Technical Report of the EAA Remote Plugtests™ Event (May-June 2026)

Reference

Keywords
Electronic Signature, EUDI
Wallet

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

Important notice

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

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

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

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

Copyright Notification

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

© European Telecommunications Standards Institute 2021.
All rights reserved.

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

July 2026

Abstract

This document is the technical report of the 2026 Remote Plugtests Event on EAA (Electronic Attestation of Attributes) ETSI TS 119 472-1, 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 6
2 Plugtests portal 7
2.1 Structure 7
2.2 General Event information 7
2.3 Testing materials areas 8
2.4 EAA Interoperability testing areas 8
2.5 Communications 9
2.5.1 Mailing list 9
2.5.2 Discord workspace 9
3 Conducting Plugtests 10
3.1 Scope 10
3.2 Type of tests 10
3.3 EAA Conformance Checker 12
4 Participants list 13
5 Plugtests conclusions 17
5.1 Remote vs. Face to Face 17
5.2 Communication supporting technologies 17
5.3 Event duration 17
6 Overall results 17
6.1 EAA uploads 17
6.2 Verification reports uploads 17
6.3 Conformance Checker uploads 18
7 EAA Plugtests related issues 18
7.1 Introduction 18
7.2 Issues raised on the technical specifications 18
7.2.1 Inconsistency between ETSI TS 119 472-1 and the ARF PID Rulebook (Annex 3.1). 18
7.2.2 Acceptance criteria of EEAs signing certificates 18
7.2.3 Clarification about iat header parameter vs JWT claim 19
7.2.4 Status claim semantic 19
7.2.5 JAdES signatures conformance 19
7.2.6 "oneTime" claim requirements 19
7.2.7 adm_nbf and adm_exp claims definition 19
7.2.8 Location where the QEAA/PubEAA signing certificate is available free of charge 20
7.2.9 EAA issuer identifier 20
7.2.10 vct#integrity claim encoding 20
7.2.11 iss claim value verification 20
7.2.12 x5chain definition in ISO/IEC 18013-5 21
7.2.13 status_service property 21
7.2.14 Successful validation of timestamps signed by expired TSU certificates still present in a member state trusted list 21
7.2.15 pseudonym usage in an mdl 22
7.2.16 Newly defined claims to be indicated if disclosable 22
7.2.17 EAA data for key binding 22
7.3 Issues raised on the EAA Conformance Checker 22
8 EAA Plugtests Interoperability Testing 25
8.1 Positive test cases 25
8.1.0 Introduction 25
8.1.1 SD-JWT VC EAA 25
8.1.2 SD-JWT VC QEAA 29
8.1.3 SD-JWT VC PuB-EAA 33
8.1.4 ISO-mdL (ISO-mdoc EAA for mdL) 36
8.1.5 ISO-mdoc EAA(no mdL) 41

8.1.6 ISO-mdoc QEAA(no mdL) 49
8.1.7 ISO-mdoc PuB-EAA(no mdL) 53
8.2 Negative test cases 57
8.2.0 Introduction 57
8.2.1 SD-JWT VC EAA Negative Test Cases 58
8.2.2 SD-JWT VC QEAA Negative Test Cases 59
8.2.3 SD-JWT VC PuB-EAA Negative Test Cases 59

Change History 61

1 Introduction

ETSI Centre for Testing and Interoperability (CTI) organized a remote Plugtests interoperability event on **EAA (**Electronic Attestation of Attributes**)**. This event was run remotely from **4 May to 30 June 2026.**

It was the first Plugtests event on the EAA specification. The proposed testing has enabled participants to test software that implements the EAA Specification, ETSI TS 119 472-1 V1.2.1 (Profiles for Electronic Attestation of Attributes; Part 1: General requirements). The participation was free of charge, and this remote event aims to conduct conformance and interoperability testing on EAA Attestations.

The EUDI Wallet is a flagship EU initiative aimed at providing citizens with secure, user-friendly, and privacy-respecting access to digital services across Europe. Proposed by the European Commission in June 2021 as part of the eIDAS Regulation revision, it was officially adopted under eIDAS 2.0 (Regulation EU 2024/1183) in May 2024.

The wallet will enable European citizens to:

- Prove their identity,
- Store and share official documents (e.g., diplomas, driving licenses, medical records),
- Access public and private services directly from their mobile devices.

It will be interoperable across all EU Member States, facilitating seamless cross-border interactions in areas such as travel, education, healthcare, and employment.

In the EUDI Wallet ecosystem, EAAs are one of the core building blocks. They are the mechanism that allows the wallet to go beyond simple identity and become a portable container of verifiable credentials.

ETSI ESI has been developing several standards to support the lifecycle of EAAs, including Trusted Services for their issuance and validation, and for the EUDI Wallet overall.

To verify the interoperability within the EUDI Wallet ecosystem, ETSI CTI has organised the first **EAA Plugtests event**. The goal is to assess the interoperability of EAAs generated by products implementing Technical Specification ETSI TS 119 472-1.

Three types of tests are planned:

- Generation and Cross-Verification Tests
  Participants generate a set of valid EAAs with defined characteristics. Other participants then verify these EAAs. The Plugtests portal automatically updates interoperability matrices accessible to all participants.
- Verification-Only Tests (Negative Tests)
  ETSI provides a set of invalid EAAs for various reasons. Participants attempt to verify these EAAs to ensure their tools correctly identify them as invalid.
- Conformance Tests
  Participants upload EAAs to a conformance checker for verification

As a remote event, participants will not need to travel to ETSI premises. All EAA exchanges and verifications will be conducted via a dedicated portal.

Testing will not occur in real time; the portal will be available 24/7 throughout the event, allowing participants from all time zones to generate, upload, and verify signatures at their convenience.

2 Plugtests portal

2.1 Structure

The portal has a private part, only visible only the registered participants of the Plugtests event. It is structured in four main areas:

- **Event area.** This area contains a set of pages that provide generic information to the participants, like the meeting details, slides and video recording of the meeting, Discord (Chat channels) link, and a forum to report any issues/feeback on the event, the specification , the checker, the testing , etc…
- **Documentations.** This area contains a number of pages that provide generic information to the participants, which is relevant to participants of interoperability tests. It includes the documentation on how to conduct the testing, the set of testcases and the PKI page where participants can request a Qualified certificate valid for the testing only and kindly provided by InfoCert.
- **EAA Interop specific area**. This area contains a number of pages that support the interoperability testing tools on EAA signatures.
- **EAA Conformance Checker area**. This area contains an online tool for checking the structure of a EAA vs the specification.

2.2 General Event information

- **Participants' List page**

This page listed the details of all the companies and people that participated in the Plugtests, as well as their username names and their associated company acronym.

- **Profile**

This page allows the particpants to update his profile (email, company details etc …) and change the password.

- **Meetings Support**

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 (Gotomeeting conference calls).
- The agenda for each meeting.
- Links to the video recording of each meeting. The Kick-off includes a full demo on how to use the portal and how to upload EAAs and verification reports.

- **Forum**

This page allow the particpants to create topics in order to provide feedback on the event or report any issue. The posts are categorised per theme (General, Specification, Portal, Testcase, EAA Checker)

2.3 Testing materials areas

- **Documentation**

This area provides a set of pages describing how to conduct the interoperability testing (cross verification and negative tests)

- **Testcases**

This area provides a set of pages providing the testcases used for producing EAAs to be uploaded.
- TC SD_JWT_VC of EAA, QEAA and PubEAA
- TC ISO mdL/mdoc : ISO-mdoc EAA for mdL , ISO-mdoc (no mdL) for EAA, QEAA and PubEAA
- TC negative for SD_JWT_VC of EAA, QEAA and PubEAA

- **PKI / Cryptographic materials pages**

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

2.4 EAA Interoperability testing areas

- **Upload**

The Upload page provided mechanisms for uploading EAA and verification reports.
Participants are invited to upload zip files containing their EAAs produced according to the proposed testcases and the Verification reports of the EAAs uploaded by other participants.

- **Results Matrix**

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

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

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

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

- **Activity page**

This area contained a page that displays, in real time, the tables and details of the EAAs and the validation reports uploaded. The participants can also download both full lists in csv files.

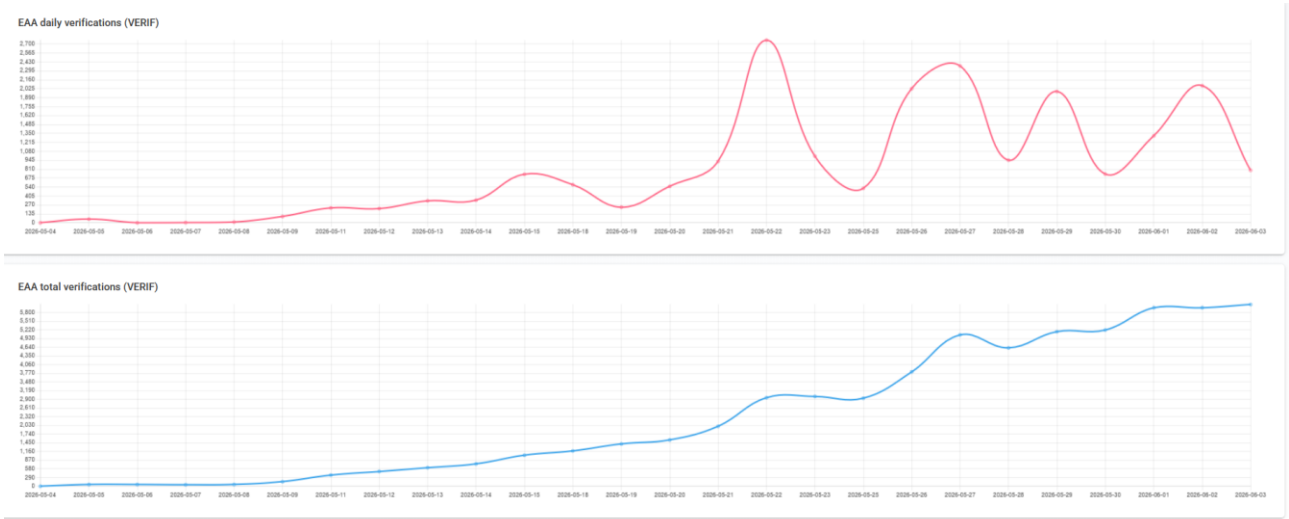
- **File explorer page**

The page was used by the participants for browsing the folders' structure where the portal stored the "pre-existing" and new EAA 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.

Participants have the possibility to download all files and company folders into a single zip file.

- **Statistics**

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



2.5 Communications

2.5.1 Mailing list

- EAA_PLUGTESTS@LIST.ETSI.ORG: used to contact the participants and exchanges information. It was used for fruitful technical discussions and to raise some issues.

2.5.2 Discord workspace

In order to allow better exchanges between participants, a Discord workspace was set up by the ETSI CTI team at https://discord.gg/C23yuX9EE

Each participant was invited to create an account and use Discord 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 Conducting Plugtests

3.1 Scope

The interoperability and conformance proposed testing allowed participants to test their software that implements the EAA Specification, ETSI TS 119 472-1 V1.2.1 (Profiles for Electronic Attestation of Attributes; Part 1: General requirements).

Scope of the Plugtests:

- The formats tested will include those based on SD-JWT VC and ISO 18013-5.
- Each participant will generate EAAs according to specific test cases and requirements and upload them to a portal.
- Other participants will then validate these EAAs and submit their verdicts.
- Test cases will be based on the attribute metadata requirements outlined in Clause 4 of TS 119 472-1 for each format.

This testing aims to identify potential issues that could lead to discrepancies in EAA creation or verification.

3.2 Type of tests

Three types of tests are planned:

- Generation and Cross-Verification Tests
  Participants generate a set of valid EAAs with defined characteristics. Other participants then verify these EAAs. The Plugtests portal automatically updates interoperability matrices accessible to all participants.
- Verification-Only Tests (Negative Tests)
  ETSI provides a set of invalid EAAs for various reasons. Participants attempt to verify these EAAs to ensure their tools correctly identify them as invalid.
- Conformance Tests
  Participants upload EAAs to a conformance checker for verification.

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.

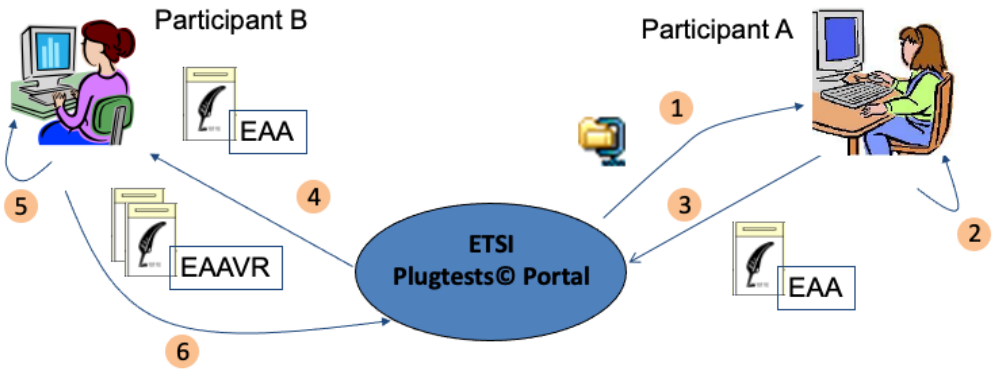
This Plugtests event allowed to conduct 3 types of tests:

1. **Generation and cross-verification of EAAs.**

   The Plugtests team has prepared a test suite which includes test cases on two profiles of EAAs specified in ETSI TS 119 472-1: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements" v1.2.1, namely: **SD-JWT VC EAAs** (clause 5 of the mentioned TS) and **ISO/IEC mdoc EAA** (clause 6 of the mentioned TS).

   For each test case, those participants with capabilities for doing it, are invited to generate a valid EAA of the specified profile according to the details defined by the test case.

   After that, the rest of the participants are invited to verify the generated EAA.

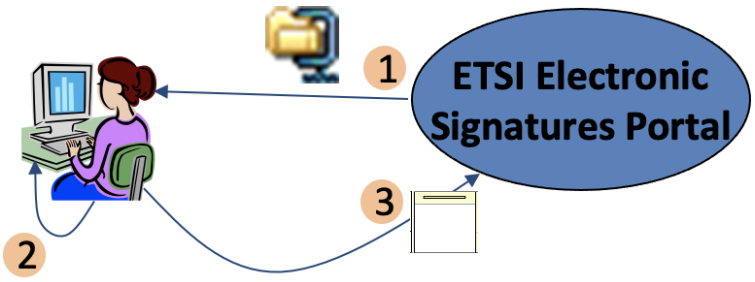


Legend:

- EAA: Electronic Attestation of Attributes
- EAAVR: Electronic Attestation of Attributes Verification Report

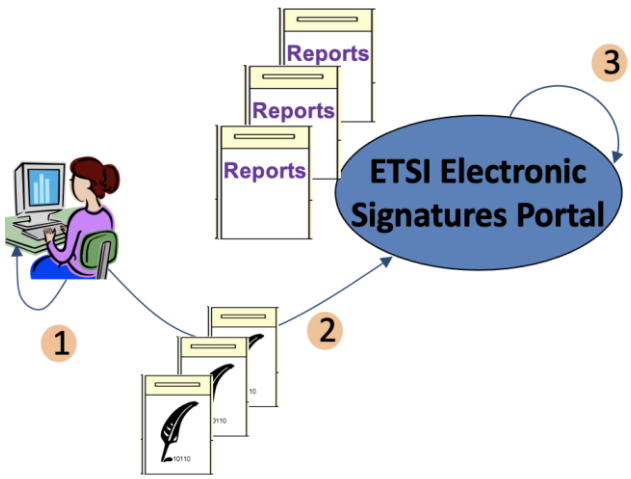
2. **Only verification tests (Negative tests)**
   Each participant is invited to validate EAAs that have been created by the Plugtests© organization team. All these EAAs have some wrong components that should make the validation fail.

   The testing is similar to cross-verification testing. only difference is that the pre-generated EAAs for these tests appear within the ETSI folder.



3. **Conformance testing.**

   In this type of tests, participants will have to upload EAA file (.json or .cbor) to the portal Conformance checker. This online tool runs a set of conformance checks against the EAA Specifications.



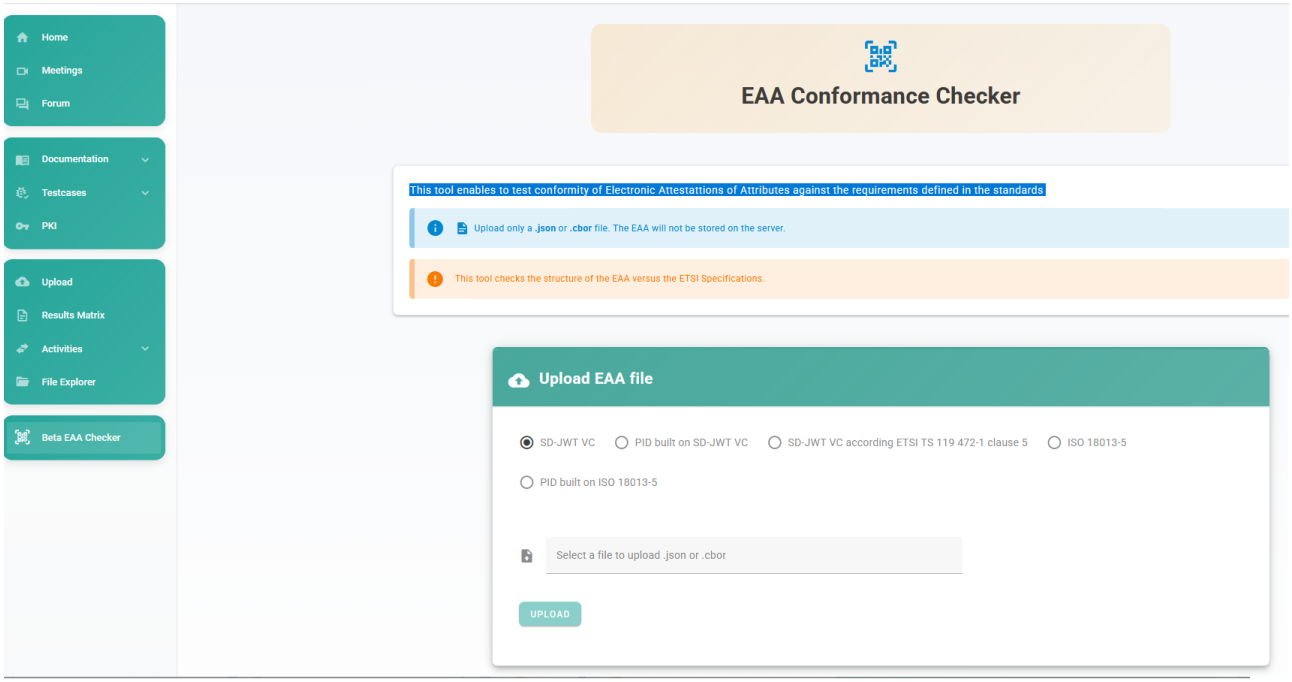
3.3 EAA Conformance Checker

In addition of Cross generation and verification testing (Interoperability tests), ETSI has provided to the participants a online tools integrated into the Plugtests portal, to allow to run EAA conformance test verifications.

During the Plugtests event, the tool was in beta version but fully operational.

It provided capability for checking conformance against different specifications.

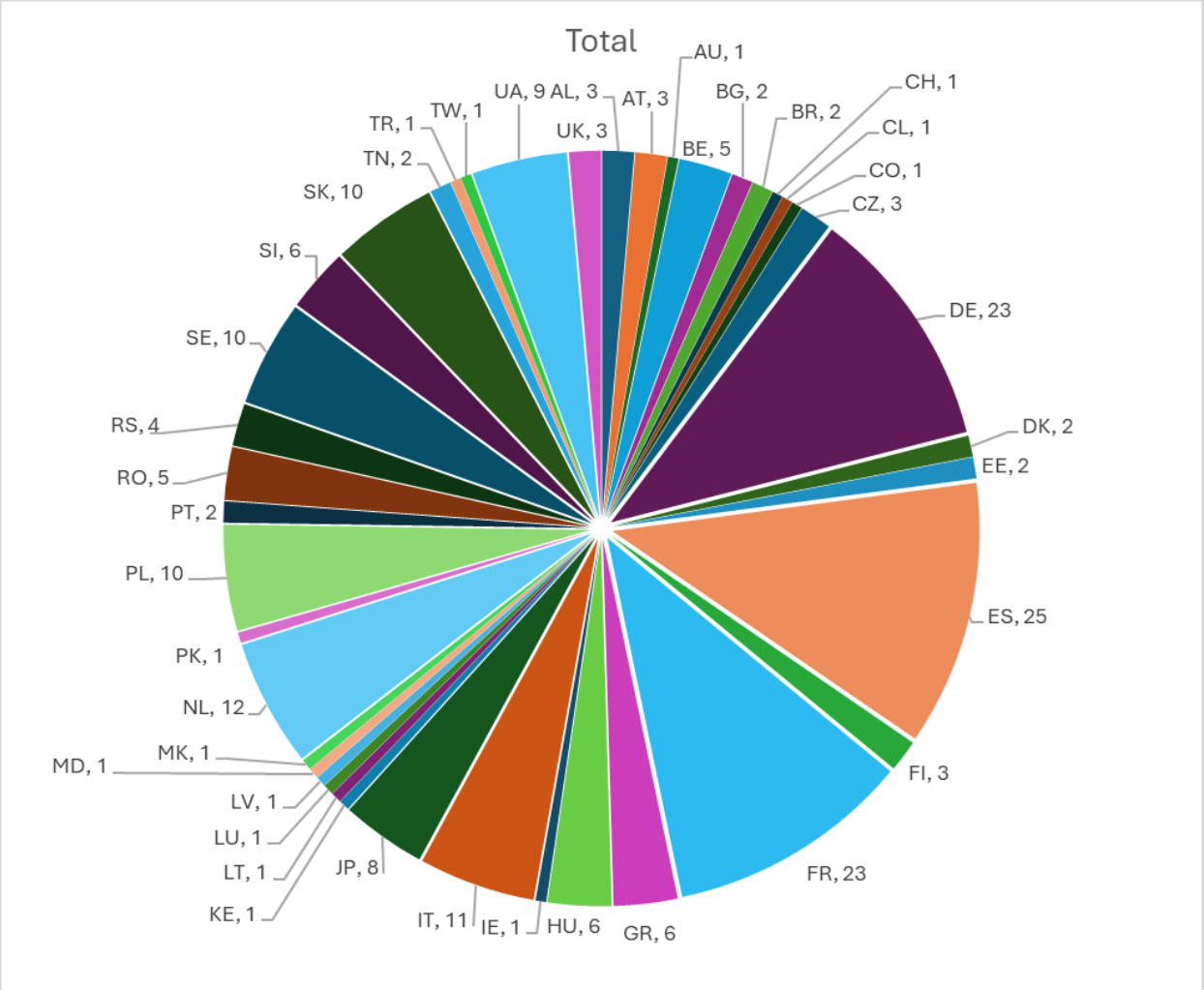
- JSON-based. Offers to check objects against
    - RFC 9901: "Selective Disclosure for JSON Web Tokens".
    - Draft IETF SD-JWT VC: "SD-JWT-based Verifiable Digital Credentials (SD-JWT VC)".
    - PIDs built on SD-JWT VC
    - SD-JWT VC EAA according to ETSI TS 119 472-1 clause 5.
- CBOR-based. Offers to check objects against
    - ISO/IEC 18013-5 mdL (Movile Driving Licence).
    - ISO/IEC 18013-5 syntax for mdoc (not mdL).
    - PID built on ISO/IEC 18013-5 for mdoc.
- To be added:
    - ISO mdoc EAA according to ETSI TS 119 472-1 clause 6.
    - EAA Presentations according to ETSI TS 119 472-2 clause 4.



4 Participants list

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

There have been **116 different organisations,** and a total of **215 people** were involved, including 207 participants, 4 ETSI staff and 4 experts.



Company	Country name
Adobe Systems Software Ireland Limited	Ireland
AlfaTrust Certification	Romania
Allied Bits Ltd.	United Kingdom
Ardaco, a.s.	Slovak republic
ARIA S.p.A.	Italy
Aruba PEC S.p.A.	Italy
Ascertia	Pakistan
A-SIT Plus	Austria
Asseco Data Systems	Poland
Atos Eviden	France
AUTHADA GmbH	Germany

Authologic Sp. z o.o.	Poland
Bankovni identita, a.s.	Czech republic
BOSA	Belgium
British Standards Institution (BSI)	United Kingdom
Bull	Spain
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany
Cabinet Louis Reynaud	France
Centro Tecnológico des Notariado	Spain
Certisign	Brazil
certSIGN	Romania
Chamber of Commerce and Industry of Serbia	Serbia
Chunghwa Telecom Laboratories (CHTTL)	Taiwan
Cleverbase	Netherlands
Comfact AB	Sweden
Credenco B.V.	Netherlands
CZ.NIC	Czech republic
Datakeeper	Netherlands
Desteba Productions, S.L.	Spain
Deutsche Telekom AG	Germany
DEVISE FUTURES - IT SOLUTIONS, LDA	Portugal
dewa ApS	Denmark
DiaLOGIKa	Germany
Digi- ja väestötietovirasto (DVV), Digital and Population Data Services Agency	Finland
Digidentity B.V.	Netherlands
Digitel on Trusted Services, S.L.U	Spain
Disig a.s.	Slovak Republic
DITEC, a.s.	Slovak republic
DOCAPOSTE CSP	France
Duru Bilişim	Turkey
ecsec GmbH	Germany
EGA	Ukraine
e-Governance Agency of Moldova	Moldova
Entrust	United Kingdom
Entrust EU	Spain
Erick Virapatrin Consulting	France
e-Sec Digital Security	Brazil
E-Smart Systems	Serbia
EUSO	Latvia
Evrotrust Technologies AD	Bulgaria
First shpk	Albania
Forkbomb B.V.	Netherlands
Gestión de Seguridad Electrónica (GSE)	Colombia
Governikus GmbH & Co. KG	Germany
Greek Universities Network (GUnet)	Greece

GrEEV	Austria
Higher School of Communications, University of Carthage (Sup'Com)	Tunisia
Hovi ID	Finland
iDAKTO	France
IdomSoft	Hungary
IDunion SCE	Germany
iLabs Technologies B.V.C	Netherlands
Independent	Germany
InfoCert	Italy
INTESI GROUP S.p.A.	Italy
Iris Development-PassportReader	Sweden
ISTEC	Spain
Izertis	Spain
KEREVAL	France
LCubed AB (iGrant.io)	Sweden
Lissi Gmbh	Germany
Lleida.net	Spain
Microsec Ltd	Hungary
MINISTERE DE L'INTERIEUR	France
Ministry for Digital Transformation and Civil Service	Spain
Ministry of Digital Governance	Greece
MIT-SOFT, UAB	Lithuania
Mobbeel Solutions, S.L.	Spain
Mobile Solution Network ltf	Kenya
Msg systems ag	Belgium
Namirial	Italy
National Agency for Information Society (NAIS)	Albania
National Agency for Network and Electronic Services (NASES)	Slovak republic
National Security Authority	Slovak republic
NEOWAVE	France
Netis d.o.o.	Slovenia
NEWPS.CZ s.r.o.	Czech republic
Nextsense	Republic of north macedonia
Nowina Solutions	Luxembourg
NTT Data	Japan
OneTech B.S. (OTBS)	Tunisia
Otip Office	Japan
Plaut Slovensko s.r.o.	Slovak republic
POLYSYS Ltd	Hungary
Post of Serbia	Serbia
procilon GmbH	Germany
Procivis AG	Switzerland
Secumail B.V.	Netherlands
Servicios de MailCertificado - Codicert	Spain
SIGN8 GmbH	Germany

SITA	Australia
SK ID Solutions AS	Estonia
Space Acceleration Industries	Germany
SPRIND GmbH	Germany
State Enterprise "DIIA"	Ukraine
Subsecretaría de Economía	Chile
Technical University of Munich (TUM)	Germany
TOPPAN Security	France
Triveria	Slovak republic
Trustvestor Ltd.	Bulgaria
Truvity	Netherlands
UPC	Spain
Validated ID, SL	Spain
Ver.iD	Netherlands
Verifiables	France
walt.id	Austria

5 Plugtests conclusions

5.1 Remote vs. Face to Face

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.

5.2 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.

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

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

5.3 Event duration

The event was initially planned to run until 1st June 2026, but it was extended to 30 June 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.

6 Overall results

6.1 EAA uploads

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

Generated	EAA	SD-JWT-VC	MDL	MDOC
Total	959	597	96	266

6.2 Verification reports uploads

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

Verified	EAA	SD-JWT-VC	MDL	MDOC
Total	11172	7842	887	2443

6.3 Conformance Checker uploads

Number of EAAs uploaded on the Conformance checker online tool.

Uploads	EAA	SD-JWT-VC	MDL/MDOC
Total	1028	698	330

7 EAA Plugtests related issues

7.1 Introduction

The present clause lists some of the issues raised during the EAA Plugtests event in May and June 2026. 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.

The present clause lists:

1. Issues raised during the EAA Plugtests on the Technical Specifications.
2. Issues raised during the EAA Plugtests on the EAA Conformance Checker beta version made available during the mentioned Plugtests.

7.2 Issues raised on the technical specifications

7.2.1 Inconsistency between ETSI TS 119 472-1 and the ARF PID Rulebook (Annex 3.1).

At the Plugtests it was reported there is a misalignment between ETSI TS 119 472-1 and the ARF PID Rulebook (Annex 3.1). The requirement EAA-6.1-03 in ETSI TS 119 472-1 states that any EAA based on ISO/IEC-mdoc which is not an mDL shall contain data elements defined in clause 6.3 of ISO/IEC 23220-2 within the namespace org.iso.23220.1. The PID, that is not an mDL, is mandated by the ARF PID Rulebook to use the namespace eu.europa.ec.eudi.pid.1 with its own data element catalogue and does not require the org.iso.23220.1 namespace or the attested attributes mandated in clause 6.3 of ETSI TS 119 472-1.

Therefore, a PID compliant with the ARF Rulebook doesn't satisfy requirement EAA-6.1-03 in ETSI TS 119 472-1.

It was asked if requirement EAA-6.1-03 should be applied to PID too. And in such cases if the Rulebook should be updated to allow/require org.iso.23220.1 alongside eu.europa.ec.eudi.pid.1.

7.2.2 Acceptance criteria of EEAs signing certificates

At the Plugtests a participant raised the issue of acceptance criteria of EEAs signing certificates stating that the certificates key usage extension shall include the digitalSignature value. Such criteria seem to be in contrast with specifications stated in ETSI EN 319 412-2/-3 about profiles for certificates issued to natural persons and to legal persons. Might it be necessary to define an ad hoc profile for EAA/pubEAA/QEAA signing certificates?

7.2.3 Clarification about iat header parameter vs JWT claim

At the Plugtests it was requested to clarify in ETSI TS 119 472-1 whether the JAdES "iat" header parameter is to be considered, or not, a replica of a present "iat" JWT claim, according to RFC 7519 section 5.3 and if such parameter shall be mandated or not.

7.2.4 Status claim semantic

At the Plugtests it was requested to align ETSI TS 119 472-1 status claim specification for SD JWT with Token Status List format defined in RFC 9901. In clause 5.2.10 of ETSI TS 119 472-1 it is specified that, in the EAA status service claim in SD-JWT, 4 mandatory elements ("type", "purpose", "index" and "uri") shall be defined. On the other side, in clause 6.2.10 for ISO/IEC 18013-5 mdoc it is specified that EAA status service claim may include the "status_list" element as defined in the draft-ietf-oauth-status-list-13, thus creating a different implementation in comparison with SD-JWT

It shall be noted that RFC 9901 refers to draft-ietf-oauth-status-list-13 of TSL while the current version of the TSL draft is draft-ietf-oauth-status-list-21.

7.2.5 JAdES signatures conformance

At the Plugtests it was noted that ETSI TS 119 472-1 does not apply the JAdES conformance (in EAA-5.6.1-01) requirement for compact serialized SD-JWT VC. Being compact and JSON Serialized or Flattened serializations mutually convertible, it was requested to consider JAdES conformance for SD-JWT VC signatures. Specifically, it shall be considered if the SD-JWT VC EAA shall be supported by a JAdES signature when using compact serialization (thus all requirements of TS 119 182-1 shall apply), or if it could be a "simple" RFC 7515 JWS (that's the part of the SD-JWT VC before the first "~" character).

7.2.6 "oneTime" claim requirements

Some participants asked why the "status" claim is mandatory for QEAA and Pub-EAA, unless a "shortLived" claim is present (see requirements QEAA-5.2.10.2-01 and PuB-EAA-5.2.10.3-01 in ETSI TS 119 472-1) but the same requirement does not apply for "oneTime" claim. According to requirement EAA-5.2.8.2-03 in ETSI TS 119 472-1, the presence of the oneTime claim shall indicate that the EAA shall be used only once, and that it shall not be retained for future use. Therefore, it was asked which is the interest of checking the status for EAAs with "oneTime" claim which should not be retained and thus are expected to be always fresh,

7.2.7 adm_nbf and adm_exp claims definition

At the Plugtests it was noted that in clause 5.2.7.2 of TS 119 472-1 there are specific requirements for the EAA administrative validity period in which "adm_nbf" and "adm_exp" claims are defined as below:

EAA-5.2.7.2-01: A SD-JWT VC EAA may include the adm_nbf claim specified in IETF RFC 7519 [4], clause 4.1.5, and further profiled in IETF SD-JWT VC [3], clause 3.2.2.2.

EAA-5.2.7.2-03: A SD-JWT VC EAA may include the adm_exp claim specified in IETF RFC 7519 [4], clause 4.1.5, further profiled in IETF SD-JWT VC [3], clause 3.2.2.2.

However, nor IETF RFC 7519, nor draft-ietf-oauth-sd-jwt-vc specify "adm_nbf" and "adm_exp" claims, but "nbf" and "exp" claims therefore it shall be considered if ETSI TS 119 472-1 needs to define these claims within its own specifications.

7.2.8 Location where the QEAA/PubEAA signing certificate is available free of charge

At the Plugtests there were many discussions about the requirements QEAA-5.6.2-02 and PuB-EAA-5.6.3-02 in TS 119 472-1, defining the mandatory inclusion of the 'x5u' and the 'x5t#S256' header parameters in the digital signature proposing the possibility to use the 'x5o' protected header, defined in TS 119 182-1, as well, without limiting implementers to SHA-256 which may become obsolete in the future, therefore, providing a possibility for implementers to specify another algorithm in the long-term.

The x5u header parameter presence is requested by eIDAS. Concerning QEAAs, Annex IV of eIDAS says: "Qualified electronic attestation of attributes shall contain: (....) (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;

and in Annex VII, it is stated: "An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source shall contain: (....) (h)the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;"

The best approach seems to be that ESI raises a question to whoever is responsible for clarifying this issue in eIDAS regulation.

It was requested also to consider to avoid enforcing the SHA-256 digest algorithm as a requirement for the signing-certificate reference. Instead of mandating x5t#S256 header parameter usage, switching to another digest algorithm, thus modifying the header parameter within the specs (e.g. switching to x5t#o for JAdES signatures) could be considered. Participants stated a strong preference for allowing any other secure digest algorithms acknowledged in the EU (e.g. the ones referenced in the ETSI TS 119 312).

7.2.9 EAA issuer identifier

At the Plugtests a bit of confusion between ETSI TS 119 472-1 and CIR 2026/248 was highlighted. EAA-5.2.4.1-03 requirement specifies that an "SD-JWT VC EAA shall not incorporate the issuing_authority claim if it incorporates the qualified certificate supporting the EAA signature", and similarly EAA-5.2.4.1-07 and EAA-5.2.4.1-11 for issuing_country and iss_reg_id.

If this incorporation refers to header parameters, it was noted that CIR 2026/248 requires including the x5c header parameter for qualified JAdES, hence including one of these claims would never determine the creation of conforming QEAAs according to CIR 2026/248 (affecting requirements QEAA-5.2.4.2-01 to 03). It was commented that it should be avoided having different EAA payload requirements based on the EAA signing certificate.

7.2.10 vct#integrity claim encoding

Some participants discussed the encoding of the digest value of the 'vct#integrity' claim. The claim shall be base64-encoded, and not base64url-encoded, as it was encoded in many uploaded EAAs.

7.2.11 iss claim value verification

At the Plugtests it was pointed out that in draft-ietf-oauth-sd-jwt-vc-09, section 3.5 it was explicitly required that when using inline X.509 certificates (x5c header), the recipient MUST verify that the iss value matches either:

- a uniformResourceIdentifier SAN entry, or
- a dNSName SAN entry

of the end-entity certificate while in draft 16 (latest), this requirement was dropped, simply stating that when x5c is present, the recipient validates the certificate chain and considers the issuer to be the subject of the end-entity certificate, without any explicit mention of matching iss claim value against a SAN entry of the end-entity certificate.

ETSI TS 119 472-1 references draft-ietf-oauth-sd-jwt-vc-13 that didn't include any requirement for matching iss claim value against a SAN entry of the EAA signing certificate therefore the mentioned requirements of draft-ietf-oauth-sd-jwt-vc-09 are out of scope of ETSI TS 119 472-1.

7.2.12 x5chain definition in ISO/IEC 18013-5

During the Plugtests a possible inconsistency between part "9.1.2.4 Signing method and structure for MSO" of ISO/IEC 18013-5 and ETSI TS 119 152-1 about x5chain inclusion in the signatures was highlighted.

ISO/IEC 18013-5 in part "9.1.2.4 Signing method and structure for MSO" defines that the certificate containing the public key belonging to the private key used to sign the MSO shall be

included as an x5chain element as described in RFC: CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates. It shall be included as an unprotected header element and the x5chain element shall include at least one certificate and may contain more.

Which implies that the "x5chain" header parameter shall be present at the root level of the unprotected header map.

However, ETSI TS 119 152-1 requires the 'x5chain' to be embedded within 'uHeaders' instead, when the header should not be signed:

The x5chain header parameter may be a signed or unsigned header parameter that qualifies the signature.

If x5chain has not to be signed, it shall be included within the uHeaders CBOR array specified in clause 5.3.1 of ETSI TS 119 152-1.

This different specification makes all mdoc COSE_Sign signatures never conform to the CB-AdES format.

ETSI TS 119 472-1 contains the following requirements:

QEAA-6.6.2-04: The Protected Header of the CB-AdES digital signature signing an ISO/IEC-mdoc QEAA should contain the x5chain header parameter, specified in IETF RFC 9360.

PuB-EAA-6.6.3-04: The Protected Header of the CB-AdES digital signature signing an ISO/IEC-mdoc PuB-EAA should contain the x5chain header parameter, specified in IETF RFC 9360.

A possible solution is to replace the shall requirement by a should requirement in ETSI TS 119 152-1 when referring to the x5chain to be included within the uHeaders being the unique element in the UnprotectedHeader.

7.2.13 status_service property

At the Plugtests, a clarification about status_service element present in Annex A of ETSI TS 119 472-1 was requested. In Annex A it is mentioned that status_service element is defined in clause 6.2.10 where, instead, the status member is defined. Should the Annex A of ETSI TS 119 472-1 be changed?

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

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

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

7.2.15 pseudonym usage in an mdl

At the Plugtests a participant reported a possible contradiction between requirement EAA-6.2.5.1-02 (allowing inclusion of property also_known_as instead of given_name + family_name + document_number) and requirement EAA-6.2.3-01, which state that an ISO/IEC-mdoc EAA shall incorporate the document_number data element. It seems that it is not correct to envisage the possibility of a pseudonym for the subject in an mdL because ISO 18013-5 mandates given_name and family_name, and document_number. Therefore, the presence of pseudonym should be allowed only in non mdL EAAs (mdoc). The document_number should be optional for non-mdL EAAs.

7.2.16 Newly defined claims to be indicated if disclosable

At the Plugtests it was requested that when ETSI TS 119 472-1 introduces new claims for SD-JWT VC, it shall be stated whether the claim is allowed to be made selectively disclosable or not.

7.2.17 EAA data for key binding

At the Plugtests it was noted that in ETSI TS 119 472-1 in clause “5.5 EAA data for key binding" the following requirement *EAA-5.5-03: For representing the EAA subject certificate, the cnf claim may contain the x5c parameter containing only the certificate itself, or the x5t#S256 parameter, or the x5u parameter as specified in IETF RFC 7517 [30]* is in contrast with RFC 7517 that defines not the "cnf" claim parameter, but its child parameter "jwk" (as defined in RFC 7800), which may contain the aforementioned claims. Therefore, for interoperability reasons, the standard shall clearly indicate that the aforementioned claims shall be incorporated within a nested "jwk" member, and not directly in the "cnf" claim.

7.3 Issues raised on the EAA Conformance Checker

The issues raised for the Conformance Checker during the EAA Plugtests are listed in the table below.

#	Issue	File	Status	Additional Comments
1	177.Warning Tool Location-{CodeTest}: root.JWS_COMPACT.jsonpid.payload-{UnknownAttribute} An unkown attribute has been found. The Conformance Checker will not perform any check on it. Unknown component has the tag 'nbf'	SD_JWT_VC_PID-01.json	Solved	Added creation of creation of checker for nbf, exp, iat to the SDJWTCheckersFactory
2	Hello, when I upload a .cbor mdoc document within the Conformance Checker, and select the "ISO 18013-5" option, nothing happens. Literally, no validation is performed, nor error is received. When I choose "PID built on 18013-5", I receive an empty report. No error reported	IssuerSigned.cbor	Solved	The participant used a tagged COSE_Sign1 instead of an untagged COSE_Sign1, as specified in ISO 18013-5. The participant agreed that using a tagged COSE_Sign1 was not compliant with the standard. While reviewing the issue, the CC was modified for raising a proper message for this case.
3	Hello, when I upload a .cbor mdoc document within the Conformance Checker, and select the "ISO 18013-5" option, nothing happens. Literally, no validation is performed, nor error is received. When I choose "PID built on 18013-5", I receive an empty report. No error reported		Solved	The CC detects an error in birth_date, as the tag used in the file is NOT 6 as mandated by the standard. The CC is modified for reporting errors in this situation. In addition to that, the CC was modified so that if the namespace is NOT "eu.europa.ec.eudi.pid.1", then no check of mandatory/optional elements is performed, as there is a lack of rulebook.

4	Hello, when validating an SD-JWT VC, CC fails to process the "5.2.2.2 The x5t#o (X509 certificate digest) header parameter ", with the following error:
	
	The set/sequence of children must meet the requirements of the component schema. Children order and number DO NOT MATCH specification
	Specification: no children allowed
	Children found: digVal digAlg
	
	However, the digVal and digAlg are the required properties accrording to the schema:
	
	"x5t#o": {
	"type": "object",
	"properties": {
	"digAlg": {"type": "string"},
	"digVal": {"type": "string", "contentEncoding": "base64"}
	},
	"required": ["digAlg","digVal"],
	"additionalProperties": false
	},
	
	Could you please let us know whether the problem is within the CC or our signature?
	Imagen
	Imagen
			Solved	Indeed the CC had a problem with TS versions when dealing with this component, which was solved.

5	When validating a non-MDL mdoc with your online conformance checker, I get: ISO/IEC1801305 PID Conformance Checker for ISO/IEC 18013-5 PID Tool version: 1.1 (May 2026) 138.Error Tool Location-{CodeTest}: org.iso.23220.1[portrait].elementValue-{ProperUnderlyingSyntaxObject} The object under test must be supported by the syntax object that its specification requires. This component must be supported by a CBORString, however, in this case it is supported by a AuthleteCBORByteArray	MDOC-PuBEAA-10.cbor	Solved	
6	Hi! We are trying to test our files with your Beta EAA checker, but we get the following error: Run error Tool Location-{CodeTest}: root.JWS_COMPACT.sdjwtvc-{RunErrorDetected}	JV-EAA-6.json JV-EAA-8.json	Solved	CC created unprotected header even if there were no disclosures (JV-EAA-6.json). This created an undesired behaviour, which has been fixed

	An execution error has occurred. Contact developer. Further details: An exception has occurred while an instance of SDJWTIndividualSigChecker was executing its check. Notify to developer. Details follow: No value present If possible, we would like to know more about the cause of the error. Please let us know if you need any additional information regarding this! I have attached a sample file to reproduce.			
7	here is a file containing a bstr portait variable, in case it helps for debugging purposes. It also gets the AuthleteCBORByteArray on PID ISO validation. Please ignore the other errors as it is just a testfile and not made to upload to the conformance tests		Solved	Problems with their COSE_Sig1: "Details: Error while trying to create the COSESign1. Details: kid (4) must be a byte string." They modified that and the CC worked fine
8	According to ISO/IEC 18013-5, an "expiry_date" data element can be encoded either as "tdate" or "full-date" (see attachment). Same applies within the PID rulebook. However, mdoc PID CC seems to expect the "expiry_date" to be of "full-date" type, requiring the corresponding 1004 tag. I think this is incorrect and "expiry_date" of tdate type (i.e. tagged with 0) shall be allowed too.		Pending	This issue shall be fixed asap
9	Both vct and vct#integrity must be present. None of them are present. Even though the EAA payload incorporates both values (see screenshot): "vct": "urn:eudi:eaa:1", "vct#integrity": "sha256-LHeAW/pku/C49aIZ77sqyXiQms8+rsxPlfFew6E9mwY=", Is it a problem within the claims or an error in CC ?		Pending	This issue shall be fixed asap

8 EAA Plugtests Interoperability Testing

8.1 Positive test cases

8.1.0 Introduction

The Plugtests team has produced a set of testcases, requesting to generate EAA built on SD-JWT VC (JSON) or on ISO/IEC 18013-5 (MDL or MDOC). The main scope of the Plugtests will be testing EAAs profiles specified in TS 119 472-1, considering both EEAs, QEAAs and Pub-EAAs, based on SD-JWT VC and on ISO/IEC-mdoc,

The testcases a named according to the following notation:

- **SJV**: for indicating that the file to be generated contains a SD-JWT VC EAA.
- **MDL**: for indicating that the file to be generated contains a mdL.
- **MDOC**: for indicating that the file to be generated contains an EAA (different than an mdL) built on the syntax defined in ISO/IEC 18013-5.

The Testcases are categorised for the following EAA Formats

- **QEAA**: for indicating that the file to be generated contains a qualified EAA.
- **PuBEAA**: for indicating that the file to be generated contains an EAA issued by or on behalf of a public body responsible for an authentic source.
- **EAA**: for indicating that the file to be generated contains an EAA that is neither qualified nor issued by or on behalf of a public body responsible for an authentic source (non QEEA hereinafter).

In the 'positive test' participants will do following:

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

8.1.1 SD-JWT VC EAA

- SJV-EAA-1

Description
Mandatory elements, without selective disclosures; without key binding; WITH: . signing certificate in x5c. . iss . issuing_authority

. given_name . family_name	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority given_name family_name

- SJV-EAA-2

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . sub . given_name . family_name . cnf with jwk component	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority sub given_name family_name cnf (contains a jwk element)

- SJV-EAA-3

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id . sub . given_name . family_name . cnf with jwk component

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id sub given_name family_name cnf (contains a jwk element)

- SJV-EAA-4 (pseudonym)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id . also_known_as . cnf with jwk component	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id also_known_as cnf (contains a jwk element)

- SJV-EAA-5 (oneTime)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id . sub . given_name . family_name . oneTime . cnf with jwk component

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id sub given_name family_name oneTime cnf (contains a jwk element)

- SJV-EAA-6 (ShortLived)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id . sub . given_name . family_name . shortLived . cnf with jwk component	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id sub given_name family_name shortLived cnf (contains a jwk element)

- SJV-EAA-7

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id . sub . given_name . family_name . cnf with jwk component . iat

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg	vct vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id sub given_name family_name cnf (contains a jwk element) iat

- SJV-EAA-8

Description
Mandatory elements only, and non-recursive selective disclosures only of JSON Objects

- SJV-EAA-9

Description
Mandatory elements only, and non-recursive selective disclosures only of JSON Arrays elements

- SJV-EAA-10

Description
Mandatory elements only, and non-recursive selective disclosures of both JSON Objects and JSON Arrays elements

- SJV-EAA-11

Description
Mandatory elements only, and recursive selective disclosures only of JSON Objects

- SJV-EAA-12

Description
Mandatory elements only, and recursive selective disclosures only of JSON Array Elements

- SJV-EAA-13

Description
Mandatory elements only, and recursive selective disclosures of both JSON Objects and JSON Array elements

8.1.2 SD-JWT VC QEAA

- SJV-QEAA-1

Description
Mandatory elements, without selective disclosures; without key binding; WITH: . signing certificate in x5c. . iss . issuing_authority

. iss_reg_id (if applicable and not in Q cert) . given_name . family_name	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) given_name family_name

- SJV-QEAA-2

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . sub . given_name . family_name . cnf with jwk component . status	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) sub given_name family_name cnf (contains a jwk element) status

- SJV-QEAA-3

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . cnf with jwk component . status

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country sub given_name family_name cnf (contains a jwk element) status

- SJV-QEAA-4 (pseudonym)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . also_known_as . cnf with jwk component . status	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country also_known_as cnf (contains a jwk element) status

- SJV-QEAA-5 (oneTime)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . oneTime . cnf with jwk component . status

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country sub given_name family_name oneTime cnf (contains a jwk element) status

- SJV-QEAA-6 (ShortLived)

Description
Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . shortLived . cnf with jwk component

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country sub given_name family_name shortLived cnf (contains a jwk element)

- SJV-QEAA-7

Description
Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . cnf with jwk component . iat . status

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id sub given_name family_name cnf (contains a jwk element) iat status

8.1.3 SD-JWT VC PuB-EAA

- SJV-PuBEAA-1

Description Mandatory elements, without selective disclosures; without key binding; WITH: . signing certificate in x5c. . iss . issuing_authority . iss_reg_id (if applicable and not in Q cert) . given_name . family_name	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) given_name family_name

- SJV-PuBEAA-2

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . sub . given_name . family_name . cnf with jwk component . status

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) sub given_name family_name cnf (contains a jwk element) status

- SJV-PUBEAA-3

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . cnf with jwk component . status	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country sub given_name family_name cnf (contains a jwk element) status

- SJV-PUBEAA-4 (pseudonym)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . also_known_as . cnf with jwk component . status

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country also_known_as cnf (contains a jwk element) status

- SJV-PUBEAA-5 (oneTime)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . oneTime . cnf with jwk component . status	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	category (as byTS 119 472-1) vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country sub given_name family_name oneTime cnf (contains a jwk element) status

- SJV-PUBEAA-6 (ShortLived)

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . shortLived . cnf with jwk component

Protected Header	Payload
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	vct vct#integrity nbf exp iss issuing_authority (if NOT in the qualified certificate) iss_reg_id (if applicable and NOT in the qualified certificate) issuing_country sub given_name family_name shortLived cnf (contains a jwk element)

- SJV-PUBEAA-7

Description Mandatory elements, without selective disclosures; WITH: . signing certificate in x5c. . iss . issuing_authority . issuing_country . iss_reg_id (if applicable and not in Q cert) . sub . given_name . family_name . cnf with jwk component . iat . status	
Protected Header	**Payload**
x5c typ (=dc+sd-jwt) alg x5u x5t#S256	vct#integrity nbf exp iss issuing_authority issuing_country iss_reg_id sub given_name family_name cnf (contains a jwk element) iat status

8.1.4 ISO-mdL (ISO-mdoc EAA for mdL)

- Test cases incorporating components defined in ETSI TS 119 472-1 clause 6.
- This defines ISO-mdoc QEAA different than mdL ISO-mdoc QEAA shall be an instance of IssuerSigned type as per section 10.3.3 of ISO 18013-5, clause 8.3.2.1.2.2

- MDL-EAA-1

Description . Mandatory elements as per section 7.2 of ISO 18013-5.

. Only mandatory elements in IssuerAuth as per section 9.1.2.4 of ISO 18013-5		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3 given_name birth_date issue_date expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign		

- MDL-EAA-2

Description Addition to validityInfo of optional element EAA-1 + expectedUpdate child of validityInfo . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . validityInfo with expectedUpdate child		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil .expectedUpdate		
NameSpace		
namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3 family_name given_name birth_date issue_date		

expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign

- MDL-EAA-3

Description Test cases with different contents of deviceKeyInfo EAA-1 + deviceKeyInfo.keyAuthorizations.nameSpaces . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . deviceKeyInfo with keyAuthorizations.nameSpaces descendant		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) .keyAuthorizations .nameSpaces docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign		

- MDL-EAA-4

Description Test cases with different contents of deviceKeyInfo EAA-1 + deviceKeyInfo.keyAuthorizations.dataElements . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . deviceKeyInfo.keyAuthorizations with dataElements child

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) .keyAuthorizations .dataElements docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign		

- MDL-EAA-5

Description Test cases with different contents of deviceKeyInfo EAA-1 + deviceKeyInfo.keyAuthorizations .dataElements and .nameSpaces . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . deviceKeyInfo.keyAuthorizations with nameSpaces and dataElements children		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) .keyAuthorizations .nameSpaces .dataElements docType (the type assigned to mdL) validityInfo .signed		

.validFrom .validUntil
NameSpace **namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign

- MDL-EAA-6

Description EAA-1 + MSO.status.identifier_list . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5 .status.identifier_list		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil status .status_list		
NameSpace **namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign		

- MDL-EAA-7

Description EAA-1 + Optional elements in section 7.2 of ISO 18013-5 . Mandatory and some Optional elements as per section 7.2.1 of ISO 18013-5. . Only mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes).Namespace(="org.iso.18013.5.1") Section 10.3.3** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority document_number portrait driving_privileges un_distinguishing_sign birth_place		

8.1.5 ISO-mdoc EAA(no mdL)

- Test cases incorporating components defined in ETSI TS 119 472-1 clause 6.
- This defines ISO-mdoc EAA different than mdL ISO-mdoc EAA shall be an instance of IssuerSigned type as per section 10.3.3 of ISO 18013-5, clause 8.3.2.1.2.2

- MDOC-EAA-1

Description . Mandatory elements as per section 7.2 of ISO 18013-5. . Only mandatory elements in IssuerAuth as per section 9.1.2.4 of ISO 18013-5 . Mandatory components of TS 119 472-1 . Some optional components of TS 119 472-1

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2)		

- MDOC-EAA-2

Description Additions to claims set MDOC-EAA-1 + iss_reg_id (TS 119 472-1 clause 6.2.4.2). Issuer:legal entity and registration identifier applicable . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . validityInfo with expectedUpdate child		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom		

.validUntil .expectedUpdate
NameSpace
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) iss_reg_id

- MDOC-EAA-3

Description EAA with pseudonym MDOC-EAA-1 - given_name - family_name - document_number + also_knwon (TS 119 472-1 clause 6.2.5.1).		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** issue_date expiry_date		

issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) also_known_as

- MDOC-EAA-4

Description Onte-time use EAA MDOC-EAA-1 + oneTime (TS 119 472-1 clause 6.28.2).		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) oneTime		

- MDOC-EAA-5

Description Short-Lived EAA MDOC-EAA-1 + shortLived (TS 119 472-1 clause 6.28.2).

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2)		

- MDOC-EAA-6

Description		
Test cases with MDOC-EAA-1 + deviceKeyInfo.keyAuthorizations.nameSpaces . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . deviceKeyInfo with keyAuthorizations.nameSpaces descendant		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		

NameSpace
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2)

- MDOC-EAA-7

Description different contents MDOC-EAA-1 + deviceKeyInfo.keyAuthorizations.dataElements . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . deviceKeyInfo.keyAuthorizations with dataElements child		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) .keyAuthorizations .dataElements docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived**		

family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2)

- MDOC-EAA-8

Description of deviceKeyInfo MDOC-EAA-1 + deviceKeyInfo.keyAuthorizations .dataElements and .nameSpaces . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . deviceKeyInfo.keyAuthorizations with nameSpaces and dataElements children		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) .keyAuthorizations .nameSpaces .dataElements docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2)		

- MDOC-EAA-9

Description
MDOC-EAA-1 + MSO.status.identifier_list
. Mandatory elements as per section 7.2.1 of ISO 18013-5.

. Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5

.status.identifier_list

Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	

Payload #6.24 (bstr .cbor MobileSecurityObject)
version ("1.0")
digestAltorithm
valueDigests
deviceKeyInfo
  .deviceKey(COSE_Key with public key of wallet)
docType (the type assigned to mdL)
validityInfo
  .signed
  .validFrom
  .validUntil
status
  .status_list

NameSpace
namespaces(attributes)
.Namespace(="org.iso.23220.1")
Section 10.3.3; for the components defined there.

.Namespace(="org.etsi.01947201.010101) for elements:
  category
  iss_reg_id
  also_known_as
  oneTime
  status_service
  shortLived
family_name
given_name
birth_date
issue_date
expiry_date
issuing_country
issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2)
document_number
(as specified in section 6.3 of ISO/IEC 23220-2)

- MDOC-EAA-10

Description
MDOC-EAA-1 + Optional elements in section 7.2 of ISO 18013-5
. Mandatory and some Optional elements as per section 7.2.1 of ISO 18013-5.

. Only mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2)		

8.1.6 ISO-mdoc QEAA(no mdL)

- Test cases incorporating components defined in ETSI TS 119 472-1 clause 6.
- This defines ISO-mdoc QEAA different than mdL ISO-mdoc QEAA shall be an instance of IssuerSigned type as per section 10.3.3 of ISO 18013-5, clause 8.3.2.1.2.2

- MDOC-QEAA-1

Description
. Mandatory elements as per section 7.2 of ISO 18013-5. . Only mandatory elements in IssuerAuth as per section 9.1.2.4 of ISO 18013-5 . Mandatory components of TS 119 472-1 . Mandatory category component identifying the QEAA as a QEAA . Some optional components of TS 119 472-1

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:qualified")		

- MDOC-QEAA-2

Description Additions to claims set MDOC-QEAA-1 + iss_reg_id (TS 119 472-1 clause 6.2.4.2). Issuer:legal entity and registration identifier applicable . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . validityInfo with expectedUpdate child		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed		

.validFrom .validUntil .expectedUpdate
NameSpace
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:qualified") iss_reg_id

- MDOC-QEAA-3

Description QEAA with pseudonym MDOC-QEAA-1 - given_name - family_name - document_number + also_knwon (TS 119 472-1 clause 6.2.5.1).		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** issue_date		

expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:qualified") also_known_as

- MDOC-QEAA-4

Description One-time use QEAA MDOC-QEAA-1 + oneTime (TS 119 472-1 clause 6.28.2).		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:qualified") oneTime		

- MDOC-QEAA-5

Description Short-Lived QEAA MDOC-QEAA-1 + shortLived (TS 119 472-1 clause 6.28.2).

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:qualified") shortLived		

8.1.7 ISO-mdoc PuB-EAA(no mdL)

- Test cases incorporating components defined in ETSI TS 119 472-1 clause 6.
- This defines ISO-mdoc PuB-EAA different than mdL ISO-mdoc PuB-EAA shall be an instance of IssuerSigned type as per section 10.3.3 of ISO 18013-5, clause 8.3.2.1.2.2

- MDOC-PUBEAA-1

Description
. Mandatory elements as per section 7.2 of ISO 18013-5. . Only mandatory elements in IssuerAuth as per section 9.1.2.4 of ISO 18013-5 . Mandatory components of TS 119 472-1 . Mandatory category component identifying the PuB-EAA as a PuB-EAA . Some optional components of TS 119 472-1

Protected Header	CWT-claims	Signature
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:pub)		

- MDOC-PUBEAA-2

Description		
Additions to claims set MDOC-PuBEAA-1 + iss_reg_id (TS 119 472-1 clause 6.2.4.2). Issuer:legal entity and registration identifier applicable . Mandatory elements as per section 7.2.1 of ISO 18013-5. . Mandatory elements in IssuerAuth as per section 12.3.3 of ISO 18013-5. . validityInfo with expectedUpdate child		
Protected Header	**CWT-claims**	**Signature**
alg (1) x5chain (33)	iat (6)	
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed		

.validFrom .validUntil .expectedUpdate
NameSpace
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:pub) iss_reg_id

- MDOC-PUBEAA-3

Description PuB-EAA with pseudonym MDOC-PuBEAA-1 - given_name - family_name - document_number + also_knwon (TS 119 472-1 clause 6.2.5.1).		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject)		
version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace		
namespaces(attributes) **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** issue_date		

expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:pub) also_known_as

- MDOC-PUBEAA-4

Description One-time use PuB-EAA MDOC-PuBEAA-1 + oneTime (TS 119 472-1 clause 6.28.2).		
Protected Header alg (1) x5chain (33)	**CWT-claims** iat (6)	**Signature**
Payload #6.24 (bstr .cbor MobileSecurityObject) version ("1.0") digestAltorithm valueDigests deviceKeyInfo .deviceKey(COSE_Key with public key of wallet) docType (the type assigned to mdL) validityInfo .signed .validFrom .validUntil		
NameSpace **namespaces(attributes)** **.Namespace(="org.iso.23220.1")** **Section 10.3.3; for the components defined there.** **.Namespace(="org.etsi.01947201.010101) for elements:** **category** **iss_reg_id** **also_known_as** **oneTime** **status_service** **shortLived** family_name given_name birth_date issue_date expiry_date issuing_country issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2) document_number (as specified in section 6.3 of ISO/IEC 23220-2) category ("urn:etsi:esi:eaa:eu:pub) oneTime		

- MDOC-PUBEAA-5

Description Short-Lived PuB-EAA MDOC-PuBEAA-1 + shortLived (TS 119 472-1 clause 6.28.2).

<table>
<tr><th>Protected Header</th><th>CWT-claims</th><th>Signature</th></tr>
<tr><td>alg (1)
x5chain (33)</td><td>iat (6)</td><td></td></tr>
<tr><td colspan="3">Payload #6.24 (bstr .cbor MobileSecurityObject)
version ("1.0")
digestAltorithm
valueDigests
deviceKeyInfo
.deviceKey(COSE_Key with public key of wallet)
docType (the type assigned to mdL)
validityInfo
.signed
.validFrom
.validUntil</td></tr>
<tr><td colspan="3">NameSpace
namespaces(attributes)
.Namespace(="org.iso.23220.1")
Section 10.3.3; for the components defined there.

.Namespace(="org.etsi.01947201.010101) for elements:
category
iss_reg_id
also_known_as
oneTime
status_service
shortLived
family_name
given_name
birth_date
issue_date
expiry_date
issuing_country
issuing_authority_unicode (as specified in clause 6.3 of ISO/IEC 23220-2)
document_number
(as specified in section 6.3 of ISO/IEC 23220-2)
category("urn:etsi:esi:eaa:eu:pub)"
shortLived</td></tr>
</table>

8.2 Negative test cases

8.2.0 Introduction

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

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

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

8.2.1 SD-JWT VC EAA Negative Test Cases

- SJV-EAAN-1
  - Description
    Malformed JWT because vct#integrity claim is missing

- SJV-EAAN-2
  - Description
    Duplicate JSON keys and conflicting values

- SJV-EAAN-3
  - Description
    EAA doesn't incorporate technical validity period

- SJV-EAAN-4
  - Description
    EAA incorporates both the EAA short-lived component and the EAA status service.

- SJV-EAAN-5
  - Description
    Tampered payload – invalid signature, valid token modified after signing altering a claim

- SJV-EAAN-6
  - Description
    Malformed JWT including wrong elements (wrong typ value)

- SJV-EAAN-7
  - Description
    Expired credential, credential has expired in the past.

- SJV-EAAN-8
  - Description
    Status check unavailable (fail-open vs fail-closed), status service returns 5xx or network outage.

- SJV-EAAN-9
  - Description
    Malformed JWT including wrong elements (wrong field name in payload).

- SJV-EAAN-10
  - Description
    JWT – Schema/namespace mismatch, verifier expects a specific schema/namespace; credential uses different one.

    1) Present credential with wrong schema identifier or namespace.

    2) Verify schema validation behavior

- SJV-EAAN-11
  - Description
    EAA with a disclosure without having the corresponding digest in the payload. The disclosure may be an object or an element of an array.

- SJV-EAAN-12
  - Description
    EAA with some mandatory PID elements not present

8.2.2 SD-JWT VC QEAA Negative Test Cases

- SJV-QEAAN-1
  - Description
    Mandatory elements, without selective disclosures; without key binding; with wrong EAA category that's different from

    - urn:etsi:esi:eaa:eu:qualified (QEAA)

    - urn:etsi:esi:eaa:eu:pub (Pub-EAA)
- SJV-QEAAN-2
  - Description
    Mandatory elements, without selective disclosures; with the issuer identifier fields including an identifier of a non-EU Member State
- SJV-QEAAN-3
  - Description
    Mandatory elements, without selective disclosures; without the issuer identifier fields
- SJV-QEAAN-4
  - Description
    Mandatory elements, without selective disclosures;
    without including either the EAA subject identifier or the pseudonym of the EAA subject.
- SJV-QEAAN-5
  - Description
    Mandatory elements, without selective disclosures;
    without including either the EAA short-lived component or the EAA status service.
- SJV-QEAAN-6
  - Description
    Mandatory elements, without selective disclosures;
    WITH:
    a digital signature that is not a qualified electronic signature or a qualified electronic seal

8.2.3 SD-JWT VC PuB-EAA Negative Test Cases

- SJV-PuBEAAN-1
  - Description
    Mandatory elements, without selective disclosures; without key binding; with wrong EAA category that's different from

- urn:etsi:esi:eaa:eu:qualified (QEAA)
- urn:etsi:esi:eaa:eu:pub (Pub-EAA)

- SJV-PuBEAAN-2
  - Description
    Mandatory elements, without selective disclosures; with the issuer identifier fields including an identifier of a non-EU Member State
- SJV-PuBEAAN-3
  - Description
    Mandatory elements, without selective disclosures; without the issuer identifier fields
- SJV-PuBEAAN-4
  - Description
    Mandatory elements, without selective disclosures;
    without including either the EAA subject identifier or the pseudonym of the EAA subject.
- SJV-PuBEAAN-5
  - Description
    Mandatory elements, without selective disclosures;
    without including either the EAA short-lived component or the EAA status service.
- SJV-PuBEAAN-6
  - Description
    Mandatory elements, without selective disclosures;
    WITH:
    a digital signature that is not a qualified electronic signature or a qualified electronic seal

Change History

Document history		
1.0	1 July 2026	First version