PLUGTESTS TECHNICAL REPORT

Technical Report of the Digital Signature Validation Plugtests Nov-Dec 2019

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

Jan 2020

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 2019 remote Plugtests event on Digital Signature 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, advanced electronic signatures and seals based on a qualified certificate and qualified electronic signatures and seals in specific formats, or alternative formats validated pursuant to specific reference methods[2].

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

To allow such testing to happen, a Digital Signature validation Plugtests was organized by ETSI in cooperation with the Commission. It has run remotely from 30th October to 20th December 2019.

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 4 main Digital Signature formats (XAdES, CAdES, PAdES and ASiC) according to the following standards:

- **European Standard EN 319 102-1** (Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation) and TS 119 102-1
- **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, under completion)

The present document is the report from the 2019 remote Plugtests Event on Digital Signature Validation. It also provides details on the specification, design and implementation of the portal supporting remote Plugtests events , including an overview of the contents of the portal .

An introduction web conference took place on 29 October to present the portal and the testing.

The event was initially planned to run until 29th November 2019, but it was extended to 20th December 2019, on the request from the participants. The reason behind was the amount of testing activities which was extremely high within

[1] OJ L 257, 28.8.2014, p. 73–114.

the initial scheduled period, due to the large number of participants (230) and the corresponding number of proposed signatures to validate.

The present document is divided into the following sections:

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

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

Section 4 lists the participants to the 2019 Digital Signature Validation Remote Plugtests Event.

Section 5 provides the conclusions of the Plugtests.

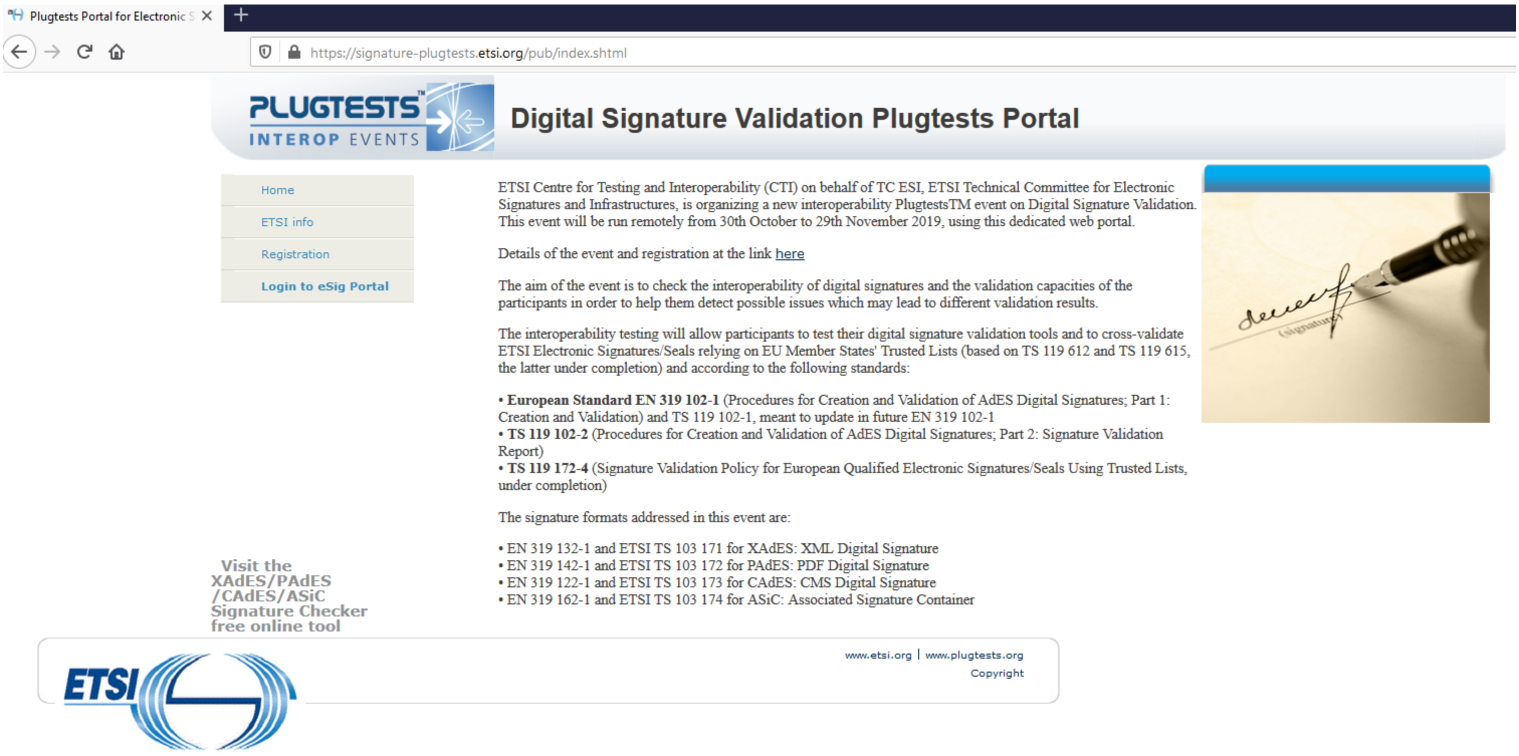
Section 6 provides the overall results.

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

2 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


Plugtests Portal for Electronic S
https://signature-plugtests.etsi.org/pub/index.shtml
PLUGTESTS INTEROP EVENTS
Home
ETSI info
Registration
Login to eSig Portal
Visit the XAdES/PAdES/CAdES/ASiC Signature Checker free online tool
ETSI
www.etsi.org | www.plugtests.org
Copyright

Digital Signature Validation Plugtests Portal

ETSI Centre for Testing and Interoperability (CTI) on behalf of TC ESI, ETSI Technical Committee for Electronic Signatures and Infrastructures, is organizing a new interoperability PlugtestsTM event on Digital Signature Validation. This event will be run remotely from 30th October to 29th November 2019, using this dedicated web portal.

Details of the event and registration at the link here

The aim of the event is to check the interoperability of digital signatures and the validation capacities of the participants in order to help them detect possible issues which may lead to different validation results.

The interoperability testing will allow 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, the latter under completion) and according to the following standards:

- **European Standard EN 319 102-1** (Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation) and TS 119 102-1, meant to update in future EN 319 102-1
- **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, under completion)

The signature formats addressed in this event are:

- EN 319 132-1 and ETSI TS 103 171 for XAdES: XML Digital Signature
- EN 319 142-1 and ETSI TS 103 172 for PAdES: PDF Digital Signature
- EN 319 122-1 and ETSI TS 103 173 for CAdES: CMS Digital Signature
- EN 319 162-1 and ETSI TS 103 174 for ASiC: Associated Signature Container

As mentioned above, this part remained as it was for previous events. It includes the following contents:

- The Plugtests page, providing some more details on the event itself, namely targeted specification, targeted audience, some general info on how to conduct such event, etc.

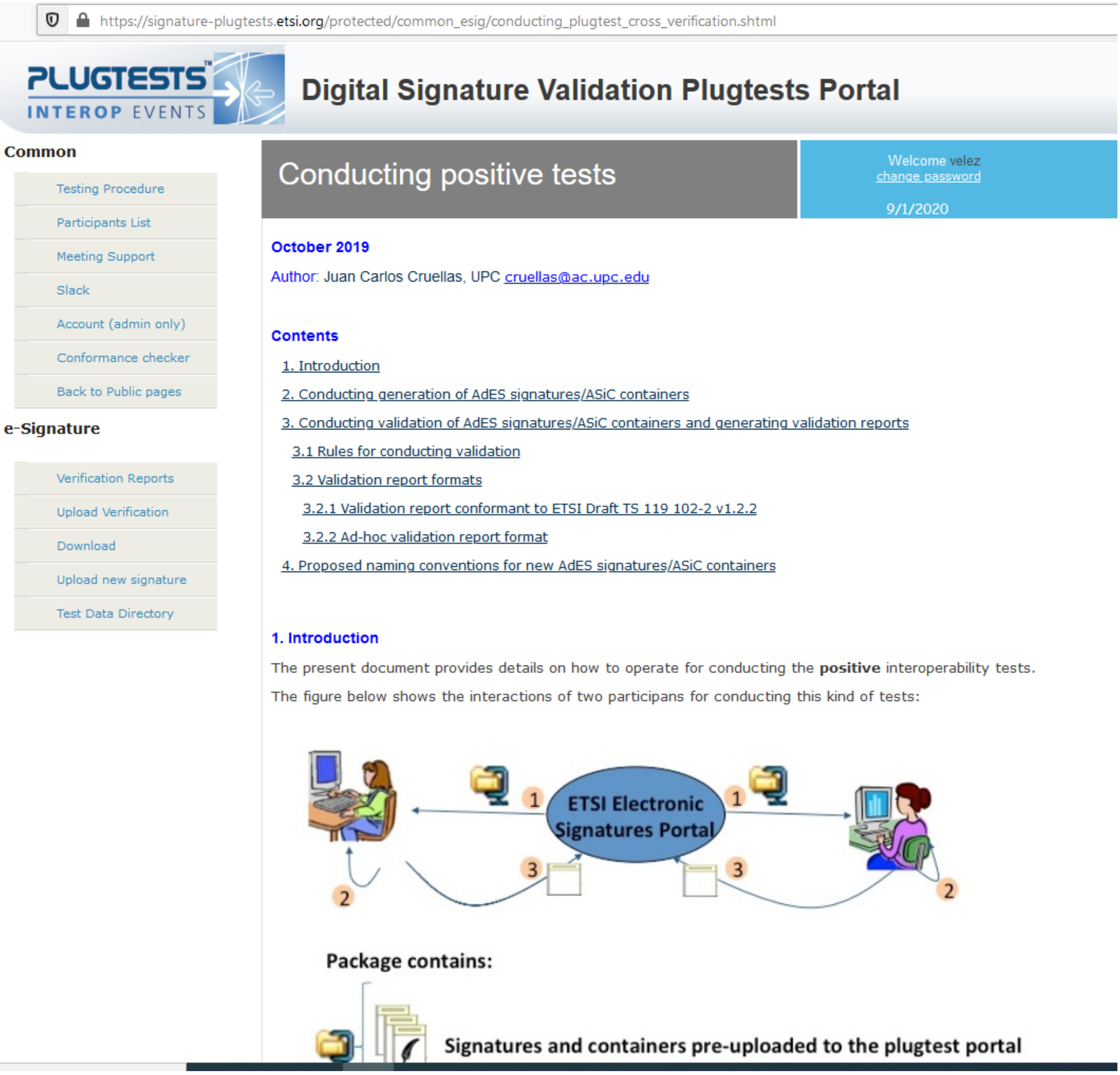
- The Mailing List page, providing some details on **public** mailing list support provided by the portal for facilitating exchange of information.
- The Registration page, providing details on the Plugtests registration process.
- The Presentation of the Plugtests team.
- The Presentation of some past events (XAdES, CAdES, PAdES, ASiC)
- The **Login to Plugtests Area** page gives access to the **protected area** of the portal.

2.2 Private part of the portal

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

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

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



https://signature-plugtests.etsi.org/protected/common_esig/conducting_plugtest_cross_verification.shtml

Digital Signature Validation Plugtests Portal

Conducting positive tests

Welcome velez
change password
9/1/2020

October 2019

Author: Juan Carlos Cruellas, UPC cruellas@ac.upc.edu

Contents

1. Introduction

The present document provides details on how to operate for conducting the **positive** interoperability tests.

The figure below shows the interactions of two participans for conducting this kind of tests:

1
ETSI Electronic Signatures Portal
1
2
3
3
2
Package contains:
Signatures and containers pre-uploaded to the plugtest portal

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 and or ASiC 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.

An access to Conformance testing tools was provided to the participants on a dedicated portal http://signatures-conformance-checker.etsi.org/

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

The tool performs conformance tests on :

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

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

- How to download material from the portal for starting conducting the Plugtests (**Downloading material page**). This material is usually a zip file enclosing a well-defined folder structure containing both signatures and verification reports on signatures.
- How to generate signatures and to upload them to the corresponding section of the portal so that the rest of participants at the interoperability tests may download and verify them (**Generating Signatures page**).
- How to verify other participants' signatures, report on verification results and uploading of these reports to the portal so that the portal keeps track of the current status of the Plugtests (**Verifying Signatures page**).

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
- Calendar for the meetings (Gotowebinar conference calls).
- URL for accessing a chat server accessible through a Web browser where the calls were minuted and participants could write their comments, questions and statements.
- The agenda for each meeting.
- Links to the minutes of each meeting.

2.2.1.4 Mailing list

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

- ESIG2019_UPLOAD@list.etsi.org : used by the Plugtests portal to automatically notify the participants after each upload of signatures or verification reports.
- ESIG2019_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://signature-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 participant to raise technical discussions and to share experience, information and best practise.

2.2.2 Contents of Digital Signature Validation Interop Specific areas of Private part

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

2.2.2.1 Upload “new” Signature page

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

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

Once uploaded, the portal re-built a new downloading package and made it available for all the participants at the Download page. Within this package, participants could find all the signatures and verification reports generated up to that moment in the Plugtests. It was a way to archive all the different uploads and keep a complete history of the interop testing of the event.

As already mentioned, the upload of a package had the immediate effect of updating the corresponding verification report matrix within the related area.

2.2.2.2 Upload Verification pages

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

The Upload Verification page provided mechanisms for uploading verification reports.

Once uploaded, the portal re-built a new downloading package and made it available for all the participants at the Download page. Within this package, participants could find all the signatures and verification reports generated up to that moment in the Plugtests. It was a way to archive all the different uploads and keep a complete history of the interop testing of the event.

As already mentioned, the upload of a package had the immediate effect of updating the verification reports within the related area.

2.2.2.3 Verification reports

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

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

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

2.2.2.4 Download pages

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

2.2.2.5 Test data directory pages

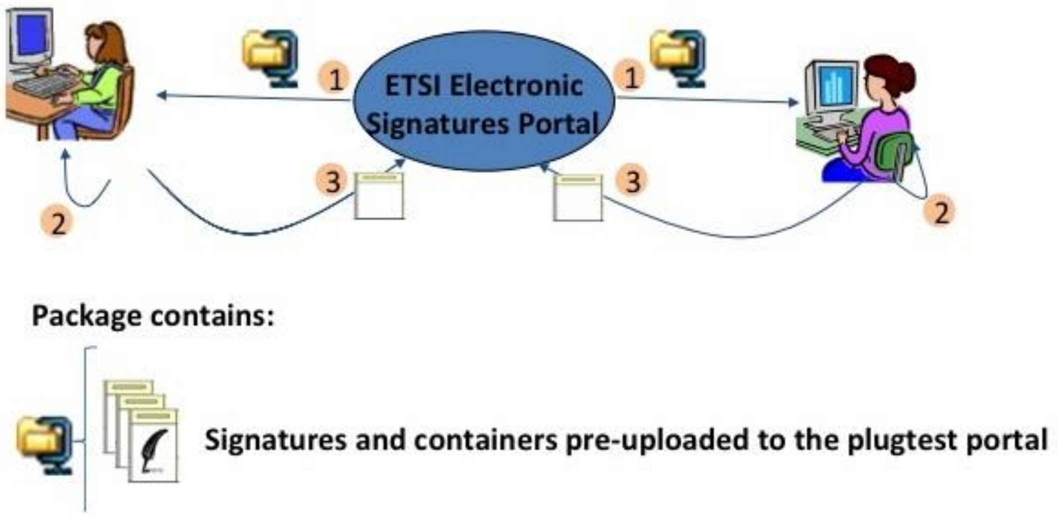
The page was used by the participants for browsing the folders structure where the portal stored the “pre-existing” and new signatures and the verification files generated by all the participants. This allowed a detailed inspection of the files uploaded to the portal at any moment during the event.

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

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.


1
1
ETSI Electronic Signatures Portal
2
3
3
2
Package contains:
Signatures and containers pre-uploaded to the plugtest portal

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 is 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 has generated a number of invalid signatures and/or ASiC containers including invalid signatures (the so-called "negative testcases") , where the invalidity would have different causes. Each participant could, at their own discretion, try to verify these signatures and/or ASiC containers, checking in this way that the corresponding tool actually detected that the involved signature/ASiC container was invalid.

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.

3.4 Signature Validation Reports

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

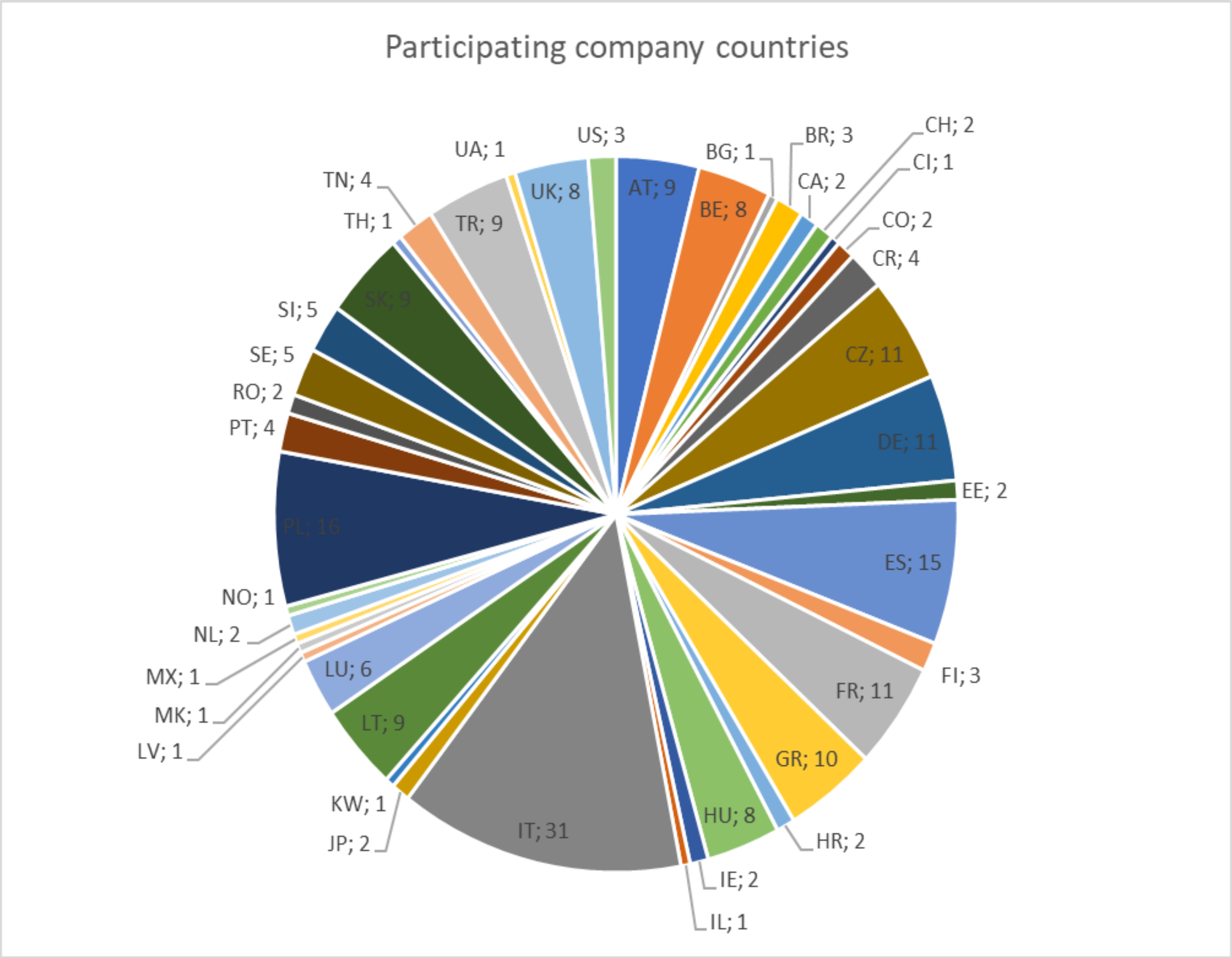
1. A validation report conformant to ETSI Draft TS 119 102-2 v1.2.2: Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report.

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 2019 Digital Signature Validation remote Plugtests event.

There were **173 different organizations** from **42 countries**, and **230 people** participating in the event.



Acronym	Company Name	Country
AT_GRA	Graz University of Technology	Austria
AT_GRE	Greev	
AT_RUN	Rundfunk und Telekom Regulierungs - GmbH	
AT_SIT	A-SIT Zentrum fur sichere Informationstechnologie Austria	
AT_TIA	Tiani Spirit GmbH	
BE_CON	Connective	Belgium
BE_DIO	Dioss Smart Solutions	
BE_ECO	e-Contract.be BVBA	
BE_EUR	external consultant at the EC	
BE_EUR	EC - European Commission	

Acronym	Company Name	Country
BE_HER	HERA - Health Research Action	
BE_POR	Porta Secura BVBA	
BG_INF	Information Services JSC	Bulgaria
BR_BRY	BRy Tecnologia	Brazil
BR_CER	Certisign	
BR_ESE	e-Sec Seguranca Digital S/A	
CA_ONE	OneSpan	Canada
CH_PDF	PDF Tools AG	Switzerland
CH_TES	Tessaris Integrated SecurityAG	
CI_CRY	CRYPTONEO	Chile
CO_ANT	Antares de la Costa	Colombia
CO_DIA	DIAN Tax & Customs Service	
CR_APO	Apololab	Costa Rica
CR_BCC	BCCR	
CR_FRA	individual	
CR_HER	Hermes Soluciones de Internet	
CZ_ALI	ALIS spol. s r.o.	Czech Republic
CZ_BLO	Blocknify	
CZ_CGI	CGI IT Czech Republic s.r.o.	
CZ_DIG	Dignita, s.r.o.	
CZ_GOR	Gordic spol. s r. o.	
CZ_MIT	M.I.T. Consulting, s.r.o.	
CZ_SEF	SEFIRA spol. s r.o.	
CZ_SIX	Software602 a.s.	
CZ_TEC	Techniserv IT, spol. s r.o.	
DE_CRY	Cryptomathic	Germany
DE_EXC	exceet Secure Solutions GmbH	
DE_GEM	gematik	
DE_GOV	Governikus	
DE_INT	intarsys AG	
DE_MEN	Mentana-Claimsoft GmbH	
DE_OPE	OpenLimit SignCubes GmbH	
DE_SCR	secrypt GmbH	
DE_SEC	SecCommerce GmbH	
DE_TEL	TeleTrusT IT Security Association Germany	
EE_CON	Consumer Protection and Technical Regulatory Authority	Estonia
EE_SKE	SK	
ES_AEM	AEMPS	Spain
ES_AGE	AGE	
ES_ANF	ANF Autoridad de Certificacion	
ES_AYE	Ayesa Advanced Technologies	
ES_BRA	Branddocs	
ES_GOV	Government, Spain	
ES_IND	Indra Sistemas S.A.	
ES_IVN	Ivnosys Solucions	

Acronym	Company Name	Country
ES_MFP	MPTFP	
ES_NAY	Nayade Group Solutions S.L.	
ES_UPC	UPC	
ES_VIA	VIAFIRMA	
FI_MET	Methics Oy	Finland
FI_VRK	Vaestorekisterikeskus	
FR_ATO	ATOS (Bull SAS)	France
FR_CEG	cegedim	
FR_COP	COPYRIGHT	
FR_CRY	Cryptolog International	
FR_LIB	Libriciel SCOP	
FR_LOL	Lol	
FR_ONE	OneSpan	
FR_REA	Real.not	
FR_SAG	SAGE SAS	
GR_ADA	Adacom SA	Greece
GR_BOG	Bank Of Greece	
GR_HAR	HARICA	
GR_HYP	Hypersystems	
GR_MDG	Ministry of Digital Governance	
GR_MOE	Ministry of Education - Greece	
GR_UAE	Uaegean	
HR_AKD	AKD d.o.o.	Croatia
HR_ASO	Asseco SEE d.o.o.	
HU_MIC	Microsec Ltd	Hungary
HU_MOB	MobilSign Ltd.	
HU_NIS	NISZ Zrt.	
HU_NOR	Noreg Ltd.	
HU_POL	Polysys Ltd	
IE_ADO	Adobe Systems Software Ireland Limited	Ireland
IE_DIG	DigiCert	
IL_COM	Comda	Israel
IT_ARI	ARIA S.p.A.	Italy
IT_ARU	ArubaPEC S.p.A.	
IT_B4I	Bit4id	
IT_CAC	Studio Caccia	
IT_CIN	CINECA	
IT_CSQ	CSQA Certificazioni srl	
IT_ELM	Elmi Srl	
IT_ENT	Entaksi Solutions Srl	
IT_ETS	IT_ETSI	
IT_INF	InfoCert S.p.A.	
IT_INS	Insiel	
IT_INT	IN.TE.S.A. S.P.A.	
IT_ITG	Intesi Group	

Acronym	Company Name	Country
IT_JSC	Information Services JSC	
IT_MAI	Mainline S.r.l.	
IT_NAM	InfoCert S.p.A.	
IT_NAM	Namirial S.p.A.	
IT_PAV	University of Pavia	
IT_SIX	Sixtema S.p.A.	
IT_SVI	Sviluppo Toscana S.p.A.	
IT_UNI	Unimatica S.p.A.	
JP_LAN	LangEdge	Japan
JP_OTI	Otip Office	
KW_DUC	Diyar United Company	Kuwait
LT_BSS	UAB BSS IT	Lithuania
LT_DOK	Dokobit	
LT_EXP	EXPLAND UAB	
LT_GAR	Garantir	
LT_INS	Insoft	
LT_ISD	ISDC	
LT_MIT	UAB MitSoft	
LT_MIT	MIT-SOFT, UAB	
LU_DOK	Dokumenta S.A.	Luxembourg
LU_EWI	eWitness S.A.	
LU_LUX	Luxtrust SA	
LU_NOW	Nowina Solutions	
LV_EUS	EUSO	Latvia
MK_KIB	KIBS AD Skopje	North Macedonia
MX_SEG	SeguriData Privada, SA de CV	Mexico
NL_GEM	Gemalto N.V.	Netherlands
NL_ZYN	Zynyo	
NO_SIG	Signicat AS	Norway
PL_ADS	Asseco Data Systems	Poland
PL_ENI	Enigma SOI	
PL_IZB	Izba Administracji Skarbowej w	
PL_KIR	KIR SA	
PL_MDA	Ministry of Digital Affairs	
PL_PWP	PWPW SA	
PL_RCL	Rzadowe Centrum Legislacji	
PL_TAX	Tax Administration Chamber	
PT_DEV	Devise Futures, Lda.	Portugal
PT_DIG	DigitalSign	
PT_GNS	GNS	
PT_MUL	Multicert S.A	
RO_CER	certSIGN	Romania
SE_AAA	3xA Security AB	Sweden
SE_COM	Comfact AB	
SE_NEX	Nexusgroup	

Acronym	Company Name	Country
SE_PHE	PhenixID	
SE_SOV	Sovos	
SI_OSI	OSI d.o.o.	Slovenia
SI_SET	SETCCE d.o.o.	
SI_VER	Bureau Veritas	
SK_APO	Archimetes	Slovakia
SK_ARD	Ardaco, a.s.	
SK_DIS	Disig, a.s.	
SK_DIT	DITEC, a.s.	
SK_MIN	Ministry of Transport and Construction (SK)	
SK_NAS	NASES	
TH_ETD	ETDA	Thailand
TN_NGT	NG Technologies	Tunisia
TN_TTN	TTN	
TR_ARK	ArkSigner Software & Hardware	Turkey
TR_ILE	Ilerian Software Tech Ltd.	
TR_SOF	Software Solutions	
TR_TUB	Tubitak Uekae	
TR_TUR	Turksat	
TR_YIL	Yildiz Technical University	
UA_NEV	IT PRO,TOV (UAB Nevda)	Ukraine
UK_ALL	Allied Bits Ltd	United Kingdom
UK_ASC	Ascertia	
UK_ITO	ITTOPPRO	
UK_QUA	Quali-Sign Ltd.	
US_AXI	AxiomSL	United States of America
US_SAF	SAFE Identity	
US_ZEV	Safe Identity (Zeva International)	

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 173 organizations gathering 230 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 :

- ESIG2019_UPLOAD@list.etsi.org : used by the Plugtests portal to automatically notify the participants after each upload of signatures or verification reports
- ESIG2019_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 30th Oct to 29th Nov 2019.

In order to allow the participants to read all the documentation and prepare for the testing, ETSI opened the portal on 28 Oct before the official beginning of the interoperability event. Kick off meeting on 29 Oct

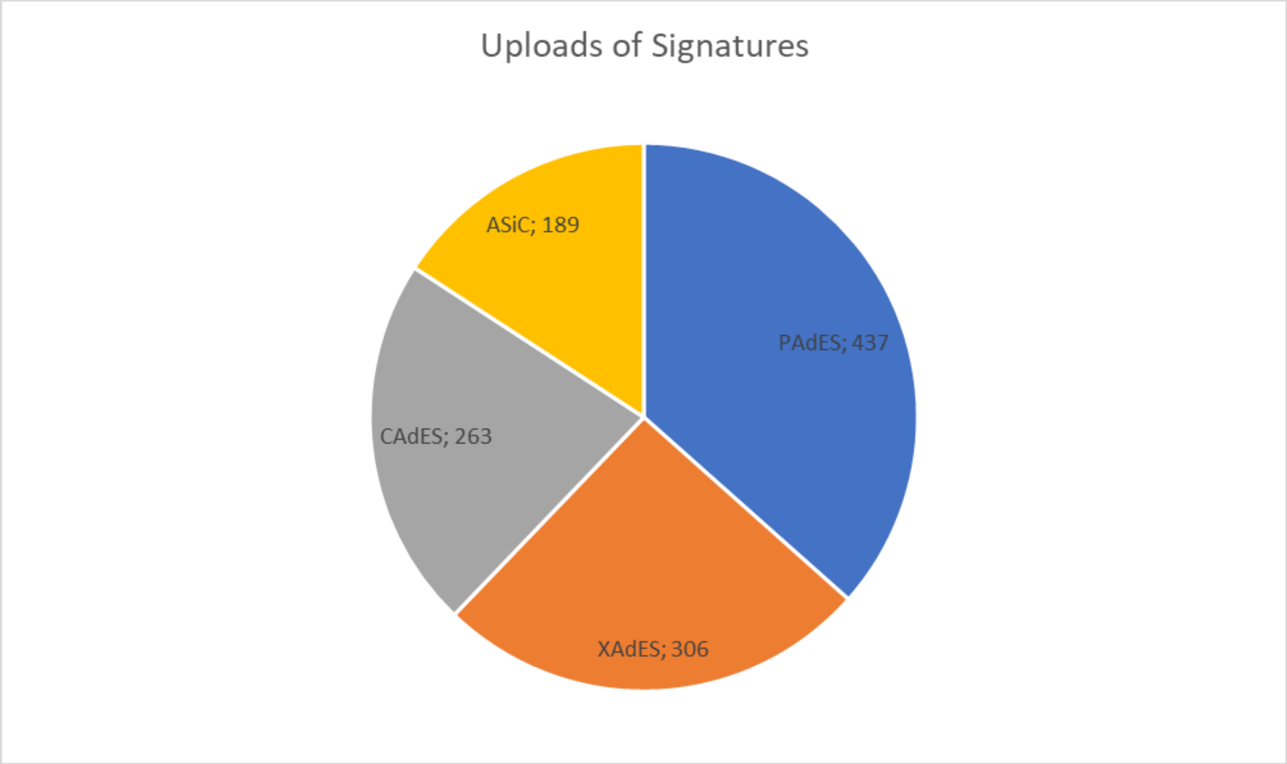
Moreover, for this event, 173 companies were registered. As each company had to verify the signatures of other participants, it was requested to extent the event until the 20 Dec 2019. Indeed, at the testing activity was still dense, ETSI close the Plugtests portal on 6 Jan 2020.

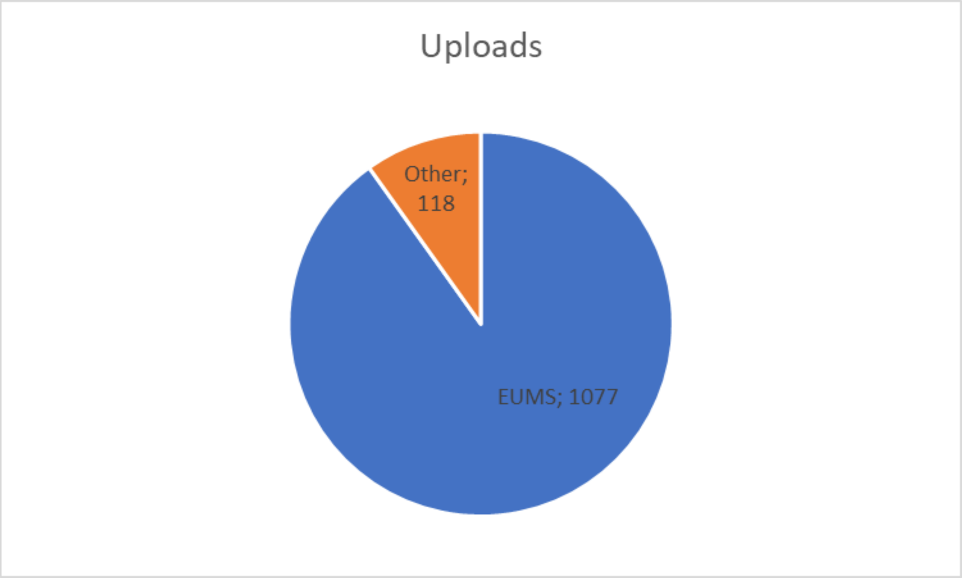
6 Overall results

The present clause lists some of the issues raised during the Digital Signature Validation Plugtests event in Nov and Dec 2019. This report will be provided to ETSI TC ESI which is the technical working group in charge of the standardization of the ETSI Electronic Signatures, for possible action/input for further changes in the standards.

6.1 Signature uploads

Format	Nb of signatures	Nb from EUMS	Nb from other
PAdES	437	394	43
XAdES	306	281	25
CAdES	263	232	31
ASiC	189	170	19
Total	1195	1077	118





6.2 Signatures validation report uploads

In total, **50641** Verification reports have been produced and uploaded to the portal.

Verified Format	Verifications	Verification of EUMS signatures	Verification of non-EUMS signatures
PAdES	20985	18818	2167
XAdES	14219	13078	1141
CAdES	11715	10291	1424
ASiC	3722	3494	228
Total	50641	45681	4960

7 Digital Signature Validation related Issues

The present clause lists some of the issues raised during the Digital Signature Validation Plugtests event. This technical report is intended be provided to ETSI TC ESI which is the technical working group in charge of the standardization of the ETSI Electronic Signatures, for possible action/input for further changes in standards.

7.1 Management of the deprecated signer-attributes attribute in CADESCC

At the Plugtests one participant reported an issue about the CAdES conformance checker with a CAdES B-B signature against the requirements defined in ETSI EN 319 122-1 V1.1.1. A new version of the CAdESCC that solved this issue was already available but not yet deployed, but when checking the contents of the CAdES B-B signature provided by the participant there were some discussions between the Plugtests organizers about the management of the signer-attributes attribute that is deprecated in ETSI EN 319 122-1 V1.1.1, clause 6 the ETSI EN 319 122-1 only includes the signer-attributes-v2 attribute.

It was agreed to instruct the CAdESCC to raise a warning when it hits a signer-attributes attribute instructing the user to ascertain whether the signature is a legacy one or a brand new because a signature including the signer-attributes attribute is not compliant to ETSI EN 319 122-1 V1.1.1. A new version of the CAdESCC that solved the above issues was deployed the 13th of November 2019.

7.2 Computation of unsignedAttrValuesHashIndex field of ats-hash-index-v3 attribute

At the Plugtests some participants asked for a clarification about the computation of the unsignedAttrValuesHashIndex field of the ats-hash-index-v3 attribute. Above all the sentence "*Each one shall contain the hash value of the octets resulting from concatenating the Attribute.attrType field and one of the instances of AttributeValue within the Attribute.attrValues within the unsignedAttrs field*" in clause 5.5.2 section Syntax is not considered so clear.

If there will be a review of ETSI EN 319 122-1 it would be appropriate adding a detailed example about how to compute this field in the case of a real CAdES B-LT signature being augmented to a CAdES B-LTA signature.

7.3 Spoofing PDF Signatures

At the Plugtests the participants discussed about the study "How To Spoof PDF Signatures" reported at the link https://pdf-insecurity.org/download/paper.pdf that presents 3 novel attack classes on PDF signatures: Universal Signature Forgery (USF), Incremental Saving Attack (ISA), and Signature Wrapping Attack (SWA).

Some participants stated that they had implemented additional restrictions within their PDF signature validation logic in order to deal with the 3 attacks mentioned above. Other participants stated that some of these additional restrictions were too strict.

The case of incremental savings in PDF was further discussed in the Plugtests mailing list. By means of incremental savings one can add variations to (signed) PDF documents. When digital signatures are applied, a revision can be aligned to changes so it's possible to roll back to a previous signed revision. From the cryptographic point of view an incremental change does not break an existing signature, but from the content perspective it can be a very disruptive operation.

PDF 32000-1:2008 and ISO 32000-2:2017 allow the use of DocMDP and FieldMDP for "Modification Detection and Prevention" in the signature reference dictionary so that the user can be informed that something has changed in previous signed contents.

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

7.4 Management of the IssuerSerialV2 element in XADESCC and ASICCC

At the Plugtests one participant reported an issue about the XAdES conformance checker with XAdES baseline signatures not including the IssuerSerialV2 element in the SigningCertificateV2 property and/or ASiC with XAdES baseline signatures not including the IssuerSerialV2 element in the SigningCertificateV2 property containers. The XAdES conformance checker raised an error if IssuerSerialV2 element was missing in SigningCertificateV2 property. A new version of the XAdESCC that solved this issue was deployed the 13th of November 2019. A new version of the ASICCC that solved this issue was deployed the 20th of November 2019

7.5 signatureAlgorithm in place of digestAlgorithm in CMS signature

At the Plugtests one participant reported an issue about a CMS signature (in PDF) that specified a signatureAlgorithm in the field SignedData.digestAlgorithms. At least one validation application was however validating such signature (ignoring this nonsense). It was confirmed that IETF RFC5652 requirements state to use a collection of message digest algorithm identifiers and not a signature algorithm identifier in the field SignedData.digestAlgorithms. Therefore. any validation application that however accepts the signature algorithm identifier instead of the message digest algorithm identifier is surely lenient.

7.6 “Sie” “Qualifications Extension” information interpretation

At the Plugtests there were some discussions concerning the interpretation of Sie Qualifications Extension. Some participants stated that QCQSCDStatusAsInCert Qualifications extension is necessary, otherwise it is not possible to rely on the QC statement in the certificate. Some other participants stated that the machine processable statement declaring that the private key resides in a QSCD is sufficient in order to consider the private key residing in a QSCD, the QCQSCDStatusAsInCert Qualifications extension is not needed. It was clarified that Annex I/III item (j) of the eIDAS regulation unambiguously requires that qualified certificates with private keys residing in a QSCD include a machine processable statement declaring that the private key resides in a QSCD.

Some participants had interpreted that overruling of missing indications in a qualified certificate by means of Sie:Q QCStatement and by Sie:Q QCWithQSCD/QCQSCDManagedOnBehalf for qualified certificates issued after eIDAS regulation entry into force seemed to be clearly in conflict with requirements (a) and (j) of Annex I/III of the eIDAS regulation. It was clarified that the Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists allows also under the Regulation regime to override the content in the qualified certificates and this is correctly considered in ETSI TS 119 615 draft contents.

7.7 Management of the rsassa-pss parameters in CADESCC

At the Plugtests one participant reported an issue about the CAdES conformance checker with a CAdES B-B signature created with rsassa-pss signatureAlgorithm with parameters. At the moment CADESCC does not process the rsassa-pss parameters that, consequently, are not checked.

7.8 Management of validation data after certificates expiration

At the Plugtests there were some discussions concerning the correct management of the validation data when validating expired certificates. When validating signatures with time some applications are not able to use fresh validation data. Such applications implement the validation time sliding process described in clause 5.6.2.2.4 of ETSI TS 119 102-1 but the condition that the issuance date of the revocation status information is before control-time is never satisfied for OCSP answers produced at validation time.

7.9 Usage of time assertions in ASiC-S containers

At the Plugtests one participant asked about the status of ASiC-S with time assertions that was formerly (in the previous ASiC TS) one of the baseline formats and that is useful in order to extend the timestamp effective period.

Now this container is part of the ASiC extended profiles (in EN 319 162-2) so it is still a valid international reference, the request was to include this in ETSI Plugtests.

7.10 Possible typo in clause 5.2.5.4 of ETSI TS 119 102-1

At the Plugtests one participant pointed out that the item 3) “If the issuance time of the revocation status information …” in clause 5.2.5.4 of ETSI TS 119 102-1 v1.2.1 quite probably is not referred to NOTE 1 but should be the item 2) of the processing.

7.11 Possible issues in ETSI TS 119 615

At the Plugtests one participant pointed out some issues concerning the procedures for QC and QSCD determination and authentication of trusted lists in draft TS 119 615 v0.0.9.

- The procedure specified in clause 4.4 (EU qualified certificate determination) makes a case distinction based on whether the date is before or after the entry into force of eIDAS (PRO-4.4.4-07). It also specifies that the procedure must be repeated with the certificate’s NotBefore date (PRO-4.4.4-34), and that the procedure must fail if the results differ (PRO-4.4.4-36). However, if the NotBefore date is before eIDAS while the assumed signing time (i.e. the Date-time argument of the first run) is after, the results are likely to differ just because of that. Given that qualified certificates issued prior to eIDAS shall remain compliant under the Regulation until their expiration/revocation (if the issuing CA confirms its qualified status by the 1st of July 2017), the NotBefore check would have to be modified in the above described situation otherwise the procedure would fail in such case (comparing table 1 and table 5 in ETSI 119 615 should clarify this issue).
- In PRO 4.3.4 03 step (b), which determines the applicable (historic) service instance, there is no check that the service history is correctly ordered (as required by ETSI TS 119 612 clause 5.5.10). If the history happens to

be incorrectly ordered, the procedure still requires the first matching entry to be selected and used. There should either be a check here causing failure in case of an incorrect order, or the service instances should be first sorted before the search.

- Clause 4.4 (EU qualified certificate determination) requires that the resulting QC-Results must be the same at the NotBefore time as at the assumed signing time, however clause 4.5 (QSCD determination) does not perform an analogous consistency check, but merely determines the QSCD status at the assumed signing time. This seems inconsistent.
- ETSI TS 119 615 requires that a freshly retrieved trusted list shall be used even if its NextUpdate date has passed, and that this case should merely produce a warning (PRO-4.1.4-13 and PRO-4.2.4-10). This is in direct conflict with ETSI TS 119 612 (Trusted Lists) clause 5.3.15, which requires that any "*TL with a Next update occurring in the past shall be discarded as expired as a measure to reduce the risk of a substitution by an attacker with an old TL*". For the reason given in the quote, it would seem preferable to comply with the behaviour mandated by TS 119 612.
- Both OJ act 2019/C 276/01 section 2.2 and ETSI TS 119 615 clause 4.1.1 stipulate that the LOTL location (URL) may change by mere indication in the LOTL itself, that is, without the new location having to be published in the OJ. On the other hand, ETSI TS 119 615 also specifies that the original LOTL location as last published in the OJ shall be configured (GPR-4.0-02, parameter LOTL-Loc), and shall be used to obtain (or have obtained) a LOTL (PRO-4.1.4-01), and shall match the location indicated in the LOTL itself whenever the contents of the LOTL has changed (PRO-4.1.4-05).
    - Taken together, this effectively means that the LOTL authentication procedure will permanently fail as soon as the location indicated in the LOTL doesn't correspond anymore to the location last published in the OJ. The procedure therefore currently seems to be ill-defined for changes to the LOTL location without a corresponding publication in the OJ.
    - Secondly, even in case of a corresponding publication in the OJ, there is a timing problem between when the OJ publication and the corresponding LOTL publication, because of the need to (manually) reconfigure the authentication procedure using the location published in the OJ (again: GPR-4.0-02, parameter LOTL-Loc). It is not clear how this is supposed to work in the context of maintaining a continuous validation service.
    - Thirdly, when there is no locally cached copy of the previous LOTL — for example in the case of initial setup, of data loss or data corruption, of just having a gap in the LOTL retrieval history, or of any other kind of bootstrapping scenario — the following points are unclear:
        - If the LOTL location can change without that change being published in the OJ, how does one determine the currently valid LOTL location in a secure and authoritative manner, given that the location cannot be determined from the OJ anymore?
        - Even if the current LOTL location is published in the OJ, how does one securely obtain and authenticate the relevant OJ publication, given that no paper versions of the OJ are published anymore, without having to rely on non-eIDAS PKI infrastructures to validate the respective web servers?
- In order to validate the current LOTL via the pivot LOTL chain, the current LOTL location, the last published set of authorized LOTL signer certificates, and the corresponding OJ publication URL have to be configured (GPR-4.0-02). Whenever a new set of authorized LOTL signer certificates is published in the OJ, the pivot LOTL chain is reset to an empty list (as recently happened with LOTL #248). It is however unclear how the authentication procedure is supposed to work in case of such a transition. There are two problems:
    - Step PRO 4.1.4 04 requires that the configured OJ URL (parameter OJEU-Loc) must match the one specified by the current LOTL. As a consequence, validation will fail as soon as the OJ URL is updated by a new LOTL. That also means that the indication of the OJ URL in the LOTL cannot be used as a notification mechanism for a new OJ publication for the purpose of updating the configuration, at least not without causing a disruption of the validation service from the time of notification until the configuration has been updated.
    - When a new set of authorized LOTL signer certificates is published in the OJ, it normally becomes effective at the date of publication and immediately replaces the previously published set, thereby resetting the pivot chain. However, as was the case for the recent transition initiated by OJ act 2019/C 276/01, the current LOTL at that date still contained the previous pivot chain and therefore required the old, now officially void set of LOTL signer certificates for validation. To be precise, the sequence of events was as follows:
        - 2019-08-13: LOTL #247 published with old pivot chain and old (2016) OJ URL
        - 2019-08-16: OJ issue 2019/C 276 published with new set of signer certificates
        - 2019-09-04: LOTL #248 published with new (empty) pivot chain and new OJ URL

      That is, between August 16 and September 4 2019, following the procedure specified by ETSI TS 119 615 clause 4.1, the old set of LOTL signer certificates would have to be configured, although it wasn't valid anymore according to the OJ publication, and hence that configuration would be in conflict with

GPR-4.0-02. The procedure only works if the information indicated by the LOTL (i.e. the OJ issue linked by it) is taken as authoritative, ignoring any more recent published OJ issue (again: in conflict with GPR-4.0-02, which requires the configured OJEU-Loc parameter to reference the latest OJ publication). Apart from the conflicts with GPR-4.0-02, doing so would be problematic for two reasons: (1) The contents of the LOTL cannot be taken as authoritative before the authentication procedure hasn't successfully completed, and (2) the contents of a LOTL cannot conceivably override the authority of a later OJ publication. Summing up, the transition procedure from one pivot chain to the next, as well as the chronological and authoritative relation between the respective LOTL updates and OJ publication, is completely unclear, and the procedure currently specified by ETSI TS 119 615 clause 4.1, if followed as written, is guaranteed to cause significant downtime in a validation service when such a transition occurs.

7.12 Possible issues in ETSI TS 119 172-4

At the Plugtests one participant pointed out some issues concerning some requirements in draft TS 119 712-4.

- REQ-4.2-01bis states "The present document gives the minimum requirements for QES as in the Regulation: a) The validation service may use additional inputs or additional requirements. b) If additional inputs are used, they shall be clearly indicated."
  - Where/to whom/in which context shall the additional inputs be clearly indicated? Does this refer to a validation report? It doesn't seem to refer to the applicability rules checking report (clause 4.5).
  - Are the "additional requirements" from item a) deliberately not included in item b) (only the "additional inputs")?
- REQ 4.2 02 c) iv) mandates that revocation freshness constraints shall not be used. It is unclear what is the aim of this requirement; not performing revocation freshness checks constitutes a major risk of (a) forged signatures not being detected, and (b) signatures being augmented with validation data that in the future might be judged to have insufficient revocation freshness.
- REQ 4.2 02 c) ii) mandates application of the RevocationInfoOnExpiredCerts validation constraint, which is defined as follows in ETSI TS 119 172-1 V1.1.1 (2015 07): "this constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound". It is unclear (a) how that constraint should be technically checked, and (b) which lower bound should apply. (The constraint can be trivially fulfilled by choosing a lower bound of zero).

7.13 URNs indicating the quality of signatures

At the Plugtests one participant asked where people can find the URNs to be used as stated in ETSI TS 119 102-2, clause 4.3.10.1, in the signature quality element, in order to indicate the quality of the signature. It was asked if they will be defined in future versions of ETSI TS 119 172-4.

7.14 Remarks concerning ETSI TS 119 102-2

At the Plugtests one participant provided the following remarks concerning ETSI TS 119 102-2 requirements.

- Different Plugtests participants calculated different SignatureIdentifier digest (using the same SHA256 digest algorithm). It means, that participants understand standards differently. The clause 4.1.1.4.2 in ETSI TS 119 102-2, needs to be clarified. The text specifying details on how to build references to signatures to be included in the validation report shall be added to the new version of ETSI TS 119 102-2.
- According to draft version at most one SignersDocument element may occur in SignatureValidationReport. One SignersDocument defines only one signed data object. It is not correct, if XAdES (or ASiC-E) signature signed several data objects (files).

Note: ETSI TS 119 102-2 does not mention ASiC as one of the possible AdES digital signatures to which it applies however ASIC baseline containers specified in EN 319 162-1 include a single AdES, therefore the eSig Plugtests team suggests an editorial modification to ETSI TS 119 102-2 to mention that it can support signature validation reports also for ASiC baseline containers.

- Mistype in Draft section A.8.4: "The SigPolicyId child element shall contain the URI present within the XAdES:Identifier child element of XAdES:SigPolicyId child element of XAdES:SignaturePolicyId child element of XAdES:CommitmentTypeIndication qualifying property of XAdES." **SignaturePolicyIdentifier** shall be used, not *CommitmentTypeIndication*.
- Mistype in Draft section A.14.2: "For every CRL or OCSP response referenced within reported attribute that is present in a validation object in the report, the CompleteRevocationRefs shall contain an AttributeObject child

referencing the validation object containing the corresponding certificate". The ending shall be "...containing the corresponding **CRL or OCSP response**", not *certificate*.

- Why VOReferenceType element attribute VOReference type is xs:IDREFS (which allows multiple references) and not xs:IDREF (which allows one reference)? If it is needed to refer several objects, report XSD schema allows to add multiple VOReferenceType elements, and, therefore, there is no need to have a list of lists of references.
- Mistype in Draft A.25.2: "The time-stamp on the references on certificates and revocation information shall be reported on in the RenewedDigests element." RenewedDigest and references (on certificates and revocation information) are not related objects.
- Validation report stores Validation objects separated from the signatures. One validation report may contain several signature validation report elements (for example this is applicable for ASiC containing several signatures). As it is written in the test it is done on purpose - to allow to have only one validation object in the reports and multiple references from different signature validation report elements. It looks nice, but Validation objects contains data which is related with one particular signature:
    - ValidationObjectType child POE depends on the signature. One signature may create one POE, and another signature may create another POE for the same validation object (certificate, CRL, ...). Which POE should be included in the ValidationObjectType?
    - ValidationObjectType child ValidationReport also depends on the signature. From one signature validation we may get one validation report for the validation object (OCSP, CRL), and from another signature validation we may get different validation report for the same validation object. Which validation report should be included?
- According to Section 4.3.4.4, ValidationStatusType element may contain multiple AssociatedValidationReportData elements. One AssociatedValidationReportData element may contain single TrustAnchor, CertificateChain, RevocationStatusInformation, CryptoInformation elements, since these elements are single for one signature validation. Element RevocationValidationObject may be multiple. AdditionalValidationReportData is single, but it may contain multiple ReportData elements. Why we need to have multiple AssociatedValidationReportData in the ValidationStatusType element?
- Section 4.3.4.4, ValidationReportDataType contains only one Revocation Status Information element. It is not clear from 4.3.12.6 if element shall be used for revoked signing certificate only, or it shall be used for the revoked CA certificates as well. If not only for the signing certificate, why it is a single element?
- It seems that if certificate is not revoked, Revocation Status Information element shall not be used at all, since its child element RevocationTime is required. In such case, there is no possibility to report particular revocation data, which was used to prove that some particular certificate was not revoked.
- Is there any suitable place in the report to present human-readable error messages describing the result of the signature validation? Subindications are very good things for advanced users, but not for the real systems. If some real system uses validation service, which produces validation report according to this standard, then it is not enough to get a report from the signature validation service, since there are no error messages. It means, that system should create error messages only based on the subindications. Therefore, these messages will be too abstract for the normal user to understand the real problem. Of course, validation service, may return 2 things (report according standard and error messages separately), but it is not a thing we want to have.
- One validation report may contain several signature validation reports. It looks nice from the ASiC usage perspective (validate one ASiC with multiple signatures and produce one report). What about Container validation - is there any possibility to report container validation result (errors, conformance and so on)?
- For the Signature Reference element XSD schema is given, but no explanations provided. Some of the child elements are not self-described (for example, XAdESSignaturePtr). Therefore, it is left totally non-understandable what the data it should contain, and why.

7.15 Misinterpretation of XAdES specifications

At the Plugtests some misinterpretations of XAdES specifications have been highlighted (EncapsulatedTimeStamp elements that contain the whole TimeStampResp instead of the TimeStampToken, EncapsulatedOCSPValue elements that contain only BasicOCSPResponse instead of the whole OCSPResponse, XAdES signatures containing DataObjectFormat element not being a child of SignedDataObjectProperties).

In case of the GenericTimeStamp type, the text should be reworded in the next revision of ETSI EN 319 132-1, in the following way.

The GenericTimeStampType type shall:
• allow encapsulating IETF RFC 3161 [7] updated by IETF RFC 5816 [16] electronic time-stamp tokens, which shall be instances of TimeStampToken type specified in clause 2.4.2 of IETF RFC 3161 [7], as well as XML electronic time-stamps.

Regarding the (Basic)OCSPResponse, readers are reminded that clause 5.4.2 of ETSI EN 319 132-1 states the following:

Each EncapsulatedOCSPValue child of OCSPValues element shall contain the base-64 encoding of a DER encoded OCSPResponse defined in IETF RFC 6960 [6].

7.16 AdES signatures including zero policy hash

At the Plugtests there were some discussions concerning the zero policy hash included in AdES signatures. It was clarified, by the editors of CAdES and XAdES specifications that a zero-hash value shall be an octet string of any length (including zero length) whose octets have the value zero. Signature creation applications that generate a zero-hash value should generate it with a length consistent with the hash algorithm specified by the hashAlgorithm field of the sigPolicyHash field. It was confirmed that the hash over the string "0" (ASCII digit zero) is definitively wrong and is not a correct "zero hash" neither now nor in the future.

7.17 signaturePolicyImplied field not allowed in CAdES

At the Plugtests the rationale of disallowing the usage of the signaturePolicyImplied field in CAdES was requested. It was not possible to provide a clear and sure answer to such request.

7.18 Validation of signatures using SHA-1 digest algorithm

At the Plugtests there were some discussions concerning different validation outcomes of signatures and/or OCSP responses using SHA-1 digest algorithm. It was concluded that the choice of accepting signatures and/or OCSP responses using SHA-1 digest algorithm depends on the validation policy used by the SVA. The AdES specifications, indeed, state that the algorithms and key lengths used to generate and augment digital signatures should be as specified in ETSI TS 119 312. Being used the term "should" instead of "shall" there is no restriction for SHA-1 usage.

7.19 Trust anchors in the trusted lists

At the Plugtests it was requested how to manage signing certificates whose trust chain does not end with a root (that's self-signed) certificate. It was confirmed that, when validating a qualified certificate (i.e. QC for electronic signatures, QC for electronic seals, QC for website authentication), the Trust Anchor is the Service digital identity (Sdi) of a trust service entry. It means that, when validating a certificate, there is no need to chain up to the Root CA of a qualified certificate but only to the related CA/QC issuer entry within the Trusted List.

7.20 Clarifications to be added in ETSI TS 119 102-1 v1.2.1

At the Plugtests there were some discussions concerning the differences between ETSI EN 319 102-1 v1.1.1 and ETSI TS 119 102-1 v1.2.1. It was pointed out that the result of 5.6.2.2.4 Validation Time Sliding algorithm (both in ETSI EN 319 102-1 and in ETSI TS 119 102-1 versions) is not consistent. It was agreed that there is a problem in the current algorithm if we have two revocation status information applicable on a certificate. Point b) should be changed. It should also be clarified in the standard that there is always a POE at current time for fresh materials because this is not very clear. It was requested to improve/complete the current conditions defining "acceptable" the revocation data for VTS. For example, if we have a corrupted revocation data with a failed basic signature or we have revocation data issued by an untrusted certificate chain.

7.21 Building a signing certificate path using the AIA extension

At the Plugtests it was noted that some SVA doesn't build a certificate path using the AIA extension and this causes QES validation issues in the context of EU Trusted Lists when the issuing CA (or 'SubCA') is not listed in the Trusted List, but instead the RootCA is; and the signature itself doesn't include the signing certificate path. To be checked if it may be worth a clarification in ETSI TS 119 102-1 about this issue.

7.22 Archival version of the signature can contain non-usable revocation information

At the Plugtests it was noted that currently the standard allows two strategies when validating a signature containing non-usable revocation information, either getting new revocation information or not. This can lead to different results. To be decided if it may be worth recommending one of these strategies in ETSI TS 119 102-1 in order to not have different results.

7.23 Should normative reference to RFC 5753 be included in AdES specifications?

At the Plugtests one participant reported two XAdES signatures including signatureValue fields that contain raw data and therefore not satisfying what stated in IETF RFC 5753. Indeed it shall be noted that IETF RFC 5753 deals with the use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS) therefore what stated in IETF RFC 5753 cannot be applied to XAdES signatures.

The signatureValue fields are specified in CMS, XMLDSIG and PDF signatures, thus the AdES specifications do not need to state anything about this.

Therefore, to XAdES signatures what stated in clause 6.4.3 ECDSA of XML Signature Syntax and Processing Version 1.1 shall be applied.

7.24 Differences between ETSI EN 319 102-1 and ETSI TS 119 102-1

For the participants it was not always clear which algorithm to follow. Some of them followed by default the EN version, and were surprised to find new features (like the validation of signatures with expired certificates) in the TS version

History

Document history		
V1.0	06 Jan 2020	Final version
V1.1	30 Jan 2020	Fixing Typo in participant list
V1.2	31 Jan 2020	Fixing Typo in participant list