be <= 0 in the QES policy
- the TSU certificates issued by a QTSA are trusted by themselves as the QTSA, that's the POE provided by the archive timestamp is not needed to prove the timestamp existence in the validation steps.

7.2 Interoperability issues for LTA level signatures freshness

At the Plugtests it was noted that since different validating/augmenting applications use different freshness, there were cases where:

- the signatures were augmented to LTA level using some big freshness value,
- but the validator of the LTA level signatures used a smaller freshness value and,

therefore, the validation outcome was the INDETERMINATE status.

A validator of already augmented LTA signature cannot augment again such signature without removing existing Archive timestamp.
Therefore,

- such LTA level signatures are not accepted as LTA level signatures according to the validation policy (because of revocation freshness), that's the LTA level signature, from the technical point of view, is compliant to signature format specifications but the validator shall retrieve new validation data in order to validate the signature not being able to use the validation data included in the signature,
- and the validator cannot augment such signatures to LTA level signatures satisfying the validation policy (without removing already existing data), that's it cannot create a signature at LTA level including acceptable validation data (according to its validation policy).

A participant asked if some maximum allowed freshness value for augmentation to LTA level should be standardized. However, shouldn't these problems be solved in the context of the policies (augmentation and validation) rather than in a document specifying the validation algorithm? It shouldn't be solved by a standard organization.

7.3 LTA ASiC-E with CAdES signatures

At the Plugtests there were some discussions about the baseline LTA level ASiC-E with CAdES containers uploaded by some participants.
There were different implementations of ASiC-E with CAdES containers regarding -LTA augmentation level across the Plugtests participants.

- The embedded CAdES signature file (META-INF/signature*.p7s) containing one or more CAdES signatures extended to B-LTA level as per ETSI EN 319 122-1; or
- The embedded CAdES signature file (META-INF/signature*.p7s) containing one or more CAdES signatures extended to B-LT level as per ETSI EN 319 122-1 and a detached time-stamp token and a linked ASiCArchiveManifest, covering the original data files and the signature file.

It was noted that in ETSI EN 319 162-1 it seems to be not very clear what augmentation option is allowed and/or preferred. The chapter "4.4.5 Long term availability and integrity of ASiC-E" says:
Long term availability and integrity of ASiC-E is achieved for the different container types as follows:
...
2) For ASiC-E containers with CAdES - time assertions either:
a) one or more ASiCArchiveManifest files and related time-stamp token shall be added to the container following the rules specified in clause A.7; or
b) one or more ASiCEvidenceRecordManifest files shall apply to all the signed and/or time-asserted data and/or signature and/or time-stamp token files requiring long term validation support.
...
Which could be understood as the option 2.a should be used (or an extension with an ER, but out-of-scope for now).
At the same time, "clause 5.1 ASiC levels" states:
This clause defines ASiC baseline containers with four levels intended to facilitate interoperability and to encompass the life cycle of ASiC containers namely:
...
d) B-LTA level provides requirements for the creation of containers incorporating signatures in compliance with the B-LTA level CAdES baseline signatures [1] or B-LTA level XAdES baseline signatures [2] that include time-stamp tokens that allow validation of the signature long time after its generation.
Which could be understood as there shall be an LTA level CAdES signature in the LTA level ASiC container.

7.4 Objects allowed to be added to a PAdES document without invalidating existing signatures

At the Plugtests the participants discussed about which object shall be allowed to be added to a PAdES document without invalidating existing cryptographic data.

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 some modifications to PAdES digital signatures validation specifications in order to clarify which objects mat be added to a PAdES document without invalidating existing signatures.

7.5 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.

7.6 PAdES signed range and end-of-line markers

Some participants discussed that PDF and PAdES specifications are not entirely clear on what constitutes an admissible end of the signed byte range with respect to the end-of-line (EOL) after the "%%EOF" marker, and with respect to subsequent incremental updates such as for LT/LTA augmentation and/or subsequent signatures.
Essentially the last line must have the content "%%EOF" but whether that last line is terminated by an end-of-line at all, let alone which one, is left to the discretion of the PDF creator.
Furthermore, because having no EOL at all at the end of that line is an option, numerous PDF processors first add one or more EOLs when creating incremental updates to prevent the start of their first added object to appear on the %%EOF line.
The issue seems to concern PDF specifications more than PAdES ones. What is signed is specified in the entry with key ByteRange in the Signature Dictionary whichever is the number of EOLs after the "%%EOF" marker.

7.7 Wrong PDF version in PAdES signatures

At the Plugtests some PAdES signatures using version PDF 1.1 were uploaded. Such signatures are not correct according to PDF specifications.
According to ISO 32000-1 (PDF 1.7), every PDF from 1.0 to 1.7 satisfies requirements of ISO 32000-1. But signature dictionary was introduced only in PDF 1.3, therefore, PAdES signatures may occur only in PDF 1.3 or later versions. DSS dictionaries and DTS may occur only from PDF 1.7 version onwards.

7.8 Non-conformant OCSP responders

At the Plugtests it was noted some inconsistent OCSP responses provided by a QTSP.
The following 2 OCSP responses were received for the same qualified signing certificate:
- OCSP1: ThisUpdate: 2023-11-27 19:01:06 +0200. Cert status is GOOD.
- OCSP2: ThisUpdate: 2023-12-10 19:54:07 +0200. Cert status is REVOKED on 2023-11-27 19:01:03 +0200

Therefore, OCSP1 response claims that the certificate was valid at 2023-11-27 19:01:06 +0200 while the OCSP2 response claims that the certificate was revoked at 2023-11-27 19:01:06 +0200 (since it was revoked 3 seconds before - at 2023-11-27 19:01:03 +0200).
Such inconsistent OCSP responses shall not be generated, at least in the case of qualified certificates.

Indeed, OCSP responses have 2 time fields to be used (RFC 6960):
ProducedAt - The time at which the OCSP responder signs the response.
ThisUpdate - The most recent time at which the status being indicated is known by the responder to be correct.

If OCSP responder takes several seconds for generating OCSP response or for storing revocation info into DB, OCSP responder shall set ThisUpdate time - some seconds in the Past so to ensure, that returned status is 100% correct at ThisUpdate time.
Validation tools cannot produce adequate results receiving such inconsistent data.

If RFC 5280 allows to issue CRL with a certificate revocation time < thisUpdate time of a previous CRL (see clause 5.3.2 of RFC 5280 when states “the revocation date SHOULD NOT precede the date of issue of earlier CRLs”) which does not contain the certificate (claiming that certificate status was GOOD), it does not mean, that it is directly applied to OCSP.
Even if OCSP is based on CRL.
The reason is that OCSP directly claims the opposite. Therefore, CRL (RFC 5280) and OCSP (RFC 6960) seem to have mutual incompatibility.
In such a case, it would be a good reason for ESI to resolve this issue in its own standards.
For example, in section 6.6 of EN 319 411-1 (or at least in EN 319 411-2), it could be clarified, that CA (or QCA) shall not create such CRLs and OCSP responses, since it creates lots of interoperability problems.

7.9 Augmentation to LTA level failures

At the Plugtests a lot of signatures claiming LTA level conformance were uploaded but many of them were not LTA level signatures according to signature formats requirements for the following main errors.

- ✓ missing timestamps,
- ✓ missing certificates (not included into the signature, that should include for every certificate the certificate path, and trusted certificate as well),
- ✓ missing revocation data, there are different reasons because existing data were rejected
- ✓ timestamps with missing validation data.

Note: if timestamp validation is NOT PASSED, the timestamp is skipped from validation process, and it may be the cause of internal validation data rejection (due to the resulting loss of proof of existence).

A list of the main reasons, because augmented signatures were not considered LTA level, follows:

-[Missing data for non-directly trusted TSU]: missing revocation data for a timestamp that is not the last ArchiveTimeStamp, being the timestamp signed by a TSU certificate that is not a trust anchor, namely the TSU certificate is issued by a TSA whose certificate is included in a member state trusted list as TSA/QTST service.

- o If the TSU certificate is not directly trusted (that’s only the issuer of the TSU certificate is included in a member state trusted list), certificate path should be built (both TSU and TSA (trust anchor) certificates) and revocation checks for TSU certificate shall be performed and TSU certificate validation data shall be included into LTA level signature.

-[Not fresh data for non-directly trusted TSU certificate (this issue is more related to the validation data freshness acceptance than the LTA level signature requirements, however it is worth considering it)]: some validation data is not fresh enough for a timestamp that is not the last ArchiveTimeStamp, being the timestamp signed by a TSU certificate that is not a trust anchor, namely the TSU certificate is issued by a TSA whose certificate is included in a member state trusted list as TSA/QTST service.

- o Usual case: there is internal time stamp, let’s call it PreviousTS, which is covered by the last archive time stamp, let’s call it LastATS; validation data for PreviousTS was collected at the time PreviousTS was generated but shall be collected at the time LastATS was created.

-[OCSP response expired]: there were LTA level signatures including OCSP responses for the signer certificate, but OCSP signing certificate was already expired at the time of covering ArchiveTimeStamp generation. Therefore, no suitable valid internal validation data is found for the signer certificate.

- If OCSP certificate validity period is very short, every included OCSP response should be covered by some archive timestamp as soon as possible, since, otherwise, included OCSP response will expire very soon, and it will no longer be usable.

-[Invalid ArchiveTimeStamp]: some signatures cannot be considered as LTA level ones because of included ArchiveTimeStamp failed hash verification. ArchiveTimeStamp hash calculation was performed not according to standard requirements (considering that augmented signatures had not been modified).

-[Different trust anchors]: a participating company included a person certificate into OtherCACertificates folder as trust anchor, and some other participating companies validated these signatures using person certificate as trust anchor, some other ones considered that only CA certificates can be trust anchors. These different choices lead to different amount of validation data needed to be included into LTA level signature and to different validation outcomes.

-[Last ArchiveTimeStamp validation failure because of the revocation freshness]: last ArchiveTimeStamp was created with non-directly trusted TSU certificate and OCSP responder (or CRL issuer as well) at validation time returned not fresh enough (very old) data (thisUpdate very much earlier than validation time). It leads to INDETERMINATE ArchiveTimeStamp validation with TRY-LATER subindication. Since, last ArchiveTimeStamp did not pass validation, it is eliminated from validation process, and this is a cause because LTA level is not reached. The only possible way to validate such signatures, is to include another new ArchiveTimeStamp and revalidate signatures in a later time.

Additional conclusions:

1. It looks like, that timestamp validation is not fully performed by some participants (only the path is built, and timestamp signature is validated, but skipping revocation validation, despite TSU certificate does not contain ocsp-no-check extension).
2. Almost all the problems are related to non-directly trusted time stamps. Non-directly trusted timestamps are a big problem for validation and augmentation procedures.

7.10 PAdES: Direct objects in signature dictionary

Some participants discussed about the PDF specification not being entirely clear on the requirements regarding direct/indirect objects in the signature dictionary, that a validator would have to check. This can be relevant to possible spoofing attacks.

PDF 32000-1:2008 section 12.8.1 specifies that "When a byte range digest is present, all values in the signature dictionary shall be direct objects". However, it is unclear what exactly "values" encompasses. It can't be recursively, because the Data entry of a signature reference dictionary contained in the Reference entry of signature dictionary is required to be an indirect object (table 253). One would think that it also can't be meant strictly non-recursively, i.e. just the primary entry-value objects themselves, because for the array-valued entries ByteRange, Cert, and Changes, the array elements should probably be direct objects as well (i.e. not just the array itself). Thirdly, Adobe's separate Digital Signature Build Dictionary Specification specifies with regard to the Prop_Build entry that "The build properties dictionary and all of its contents shall be direct objects", where one would interpret "all of its contents" to mean "fully recursively".

PDF 32000-2:2020 (currently not normative for PAdES) specifies for the ByteRange entry "shall be direct objects", which, based on the use of plural, probably refers to the array elements (the wording isn't really clear). This in turn would seem to indicate that the requirement regarding "all values" is to be interpreted non-recursively by default, unless specified otherwise for a particular entry (such as for the ByteRange entry here).

The Cert entry shall not be used in PAdES signatures, and it is not sure if the Changes entry is security-relevant, but regarding the value of the Reference entry, it would seem important that most of it be direct objects as well.

A clarification would be appreciated.

7.11 QTSA with unacceptable revocation service

At the Plugtests there were some cases where OCSP services (CRLs as well) returned unacceptably old revocation data, i.e. having thisUpdate set to 2023-07-12 18:00:00 +0300, that's half a year old.
In such case there is no possibility to complete the validation if the TSU certificate (which is not a trust anchor) was currently valid, or valid at the covering time stamp creation time.

There are 2 problems to be mentioned:

1) There is no possibility to validate such a timestamp, since it is not a trust anchor and there is no fresh revocation data available. But some validation tools succeeding in validating these timestamps and this was considered quite strange/unusual.
2) Is such a behavior of QTSA (not providing fresh revocation data) aligned with standards or eIDAS regulation?

If nextUpdate is not reached yet, then such revocation information can in principle be accepted. For online revocation checks, the underlying assumption is that if there was a revocation since thisUpdate, then newer revocation information would have been issued. Conversely, if no newer revocation information was issued, then the implication is that no newer revocation has occurred (before nextUpdate). Consistent with that, EN 319 102-1 clause 5.2.5.4 step 1 sets the freshness constraint to the difference between nextUpdate and thisUpdate if no explicit freshness constraint has been configured.

TS 119 172-4 requires a freshness constraint to be set (REQ-4.2-03 c) ii)) for the validation of EU QES, so the mentioned default of clause 5.2.5.4 does not apply. This is of particular importance for long-term validation with stored revocation information, because in such case the assumption mentioned above for online revocation checks does not hold, because it is not known whether newer revocation information was available or not at best-signature-time.

EN 319 411-1 requirement CSS-6.3.9-05 mandates that CRLs "concerning end users certificates […] shall be published at least every 24 hours". However, this doesn't concern TSU certificates, and also OCSP is not mentioned here.

For intermediate CAs and cross-certificates, the intervals are much laxer:

"CSS-6.3.9-12 [CONDITIONAL]: If CARL is used, a new CARL shall be generated at least once a year with a nextUpdate of at most 1 year after the issuing date."

"CSS-6.3.9-14: In the case of any cross-certificates issued by the CA to other TSPs, the CARL should be issued at least every 31 days."

EN 319 421 regarding TSAs does not add any further requirements regarding the publication schedule of revocation information.

This is an issue for LTA validation. In the case of intermediate CAs, one might have to wait one year before being able to collect revocation information suitable for LTA level signatures.

7.12 adbe-revocationInfoArchival usage

During the Plugtests a set of PAdES signatures having SubFilter "ETSI.CAdES.detached" and also including adbe-revocationInfoArchival attribute in the CMS signature were uploaded.

PAdES profile for CMS Signatures in PDF (if SubFilter is "adbe.pkcs7.detached" or "adbe.pkcs7.sha1") allows to use adbe-revocationInfoArchival attribute (in ETSI TS 102 778-2 and in ETSI EN 319 142-2).

In the standards ETSI TS 102 778-3 and ETSI EN 319 142-1, this attribute is not allowed in other PAdES profiles (that's if SubFilter is "ETSI.CAdES.detached").

ETSI TS 102 778-3 section 4.5:
"The following attributes may be present with the signed-data depending on the profile employed. The use of these attributes shall be as defined in CAdES (see TS 101 733 [2]) qualified by the present document which takes precedence."
Note that adbe-revocationInfoArchival attribute is not listed.

ETSI EN 319 142-1 section 5.2
"The attributes included in the following list may be used to generate the DER-encoded SignedData object included as the PDF signature in the entry with the key Contents of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1."
Note that adbe-revocationInfoArchival attribute is not listed.

If attribute is not listed, it means it "may NOT be used" - means it is forbidden in PAdES profile.

Additionally, if we talk about baseline signatures:

ETSI EN 319 142-1 section 6.3
"6.3 PAdES baseline signatures
This clause defines requirements on attributes, fields and services that PAdES baseline signatures have to fulfil. The attributes defined in ETSI EN 319 122-1 [2] and not listed in table 1 shall not be present."
And attribute adbe-revocationInfoArchival is not listed.
Therefore, at least for baseline signatures adbe-revocationInfoArchival shall be considered forbidden.

7.13 Evidence Record Syntax in ETSI TS 119 122-3

At the Plugtests, there were some discussions about the possibility to use ERs with the same functionality of the signature timestamps. A participant noted that the outcome of the signature timestamp requirement to enforce freshness of validation data can be achieved with an ER too:
- applying an ER within the required freshness interval after the revocation information issuance;
- or applying an ER whenever needed;
then generate and add revocation information to the timestamp of the ER. Finally, perform ER's Timestamp Renewal. Now both the document and the validation data are protected by the ER and it proves that the certificate was not revoked at the time of signing.

The participant, working in a healthcare industry, highlighted that the seemingly unwarranted signature timestamp requirement has huge economical implications.
Consider a lab, which produces tens of thousands documents a day.
Without the signature timestamp requirement it would need just a few qualified timestamps a day. The documents format is PDF with machine readable data in its attachment and sometimes the documents must be preserved for the life of a patient. So it's better not relying on a third party service and having all the data needed for validation within the document itself. This could be achieved by allowing an ER in the Document Timestamp Dictionary (e.g. SubFilter could be ETSI.RFC4998) considering that an ER is usually just a RFC3161 timestamp wrapped in a data structure.

Some implementation notes on ERS:
- Digest function for the whole ArchiveTimestampChain and all the timestamp fields within the chain must be the same (follows from the RFC4998). Some participants used different hash functions for hash-tree and timestamps.
- When renewing the hash-tree, the hashes of data object and ArchiveTimeStampSequence are not sorted before concatenation. Those hashes are distinguishable, so there's no need to sort them before concatenation like in the case of hash-tree construction; ordering is given. There is an error in Figure 4 of RFC4998, which states "h1' = H(binary sorted and concatenated (H(d1), ha(1)))", but 5.2. point 4. clearly states "Concatenate each h(i) with ha(i) and generate hash values h(i)' = H (h(i)+ ha(i)).".

Some notes on validation:
Often ER attribute is not taken into account during validation. E.g. there was a signature that was a valid CMS, but the CMS data were modified and the ER was no longer valid, since the hash of the CMS had changed but, in any case, there were some successful validation reports.

7.14 Successful validation of timestamps signed by expired TSU certificates still present in a member state trusted list

At the Plugtests it was noted that the successful validation, mentioned in the clause title, is correct, and it will be more explicitly specified in the next versions of EN 319 102-1, TS 119 615 and TS 119 172-4. However, services in the trusted list can be withdrawn (= be marked as withdrawn from a certain date in the trusted list), after which the validation of the timestamp will fail. The downside here is that you don't know in advance when this will happen,

compared to the expiration date of a certificate. However, maybe the expiration date of the certificate can be taken as a likely lower bound for withdrawal of the service from the trusted list, assuming no earlier key compromise or similar.

7.15 Validation procedures in ETSI EN 319 102-1

At the Plugtests a participant reported a possible bug in the validation process defined in EN 319 102-1 v1.3.1 that can cause an invalid signature to be evaluated as TOTAL-PASSED.
Let's have a document with one signature and one signature timestamp. Let's assume that there is some issue with the signing certificate's chain which causes the chain to not match the X.509 validation constraints. Now when the signature is being verified, it will be detected in the X.509 certificate validation block (clause 5.2.6.4, step 3) that the certificate chain does not match the validation constraints and the building block will end with the indication INDETERMINATE/CHAIN_CONSTRAINTS_FAILURE. Finally, the signature verification will end with this result, which is correct.
Now let's assume that the signing certificate has been revoked. This time the X.509 certificate validation block will end already in step 2b) and the indication INDETERMINATE/REVOKED_NO_POE will be returned from the validation block. Step 3) will not be performed at all. Later, as part of the validation process for Signatures with Time (clause 5.5.4, step 4a), it is determined that the revocation time is posterior to best-signature-time, which can help to go from INDETERMINATE to TOTAL-PASSED, and the validation process continues. However, the X.509 validation constraints verification that was skipped in the X.509 certificate validation block is not performed in any of the remaining steps. Thus, the final result of the signature verification will be TOTAL-PASSED, which is wrong.

Another issue can be in step 8) of the Validation process for Signatures with Time and Signatures with Long-Term Validation Material (clause 5.5.4), where the SVA performs the Signature Acceptance Validation. NOTE 6 states about this step:
NOTE 6: This check has been performed already in step 2) as part of basic signature validation for current time but is repeated here for the earliest time the signature is known to have existed to e.g. check if the algorithms were reliable at that time. Signature elements constraints have already been dealt with in step 2) and need not be rechecked.
However, this is inaccurate. The Signature Acceptance Validation might not have been performed as part of the basic signature validation at all. Specifically, Signature Acceptance Validation occurs in step 6) of the basic signature validation process, but the process may end prematurely in one of the prior steps, such as when the X.509 Certificate Validation ends with status INDETERMINATE/REVOKED_NO_POE or INDETERMINATE/OUT_OF_BOUNDS_NOT_REVOKED.
So, for instance, if the basic signature validation process ends with a status INDETERMINATE/REVOKED_NO_POE and it is subsequently found that the certificate's revocation is not a problem due to the presence of a signature timestamp, the validation process proceeds to step 8). If the SVA follows the advice that signature elements constraints don't need to be rechecked, the validation will end with a TOTAL-PASSED result without the signature elements constraints being checked at all.
The same applies to the Signature Acceptance Validation carried out in step 8) of the Validation Process for Signatures providing Long Term Availability and Integrity of Validation Material (clause 5.6.3.4). Note 6 states that the Signature Acceptance Validation has already been performed in step 3), suggesting that the signature elements constraints need not be rechecked. However, the Signature Acceptance Validation might not have occurred during step 3) at all.

There is a similar but even more serious issue with the Signature Acceptance Validation and the validation of timestamps.
In step 5) a) of the Validation Process for Signatures providing Long Term Availability and Integrity of Validation Material (clause 5.6.3.4), the validation of timestamps takes place. As before, the validation process may proceed in such a manner where the Signature Acceptance Validation is not performed (e.g., if the timestamp certificate has expired, leading the process to conclude with the INDETERMINATE/OUT_OF_BOUNDS_NO_POE state).
Moving to step 5) c), past signature validation process is conducted, during which the timestamp can be successfully verified due to the sliding of the validation time into the past. However, the past signature validation process does not include Signature Acceptance Validation at all. Consequently, in this scenario, neither the signature element constraints nor the cryptographic constraints will be checked. As a result, the validation process will accept timestamps that, for example, use an unreliable signature algorithm.

In some implementation Signature Acceptance Validation is performed if X509Certificate validation finishes with some NO_POE subindication, which may be resolved later on.

History

Document history		
V1.0	30 Jan 2024	First version
V1.1	07 Feb 2024	Updated the number of participating companies