Technical Report of the JAdES Remote Plugtests™ Event (Nov-Dec 2021)

Reference

Keywords
Electronic Signature,

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

Jan 2022

Abstract

This document is the technical report of the 2021 Remote Plugtests Event on JAdES (JSON Advanced Electronic Signature) ETSI TS 119 182-1, organized by ETSI Centre of Testing and Interoperability (CTI) conducted using the ETSI portal supporting remote interoperability Plugtests.

For Non Disclosure Agreement reason, the 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: https://www.etsi.org/about/our-expertise

.

Contents

1 Introduction

ETSI Centre for Testing and Interoperability (CTI) organized a remote Plugtests interoperability event on **JAdES (JSON Advanced Electronic Signature)**. This event was run remotely from **8 Nov to 17 Dec 2021.**

It was the first Plugtests event on the JAdES standard. The proposed testing has allowed participants to test software implementing the JAdES Specification ETSI TS 119 182-1 V1.1.1 (Part 1: Building blocks and JAdES baseline signatures). The participation was free of charge, and this remote event aims to conduct conformance and interoperability testing on JAdES Signatures.

The JAdES digital signature specification is based on JSON Web Signature. It contains the features already defined in the related ETSI standards for AdES (advanced electronic signature/seal) applied to other data formats, including XML, PDF and binary.

This new standard supports secure communications fulfilling the requirements of the European Union eIDAS Regulation (No 910/2014) for advanced electronic signatures and seals and regulatory requirements for services such as open banking.

The present document is organized as indicated below.

Clause 2 provides details on the scope of the testing and how the material of the portal is organized and the services it provides to the participants of the Plugtests Events.

Clause 3 lists the participants to the 2021 JAdES Remote Plugtests Event.

Clause 4 provides some conclusions of the Plugtests.

Clause 5 provides overall results.

Clause 6 provides details of JAdES issues raised at the Plugtests.

Section 7 provides details on the Interoperability testcases provided for the Plugtests event.

2 JAdES Plugtests

2.1 Scope

The interoperability and conformance proposed testing allowed participants to test their JAdES Implementation, according to the recent ETSI TS 119 182-1 V1.1.1 (Part 1: Building blocks and JAdES baseline signatures).

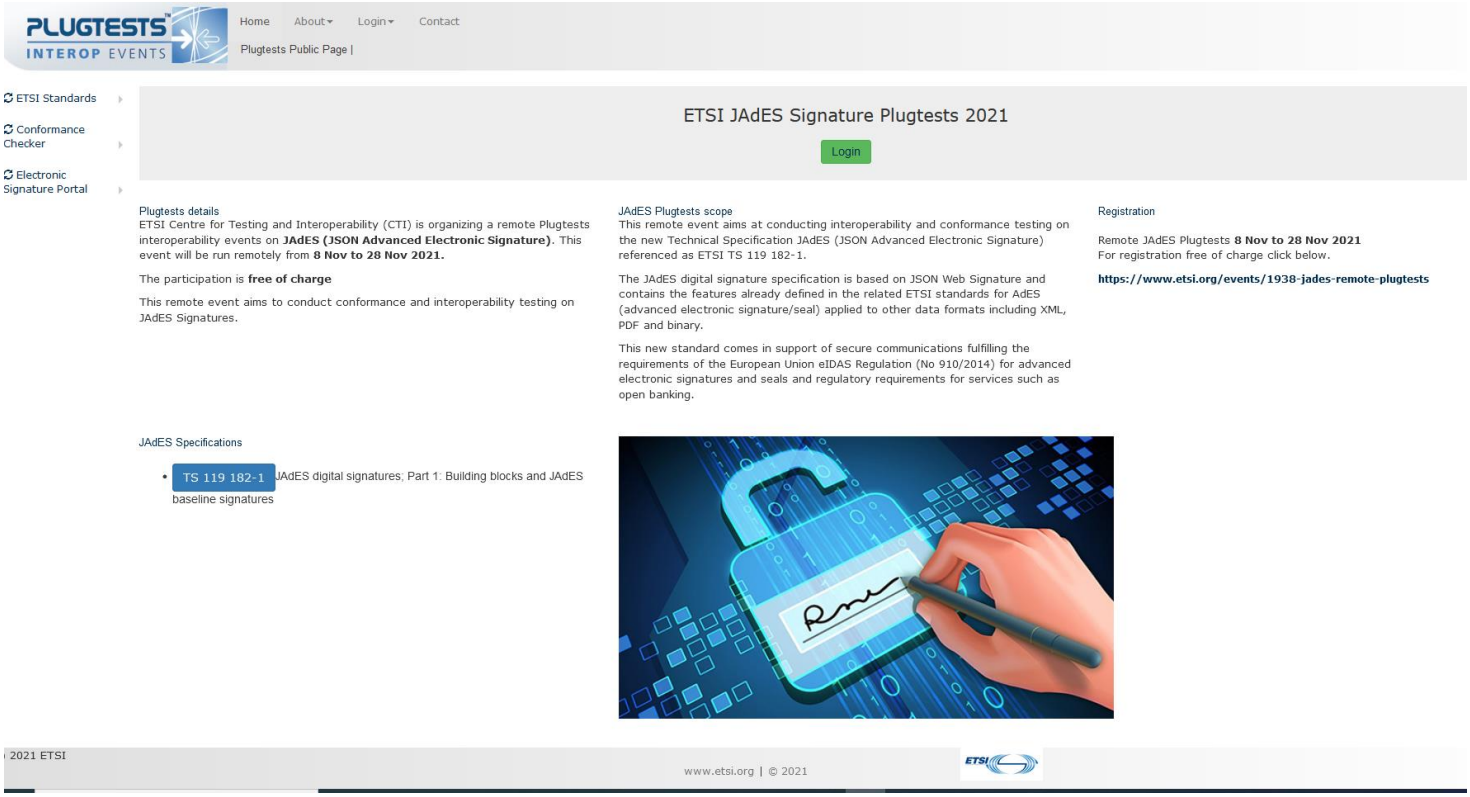
This Plugtests event allowed to conduct 4 types of tests:

- Generation and cross-verification of JAdES signatures
- Augmentation and verification of augmented JAdES signatures.
- Only verification tests.
- Conformance testing.

A dedicated Plugtests portal has been set up to host and run the testing. The url is https://signature-plugtests.etsi.org. it was only accessible to registered participants.

2.2 Plugtests portal

2.2.1 Public part of the portal



It includes the following contents:

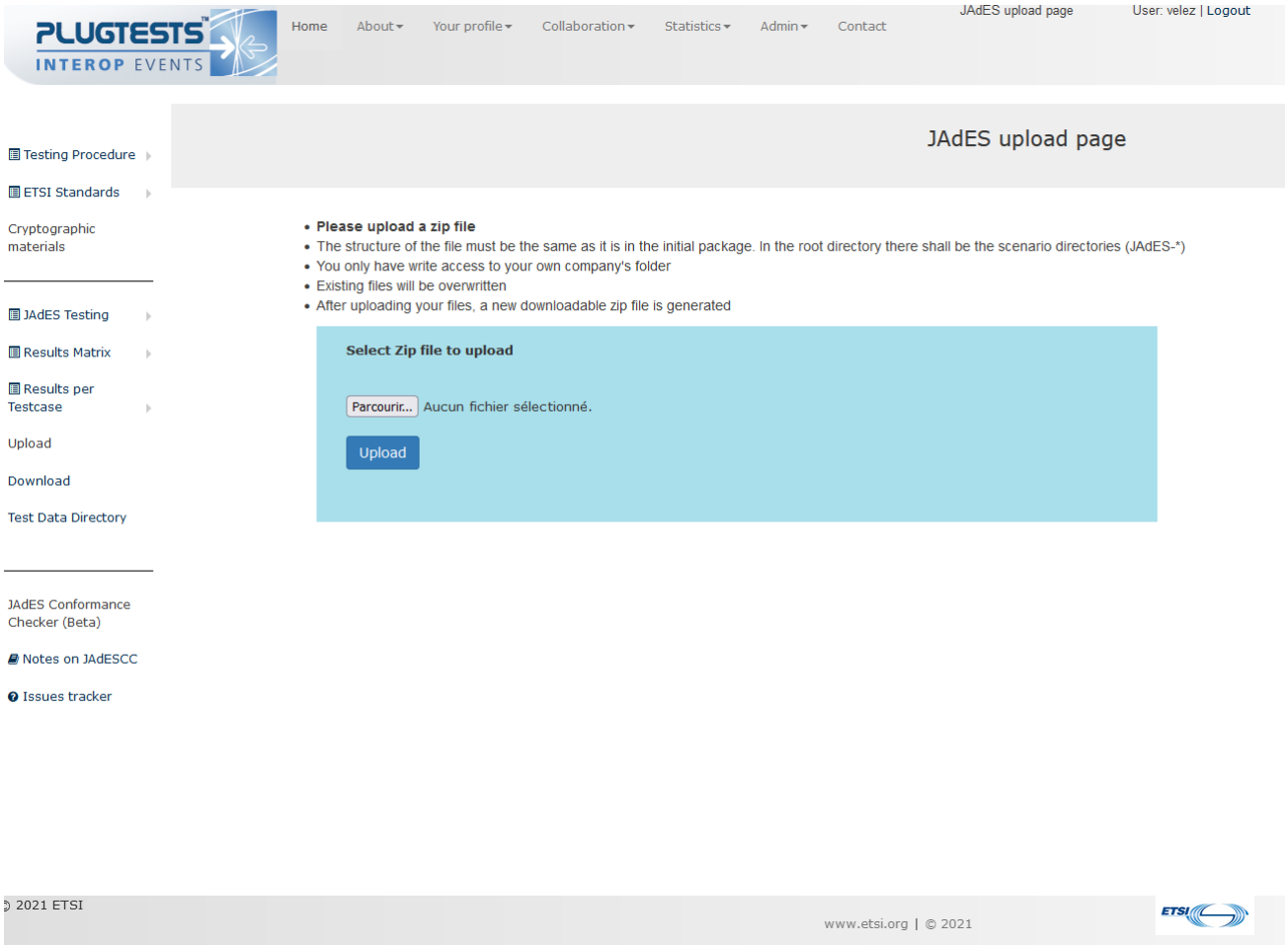
- The JAdES Plugtests page, providing some more details on the event itself, namely targeted specification, targeted audience, some general info on how to conduct such event, etc.
- The Registration page, providing details on the Plugtests registration process.
- The **Login to Plugtests Area** page gives access to the **protected area** of the portal.

2.2.2 Private part of the portal

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

- **Common area**. This area contains a number of pages that provide generic information to the participants, which is relevant to participants of interoperability tests.
- **JAdES Interop specific area**. This area contains a number of pages that support the interoperability tests on JAdES signatures.
- **JAdES Conformance Checker area**. This area contains an online tool for checking the structure of a JAdES signature vs the specification.

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



2.3 Conducting Plugtests

This Plugtests event allows to conduct 4 types of tests:

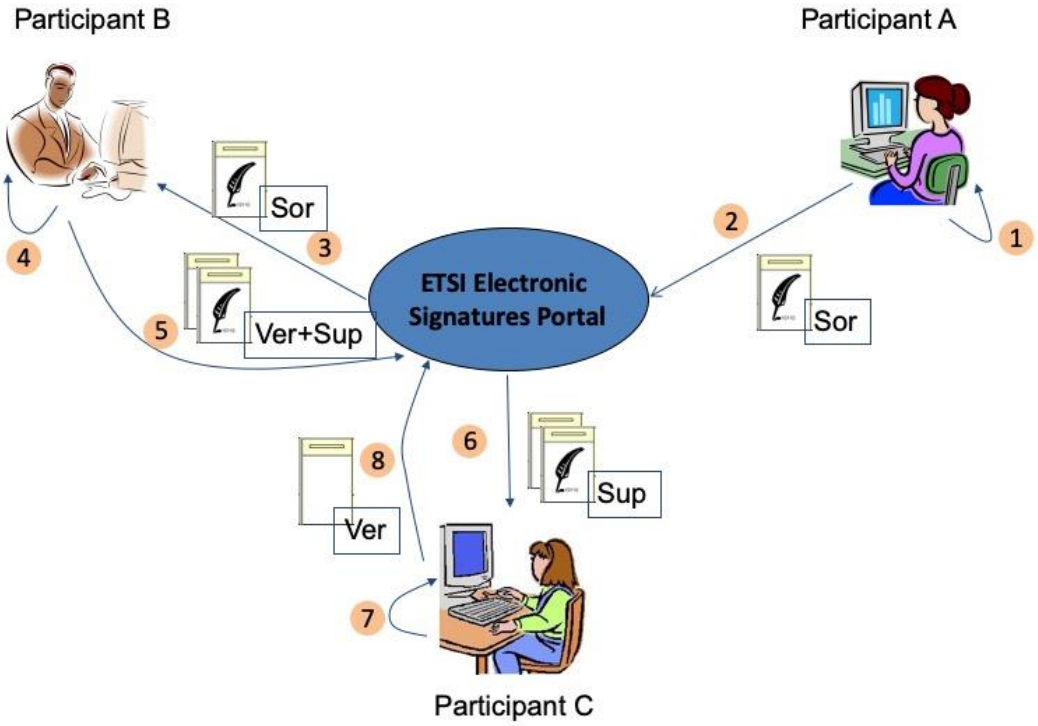
1. **Generation and cross-verification of JAdES signatures.** Each participant is invited to generate (generation phase) a certain set of JAdES baseline signatures compliant with ETSI TS 119 182-1 v1.1.1 : "Electronic Signatures and Infrastructures (ESI);JAdES digital signatures;Part 1: Building blocks and JAdES baseline signatures".

   The rest of participants are invited afterwards to validate these JAdES signatures (cross-verification phase) and upload their results. Upon the upload of these results, the ETSI Plugtests Portal shall automatically generate and update a set of interoperability matrixes showing the validation results that all the participants may access.

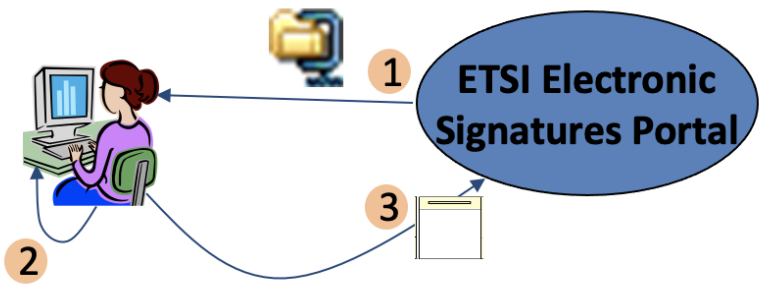
2. **Augmentation and verification of augmented JAdES signatures.**
Each participant is invited to augment (augmenting phase) a certain set of JAdES baseline signatures previously generated by other participants, according to the rules that are defined in ETSI TS 119 182-1 for augmenting JAdES signatures from one level to another.

   The rest of participants are invited afterwards to validate these augmented JAdES signatures (verification of augmented signatures phase) and upload their results. As with cross-verification tests, upon the upload of these results, the ETSI Plugtests© Portal shall automatically generate and update a set of interoperability matrixes showing the validation results that all the participants may access.

   This type of tests may involve two (when the initial generation of the signature and the validation of the augmented signature are performed by the same participant, while the augmentation of the initial signature is performed by a second participant) or three participants (when each step -generation, augmentation, and validation of the augmented signature- is performed by a different participant).

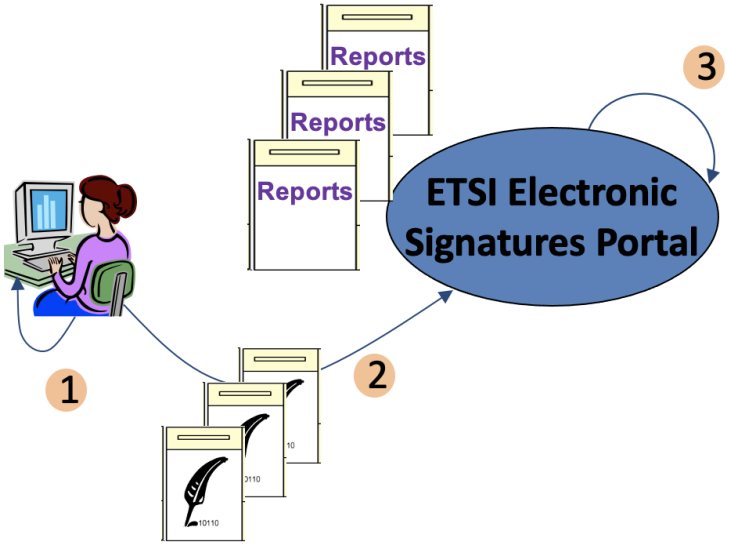


3. **Only verification tests.**
Each participant is invited to validate JAdES baseline signatures that will have been created by the Plugtests© organization team. All these JAdES signatures shall have some wrong component that should make the validation to fail.



4. **Conformance testing.**

In this type of tests, participants will have to upload JAdES signatures to the portal Conformance checker. This online tool runs a set of conformance checks against the JAdES Specification ETSI TS 119 182-1 v1.1.1



2.4 Event details

2.4.1 Meeting Support page

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

- Introduction presentation. This presentation was made available before the start of the Plugtests, and it 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).
- The agenda for each meeting.
- Links to the minutes of each meeting.

2.4.2 Mailing list

2 Mailing lists were set up :

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

2.4.3 Slack workspace

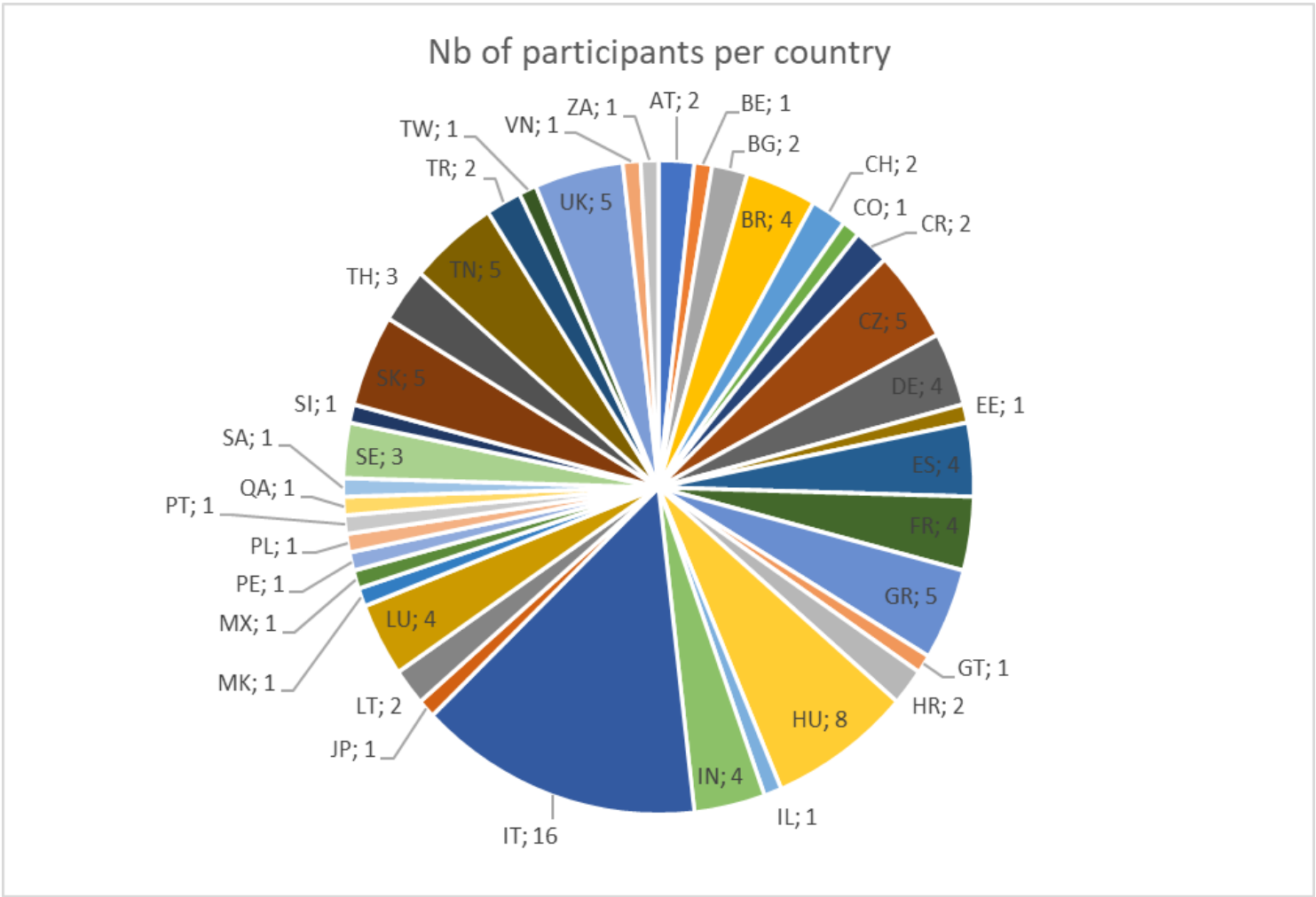
In order to allow better exchanges between participants, a slack workspace was set up by the ETSI CTI team at jades-plugtests.slack.com

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 participants to raise technical discussions and to share experience, information, and best practise.

3 Participants list

The table below shows the details of all the organizations and persons that have registered to the JAdES Plugtests.

There have been **87 different organizations** and 110 persons participating in the event.



Company	Country name
3xA Security AB	SWEDEN
ADACOM SA	GREECE
Asseco Data Systems	POLAND
Allied Bits Ltd	UNITED KINGDOM
ANCE	TUNISIA
Archimetes	SLOVAKIA
ARIA S.p.A.	ITALY

Company	Country name
ArubaPEC S.p.A	ITALY
Ascertia	UNITED KINGDOM
Asseco SEE d.o.o.	CROATIA
Autentique	BRAZIL
Bit4id	ITALY
Bureau Veritas	TAIWAN
Certisign	BRAZIL
Cybersign	GUATEMALA
Devise Futures	PORTUGAL
DIAN, Impuestos y Aduanas de C	COLOMBIA
DIGG	SWEDEN
DITEC, a.s.	SLOVAKIA
Comitee DUES	ITALY
Duru Bilişim	TURKEY
Ecocerved SCARL	ITALY
eDesign	BULGARIA
Elbit Systems C4I and Cyber Ltd	ISRAEL
Emdha Trust Service Provider	SAUDI ARABIA
eMudhra	INDIA
Entaksi Solutions SpA	ITALY
European Public Prosecutor's O	LUXEMBOURG
e-Sec Data Security	BRAZIL
ETDA	THAILAND
ETSI	FRANCE
Individual	COSTA RICA
GetAccept	SWEDEN
Gordic spol. s r. o.	CZECH REPUBLIC
Governikus GmbH & Co. KG	GERMANY
Graz University of Technology	AUSTRIA
Greev	AUSTRIA
GUnet	GREECE
Hermes Soluciones de Internet	COSTA RICA
I.CA (První certifikační autorita, a.s.)	CZECH REPUBLIC
IDnow GmbH	GERMANY
Impression Signatures	SOUTH AFRICA
InfoCert S.p.A.	ITALY
Ministry of IT	INDIA
INTESI GROUP S.p.A.	ITALY
IPZS	ITALY
Information Services JSC.	BULGARIA
Jemmic	LUXEMBOURG
KIBS AD Skopje	NORTH MACEDONIA
Kryptus Information Security SA	SWITZERLAND
Lacuna Software	BRAZIL
Ministry of Digital Governance	GREECE
Microsec Ltd	HUNGARY
MitSoft	LITHUANIA
Monet+	CZECH REPUBLIC
MoTC	QATAR

Company	Country name
MVM CEEnergy Zrt.	HUNGARY
National Archives CZ	CZECH REPUBLIC
NASES	SLOVAKIA
Ministry of Transport and Construction	SLOVAKIA
Netis	SLOVENIA
NG Technologies	TUNISIA
NISZ Zrt.	HUNGARY
Noreg Ltd.	HUNGARY
Nowina Solutions	LUXEMBOURG
Otip Office	JAPAN
POLYSYS Ltd.	HUNGARY
ProBaltic Consulting JSC	LITHUANIA
Quali-Sign LTD	UNITED KINGDOM
Reliance Jio	INDIA
Software602 a.s.	CZECH REPUBLIC
SecCommerce Informations. GmbH	GERMANY
Secrypt GmbH	GERMANY
SeguriData Privada, SA de CV	MEXICO
SK ID Solutions AS	ESTONIA
TDRA UAE	INDIA
Tessaris Integrated Security A	SWITZERLAND
Thammanichanon	THAILAND
Constitutional court of Spain	SPAIN
TTN	TUNISIA
Tubitak Uekae	TURKEY
Trust Warp	BELGIUM
UPC	SPAIN
Viafirma	SPAIN
Vizibit	CROATIA
Ministry of Information and Co	VIETNAM
ZyTrust SA	PERU

4 Plugtests conclusions

4.1 Remote vs. Face to Face

Due to Covid crisis, the remote event was the best option to run such testing activity. It would have been impossible to organise it in a face-to-face event, in any case experience shows that for this type of event remote participation is the most convenient option for the participants.

4.2 Communication supporting technologies

The utilization of Web conference (GotoWebinar) has been very appreciated by participants. It 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 testing by making a real case demo.

3 conference calls have been organized during the event, one kick off conf call to present the testing and 2 other ones regularly to discuss the issues and answer to any technical questions.

The chat of the slack workspace has also been very important for the participants to write their questions or request and also it has been used as meeting minutes.

4.3 Event duration

The event was initially planned to run until 28 Nov, but it was extended to 17 Dec on request from the participants. The reason was that due to the important number of tests proposed, some participants needed more time to complete the testing. The portal was finally left open and accessible to participants until **3rd January 2022**.

5 Overall results

5.1 Signature uploads

Here is a table of the overall number of **GENERATED** JAdES signatures per test case sets

Tests	B-B	B-T	B-LT	B-LTA	B-Aug	Total
Total	132	22	6	7	78	245

5.2 Verification reports uploads

Here is a table of the overall number of **VERIFIIED** JAdES signatures per test case sets

Tests	B-B	B-T	B-LT	B-LTA	B-Aug	Total
Total	809	203	64	70	289	1435

Here is a table of the overall number of **VERIFIIED** JAdES signatures per **Negative** test case sets

Tests	B-BN	B-TN	B-LTN	B-LTAN	Total
Total	80	40	20	10	150

5.3 Conformance Checker uploads

Number of JAdES signatures uploaded on the Conformance checker online tool = 343 signatures

6 JAdES Plugtests related issues

6.0 Introduction

The present clause lists some of the issues raised during the JAdES Plugtests event in November and December 2021. This technical report will be provided to ETSI TC ESI which is the technical working group in charge of the standardization of the ETSI Electronic Signatures, for possible action/input for further changes in standards.

6.1 "crit" header parameter contents

At the plugtests one participant reported an issue about which parameters may be indicated in the "crit" header parameter. According to RFC 7515, clause “4.1.11. "crit" (Critical) Header Parameter”, the "crit" (critical) Header Parameter indicates that extensions to RFC 7515 and/or RFC 7518 specification are being used that MUST be understood and processed. Its value is an array listing the Header Parameter names present in the JOSE Header that use those extensions.

JOSE Header, according to RFC 7515, is a protected header in case of a Compact Serialization or a union of protected and unprotected members in case of a JSON Serialization format, therefore one may conclude that “crit” header may contain both protected and unprotected header extensions, used within a JWS signature, but not defined by RFC 7515 and/or RFC 7518.

ETSI TS 119 182-1 has the following wording that is considered ambiguous, “The elements of the crit JSON array shall be the names of all the signed header parameters that are present in the JAdES signatures and specified in clause 5.2.”

This sentence states that only the signed header parameters which are defined by TS 119 182-1 shall be present within the "crit" header parameter. This does not allow inclusion of unsigned headers, but also restricts further addition of new custom parameters within the "crit" header parameter.

One of the concerns is the "b64" header parameter (defined in RFC 7797), referenced in TS 119 182-1 in clause “5.1.10 The b64 header parameter”, which is not part of RFC 7515, RFC 7518, and TS 119 182-1 clause 5.2. When using the "b64" header parameter, the value "b64", shall be included in the "crit" header parameter as stated in clause 6 of RFC 7797. Therefore, the current wording in clause 4.1.11 of ETSI TS 119 182-1 contradicts the RFC 7797, and should be changed.

The editor of TS 119 182-1 proposed to

- add in clause “5.1.10 The b64 header parameter” the sentence “As RFC 7797 [14] states in its clause 6, if the b64 header parameter is present, then its name shall be included in the list of values of the "crit" header parameter.”
- add in clause “5.1.9 The crit (critical) header parameter"
    - the sentence “The crit JSON array shall contain the names of all the signed header parameters that are present in the JAdES signature and specified in clause 5.2.”
    - a note immediately below the above sentence stating that this requirement does not restrict the set of names for the content of the crit header parameter, see the requirement on b64 header parameter in clause 5.1.10 of the present document.

6.2 "crit" header parameter cardinality

At the Plugtests one participant reported an issue about the RFC 7515 schema provided within TS 119 182-1. Indeed the "crit" header parameter shall not be empty, therefore the definition should change from the current one

```
"crit": {
    "type": "array",
    "items": {
```

```
        "type": "string"
    }
}
```

to the following one

```
"crit": {
    "type": "array",
    "items": {
        "type": "string"
    },
    "minItems": 1
}
```

6.3 Line breaks included in JWS Compact Serialization format signatures

At the plugtests the participants discussed if JWS Compact Serialization format signatures containing line break character(s) should be considered valid or not.

Some participants stated that such signatures are not URL-safe because line breaks within a JWS signature can break the HTTP header section therefore should be rejected. Other participants stated that depending on the use case, if a signature validation implementation is able to successfully parse the signature, it should not reject the signature itself.

It was agreed that a SCA (Signature Creation Application) shall not create JWS/JAdES signatures in Compact Serialization format containing line breaks, therefore a SVA (Signature Validation Application) may reject such signatures.

6.4 Encoding of the digVal member of the sigPId header parameter

At the plugtests one participant reported that TS 119 182-1 does not define the encoding of the digVal member of the sigPId header, assuming that it is expected that the digVal member is base64url-encoded for keeping the same encoding in the digest values of the other components of JAdES signatures. Such encoding should be made clear in the next version of TS 119 182-1.

6.5 URI references percent-encoding

At the plugtests it was requested a clarification concerning if a URI reference shall be percent-encoded, especially when referencing external documents, as within the "pars" member of the "sigD" header.

RFC 3986, referenced in clause 5.2.8.3 of TS 119 182-1, recommends but does not mandate percent-encoding of URIs that can be classified as locators.

6.6 Computation of the message imprint of Archive TimeStamps

At the plugtests there were some discussions concerning the computation of the message imprint of Archive TimeStamps when the "etsiU" header incorporates clear objects, particularly when dealing with the rVals JSON object and/or crlVals and ocspVals arrays. It was stated that it is not clear the order in which the values ocspVals and crlVals and/or the fields of the rVals JSON object shall be considered for the message imprint computation.

It was clarified that when computing a message imprint for a timestamp in the case of a signature with a clear json "etsiU" header, the elements shall be canonicalized before message imprint computation. Indeed the canonicalization should take care of the JSON parameters ordering even if there is not any accepted JSON canonicalization algorithm yet. TS 119 182-1 offers the possibility of using any new algorithm, whenever it will be defined, without any problem.

6.7 "srAts" header certifiedAttrs member

At the plugtests it was asked if the certifiedAttrs member may contain a public key certificate. It was clarified that this component may only contain attribute certificates.

6.8 Multiple signers in JAdES signatures including the "sigD" parameter

At the plugtests it was asked if there is the possibility of having multiple signers in JAdES signatures that include the "sigD" parameter. As stated in TS 119 182-1, "The sigD header parameter may appear in JAdES signatures whose JWS Payload is detached. A JAdES signature shall have at most one sigD header parameter". In clause 3.1 the term JAdES signature is defined as JSON Web Signature, as specified in IETF RFC 7515, or other parts of this multi-part deliverable. In clause 2 of RFC 7515 the term JSON Web Signature (JWS) is defined as a data structure representing a digitally signed or MACed message, therefore the understanding is that the "sigD" parameter may not be used with multiple signers. A clarification of this possibility in TS 119 182-1 would be appropriate.

6.9 JAdES signature term definition and usage

At the plugtests it was underlined that the term "JAdES Signature" or "JWS" seems being used with two different meanings throughout the TS 119 182-1 document. As the whole data structure representing a digitally signed message or as the single signature included in the whole data structure. It was requested to clarify the terminology JAdES signature and consequently to use such terminology consistently throughout the document.

6.10 Note 1 in clause 5.2.2.2

The note 1 defined in clause “5.2.2.2 The x5t#o (X509 certificate digest) header parameter” of TS 119 182-1 does not seem to be relevant to the clause topic.

6.11 addressCountry member in the sigPl header parameter

In the Syntax clause of 5.2.4 clause in TS 119 182-1 the following sentence shall be amended “This addressCountry member shall contain may contain either the name of the country or its two-letter ISO 3166-1 alpha-2 country code” in order to clarify if it is a mandated or an allowed statement.

6.12 "sigD" schema

If the "pars" member shall be present, as stated in clause 5.2.8.1 of TS 119 182-1, shouldn’t the "pars" member be required in the "sigD" schema definition?

It is not very clear if the "ctys" member shall always be present or not. In clause 5.2.8.1 of TS 119 182-1 it is stated “There shall be as many elements within the ctys array as elements within the array pars” therefore it seems that it shall always be present, but, in such case, shouldn’t the "ctys" member be required in the "sigD" schema definition?

6.13 Requirement for "sigPSt" parameter

The item b) in clause 6.3 of TS 119 182-1 states that the "sigPSt" header parameter may be incorporated into the JAdES signature only if the sigPId is also incorporated and it contains the hashAV member with the digest value of the signature policy document. Otherwise the sigPSt shall not be incorporated into the JAdES signature. Therefore in table 1 the condition about the presence of the "sigPSt" header parameter should be “conditioned presence” instead of “may be present”. Moreover the term “hashAV” mentioned in item b) should be amended.

6.14 Service "signing a reference of the signing certificate"

In Note 3 in clause 6.3 of TS 119 182-1 the "sigX5ts" header parameter should be mentioned too.

6.15 Undefined JAdES component tags

In column JAdES tag in table C.1 the two terms "sdF" and "idoTst" are mentioned without there being their definitions in TS 119 182-1.

7 JAdES Plugtests Interoperability Testing

7.1 Positive test cases

7.1.0 Introduction

The Form can be

- `B-B` - JAdES-B-B signatures
- `B-T` - JAdES-B-T signatures
- `B-LT` - JAdES-B-LT signatures
- `B-LTA` - JAdES-B-LTA signatures
- `UpdArb` - Upgrade and Arbitration of JAdES signatures

In the 'positive test' participants will do following:

1. A partiticipating implementation generates JAdES signatures following the proposed test cases.. Generated JAdES signatures shall be valid. That's why we say 'positive test' for these tests.
2. A participant will upload JAdES signatures to the portal.
3. A participant will download JAdES signatures generated by other participants.
4. Verify JAdES signatures from other participants.
5. Upload verification results as XML files.
6. See test result matrix in the portal

7.1.1 JAdES B-B level

- J-B-B-1

contains the following Properties:

++alg
++x5t#S256
++x5c
++crit
++sigT

Description:
This case tests a simple JAdES-B-B signature using JWS Compact Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, crit, sigT. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-2

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT

Description:
This case tests a simple JAdES-B-B signature using complete JWS JSON Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-3

contains the following Properties:

++alg
++x5t#S256
++x5c
++crit
++sigT

Description:
This case tests a simple JAdES-B-B signature using flattened JWS JSON Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, crit, sigT. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-4

contains the following Properties:

++alg
++x5t#o
++x5c
++cty
++crit
++sigT

Description:
This case tests a JAdES-B-B signature using JWS Compact Serialization. Implementation shall add at least the header parameters alg, x5t#o, x5c, cty, crit, sigT. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-5

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT

Description:

This case tests a JAdES-B-B signature using JWS Compact Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-6

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT
++srCms
++sigPl
++adoTst

Description:
This case tests a JAdES-B-B signature using JWS Compact Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT, srCms, sigPl, adoTst. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-7

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT
++srAts
+++claimed
++sigPl
++adoTst

Description:
This case tests a simple JAdES-B-B signature using JWS Compact Serialization with a srAts header parameter encapsulating a signer's claimed attribute. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT, srCms, sigPl, adoTst. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-8

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT
++srAts
+++certified
++++x509AttrCert
++sigPl

++adoTst

Description:
This case tests a JAdES-B-B signature using JWS Compact Serialization with a srAts header parameter encapsulating a signer's certified attribute. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT, srCms. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-9

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT

Description:
This case tests a JAdES-B-B signature with multiple independent signatures using complete JWS JSON Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT for each signature. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-10

contains the following Properties:

++alg
++x5t#S256
++x5c
++crit
++b64
++sigT
++sigD
+++mId
+++pars

Description:
This test case tests a JAdES-B-B detached signature, using the sigD header parameter with the HttpHeaders mechanism,.and using JWS Compact Serialization. The HTTP headers listed in the page https://signature-plugtests.etsi.org/pub/JAdES/toBeSignedHttp.txt shall be used as items of the pars array. The b64 header parameter shall be set to "false" The mId member shall be set to the URL "http://uri.etsi.org/19182/HttpHeaders". Implementation shall add at least the header parameters alg, x5t#S256, x5c, crit, b64, sigT, sigD. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-11

contains the following Properties:

++alg

++x5t#S256
++x5c
++crit
++b64
++sigT
++sigD
+++mId
+++pars
+++ctys

Description:
This test case tests a JAdES-B-B detached signature using the sigD header parameter with the ObjectIdByURI mechanism, and using JWS Compact Serialization. The URIs https://signature-plugtests.etsi.org/pub/JAdES/ObjectIdByURI-1.html and https://signature-plugtests.etsi.org/pub/JAdES/ObjectIdByURI-2.html shall be used as items of the pars array. The b64 header parameter shall be set to "true". The mId member shall be set to the URL "http://uri.etsi.org/19182/ObjectIdByURI". The items of the ctys array shall be set to "text/html". Implementation shall add at least the header parameters alg, x5t#S256, x5c, crit, b64, sigT, sigD. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-12

contains the following Properties:

++alg
++x5t#S256
++x5c
++crit
++b64
++sigT
++sigD
+++mId
+++pars
+++hashM
+++hashV
+++ctys

Description:
This test case tests a JAdES-B-B detached signature using the sigD header parameter with the ObjectIdByURIHash mechanism, and using JWS Compact Serialization. The URIs https://signature-plugtests.etsi.org/pub/JAdES/ObjectIdByURIHash-1.html and https://signature-plugtests.etsi.org/pub/JAdES/ObjectIdByURIHash-2.html shall be used as items of the pars array. The b64 header parameter shall be set to "false". The mId member shall be set to the URL "http://uri.etsi.org/19182/ObjectIdByURIHash". The items of the ctys array shall be set to "text/html".The hashM member shall be a string identifying a digest algorithm. The hashV member shall be a non-empty array of strings. Each element of the array shall contain the base64url-encoded digest value of the data object referenced by the parameter value that is present in the same position of the pars array. Implementation shall add at least the header parameters alg, x5t#S256, x5c, crit, b64, sigT, sigD. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-13

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT

++sigPId
+++id
+++digAlg
+++digVal

Description:
This case tests a JAdES-B-B signature including a signature policy identifier header parameter using JWS Compact Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT, sigPId (with members id, digAlg, digVal). The file available at the link https://signature-plugtests.etsi.org/pub/JAdES/JAdES-SignaturePolicy.der shall be used as signature policy. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-14

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT
++sigPId
+++id
+++digAlg
+++digVal
+++sigPQuals
++++spURI
++++spUserNotice

Description:
This case tests a JAdES-B-B signature including a signature policy identifier header parameter using JWS Compact Serialization. Implementation shall add at least the header parameters alg, x5t#S256, x5c, cty, crit, sigT, sigPId (with members id, digAlg, digVal, sigPQuals). At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-15

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
+++sigPId
++++id
++++digAlg
++++digVal
++++sigPSt
+++++sigPolDoc

Description:
This case tests a JAdES-B-B signature including a signature policy identifier header parameter sigPId and a sigPSt JSON object containing the signature policy document which is referenced in the sigPId header parameter using complete JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT, sigPId (with members id, digAlg, digVal). and the unsigned header parameter sigPSt (with the member sigPolDoc). The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-B-16

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT

Description:
This case tests a JAdES-B-B signature with a countersignature using complete JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT.and the unsigned header parameter csig. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

7.1.2 JAdES B-T level

- J-B-T-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst

Description:
This test case tests a JAdES-B-T signature including a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, using complete JWS JSON Serialization (default in JAdES-B-T,-LT,-LTA testcases). Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameter sigTst. The contents of the etsiU header parameters appear as base64url encoded (default in JAdES-B-T,-LT,-LTA testcases). At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-T-2

contains the following Properties:

++alg
++x5t#S256
++x5c
++cty
++crit
++sigT
+++sigTst

Description:
This test case tests a JAdES-B-T signature including a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, using flattened JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameter sigTst. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

- J-B-T-3

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst

Description:
This test case tests a JAdES-B-T signature with two different JWS signatures each one including a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, using complete JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameter sigTst. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too.

7.1.3 JAdES B-LT level

- J-B-LT-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals

Description:
This test case tests a JAdES-B-LT signature using complete JWS JSON Serialization. Participants should use ocsp responses as revocation values, as far as possible. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameter sigTst, tstVD, xVals, rVals. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too (in this latter case such certificates should not be included in xVals unsigned parameter).

- J-B-LT-2

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals

Description:
This test case tests a JAdES-B-LT signature using complete JWS JSON Serialization. Participants should use crls as revocation values, as far as possible. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameter sigTst, tstVD, xVals, rVals. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too (in this latter case such certificates should not be included in xVals unsigned parameter).

7.1.4 JAdES B-LTA level

- J-B-LTA-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests a JAdES-B-LTA signature using ocsp responses as preferred revocation values, using complete JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameters sigTst, tstVD, xVals, rVals, arcTst. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too (in this latter case such certificates should not be included in xVals unsigned parameter).

- J-B-LTA-2

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests a JAdES-B-LTA signature using crls as preferred revocation values, using complete JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameters sigTst, tstVD, xVals, rVals, arcTst. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be included in the x5c parameter. All certificates needed for path building should be included too (in this latter case such certificates should not be included in xVals unsigned parameter).

- J-B-LTA-3

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests a JAdES-B-LTA signature using ocsp responses as preferred revocation values, with 2 arcTst tstToken parameters, using complete JWS JSON Serialization. Implementation shall add at least the signed header parameters alg, x5t#S256, x5c, cty, crit, sigT and the unsigned header parameters sigTst, tstVD, xVals, rVals, arcTst. The contents of the etsiU header parameters appear as base64url encoded. At least the signing certificate shall be

included in the x5c parameter. All certificates needed for path building should be included too (in this latter case such certificates should not be included in xVals unsigned parameter).

7.1.5 JAdES Upgrade and Arbitration Test Cases

- J-B-T_B-B-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst

Description:
This test case tests the augmentation of a JAdES-B-B signature to a JAdES-B-T signature. The input to this test may be a JAdES-B-B signature as specified in J-B-2 testcase. The result JAdES-B-T signature includes a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value using complete JWS JSON Serialization (default in JAdES Upgrade and Audit testcases). The contents of the etsiU header parameters appear as base64url encoded (default in JAdES Upgrade and Audit testcases).

- J-B-T_B-B-2

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
+++sigD
++++mId
++++pars
++++sigTst

Description:
This test case tests the augmentation of a JAdES-B-B signature to a JAdES-B-T signature. The input to this test may be a JAdES-B-B signature as specified in J-B-10 testcase.but using complete JWS JSON Serialization. The result JAdES-B-T signature includes a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LT_B-B-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals

+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals

Description:
This test case tests the augmentation of a JAdES-B-B signature to a JAdES-B-LT signature. Participants should use ocsp responses as revocation values, as far as possible. The input to this test may be a JAdES-B-B signature as specified in J-B-2 testcase. The result JAdES-B-LT signature includes a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, tstVD, xVals and rVals unsigned header parameters encapsulating timestamp and signature validation data, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LT_B-B-2

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals

Description:
This test case tests the augmentation of a JAdES-B-B signature to a JAdES-B-LT signature. Participants should use crls as revocation values, as far as possible. The input to this test may be a JAdES-B-B signature as specified in J-B-2 testcase. The result JAdES-B-LT signature includes a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, tstVD, xVals and rVals unsigned header parameters encapsulating timestamp and signature validation data, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LT_B-T-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals

++++xVals
++++rVals
+++++ocspVals
+++++crlVals

Description:
This test case tests the augmentation of a JAdES-B-T signature to a JAdES-B-LT signature using ocsp responses and/or crls as revocation values. The input to this test may be a JAdES-B-T signature as specified in J-T-1 testcase. The result JAdES-B-LT signature includes tstVD, xVals and rVals unsigned header parameters encapsulating timestamp and signature validation data, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LTA_B-B-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests the augmentation of a JAdES-B-B signature to a JAdES-B-LTA signature using ocsp responses as preferred revocation values. The input to this test may be a JAdES-B-B signature as specified in J-B-2 testcase. The result JAdES-B-LTA signature includes a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, tstVD, xVals and rVals unsigned header parameters encapsulating timestamp and signature validation data, arcTst unsigned header parameter encapsulating an electronic time-stamp, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LTA_B-B-2

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals

+++++crlVals
++++arcTst

Description:
This test case tests the augmentation of a JAdES-B-B signature to a JAdES-B-LTA signature using crls as preferred revocation values. The input to this test may be a JAdES-B-B signature as specified in J-B-2 testcase. The result JAdES-B-LTA signature includes a sigTst unsigned header parameter encapsulating one electronic time-stamp time-stamping the JWS Signature Value, tstVD, xVals and rVals unsigned header parameters encapsulating timestamp and signature validation data, arcTst unsigned header parameter encapsulating an electronic time-stamp, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LTA_B-T-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests the augmentation of a JAdES-B-T signature to a JAdES-B-LTA signature using ocsp responses as preferred revocation values. The input to this test may be a JAdES-B-T signature as specified in J-T-1 testcase. The result JAdES-B-LTA signature includes tstVD, xVals and rVals unsigned header parameters encapsulating timestamp and signature validation data, arcTst unsigned header parameter encapsulating an electronic time-stamp, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LTA_B-LT-1

contains the following Properties:
+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests the augmentation of a JAdES-B-LT signature to a JAdES-B-LTA signature. The input to this test may be a JAdES-B-LT signature as specified in J-LT-1 testcase. The result JAdES-B-LTA signature includes arcTst unsigned header parameter encapsulating an electronic time-stamp, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

- J-B-LTA_B-LTA-1

contains the following Properties:

+++alg
+++x5t#S256
+++x5c
+++cty
+++crit
+++sigT
++++sigTst
++++tstVD
+++++xVals
+++++rVals
++++++ocspVals
++++++crlVals
++++xVals
++++rVals
+++++ocspVals
+++++crlVals
++++arcTst

Description:
This test case tests the inclusion of a second arcTst tstToken in a JAdES-B-LTA signature. The input to this test may be a JAdES-B-LTA signature as specified in J-LTA-1 testcase. The result JAdES-B-LTA signature includes arcTst unsigned header parameter encapsulating two electronic time-stamps, using complete JWS JSON Serialization. The contents of the etsiU header parameters appear as base64url encoded.

7.2 Negative test cases

7.2.0 Introduction

This clause describes 'Negative Verification-Only' tests in which the test JAdES signatures are verified as invalid by participating implementations. In the negative test, participants do not need to generate signatures.

In the 'negative test' participants will do the following:

1. A participating implementation shall verify the JAdES signatures. Verification of the JAdES signatures shall be negative. That's why we say 'negative test' for these tests.
2. A participant will download JAdES signatures generated by the organizers.
3. Verify JAdES signatures.
4. Upload verification results as XML files.
5. See test result matrix.

7.2.1 JAdES B-BN Test Cases

The following list summarizes negative test cases for JAdES Baseline level B signatures

1. Verify a JAdES-B-B signature having a wrong signature (the hash that was signed isn't the hash computed on the specified JWS Protected Header and JWS Payload elements)
2. Verify a JAdES-B-B signature that DOES NOT CONTAIN the mandatory sigT header parameter
3. Verify a document signed with an expired signing certificate
4. Verify a document signed with a revoked/suspended signing certificate
5. Verify a JAdES-B-B signature including a wrong value in the x5t#S256 parameter (such value does *NOT* match to the hash value of the signing certificate)
6. Verify a JAdES-B-B signature with a crit parameter that does *NOT* include all the needed names of the signed header parameters (that's all the newly specified ones)
7. Verify a JAdES-B-B signature that includes a SigPId parameter whose value of digVal component does *NOT* match to the hash value of the object identified by the id component
8. Verify a JAdES-B-B signature that includes in the crit array a critical extension that cannot be understood/processed. The crit array included in this signature contains a parameter name "UNDEFINED" that cannot be understood/processed

- J-B-BN-1

Description:
This is a negative test case for checking a wrong signature. This test data has a wrong signature because the hash that was signed isn't the hash of the specified JWS Protected Header and JWS Payload elements.

- J-B-BN-2

Description:
This test case tests the verification of a JAdES-B-B signature that DOES NOT CONTAIN the mandatory sigT header parameter.

- J-B-BN-3

Description:
This is a negative test case for checking an expired signing certificate. This test data has a signature created by a signer whose certificate is expired. ETSI Invalid-Cert Expired SN:7CE2B9 25-Oct-2021 10:00:00Z - signer certificate expired SN:7CE2B9

- J-B-BN-4

Description:
This is a negative test case for checking a revoked signing certificate. This test data has a signature created by a signer whose certificate is revoked. ETSI Invalid-Cert Revoked SN:7CE2FF 22-Oct-2021 14:23:23Z - signer certificate revoked SN:7CE2FF

- J-B-BN-5

Description:

This is a negative test case for checking x5t#S256 parameter. This test data has an x5t#S256 parameter whose value does *NOT* match to the hash value of the signing certificate.

- J-B-BN-6

Description:
This is a negative test case for checking the crit parameter. This test data has a crit parameter that does *NOT* include all the needed names of the signed header parameters (the ones included in the header that are newly specified).

- J-B-BN-7

Description:
This is a negative test case for checking sigPId parameter. This test data has a sigPId parameter whose value of digVal component does *NOT* match to the hash value of the object identified by the id component.

- J-B-BN-8

Description:
This is a negative test case for checking the inclusion in the crit array of a critical extension that cannot be understood/processed. This test data has a crit array containing a parameter name "UNDEFINED" that cannot be understood/processed.

7.2.2 JAdES B-TN Test Cases

The following list summarizes negative test cases for JAdES Baseline level T signatures

1. A negative test case for verifying signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the signer certificate had been already expired
2. A negative test case for verifying signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the signer certificate had been already revoked
3. Verify a JAdES-B-T signature in which the hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding base64url-encoded JWS signature value
4. A negative test case for verifying timestamp signer certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the timestamp signer certificate had been already revoked

- J-B-TN-1

Description:
This is a negative test case for verifying signing certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the signer certificate had already expired. ETSI Invalid-Cert Expired SN:7CE2B9 25-Oct-2021 10:00:00Z - signer certificate expired SN:7CE2B9 25-Oct 2021 10:23:04Z – SignatureTimeStamp.

- J-B-TN-2

Description:
This is a negative test case for verifying signing certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the signer certificate had already been revoked. ETSI Invalid-Cert Revoked SN:7CE2FF 22-Oct-2021 14:23:23Z - signer certificate revoked SN:7CE2FF 22-Oct 2021 15:12:09Z – SignatureTimeStamp

- J-B-TN-3

Description:
This is a negative test case for SignatureTimeStamp. The hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of the corresponding base64url-encoded JWS Signature Value.

- J-B-TN-4

Description:
This is a negative test case for verifying timestamp signing certificate at the time in SignatureTimeStamp. At the time in SignatureTimeStamp, the timestamp signer certificate had already been revoked. ETSI Invalid-Cert Revoked SN:57 27-Oct-2021 11:01:01Z - timestamp signer certificate revoked SN:57 27-Oct 2021 13:19:54Z - SignatureTimeStamp

7.2.3 JAdES B-LTN Test Cases

The following list summarizes negative test cases for JAdES Baseline level LT signatures

1. A negative test case for verifying an expired signing certificate, the JAdES-B-LT signature includes signing-time, POE and validation data after signing certificate expiration

2. A negative test case for verifying a revoked signing certificate, the JAdES-B-LT signature includes signing-time, POE and validation data after signing certificate revocation

- J-B-LTN-1

Description:
This is a negative test case for verifying a JAdES-B-LT signature created with a signing certificate expiring in date 2021/10/25, signing-time, POE and validation data after signing certificate expiration. ETSI Invalid-Cert Expired SN:7CE2B9 25-Oct-2021 10:00:00Z - signer certificate expired SN:7CE2B9 25-Oct 2021 10:23:04Z – SignatureTimeStamp

- J-B-LTN-2

Description:
This is a negative test case for verifying a JAdES-B-LT signature created with a signing certificate revoked in date 2021/10/22 signing-time, POE and validation data after signing certificate revocation. ETSI Invalid-Cert Revoked SN:7CE2FF 22-Oct-2021 14:23:23Z - signer certificate revoked SN:7CE2FF 25-Oct 2021 12:48:59Z – SignatureTimeStamp

7.2.4 JAdES B-LTAN Test Cases

The following list summarizes negative test cases for JAdES Baseline level LTA signatures

1. A negative test case for verifying time ordering between time stamps. In this test case, the time in the sigTst parameter is ulterior than the time in the arctTst one

2. A negative test case for verifying computation of messageImprint input to arcTst. In this test case, the messageImprint hasn’t the right value related to the JAdES signature to which has been applied

- J-B-LTAN-1

Description:

This is a negative test case for verifying time ordering between time stamps. In this test case, the time in the sigTst parameter is ulterior than the time in arcTst one. ETSI Invalid-Sig Valid-Cert 27-Oct-2021 14:18:31Z - SignatureTimeStamp (*) 04-Nov-2021 09:00:02Z – ArchiveTimeStamp

- J-B-LTAN-2

Description:
This is a negative test case for verifying computation of messageImprint input to arcTst. In this test case, the messageImprint hasn’t the right value related to the JAdES signature to which has been applied.

Change History

Document history		
1.0	10 Jan 2022	First version
1.1	14 Jan 2022	Editorial update