DRAFT ETSI TS 119 472-1 V0.0.6 (2025-01)

Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestations of Attributes; Part 1: General requirements

Reference
DTS/ESI-0019472-1

Keywords
Attribute Attestation, digital identity, EUDI Wallet, trust services

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document:

1) Specifies a data model (semantics) for Electronic Attestations of Attributes, a new object defined by the "REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework" [22] (clause 4).

2) Defines data model (semantics) requirements for two types of Electronic Attestations of Attributes, namely: the Qualified Attestations of Attributes, and the Electronic Attestations of Attributes issued by or on behalf of a public body responsible for an authentic source, also defined in [22] (clause 4).

3) Defines 6 realizations for the former data model. These realizations include, wherever needed, specific requirements for the Qualified Attestations of Attributes, and the Electronic Attestations of Attributes issued by or on behalf of a public body responsible for an authentic source, defined in [22], particularized for the different realizations. Below follow the list of realizations:

   a) Realization based on SD-JWT VC (clause 5). SD-JWT VC is specified in IETF SD-JWT: "Selective Disclosure for JWTs (SD-JWT)" [6].

   b) Realization based on SD-JWT VC DM (clause 6). SD-JWT VC DM is, at the moment of writing the present draft, partially specified in SD-JWT VC DM [28].

NOTE 1: This realization will be developed when a complete specification is publicly available for SD-JWT VC DM.

   c) Realization based on ISO/IEC 18013-5: "Personal identification – ISO – compliant driving licence – Part 5: Mobile driving licence (mDL) application" [17] (clause 7).

   d) Realization based on W3C Verifiable Credentials Data Model (clause 8). W3C Verifiable Credentials Data Model is specified in W3C Candidate Recommendation Draft (19 October 2024): "Verifiable Credentials Data Model v2.0" [1].

   e) Realization based on X.509 Attribute Certificates (clause 9). X.509 Attribute Certificates are specified in RFC 5755: "An Internet Attribute Certificate Profile for Authorization" [10].

   f) Realization of hybrid Electronic Attestations of Attributes (clause 10).

NOTE 2: This realization is not developed yet.

4) Aims to support the EU Commission Decision "COMMISSION IMPLEMENTING REGULATION (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets" [i.5].

NOTE 3: The present document supports, in its clauses 7 and 8, the encoding of person identification data attributes as required in [i.5], Annex I, section 4.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] W3C Candidate Recommendation Draft (19 October 2024): "Verifiable Credentials Data Model v2.0".

NOTE 1: Available at https://www.w3.org/TR/vc-data-model/ - what-is-a-verifiable-credential.

[2] IETF SD-JWT VC: "SD-JWT-based Verifiable Credentials (SD-JWT VC) draft-ietf-oauth-sd-jwt-vc-03".

[3] OASIS Standard SAML 2.0: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", 15 March 2005.

NOTE 2: Available at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[4] OASIS Approved Errata SAML 2.0: "SAML Version 2.0 Errata 05", 01 May 2012.

NOTE 3: Available at http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.pdf.

[5] IETF RFC 7519: "JSON Web Token (JWT)", May 2015.

[6] IETF SD-JWT: "Selective Disclosure for JWTs (SD-JWT)", June 2023; expires January 2024.

NOTE 4: Available at https://datatracker.ietf.org/doc/html/rfc7519.

[7] OpenID Core 1.0: "OpenID Connect Core 1.0 incorporating errata set 1".

NOTE 5: Available at https://openid.net/specs/openid-connect-core-1_0.html.

[8] OpenID Verifiable Presentations: "OpenID Connect for Verifiable Presentations". Internet-Draft December 2021.

NOTE 6: Available at https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0-07.html - name-vp_token.

NOTE 7: This is an specification which is, at present, under review process, and shall be voted from 1/2/2022 to 8/2/2022 .

[9] OpenID Presentation Exchange: "Presentation Exchange 2.0.0". Working Group Draft.

[10] IETF RFC 5755: "An Internet Attribute Certificate Profile for Authorization". January 2010.

[11] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile". March 2004.

[12] Recommendation ITU-T X.680-X.683: "Information technology - Abstract Syntax Notation One (ASN.1)".

[13] IETF RFC 7515: "JSON Web Signature (JWS)", May 2015.

[14] IETF RFC 5280: "PKIX Certificate and CRL Profile". May 2008.

[15] W3C Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes". April 2012.

[16] ETSI TS 119 182: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[17] ISO/IEC 18013-5: "Personal identification – ISO – compliant driving licence – Part 5: Mobile driving licence (mDL) application".

[18] ISO/IEC 23220-1: "Cards and security devices for personal identification – Building blocks for identity management via mobile devices - Part 1: Generic system architectures of mobile eIDS systems".

[19] ISO/IEC 23220-2: "Cards and security devices for personal identification – Building blocks for identity management via mobile devices - Part 2: Data objects and encoding rules for generic eID-System".

[20] ISO/IEC 23220-3: "Cards and security devices for personal identification – Building blocks for identity management via mobile devices - Part 3: Protocols and services for installation and issuing phase".

[21] ISO/IEC 23220-4: "Cards and security devices for personal identification – Building blocks for identity management via mobile devices - Part 4: Protocols and services for operational phase".

[22] REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[23] IETF RFC 78000: "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)". April 2016.

[24] OpenID Connect for Identity Assurance Claims Registration 1.0.

[25] ISO 3166-1:2020: "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes".

[26] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[27] RFC 1779: "A String Representation of Distinguished Names", March 1995.

[28] SD-JWT VC DM: "SD-JWT VC DM Credential Format" (https://github.com/danielfett/sd-jwt-vc-dm?tab=readme-ov-file).

[29] draft-ietf-rats-eat-30: "The Entity Attestation Token (EAT)" (https://datatracker.ietf.org/doc/draft-ietf-rats-eat/30/).

[30] OpenID CC 1.0: "OpenID Connect Core 1.0 incorporating errata set" (https://openid.net/specs/openid-connect-core-1_0.html - ClaimsLanguagesAndScripts).

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 119 471:" Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Electronic Attestation of Attributes Services".

[i.2] ETSI TS 119 462:" Electronic Signatures and Infrastructures (ESI); Wallet interfaces for trust services and signings".

[i.3] W3C Candidate Recommendation: "Bitstring Status List v1.0" June 2024".

[i.4] ETSI TS 119 612: " Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists".

[i.5] EU Commission Decision "COMMISSION IMPLEMENTING REGULATION (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms and definitions given in ETSI TS 119 471:" Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Electronic Attestation of Attributes Services [i.1], and the following terms and definitions apply:

NOTE 1: For the sake of completeness, for facilitating its review, the present clause incorporates some definitions given in clause 3.1 of ETSI TS 119 471 [i.1]. These definitions are signalled by a note. These definitions will be deleted in the final version.

Attribute: characteristic, quality, right or permission of a natural or legal person or of an object.

NOTE 2: As per eIDAS2 definition [i.1].

NOTE 3: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Attribute(s) subject: natural, legal person or entity the attribute(s) is(are) referring to**.**

NOTE 4: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Electronic attestation of attributes (EAA): an attestation in electronic form that allows the authentication of attributes.

NOTE 5: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Electronic attestation of attributes context: the information, additional to the electronic attestation of attributes itself, that the relying party may require for being fully able to process it.

Electronic attestation of attributes Presentation (EAAP): TBD.

Electronic attestation of attributes trust service provider (EAASP): natural or a legal person who provides one or more EAA services either as a qualified or as a non-qualified trust service provider.

NOTE 6: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Electronic attestation of attributes subscriber (EAA Subscriber): natural or legal person bound by agreement with an Electronic Attestation of Attributes service provider to any subscriber obligations.

NOTE 7: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Electronic attestation of attributes subject (EAA Subject): natural or legal person that holds the Electronic Attestation of Attributes.

NOTE 8: As per eIDAS definition [i.2]

NOTE 9: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

European Digital Identity Wallet: electronic identification means, which allows the user to securely store, manage and validate identity data and electronic attestations of attributes, to provide them to relying parties and to other users of

European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.

NOTE 10: As per eIDAS2 definition [i.1].

NOTE 11: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Qualified electronic attestation of attributes (EU-QEAA): electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V of eIDAS2 Regulation [i.1].

NOTE 12: As per eIDAS2 definition [i.1].

NOTE 13: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

Qualified electronic attestation of attribute services provider (QEAASP): electronic attestation of attribute services provider who is granted the qualified status by an EU National Supervisory Authority.

NOTE 14: As per eIDAS2 definition [i.1]

NOTE 15: Definition taken from clause 3.1 of ETSI TS 119 471 [i.1]. This definition shall be deleted in the final version of the present document.

3.2 Abbreviations

For the purposes of the present document, the followingabbreviations apply:

EAA Electronic Attestation of Attributes

EAAP Electronic Attestation of Attributes Presentation

EAASP Electronic Attestation of Attributes Trust Service Provider

EU-EAA-PubA Electronic Attestation of Attributes issued by or on behalf of a public body responsible for an authentic source, according to "REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework" [22]

EU-QEAA Qualified Electronic Attestation of Attributes as defined in "REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework" [22]

SD-JWT Selective Disclosure based JSON Web Token

SD-JWT VC Selective Disclosure based JSON Web Token Verifiable Credentials

SD-JWT VC EAA EAA implemented with IETF SD-JWT VC [2] as specified in the present document

SD-JWT VC EU-EAA-PubA EU-EAA-PubA implemented with IETF SD-JWT VC [2] as specified in the present document

SD-JWT VC EU-QEAA EU-QEAA implemented with IETF SD-JWT VC [2] as specified in the present document

SD-JWT VC DM Selective Disclosure based JSON Web Token Verifiable Credentials Data Model [28]

SD-JWT VC DM EAA EAA implemented with SD-JWT VC DM [28] as specified in the present document

SD-JWT VC DM EU-EAA-PubA EU-EAA-PubA implemented with SD-JWT VC DM [28] as specified in the present document

SD-JWT VC DM EU-QEAA EU-QEAA implemented with SD-JWT VC DM [28] as specified in the present document

ISO/IEC 18013-5 EAA EAA implemented with ISO/IEC 18013-5 [17] as specified in the present document

ISO/IEC 18013-5 EU-EAA-PubA EU-EAA-PubA implemented with ISO/IEC 18013-5 [17] as specified in the present document

ISO/IEC 18013-5 EU-QEAA EU-QEAA implemented with ISO/IEC 18013-5 [17] as specified in the present document

URI Uniform Resource Identifier

URN Uniform Resource Name

W3C-VC W3C Verifiable Credentials

W3C-VC EAA EAA implemented with Verifiable Credentials Data Model v2.0 [1] as specified in the present document

W3C-VC EU-EAA-PubA EU-EAA-PubA implemented with Verifiable Credentials Data Model v2.0 [1] as specified in the present document

W3C-VC EU-QEAA EU-QEAA implemented with Verifiable Credentials Data Model v2.0 [1] as specified in the present document

X.509-AC X.509 Attribute Certificate

X.509-AC EAA EAA implemented with RFC 5755: "An Internet Attribute Certificate Profile for Authorization" [10] as specified in the present document

X.509-AC EU-EAA-PubA EU-EAA-PubA implemented with RFC 5755 [10] as specified in the present document

X.509-AC EU-QEAA EU-QEAA implemented with RFC 5755 [10] as specified in the present document

3.3 Notation

The present document assigns one identifier for each requirement.

General requirements for EAAs (including generally applicable requirements for Qualified EAAs and EAAs issued by or on behalf of a public body responsible for an authentic source) are assigned identifiers resulting from the concatenation of the following components:

1) The initial string "EAA-".

2) The number of the clause where the requirement is defined.

3) A number of 2 digits. In each clause the number will start in 01 and it will increase in one unity for each requirement.

Wherever it is required, the present document defines specific requirements only applicable to Qualified Electronic Attestation of Attributes, as defined in Annex V of “REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework" [22]. The present document refers to this type of EAAs either as "EU Qualified EAA" or by the abbreviation EU-QEAA.

Some of these specific requirements for EU-QEAA may replace general EAAs requirements (those ones whose identifiers start with "EAA-") already defined.

These requirements are defined within specific clauses clearly identified with the title: "Requirements for EU Qualified Electronic Attestation of Attributes (EU-QEAA)".

The present document assigns an identifier for each of these requirements as per the concatenation of the following components:

1) The initial string "EU-QEAA-”.

2) The number of the clause where the requirement is defined.

3) A number of 2 digits. In each clause the number will start in 01 and it will increase in one unity for each requirement.

NOTE 1: Table 1of Annex D shows how the full set of requirements of Annex V of [22] are supported in the present document.

Wherever it is required, the present document defines specific requirements only applicable to Electronic Attestation of Attributes issued by or on behalf of a public body responsible for an authentic source, as defined in Annex VII of [22]. The present document refers to this type of EAAs either as "EU EAA issued by or on behalf of a public body responsible for an authentic source" or by the abbreviation EU-EAA-PubA.

Some of the requirements for EU-EAA-PubA may replace general requirements (those ones whose identifiers start with "EAA-") already defined.

These requirements are defined within specific clauses clearly identified with the title: "Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)".

The present document assigns an identifier for each of these requirements as per the concatenation of the following components:

1) The initial string "EU-EAA-PubA-".

2) The number of the clause where the requirement is defined.

3) A number of 2 digits. In each clause the number will start in 01 and it will increase in one unity for each requirement.

NOTE 2: Table 1of Annex D shows how the full set of requirements of Annex VII of [22] are supported in the present document.

4 Semantics of Electronic Attestation of Attributes

4.1 Introduction. Semantic areas for EAA

The present document specifies the semantics of EAA data as follows:

1) Clause 4.2 EAA metadata defines semantics for EAA metadata.

2) Clause 4.3 Attested attributes defines semantics for EAA data directly related with the incorporation of attested attributes.

3) Clause 4.4 defines semantics for attested attributes metadata.

4) Clause 4.5 defines semantics for the signature of the EAA and the EAA signing certificate.

4.2 EAA metadata

4.2.1 EAA Context

4.2.1.1 General requirements

EAA-4.2.1.1-01: The EAA context data shall identify the context where the EAA is issued.

NOTE: The EAA context allows to identify the entities implied in the EAA and the attributes attested.

EAA-4.2.1.1-02: An EAA may incorporate the EAA context.

EAA-4.2.1.1-03: The incorporation, value, and placement of the of the EAA context data shall depend on the specific EAA implementation.

4.2.1.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.2.1.2-01: Wherever applicable, an EU-QEAA shall include the indication of the scheme of attestations that the EU-QEAA is part of.

NOTE: This requirement meets the second part of requirement (f) in Annex V of [22] for EU-QEAA, which requires the presence of "(f) (..) and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of".

4.2.1.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-4.2.1.3-01: Wherever applicable, an EU-EAA-PubA shall include the indication of the scheme of attestations that the EU-EAA-PubA is part of.

NOTE: This requirement meets the second part of requirement (f) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(f) (..) and, if applicable, an indication of the scheme of attestations that the attestation of attributes is part of".

4.2.2 EAA type

4.2.2.1 Introduction

The next sub-clauses of 4.2.2 define:

1) General requirements for the identification of the type of an EAA (clause 4.2.2.2).
2) Requirements for mechanisms to be used for signalling that the EAA is an EU-QEAA (clause 4.2.2.3).
3) Requirements for mechanisms to be used for signalling that the EAA is an EU-EAA-PubA (clause 4.2.2.4).

4.2.2.2 General requirements

EAA-4.2.2.2-01: This data shall indicate the type of the EAA.

EXAMPLE 1: In the context of the European Union, this component can indicate, for instance, that the EAA is a EU-QEAA, or an EU-EAA-PubA, which confers to the EAA special characteristics.

EAA-4.2.2.2-02: An EAA may incorporate the EAA type.

EAA-4.2.2.2-03: The incorporation, value, and placement of the EAA type data shall depend on the specific EAA implementation.

4.2.2.3 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.2.2.3-01: An EU-QEAA shall include an explicit signal of its condition of EU-QEAA.

EU-QEAA-4.2.2.3-02: For EU-QEAA realizations using URIs as identifiers, this signal shall be the following URN: `urn:etsi:eaa:eu:qualified`.

Editor's Note: Pending to request register to pnns@etsi.org

Editor's Note: Clause 9.2.2.2 of the present document defines an ASN.1 equivalent component for X.509-AC EU-QEAA. TO BE DECIDED: if such definition is moved to the present clause.

Editor's Note: TO BE DECIDED: if another identifier is required for indicating the country or set of countries under the legislation of which the Electronic Attestation of Attributes is issued as a Qualified Electronic Attestation of Attributes as it was specified for qualified certificates. If so, a new URN will be defined here, and a new `QEAA-Statement` will be defined in the implementation based on X.509 Attribute Certificate

EU-QEAA-4.2.2.3-03: The mechanism used for including the former URN within the EAA shall depend on the specific EAA implementation.

NOTE: These requirements meet the requirement (a) in Annex V of [22] for EU-QEAA, which requires the presence of "(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes".

4.2.2.4 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-4.2.2.4-01: An EU-EAA-PubA, shall include an explicit signal of its condition of EU-EAA-PubA.

EU-EAA-PubA-4.2.2.4-02: For EU-EAA-PubA realizations using URIs as identifiers, this signal shall be the following URN: `urn:etsi:eaa:eu:pubA`.

Editor's Note: Pending to request register to pnns@etsi.org

EU-EAA-PubA-4.2.2.4-03: The mechanism used for including the former URN within the EAA shall depend on the specific EAA implementation.

Editor's Note: Clause 9.2.2.3 of the present document defines an ASN.1 equivalent component for X.509-AC EU-EAA-PubA.

NOTE: These requirements meet the of requirement (a) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source".

4.2.3 The EAA identifier

EAA-4.2.3-01: The EAA identifier shall contain an identifier that allows to unambiguously identify the EAA itself.

EAA-4.2.3-02: An EAA shall incorporate the EAA identifier.

EAA-4.2.3-03: The incorporation, value, and placement of the EAA identifier shall depend on the specific EAA implementation.

NOTE: The requirements in the present clause meet the first part of requirement (f) in Annex V of [22] for EU-QEAA, which requires the presence of "(f) the attestation identity code, which must be unique for the qualified trust service provider".

NOTE: The requirements in the present clause meet the first part of requirement (e) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(f) the attestation identity code, which must be unique for the issuing public body".

4.2.4 EAA issuer identifier

4.2.4.1 General requirements

EAA-4.2.4.1-01: The EAA issuer identifier shall have a value that unambiguously identifies the EAA Trust Service Provider which issues the EAA.

EAA-4.2.4.1-02: An EAA shall incorporate the EAA issuer identifier.

EAA-4.2.4.1-03: The incorporation, value, and placement of the EAA issuer identifier shall depend on the specific EAA implementation.

EAA-4.2.4.1-04: The EAA may include an identifier of the EU Member State, in which the EAA issuer is stablished.

EAA-4.2.4.1-05: The value of the identifier of an EU Member State shall be the Alpha 2 characters country code as specified in ISO 3166-1:2020 [25] corresponding to this EU Member State.

EAA-4.2.4.1-06: If the issuer of the EAA is a legal person, the EAA may include a registration identifier as stated in the official records, where such a registration identifier exists.

EAA-4.2.4.1-07: If the issuer of the EAA is a legal person, the registration identifier may be expressed using the following structure for the corresponding character string in the presented order:

a) 3 characters legal person identity type reference, having one of the following defined values:

- "VAT" for identification based on a national value added tax identification number; or
- "NTR" for identification based on an identifier from a national register, e.g. a national trade register.

When both a national value added tax identification number and one (or more) other national identification number exist, the national value added tax identification number shall be used to identify the EAA issuer;

b) 2 characters ISO 3166-1:2020 [25] country code corresponding to the EU Member State where the EU-QEAA issuer is established;

c) hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and

d) identifier (according to country and identity type reference).

NOTE: the text in this requirement is a copy of the text in ETSI TS 119 612 clause 5.4.2 for identifying trust service providers in the EU Trusted Lists.

EAA-4.2.4.1-08: If the issuer of the EAA is a legal person, the EU-QEAA may include the name of this legal person.

EAA-4.2.4.1-09: If the issuer of the EAA is a natural person, the EU-QEAA may include the name of this natural person.

4.2.4.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.2.4.2-01: EU-QEAA shall include an identifier of the EU Member State, in which the QEAA issuer is stablished.

EU-QEAA-4.2.4.2-02: The value of the identifier of an EU Member State shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

EU-QEAA-4.2.4.2-03: If the issuer of the EU-QEAA is a legal person, the EU-QEAA shall include a registration identifier as stated in the official records, where such a registration identifier exists.

EU-QEAA-4.2.4.2-04: If the issuer of the EU-QEAA is a legal person, the registration identifier shall be expressed using the structure for the corresponding character string specified in requirement EAA-4.2.4.1-07 of the present document.

EU-QEAA-4.2.4.2-05: If the issuer of the EU-QEAA is a legal person, the EU-QEAA shall include the name of this legal person.

EU-QEAA-4.2.4.2-06: If the issuer of the EU-QEAA is a natural person, the EU-QEAA shall include the name of this natural person.

NOTE: These requirements meet requirement (b) in Annex V of [22] for EU-QEAA, which requires the presence of "(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and: (i) for a legal person: the name and, where applicable, registration number as stated in the official records; (ii) for a natural person: the person’s name".

4.2.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-4.2.4.3-01: EU-EAA-PubA shall include an identifier of the EU Member State, in which the public body is stablished.

EU-EAA-PubA-4.2.4.3-02: The value of the identifier of an EU Member State shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

EU-EAA-PubA-4.2.4.3-03: EU-EAA-PubA shall include the registration identifier of the public body, as stated in the official records, where such a registration identifier exists.

EU-EAA-PubA-4.2.4.3-04: If the registration identifier mentioned in requirement EU-EAA-PubA-4.2.4.3-03 exists, it shall be expressed using the structure for the corresponding character string specified in requirement EAA-4.2.4.1-07 of the present document.

EU-EAA-PubA-4.2.4.3-05: EU-EAA-PubA shall include the name of the public body that has issued it, or on behalf of which it has been issued.

NOTE: These requirements meet requirement requirement (b) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official record".

4.2.5 EAA and attribute subject identifiers and pseudonyms

4.2.5.1 Introduction

The present clause defines requirements on identifiers identifying the EAA subject and the attribute subjects.

The present clause also defines requirements on pseudonyms for the EAA subject and the attribute subjects.

4.2.5.2 The EAA subject identifier

EAA-4.2.5.2-01: An EAA shall include either the EAA subject identifier or the pseudonym of the EAA subject.

NOTE: This presence of the EAA subject can be provided by a component specifically defined for containing ONLY the EAA subject identifier, or by a component defined for containing the attribute subject identifier.

EXAMPLE: Implementations based on Verifiable Credentials Data Model v2.0 [1], only define a component for identifiers bound to sets of attributes. Each `id` field within each element of the `credentialSubject` array contains the identifier of the attribute subject referred by the attributes that are present within this array element. If the `credentialSubject` array has only one element, the value of this `id` field is the value of the EAA subject identifier. If the `credentialSubject` array has several elements, each `id` field contains one attribute subject identifier and the value of the EAA subject identifier is the value of one of these `id` fields. In any case, the EAA subject identifier is present within the EAA even if there is not a specific component allocated for containing only the EAA identifier value.

EAA-4.2.5.2-02: The incorporation, value, and placement of the EAA subject identifier shall depend on the specific EAA implementation.

4.2.5.3 The EAA subject pseudonym

EAA-4.2.5.3-01: The presence of the EAA subject pseudonym instead of the EAA subject identifier shall be clearly indicated.

EAA-4.2.5.3-02: The mechanism used for incorporating the EAA subject pseudonym within the EAA, shall depend on the specific EAA implementation.

4.2.5.4 The attribute subject identifier

EAA-4.2.5.4-01: The EAA shall bind each attribute either to the identifier or to the pseudonym of the entity (attribute subject) that this attribute refers to.

NOTE 1: In an EAA where all the attributes refer to the same entity, the attribute subject identifier and the EAA subject identifier are the same.

NOTE 2: In EAA containing several sets of attributes, each one referring to a different attribute subject, the EAA can bind each set of attributes to the identifier of the corresponding attribute subject using specific components defined for containing identifiers of subject attributes, as Verifiable Credentials Data Model v2.0 [1] does.

EAA-4.2.5.4-02: The incorporation, value, and placement of the attribute subject identifiers shall depend on the specific EAA implementation.

EXAMPLE: Implementations based on Verifiable Credentials Data Model v2.0 [1], only define fields for identifiers bound to sets of attributes. Each `id` field within each element of the `credentialSubject` array contains the identifier of the attribute subject referred by the attributes that are present within this array element.

4.2.5.5 The attribute subject pseudonym

EAA-4.2.5.5-01: An EAA may incorporate pseudonym(s) for attribute subject(s).

EAA-4.2.5.5-02: The mechanism used for incorporating the pseudonym(s) for attribute subject(s) within the EAA, shall depend on the specific EAA implementation.

EAA-4.2.5.5-03: The mechanism used for binding one attribute or a set of attributes to the pseudonym of the attribute subject, shall depend on the specific EAA implementation.

EAA-4.2.5.5-04: The presence of the pseudonym(s) for attribute subject(s) instead of identifier(s) for the attribute subject(s), shall be clearly indicated within the EAA.

4.2.5.6 Additional requirements

EAA-4.2.5.6-01: If the EAA contains several attribute subject identifiers, one of them shall be the the EAA subject identifier.

EAA-4.2.5.6-02: If the EAA contains attribute subject pseudonyms, does not contain any attribute subject identifier, and does not contain the EAA subject identifier, then the pseudonym of the EAA subject shall be one of the aforementioned pseudonyms.

4.2.5.7 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.2.5.7-01: All the attributes present within an EU-QEAA shall refer to one entity: the EAA subject.

NOTE: This requirement and requirement EAA-4.2.5.2-01 meet the requirement (c) in Annex V of [22] for EU-QEAA, which requires the presence of "(c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated".

4.2.5.8 Requirements for Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EAA-PubA-4.2.5.8-01: All the attributes present within EU-EAA-PubA shall refer to one entity: the EAA subject.

NOTE: This requirement and requirement EAA-4.2.5.2-01meet the requirement (c) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated".

4.2.6 EAA issuance time

4.2.6.1 General requirements

EAA-4.2.6.1-01: The EAA issuance time data shall unambiguously identify the instant when the EAA was issued.

EAA-4.2.6.1-02: An EAA may incorporate the EAA issuance time.

4.2.6.2 Time indication content

EAA-4.2.6.2-01: The EAA issuance time:

1) Shall be expressed as an instant time in Coordinated Universal Time (UTC).
2) Shall include indication of seconds, even when the number of seconds is zero.
3) Shall not include fractions of seconds.
4) Shall not use local offset from UTC.

EAA-4.2.6.2-02: The incorporation and placement of the EAA issuance time data shall depend on the specific EAA implementation.

4.2.7 EAA validity period

EAA-4.2.7-01: The EAA validity period data shall identify the time period while the EAA may be used.

EAA-4.2.7-02: An EAA shall incorporate the EAA validity period.

EAA-4.2.7-03: The EAA validity period shall be expressed by two instant times in Coordinated Universal Time (UTC).

EAA-4.2.7-04: The first instant time shall indicate the date and time when the EAA becomes valid.

EAA-4.2.7-05: The second instant time shall indicate the date and time when the EAA ceases to be valid.

EAA-4.2.7-06: The content of each instant time shall meet the requirements specified in clause 4.2.6.2 of the present document.

EAA-4.2.7-07: The incorporation and placement of the information on the EAA validity period shall depend on the specific EAA implementation.

NOTE: The requirements in the present clause meet the requirement (e) in Annex V of [22] for EU-QEAA, which requires the presence of "(e) details of the beginning and end of the attestation’s period of validity".

NOTE: The requirements in the present clause meet the requirement (e) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(e) details of the beginning and end of the attestation’s period of validity".

4.2.8 Data constraining the usage of EAA

4.2.8.1 Introduction

The present clause specifies semantics for data providing details on the terms under which the EAA has been issued and may be used by relying parties.

4.2.8.2 EAA audience

EAA-4.2.8.2-01: The EAA audience shall identify the set of relying parties the EAA is intended for.

EAA-4.2.8.2-02: An EAA may incorporate the EAA audience.

EAA-4.2.8.2-03: Absence of this data shall mean that there is not any restriction on the relying parties that the EAA is intended for.

EAA-4.2.8.2-04: Presence of this data shall mean that the EAA is intended only for the relying parties identified in it.

EAA-4.2.8.2-05: The value of this data shall be either:

1) a sequence of relying parties’ identifiers (in this sequence it is not mandatory that all the members in the mentioned sequence are of the same type; instead, they may be of different types), or
2) a sequence of identifiers of groups of relying parties (relying parties of a certain type, for instance), or

3) a combination of both types of sequences mentioned in the previous bullets.

NOTE: The sequence in bullet 2) allows to identify a high number of relying parties with one identifier, and also allows to extend its number as new relying parties are incorporated to the group identified.

EAA-4.2.8.2-06: The values of the identifiers of the relying parties or the groups of relying parties shall depend on the specific EAA implementation.

EAA-4.2.8.2-07: The incorporation and placement of the EAA audience shall depend on the specific EAA implementation.

4.2.8.3 Signal of one-time use

EAA-4.2.8.3-01: An EAA may incorporate the signal of one-time-use within the EAA.

EAA-4.2.8.3-02: The presence of this signal shall indicate that the EAA shall be used only once, and that it shall not be retained for future use.

EAA-4.2.8.3-03: Its absence shall indicate that the aforementioned constraint shall not apply to the EAA.

EAA-4.2.8.3-04: The incorporation, value, and placement of this signal shall depend on the specific EAA implementation.

4.2.9 Attributes evidence

EAA-4.2.9-01: The attributes evidence shall contain a set of evidence from the EAA subject (and the attribute subjects when required) that the EAA issuer used for completing the issuance of the EAA.

NOTE: The attributes evidence can be used by the relying party in asserting whether the EAA issuer met its expectations for relying in the EAA.

EAA-4.2.9-02: An EAA may incorporate the attributes evidence.

EAA-4.2.9-03: The attributes evidence shall consist in a sequence of one or more evidence.

EAA-4.2.9-04: Each evidence:

- Shall include an identifier of its type, which shall be an URI Reference.
- Shall include an identifier of the entity that verified this evidence.

NOTE: This entity may be either the EAA issuer or other delegated trusted entity.

- Shall include a collection of data items that provide details that are particular to each type of evidence.
- May include an identifier which allows to externally make reference to this evidence.

EAA-4.2.9-05: The incorporation and placement of attributes evidence shall depend on the specific EAA implementation.

4.2.10 EAA status service

4.2.10.1 General requirements

EAA-4.2.10.1-01: The EAA status service shall contain details of the services (including its location), that can be used to enquire about the validity status of the EAA.

EAA-4.2.10.1-02: An EAA may incorporate the EAA status service.

EAA-4.2.10.1-03: The attestation status service:

1) Shall include a URI to the service.

2) May also include an identifier of the type of the status information provided by the service.

EXAMPLE: A service issuing Bitstring Status Lists as specified in W3C Candidate Recommendation: "Bitstring Status List v1.0" [i.3].

EAA-4.2.10.1-04: The incorporation, value, and placement of the EAA status service shall depend on the specific EAA implementation.

4.2.10.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.2.10.2-01: An EU-QEAA shall include the EAA status service.

NOTE: This requirement meets the requirement (i) in Annex V of [22] for EU-QEAA, which requires the presence of "(i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation".

4.2.10.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EAA-PubA-4.2.10.3-01: An EU-EAA-PubA shall include the EAA status service.

NOTE: This requirement meets the requirement (i) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(i) the information or location of the services that can be used to enquire about the validity status of the attestation".

4.2.11 EAA refresh service

EAA-4.2.11-01: The EAA refresh service shall contain details allowing to request to refresh the EAA to a refresh service.

EAA-4.2.11-02: An EAA may incorporate EAA refresh service.

EAA-4.2.11-03: The attestation refresh service data:

1) Shall include a URI to the service.

2) May also include an identifier of the type of the refresh service itself.

EAA-4.2.11-04: The incorporation and placement of the EAA refresh service shall depend on the specific EAA implementation.

4.2.12 EAA verification schema

EAA-4.2.12-01: The EAA verification schema shall contain details that allow to verify that the contents and the structure of an attribute or an EAA are conformant against a specific schema.

EAA-4.2.12-02: An EAA may incorporate the EAA verification schema.

EAA-4.2.12-03: The EAA verification schema shall include a sequence of components, each one providing the details of a schema against which to verify either an attribute or the EAA.

EAA-4.2.12-04: Each component of the aforementioned sequence shall include:

1) A type identifier.

2) An URI Reference which identifies the schema itself.

EAA-4.2.12-05: The incorporation and placement of the EAA verification schema shall depend on the specific EAA implementation.

4.2.13 EAA encoding schema

EAA-4.2.13-01: The EAA encoding schema shall contain details that allow to map the contents of an EAA to an alternative representation format.

EAA-4.2.13-02: An EAA may incorporate the EAA encoding schema.

EAA-4.2.13-03: The EAA encoding schema shall include:

1) A type identifier.

2) An URI Reference which identifies the encoding method.

EAA-4.2.13-04: The incorporation and placement of the EAA encoding schema shall depend on the specific EAA implementation.

4.3 Attested attributes

EAA-4.3-01: Each attribute within an EAA:

- Shall have an attribute identifier, which uniquely and unambiguously identifies the attribute itself within the environment where the EAA is used.

EXAMPLE: This can be, for instance, the environment identified in the EAA context, if present, or implicitly known for all the participants in this environment, if the EAA context is absent.

- May have a component indicating the format used by the attribute identifier.
- May have a component identifying its type.
- May have a component where a friendly identifier of the attribute is available.
- May have a component that allows to individually reference the attribute.
- Shall have a value, whose semantics and inner structure shall depend on the specific Attribute.

EAA-4.3-02: The incorporation and placement of the attributes shall depend on the specific EAA implementation.

4.4 Attested attributes metadata

4.4.1 Introduction

The present clause specifies the semantics of a set of data that support the disclosure of electronic attributes.

4.4.2 Support to selective disclosure of attested attributes

4.4.2.1 Introduction

Clause 4.4.2 specifies the semantics of:

- The identifier of the selective disclosure schema used in the EAA. This identifier may appear explicitly within the EAA or be implicit (clause 4.4.2.2 of the present document).
- The disclosure, which is a structure that contains, among other data, the attested attribute to be selectively disclosed (clause 4.4.2.3 of the present document).
- The disclosure reference, which is a data bound to one disclosure, built in a way that this binding can be ascertained using a certain algorithm, and from which it is not computationally feasible to get the value of the attested attribute (clause 4.4.2.4 of the present document).
- The identifier and any required parameter(s) of the algorithm for computing the disclosure reference, based on the bound disclosure, and ensure their binding (clause 4.4.2.5 of the present document).

4.4.2.2 Disclosure schema identifier

EAA-4.4.2.2-01: An EAA may incorporate the disclosure schema.

EAA-4.4.2.2-02: This disclosure schema identifier:

1) Shall univocally identify the mechanism used within the EAA for making certain attested attributes disclosable.

2) May also contain an identifier or reference to the standard/specification that defines the mechanism itself.

EAA-4.4.2.2-03: The incorporation and placement of the disclosure schema identifier shall depend on the specific EAA implementation.

4.4.2.3 Disclosure

EAA-4.4.2.3-01: An EAA may have one or more disclosures.

EAA-4.4.2.3-02: Each disclosure:

1) Shall contain the disclosed attested attribute.

2) Shall contain additional data that allows to bind one disclosure with a disclosure reference.

3) May include an identifier of its version.

EAA-4.4.2.3-03: The incorporation and placement of the disclosures shall depend on the specific EAA implementation.

4.4.2.4 Disclosure reference

EAA-4.4.2.4-01: Each disclosure reference shall be unambiguously bound to one disclosure.

EAA-4.4.2.4-02: Each disclosure reference shall be built in such a way that this bound can be ascertained using a certain algorithm.

EAA-4.4.2.4-03: The EAA may include information on the validity of a set of disclosure references.

EAA-4.4.2.4-04: All the disclosure references present within an EAA shall be signed by the EAA issuer.

EAA-4.4.2.4-05: If an EAA has disclosures, then it shall have disclosure references. If an EAA has not disclosures, then it shall not have disclosure references.

EAA-4.4.2.4-06: The computation, incorporation and placement of the disclosure references shall depend on the specific EAA implementation.

4.4.2.5 Disclosure algorithm identifier

EAA-4.4.2.5-01: The disclosure algorithm identifier shall identify the algorithm for ascertaining the binding between a disclosure reference and its bound disclosure.

EAA-4.4.2.5-02: An EAA may incorporate the disclosure algorithm identifier.

EAA-4.4.2.5-03: The disclosure algorithm identifier:

1) Shall contain an identifier that univocally identifies the algorithm.

2) May also contain any parameter required for its operation.

EAA-4.4.2.5-04: The incorporation and placement of the disclosure algorithm identifier shall depend on the specific EAA implementation.

4.5 EAA digital signature

4.5.1 General requirements

EAA-4.5.1-01: An EAA shall incorporate a digital signature generateD by the EAA issuer with its private key.

EAA-4.5.1-02: The incorporation and placement of the digital signature shall depend on the specific EAA implementation.

Editor's Note: To be completed.

4.5.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.5.2-01: The signing certificate of the aforementioned digital signature shall be a Qualified Certificate issued by a Qualified Trust Service Provider, using a Qualified Electronic Signature Creation Device.

EU-QEAA-4.5.2-02: The digital signature shall be generated using a Qualified Electronic Signature Creation Device.

NOTE: These requirements meet requirement requirement (g) in Annex V of [22] for EU-QEAA, which requires the presence of "(g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider"

4.5.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-4.5.3-01: The signing certificate of the aforementioned digital signature shall be a Qualified Certificate issued by a Qualified Trust Service Provider, using a Qualified Electronic Signature Creation Device.

EU-EAA-PubA-4.5.3-02: The digital signature shall be generated using a Qualified Electronic Signature Creation Device.

NOTE: These requirements meet requirement requirement (g) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(g) the qualified electronic signature or qualified electronic seal of the issuing body".

4.5.4 Requirements for the signing certificate

4.5.4.1 General requirements

Editor's Note: to be completed.

4.5.4.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-4.5.4.2-01: If the EU-QEAA does contain the qualified certificate supporting its digital signature, it shall contain an indication of the location where this certificate is available.

EU-QEAA-4.5.4.2-02: If the EU-QEAA does contain the qualified certificate supporting its digital signature, this certificate shall be available free of charge in the indicated.

NOTE: These requirements meet requirement requirement (h) in Annex V of [22] for EU-QEAA, which requires the presence of "(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".

Editor's Note: Annex V does not explicitly forbid the presence of the signing certificate. If the certificate is present within the EU-QEAA, then the location is actually the EU-QEAA itself.

4.5.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-4.5.4.3-01: If the EU-EAA-PubA does contain the qualified certificate supporting its digital signature, it shall contain an indication of the location where this certificate is available.

EU-EAA-PubA-4.5.4.3-02: If the EU-EAA-PubA does contain the qualified certificate supporting its digital signature, this certificate shall be available free of charge in the indicated.

NOTE: These requirements meet requirement requirement (h) in Annex VII of [22] for EU-EAA-PubA, which requires the presence of "(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".

Editor's Note: Annex VII does not explicitly forbid the presence of the signing certificate. If the certificate is present within the EU-EAA-PubA, then the location is actually the EU-EAA-PubA itself.

5 Implementation of EAA based on SD-JWT VC

5.1 General requirements

The present clause specifies a realization of EAA that implements EAA as a JSON Web Signature as specified in IETF RFC 7515: "JSON Web Signature (JWS)" [13], built on IETF SD-JWT VC: "SD-JWT-based Verifiable Credentials (SD-JWT VC) draft-ietf-oauth-sd-jwt-vc-03" [2], which further profiles a Selective Disclosure JSON Web Token as specified in IETF SD-JWT: "Selective Disclosure for JWTs (SD-JWT)" [6].

The EAAs implemented according to clause 5 of the present document, will be designated as SD-JWT VC EAA hereinafter. SD-JWT VC EAA shall meet the following requirements:

1) The whole SD-JWT VC EAA shall be implemented as a Selective Disclosure JSON Web Token based Verifiable Credential (SD-JWT VC) as specified in IETF SD-JWT VC: "SD-JWT-based Verifiable Credentials (SD-JWT VC) draft-ietf-oauth-sd-jwt-vc-03" [2], signed by a JSON Web Signature as specified in IETF RFC 7515.

2) The JSON Web Signature shall include a JOSE Header as specified in clause 5.5 of the present document.

SD-JWT VC EAA may contain additional data not specified within the present document.

5.2 EAA metadata

5.2.1 EAA Context

5.2.1.1 General requirements

EAA-5.2.1.1-01: The `@context` component shall implement the semantics specified in clause 4.2.1 of the present document.

Editor's Note: Not registered claim is known with this semantics. It is proposed to use the claim specified in Verifiable Credentials Data Model v2.0 [1], clause 4.1.

EAA-5.2.1.1-02: The contents of the `@context` component shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 4.1.

EAA-5.2.1.1-03: A SD-JWT VC EAA may incorporate the `@context` component.

EAA-5.2.1.1-04: A SD-JWT VC EAA may include the indication of the scheme of attestations that the SD-JWT VC EU-QEAA is part of, as one element within the `@context` array.

5.2.1.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-5.2.1.2-01: Wherever applicable, a SD-JWT VC EU-QEAA shall include the indication of the scheme of attestations that the SD-JWT VC EU-QEAA is part of, as one element within the `@context` array.

Editor's Note: Remaining issue: whether this indication has to have something that identifies it as the indication of the scheme of attestations in an array where there are other identifiers. Feedback is requested.

5.2.1.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-5.2.1.3-01: Wherever applicable, a SD-JWT VC EU-EAA-PubA shall include the indication of the scheme of attestations that the SD-JWT VC EU-EAA-Pub is part of, as one element within the `@context` array.

Editor's Note: Remaining issue: whether this indication has to have something that identifies it as the indication of the scheme of attestations in an array where there are other identifiers. Feedback is requested.

5.2.2 EAA type

5.2.2.1 General requirements

EAA-5.2.2.15.2.1.1-01: The `vct` component, as specified in IETF SD-JWT VC [2], clause 3.2.2.1.1, shall implement the semantics specified in clause 4.2.2 of the present document.

EAA-5.2.2.15.2.1.1-02: A SD-JWT VC EAA shall incorporate the `vct` component.

5.2.2.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-5.2.2.2-01: A SD-JWT VC EU-QEAA shall include the `euQual` claim.

Editor's Note: The JSON schema definition of this claim will be added if it is kept.

EU-QEAA-5.2.2.2-02: The `euQual` claim shall not be present in SD-JWT VC EAA that have not been issued as EU-QEAA.

EU-QEAA-5.2.2.2-03: The value of the `euQual` claim shall be the URI defined in requirement EU-QEAA-4.2.2.3-02 (`urn:etsi:eaa:eu:qualified`).

Editor's Note: This requires a new claim, not specified anywhere else. Another alternative could have been to include within the vct two URIs separated by a ',': one indicating the type, and this one indicating that the EAA is actually an EU-QEAA. In fact, in W3C VC, the type is an array of elements. Feedback on these two options is required.

5.2.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-5.2.2.3-01: A SD-JWT VC EU-EAA-PubA shall include the `euPubA` claim.

Editor's Note: The JSON schema definition of this claim will be added if it is kept.

EU-EAA-PubA-5.2.2.3-02: The `euPubA` claim shall not be present in SD-JWT VC EAA that are not EU-EAA-PubA.

EU-EAA-PubA-5.2.2.3-03: The value of the `euPubA` claim shall be the URI defined in requirement EU-EAA-PubA-4.2.2.4-02 (`urn:etsi:eaa:eu:pubA`).

Editor's Note: This requires a new claim, not specified anywhere else. Another alternative could have been to include within the vct two URIs separated by a ',': one indicating the type, and this one indicating that the EAA is actually an EU-QEAA. In fact, in W3C VC, the type is an array of elements. Feedback on these two options is required.

5.2.3 EAA identifier

EAA-5.2.3-01: The `jti` component specified in IETF RFC 7519 [5], clause 4.1.7, shall implement the semantics specified in clause 4.2.3 of the present document.

EAA-5.2.3-02: A SD-JWT VC EAA shall incorporate the `jti` component.

5.2.4 EAA issuer identifier

5.2.4.1 General requirements

EAA-5.2.4.1-01: The `iss` component specified in IETF RFC 7519 [5], clause 4.1.1, and further profiled in IETF SD-JWT VC [2], clause 3.2.2.2, shall implement the semantics specified in clause 4.2.4 of the present document.

EAA-5.2.4.1-02: A SD-JWT VC EAA shall incorporate the `iss` component.

Editor's Note: IETF RFC 7519 [5] specifies that this element can be a string or an URI. IETF SD-JWT VC [2] draft, proposes that this element is an URI. In order to meet the requirements in "REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework" [22], regarding the inclusion of registration numbers, it is considered that a String is better.

EAA-5.2.4.1-03: A SD-JWT VC EAA may also include the `name` claim, specified in OpenID CC 1.0: "OpenID Connect Core 1.0 incorporating errata set" [30], whose value shall be the name of the issuer.

EAA-5.2.4.1-04: Where a registration identifier is applicable, a SD-JWT VC EAA may include the `iss_reg_id` claim, whose value shall be the registration identifier of the SD-JWT VC EAA issuer.

EAA-5.2.4.1-05: In a SD-JWT VC EAA, wherever applicable, the optional registration identifier of the SD-JWT VC EAA issuer may be expressed as specified in requirement EU-QEAA-4.2.4.2-04 of the present document.

Editor's Note: new claim. JSON schema will be added.

EAA-5.2.4.1-06: Where a registration identifier built as expressed as specified in requirement EU-QEAA-4.2.4.2-04 of the present document is not used, a SD-JWT VC EAA may include the `country` claim, which shall identify the EU Member State, in which the EAA issuer is stablished.

Editor's Note: new claim. JSON schema will be added.

EAA-5.2.4.1-07: The value of the optional `country` claim shall be as specified in requirement EU-QEAA-4.2.4.2-02 of the present document.

Editor's Note: this is a consequence of the definition, within IETF SD-JWT VC [2] of `iss` claim as an URI. If it would allow `iss` to also be a regular string, then neither the `country` nor the `iss_reg_id` would have been needed.

5.2.4.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-5.2.4.2-01: A SD-JWT VC EU-QEAA shall include the `name` claim, specified in OpenID CC 1.0: "OpenID Connect Core 1.0 incorporating errata set" [30], whose value shall be the name of the issuer.

EU-QEAA-5.2.4.2-02: Where a registration identifier is applicable, a SD-JWT VC EU-QEAA shall include the `iss_reg_id` claim, whose value shall be the registration identifier of the SD-JWT VC EU-QEAA issuer.

EU-QEAA-5.2.4.2-03: In a SD-JWT VC EU-QEAA, wherever applicable, the registration identifier of the SD-JWT VC EU-QEAA issuer shall be expressed using the structure for the corresponding character string specified in requirement EAA-4.2.4.1-07 of the present document.

EU-QEAA-5.2.4.2-04: Where a registration identifier is not applicable, a SD-JWT VC EU-QEAA shall include the `country` claim, which shall identify the EU Member State, in which the QEAA issuer is stablished.

EU-QEAA-5.2.4.2-05: The value of the `country` claim shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

5.2.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-5.2.4.3-01: A SD-JWT VC EU-EAA-PubA shall include the `name` claim, specified in OpenID CC 1.0: "OpenID Connect Core 1.0 incorporating errata set" [30], whose value shall be the name of the public body.

EU-EAA-PubA-5.2.4.3-02: Where a registration identifier is applicable, a SD-JWT VC EU-EAA-PubA shall include the `iss_reg_id` claim, whose value shall be the registration identifier of the SD-JWT VC EU-QEAA issuer.

EU-EAA-PubA-5.2.4.3-03: In a SD-JWT VC EU-EAA-PubA, wherever applicable, the registration identifier of the public body shall be expressed using the structure for the corresponding character string specified in requirement EAA-4.2.4.1-07 of the present document.

EU-EAA-PubA-5.2.4.3-04: Where a registration identifier is not applicable, a SD-JWT VC EU-EAA-PubA shall include the `country` claim, which shall identify the EU Member State, in which the public body is stablished.

EU-EAA-PubA-5.2.4.3-05: The value of the `country` claim shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

5.2.5 EAA and attribute subject identifiers and pseudonyms

5.2.5.1 The EAA subject identifier

EAA-5.2.5.1-01: The `sub` claim specified in IETF RFC 7519 [5], clause 4.1.2, and further profiled in clause 3.2.2.2 of IETF SD-JWT VC [2], shall implement the semantics specified in clause 4.2.5.2 of the present document.

EAA-5.2.5.1-02: An EAA shall include either the `sub` claim or the `also_known_as` claim specified specified in OpenID Connect for Identity Assurance Claims Registration 1.0 [24] clause 4.1.

Editor's Note: this requirement implements the requirement EAA-4.2.5.2-01 on mandatory presence of the EAA subject or its pseudonym.

5.2.5.2 The EAA subject pseudonym

EAA-5.2.5.2-01: The `also_known_as` claim specified in OpenID Connect for Identity Assurance Claims Registration 1.0 [24] clause 4.1, shall implement the semantics specified in clause 4.2.5.3 of the present document.

5.2.5.3 The attribute subject identifier

Editor's Note: To be completed.

5.2.5.4 The attribute subject pseudonym

Editor's Note: To be completed.

5.2.5.5 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-5.2.5.5-01: In a SD-JWT VC EU-QEAA the value of the `sub` component shall be the identifier of the EAA subject.

EU-QEAA-5.2.5.5-02: In a SD-JWT VC EU-QEAA the value of the `also_known_as` component shall be the pseudonym of the EAA subject.

5.2.5.6 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU- EAA-PubA-5.2.5.6-01: In a SD-JWT EU-EAA-PubA the value of the `sub` component shall be the identifier of the EAA subject.

EU- EAA-PubA-5.2.5.6-02: In a SD-JWT VC EU-EAA-PubA the value of the `also_known_as` component shall be the pseudonym of the EAA subject.

5.2.6 EAA issuance time

EAA-5.2.6-01: The `iat` component, specified in IETF RFC 7519 [5] clause 4.1.6, and further profiled in IETF SD-JWT VC [2] clause 3.2.2.2, shall implement semantics specified in clause 4.2.6 of the present document.

EAA-5.2.6-02: A SD-JWT VC EAA may incorporate the `iat` component.

EAA-5.2.6-03: The content of `iat` component shall meet the requirements specified in clause 4.2.6.2 of the present document.

5.2.7 EAA validity period

5.2.7.1 Introduction

EAA-5.2.7.1-01: The EAA validity period of SD-JWT VC EAA shall be defined by the `nbf` and `exp` claims specified in the next two clauses.

5.2.7.2 The not before component

EAA-5.2.7.2-01: The `nbf` component specified in IETF RFC 7519 [5], clause 4.1.5, and further profiled in IETF SD-JWT VC [2] clause 3.2.2.2, shall implement the semantics of the first instant time specified in clause 4.2.7.

EAA-5.2.7.2-02: A SD-JWT VC EAA shall incorporate the `nbf` component.

EAA-5.2.7.2-03: The content of `nbf` component shall meet the requirements specified in clause 4.2.6.2 of the present document.

5.2.7.3 The expiration component

EAA-5.2.7.3-01: The `exp` component specified in IETF RFC 7519 [5], clause 4.1.4, and further profiled in IETF SD-JWT VC [2] clause 3.2.2.2,shall implement the semantics of the second instant time specified in clause 4.2.7.

EAA-5.2.7.3-02: A SD-JWT VC EAA shall incorporate the `exp` component.

EAA-5.2.7.3-03: The content of `exp` component shall meet the requirements specified in clause 4.2.6.2 of the present document.

5.2.8 Components constraining the usage of EAA

5.2.8.1 EAA audience

EAA-5.2.8.1-01: A SD-JWT VC EAA shall not incorporate any component implementing the semantics specified in clause 4.2.8.2 of the present document.

5.2.8.2 Signal of one-time use

EAA-5.2.8.2-01: The `oneTime` component shall implement the semantics specified in clause 4.2.8.3 of the present document.

EAA-5.2.8.2-02: A SD-JWT VC EAA may incorporate the `oneTime` component.

EAA-5.2.8.2-03: The presence of the `oneTime` component shall indicate that the EAA shall be used only once, and that it shall not be retained for future use.

EAA-5.2.8.2-04: Its absence shall indicate that the aforementioned constraint shall not apply to the EAA.

EAA-5.2.8.2-05: The `oneTime` shall not have any value.

Editor's Note: JSON schema for defining this component TO BE DEVELOPED.

5.2.9 Attributes evidence

EAA-5.2.9-01: A SD-JWT VC EAA shall not incorporate any component implementing the semantics specified in clause 4.2.9 of the present document.

5.2.10 EAA status service

5.2.10.1 General requirements

EAA-5.2.10.1-01: The `status` component shall implement the semantics specified in clause 4.2.10 of the present document.

EAA-5.2.10.1-02: A SD-JWT VC EAA may incorporate the `status` component.

Below follows the definition of `status` component, as defined within the definitions section in the JSON Schema file whose location is detailed in Annex C, and is copied below for information:

```
"status": {"$ref": "#/definitions/service"}
```

Below follows the definition of `service` JSON type, which shall be defined within the definitions section in the JSON Schema file JSON_FILE_IN_ETSI_FORGE, whose location is detailed in Annex C, and is copied below for information.

```
"service": {
    "type": "object",
    "properties": {
        "id": {"type": "string", "format": "uri-reference"},
        "type": {"type": "string"}
    },
    "required": ["id","type"],
    "additionalProperties": false
}
```

EAA-5.2.10.1-03: Within this JSON object, `id` member shall contain an URI reference referencing the service that provides the EAA status information.

EAA-5.2.10.1-04: Within this JSON object, `type` member shall contain the name of the protocol to be used for requesting the EAA status information to the service.

5.2.10.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-5.2.10.2-01: A SD-JWT VC EU-QEAA shall contain the `status` claim.

5.2.10.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-5.2.10.3-01: A SD-JWT VC EU-EAA-PubA shall contain the `status` claim.

5.2.11 EAA refresh service

EAA-5.2.11-01: A SD-JWT VC EAA shall not incorporate any component implementing the semantics specified in clause 4.2.11 of the present document.

5.2.12 EAA verification schema (`credentialSchema`)

EAA-5.2.12-01: The `credentialSchema` component shall implement the semantics specified in clause 4.2.12 of the present document.

EAA-5.2.12-02: A SD-JWT VC EAA may incorporate the `credentialSchema`.

EAA-5.2.12-03: Its contents shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 5.4 for data verification schemas.

5.2.13 EAA encoding schema (`encodingSchema`)

EAA-5.2.13-01: A SD-JWT VC EAA shall not incorporate any component implementing the semantics specified in clause 4.2.13 of the present document.

5.3 Attested Attributes

EAA-5.3-01: A SD-JWT VC EAA shall incorporate the disclosed attested attributes as regular JWT claims, as specified in clause of IETF SD-JWT VC [2].

If disclosable attested attributes are required, the SD-JWT VC EAA shall incorporate them in their corresponding disclosures, as specified in clause 5.4.2 of the present document.

5.4 Attested Attributes metadata

5.4.1 Introduction

Editor's Note: to be completed.

5.4.2 Support to selective disclosure of attested attributes

5.4.2.1 General requirements

EAA-5.4.2.1-01: A SD-JWT VC EAA shall support the selective disclosure of attributes using components specified in IETF SD-JWT VC [2] and IETF SD-JWT [6].

5.4.2.2 Disclosure schema identifier

EAA-5.4.2.2-01: A SD-JWT VC EAA shall not incorporate any component for identifying the disclosure schema.

NOTE: The information about the schema used for implementing Selective Disclosure of attested attributes is implicit in the media type of the SD-JWT.

5.4.2.3 Disclosure

EAA-5.4.2.3-01: A SD-JWT VC EAA shall contain one disclosure for each selectively disclosable Attested Attribute.

EAA-5.4.2.3-02: If the SD-JWT VC EAA is serialized using JWS Compact Serialization, the disclosures shall be incorporated in the SD-JWT VC EAA as specified in clause 6.1 of IETF SD-JWT [6].

EAA-5.4.2.3-03: If the SD-JWT VC EAA is serialized using JWS JSON Serialization, the disclosures shall be incorporated within the `disclosures` JSON array specified in clause 9 of IETF SD-JWT [6].

5.4.2.4 Disclosure reference

EAA-5.4.2.4-01: A SD-JWT VC EAA containing one or more selectively disclosable attested attributes that are JSON Properties (clause 4.2.1 of IETF SD-JWT [6]), shall include the `_sd` component containing their disclosure digests computed as specified in in clause 5.2.4.1 of IETF SD-JWT [6].

EAA-5.4.2.4-02: A SD-JWT VC EAA requiring that one or more individual elements of JSON arrays are selectively disclosable (clause 4.2.2 of IETF SD-JWT [6]), shall incorporate in the payload the mentioned JSON arrays where the individual elements that are selectively disclosable have been replaced by their corresponding disclosure digests computed as specified in clause 5.2.4.2 of IETF SD-JWT [6].

5.4.2.5 Disclosure algorithm identifier (_sd_alg)

EAA-5.4.2.5-01: The `_sd_alg` component, specified in IETF IETF SD-JWT [6], clause 5.1.1, and further profiled in IETF SD-JWT VC [2], shall implement the semantics specified in clause 4.4.2.5 of the present document.

EAA-5.4.2.5-02: If the SD-JWT VC EAA contains one or more disclosures, then the `_sd_alg` component shall be present.

5.5 EAA digital signature

5.5.1 General requirements

EAA-5.5.1-01: A SD-JWT VC EAA shall include the `signature` member specified in IETF RFC 7515 [13].

EAA-5.5.1-02: The JOSE header shall include the `alg` header parameter. Its value shall be the identifier of a signature algorithm.

EAA-5.5.1-03: The JOSE header shall include an identifier of the signing certificate of the EAA as per IETF RFC 7515 [13].

EAA-5.5.1-04: The JOSE header shall include the `typ` header parameter, in which case, its value shall be "application/vc+sd-jwt".

EAA-5.5.1-05: The JOSE header may include other header parameters as specified in either IETF RFC 7515 [13] or ETSI TS 119 182: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures" [16].

Editor's Note: to be completed.

5.5.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed.

5.5.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed.

5.5.4 Requirements for the signing certificate

5.5.4.1 General requirements

Editor's Note: to be completed.

5.5.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed. Either the certificate is within the QEAA (in the signature, for instance) or the QEAA has data indicating from where the certificate can download it free of charge.

5.5.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed. Either the certificate is within the EU-EAA-PubA (in the signature, for instance) or the EU-EAA-PubA has data indicating from where the certificate can download it free of charge.

6 Implementation of EAA based on SD-JWT VC DM

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2 EAA metadata

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.1 EAA Context

6.2.1.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.1.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: To be completed. For EU-QEAA the presence of the EAA context, understood as the identifier of attestations the EAA is part of the scheme will be conditional. Second part of requirement (f) of annex V of eIDAS2.

6.2.1.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: To be completed. For EU EU-EAA-PubA the presence of the EAA context, understood as the identifier of attestations the EAA is part of the scheme will be conditional. Second part of requirement (f) of annex VII of eIDAS2.

6.2.2 EAA type

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.2.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.2.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.3 EAA identifier

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.4 EAA issuer identifier

6.2.4.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available

6.2.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available

6.2.5 EAA and attribute subject identifiers and pseudonyms

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.5.1 The EAA subject identifier

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.5.2 The EAA subject pseudonym

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.5.3 The attribute subject identifier

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.5.4 The attribute subject pseudonym

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.5.5 Requirements for EU Qualified Attestation of Attributes

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.6 EAA issuance time

6.2.6.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.6.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.7 EAA validity period

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.8 Components constraining the usage of EAA

6.2.8.1 EAA audience

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.8.2 Signal of one-time use

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.9 Attributes evidence

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.10 EAA status service

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.10.1 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available. For EU-QEAA the presence of the EAA status service will be mandatory.

6.2.10.2 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available. For EU-EAA-PubA the presence of the EAA status service will be mandatory

6.2.11 EAA refresh service

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.12 EAA verification schema service

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.2.13 EAA encoding schema

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.3 Attested Attributes

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.4 Attested Attributes metadata

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.4.1 Introduction

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.4.2 support to selective disclosure of attested attributes

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.5 EAA digital signature

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.5.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.5.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.5.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.5.4 Requirements for the signing certificate

6.5.4.1 General requirements

Editor's Note: to be completed as soon a complete technical specification of SD-JWT VC DM Credential format is available.

6.5.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed. Either the certificate is within the EU-QEAA (in the signature, for instance) or the EU-QEAA has data indicating from where the certificate can download it free of charge.

6.5.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed. Either the certificate is within the EU-EAA-PubA (in the signature, for instance) or the EU-EAA-PubA has data indicating from where the certificate can download it free of charge.

7 Implementation of EAA based on ISO 18013-5:2021

7.1 General requirements

Clause 7 of the present document specifies a realization of EAA based on ISO/IEC 18013-5: "Personal identification – ISO – compliant driving licence – Part 5: Mobile driving licence (mDL) application" [17] (ISO 18013-5:2021 implementation hereinafter).

The EAAs implemented according to clause 7 of the present document, will be designated as ISO/IEC 18013-5 EAA hereinafter.

EAA-7.1-01: ISO/IEC 18013-5 EAA shall be an instance of `IssuerSigned` type defined in ISO 18013-5:2021 [17] clause 8.3.2.1.2.2.

EAA-7.1-02: If in the context where an ISO/IEC 18013-5 EAA is issued there is not any value for a data element defined in ISO/IEC 18013-5 as mandatory OR if the issuing policy prevents the inclusion of this value in the ISO/IEC 18013-5 EAA, the ISO/IEC 18013-5 EAA shall incorporate such data element with an empty value (empty string, empty bitstring).

EXAMPLE 1: An example of the first case is, for instance, the `family_name` data element, as in some countries there are natural persons that do not have family name.

EXAMPLE 2: An example of the second case could be, for instance, the `portrait` data element. While the inclusion of the portrait of the driver is logical in a mobile driving licence, there could be reasons for preventing the inclusion of a portrait of the EAA subject in an EAA.

7.2 EAA metadata

7.2.1 EAA Context

7.2.1.1 General requirements

Editor's Note: to be completed.

7.2.1.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed. Either the certificate is within the EU-QEAA (in the signature, for instance) or the EU-QEAA has data indicating from where the certificate can download it free of charge.

7.2.1.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed. Either the certificate is within the EU-EAA-PubA (in the signature, for instance) or the EU-EAA-PubA has data indicating from where the certificate can download it free of charge.

7.2.2 EAA type

7.2.2.1 General requirements

EAA-7.2.2.1-01: ISO/IEC 18013-5 EAA may include the `docType` data element as specified in clause 6.3.4 of ISO/IEC 23220-2 [19].

EAA-7.2.2.1-02: The optional `docType` data element shall implement the semantics of clause 4.2.2 of the present document.

Editor's Note: As ISO/IEC 18013-5 is a specification for mdL, it does not define, in its table 5 of clause 7.2.1, any data element for the type of document. That is why the present document proposes to use the `docType` data element defined by ISO/IEC 23220-2.

7.2.2.2 Requirements for EU Qualified EAA (EU-QEAA)

EU- QEAA-7.2.2.2-01: ISO/IEC 18013-5 EU-QEAA shall include the `docType` data element.

EU-QEAA-7.2.2.2-01: The value of the `docType` data element shall be the value defined in requirement EU-QEAA-4.2.2.3-02 (`urn:etsi:eaa:eu:qualified`).

7.2.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-7.2.2.3-01: ISO/IEC 18013-5 EU-EAA-PubA shall include the `docType` data element.

EU-EAA-PubA-7.2.2.3-02: The value of the `docType` data element shall be the URI defined in requirement EU-EAA-PubA-4.2.2.4-02 (`urn:etsi:eaa:eu:pubA`).

7.2.3 EAA identifier

EAA-7.2.3-01: The `document_number` data element, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [17], shall implement the semantics of clause 4.2.3 of the present document.

EAA-7.2.3-02: An ISO/IEC 18013-5 EAA shall incorporate the `document_number` data.

7.2.4 EAA issuer identifier

7.2.4.1 General requirements

EAA-7.2.4.1-01: The `issuing_authority` and `issuing_country` data elements, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [17], shall jointly implement the semantics of clause 4.2.4 of the present document.

EAA-7.2.4.1-02: ISO/IEC 18013-5 EAA may include the `issuing_country` data element.

EAA-7.2.4.1-03: The value of the optional `issuing_country` data element shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

EAA-7.2.4.1-04: An ISO/IEC 18013-5 EAA shall incorporate the `issuing_authority` data element.

Requirements when the EAA issuer is a legal person

EAA-7.2.4.1-05: If the issuer of the ISO/IEC 18013-5 EAA is a legal person, the `issuing_authority` data element may include a registration identifier as stated in the official records, where such a registration identifier exists.

EAA-7.2.4.1-06: If the issuer of the ISO/IEC 18013-5 EAA is a legal person, and there exists a registration identifier for it, the registration identifier may be expressed as specified in requirement EAA-4.2.4.1-07 of the present document.

EAA-7.2.4.1-07: If the issuer of the ISO/IEC 18013-5 EAA is a legal person, the `issuing_authority` data element may include the name of this legal person.

EAA-7.2.4.1-08: The name of a legal person may be expressed using the string representation of X.500 attributes organizationName (O), and optionally organizationalUnitName (OU) as specified in RFC 1779: "A String Representation of Distinguished Names" [27] .

EAA-7.2.4.1-09: If the issuer of the ISO/IEC 18013-5 EAA is a legal person, and the `issuing_authority` data element contains both its registration identifier and its name as specified in requirements EAA-7.2.4.1-04 and EAA-7.2.4.1-06, then both data shall be separated by the '#' character (0x23 (ASCII), U+0023 (UTF-8)).

EXAMPLE 1: "VATBE-1234567890#O=FooOrgName, OU=FooOrgUnitName"

Requirements when the EAA issuer is a natural person

EAA-7.2.4.1-10: If the issuer of the ISO/IEC 18013-5 EAA is a natural person, the name of this person may be placed within the `issuing_authority` data element, and may be expressed using the string representation of the X.500 attribute commonName (CN) as specified in RFC 1779: "A String Representation of Distinguished Names" [27].

EXAMPLE 2: "CN=John Smith"

7.2.4.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-7.2.4.2-01: ISO/IEC 18013-5 EU-QEAA shall include the `issuing_country` data element.

EU-QEAA-7.2.4.2-02: The value of the identifier of an EU Member State shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

Requirements when the QEAA issuer is a legal person

EU-QEAA-7.2.4.2-03: If the issuer of the ISO/IEC 18013-5 EU-QEAA is a legal person, the `issuing_authority` data element shall include a registration identifier as stated in the official records, where such a registration identifier exists.

EU-QEAA-7.2.4.2-04: If the issuer of the ISO/IEC 18013-5 EU-QEAA is a legal person, and there exists a registration identifier for it, the registration identifier shall be expressed as specified in requirement EAA-4.2.4.1-07 of the present document.

EU-QEAA-7.2.4.2-05: If the issuer of the ISO/IEC 18013-5 EU-QEAA is a legal person, the `issuing_authority` data element shall include the name of this legal person.

EU-QEAA-7.2.4.2-06: The name of a legal person shall be expressed using the string representation specified in requirement EAA-7.2.4.1-08 of the present document.

EU-QEAA-7.2.4.2-07: If the issuer of the ISO/IEC 18013-5 EU-QEAA is a legal person, and the `issuing_authority` data element contains both its registration identifier and its name, then both data shall be separated by the '#' character (0x23 (ASCII), U+0023 (UTF-8)).

EXAMPLE 1: "VATBE-1234567890#O=FooOrgName, OU=FooOrgUnitName"

Requirements when the QEAA issuer is a natural person

EU-QEAA-7.2.4.2-08: If the issuer of the ISO/IEC 18013-5 EU-QEAA is a natural person, the name of this person shall be placed within the `issuing_authority` data element, and shall be expressed using the string specified in requirement EAA-7.2.4.1-10 of the present document.

EXAMPLE 2: "CN=John Smith"

7.2.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-7.2.4.3-01: ISO/IEC 18013-5 EU-EAA-PubA shall include the `issuing_country` data element.

EU-EAA-PubA-7.2.4.3-02: The value of the identifier of an EU Member State shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

EU-EAA-PubA-7.2.4.3-03: The `issuing_authority` data element shall include the registration identifier of the public body as stated in the official records, where such a registration identifier exists.

EU-EAA-PubA-7.2.4.3-04: If there exists a registration identifier for the public body, the registration identifier shall be expressed as specified in requirement EAA-4.2.4.1-07 of the present document.

EU-EAA-PubA-7.2.4.3-05: The `issuing_authority` data element shall include the name of the public body.

EU-EAA-PubA-7.2.4.3-06: The name of the public body shall be expressed using the string representation specified in requirement EAA-7.2.4.1-08 of the present document.

EU-EAA-PubA-7.2.4.3-07: If the `issuing_authority` data element contains both the registration identifier and the name of the public body, then both data shall be separated by the '#' character (0x23 (ASCII), U+0023 (UTF-8)).

EXAMPLE 1: "VATBE-1234567890#O=FooOrgName, OU=FooOrgUnitName"

7.2.5 EAA and attribute subject identifiers and pseudonyms

7.2.5.1 EAA subject identifier

EAA-7.2.5.1-01: The EAA subject identifier shall be a combination of the data elements, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [17], which univocally identifies the entity to whom the EAA is issued.

Editor's Note: As of ISO/IEC 18013-5 [17] is a standard for driving licenses, it only provides data elements for identifying natural or legal persons, but not objects. EAA, according to [22] can also include attributes on objects. Draft IETF draft-ietf-rats-eat-30: "The Entity Attestation Token (EAT)" [29] shall be taken into account for these purposes.

7.2.5.2 EAA subject pseudonym

Editor's Note: Table 5 of ISO/IEC 18013-5 [17] does not include any data element for a pseudonym. I this profile has also to cover this case, it is required to define new data elements. To be completed.

7.2.5.3 Attribute subject identifier

EAA-7.2.5.3-01: An attribute subject identifier shall be a combination of the data elements, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [17], which univocally identifies the entity to whom a set of attributes is referring.

Editor's Note: As of ISO/IEC 18013-5 [17] is a standard for driving licenses, it only provides data elements for identifying natural or legal persons, but not objects. EAA, according to [22] can also include attributes on objects. If this profile has also to cover this case, it is required to define new data elements.

7.2.5.4 Attribute subject pseudonym

Editor's Note: Table 5 of ISO/IEC 18013-5 [17] does not include any data element for a pseudonym. If this profile has also to cover this case, it is required to define new data elements. To be completed.

7.2.5.5 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed once the issue of the subject pseudonym is solved.

7.2.5.6 Requirements for Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed once the issue of the subject pseudonym is solved.

7.2.6 EAA issuance time

EAA-7.2.6-01: The `issue_date` data element, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [17], shall implement the semantics of clause 4.2.6 of the present document.

EAA-7.2.6-01: An ISO/IEC 18013-5 EAA shall incorporate the `issue_date` data element.

EAA-7.2.6-01: The content of `issue_date` data element shall meet the requirements specified in clause 4.2.6.2 of the present document.

Editor's Note: issue_date data element is specified as a "full-date = #6.1004(tstr), where tag 1004 is specified in RFC 8943". This tag is only applied to dates, but not to times. However, the present document requires that this data element also incorporates information of time. The alternative would be to define a new data element. Feedback on this issue is requested.

7.2.7 EAA validity period

EAA-7.2.7-01: The members `validFrom` and `validUntil` of the `validityInfo` member of the instance of `MobileSecurityObject` type specified in clause 9.1.2.4 of ISO/IEC 18013-5 [17] shall implement the semantics of clause 4.2.7 of the present document.

EAA-7.2.7-02: An ISO/IEC 18013-5 EAA shall incorporate the `validFrom` and the `validUntil` members.

Editor's Note: Both `validFrom` and `validUntil` are defined as tdate. This type does not support indication of time. Therefore, either new elements are defined for indication of the times or ISO 18013-5:2021 EAA validity periods are defined at a constant time for the dates indicated above. Feedback is required.

Editor's Note: to be completed

Editor's Note: The actual semantics of these members is related to the validity of the MSO and its signature; the question is whether this can be assimilated to the EAA validity period of the EAA itself.

Editor's Note: ISO/IEC 18013-5 [17] makes the signed member of ValidityInfo type mandatory. This is the MSO signing date. This text relates this with `issue_date`?

Editor's Note: ISO/IEC 23220-2 [19] defines expiry_date as the "Date mobile eID document expires", and the issue_date as the "Date mobile eID document was issued". It does not have any data element for indicating the date of validity start.

7.2.8 Components constraining the usage of EAA

7.2.8.1 EAA audience

EAA-7.2.8.1-01: An ISO/IEC 18013-5 EAA shall not incorporate any component implementing the semantics specified in clause 4.2.8.2 of the present document

7.2.8.2 Signal of one-time use

Editor's Note: to be completed.

7.2.9 Attributes evidence

EAA-7.2.9-01: An ISO/IEC 18013-5 EAA shall not incorporate any component implementing the semantics specified in clause 4.2.9 of the present document.

7.2.10 EAA status service

7.2.10.1 General requirements

EAA-7.2.10.1-01: The `status_service` data element shall implement the semantics specified in clause 4.2.10 of the present document.

EAA-7.2.10.1-02: An ISO/IEC 18013-5 EAA may incorporate the `status_service` data element.

EAA-7.2.10.1-03: The `status_service` data element shall be incorporated as the data elements specified in Table 5 of clause 7.2.1 of of ISO/IEC 18013-5 [17].

EAA-7.2.10.1-04: The `status_service` data element shall be an instance of `StatusService` type, which is defined is defined within file CBOR_FILE_IN_ETSI_FORGE, whose location is detailed in Annex B, and is copied below for information.

```
StatusService = {
    "id": tstr; a reference allowing to access the service,
    "type": tstr; the type of the service
},
```

7.2.10.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-7.2.10.2-01: An ISO/IEC 18013-5 EU-QEAA shall contain the `status_service` claim.

7.2.10.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-7.2.10.3-01: An ISO/IEC 18013-5 EU-EAA-PubA shall contain the `status_service` claim.

7.2.11 EAA refresh service

EAA-7.2.11-01: An ISO/IEC 18013-5 EAA shall not incorporate any component implementing the semantics specified in clause 4.2.11 of the present document.

7.2.12 EAA verification schema service

Editor's Note: to be completed

7.2.13 EAA encoding schema

EAA-7.2.13-01: An ISO/IEC 18013-5 EAA shall not incorporate any component implementing the semantics specified in clause 4.2.13 of the present document.

7.3 Attested attributes

EAA-7.2.13-01: An ISO/IEC 18013-5 EAA shall include each attested attribute, regardless it is disclosable or not, in one `IssuerSignedItem` component, and shall be incorporated to the ISO/IEC 18013-5 EAA as specified in clause 8.3.2.1.2.2 of ISO/IEC 18013-5 [17].

7.4 Attested Attributes metadata

7.4.1 Introduction

Editor's Note: To be completed

7.4.2 Support to selective disclosure of attested attributes

7.4.2.1 General requirements

EAA-7.4.2.1-01: An ISO/IEC 18013-5 EAA shall use the `MobileSecurityObject` for supporting the selective disclosure of attested attributes.

7.4.2.2 Disclosure schema identifier

EAA-7.4.2.2-01: An ISO/IEC 18013-5 EAA shall include the `version` component within its `MobileSecurityObject`.

7.4.2.3 Disclosure

EAA-7.4.2.3-01: An ISO/IEC 18013-5 EAA containing disclosable attributes, shall include each disclosure in one `IssuerSignedItem` component, and shall be incorporated to the ISO/IEC 18013-5 EAA as specified in clause 8.3.2.1.2.2 of ISO/IEC 18013-5 [17].

7.4.2.4 Disclosure reference

EAA-7.4.2.4-01: For an ISO/IEC 18013-5 EAA, the `valueDigests` component shall implement the semantics specified in clause 4.4.2.3 of the present document.

EAA-7.4.2.4-02: If an ISO/IEC 18013-5 EAA includes selectively disclosable attested attributes, it shall include the `valueDigests` component within its `MobileSecurityObject`, as specified in clause 9.1.2.4 of ISO/IEC 18013-5 [17] for supporting the semantics specified in clause 4.4.2.3 of the present document.

7.4.2.5 Disclosure algorithm identifier

EAA-7.4.2.5-01: An ISO/IEC 18013-5 EAA containing disclosable attributes, shall include the `digestAlgorithm` component within its `MobileSecurityObject`.

7.5 EAA digital signature

7.5.1 General requirements

Editor's Note: to be completed.

7.5.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed.

7.5.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed.

7.5.4 Requirements for the signing certificate

7.5.4.1 General requirements

Editor's Note: to be completed.

7.5.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed. Either the certificate is within the EU-QEAA (in the signature, for instance) or the EU-QEAA has data indicating from where the certificate can download it free of charge.

7.5.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed. Either the certificate is within the EU-EAA-PubA (in the signature, for instance) or the EU-EAA-PubA has data indicating from where the certificate can download it free of charge.

8 Implementation of EAA based on W3C Verifiable Credentials (W3C-VC)

8.1 General requirements

Clause 8 of the present document specifies a realization of EAA based on W3C Candidate Recommendation Draft (19 October 2024): "Verifiable Credentials Data Model v2.0" [1].

The EAAs implemented according to clause 8 of the present document, will be designated as W3C-VC EAA hereinafter.

Editor's Note: to be completed

8.2 EAA metadata

8.2.1 EAA Context

8.2.1.1 General requirements

EAA-8.2.1.1-01: The `@context` component shall implement the semantics specified in clause 4.2.1 of the present document.

EAA-8.2.1.1-02: A W3C-VC EAA shall incorporate the `@context` component.

EAA-8.2.1.1-03: In a W3C-VC EAA the contents of the `@context` component shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 4.1.

8.2.1.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: To be completed.

8.2.1.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: To be completed.

8.2.2 EAA type

8.2.2.1 General requirements

EAA-8.2.2.1-01: The `type` component shall implement the semantics specified in clause 4.2.2 of the present document.

EAA-8.2.2.1-02: A W3C-VC EAA shall incorporate the `type` component.

EAA-8.2.2.1-03: In a W3C-VC EAA the contents of the `type` component shall be as specified in Verifiable Credentials Data Model v2.0, [1], clause 4.5.

8.2.2.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-8.2.2.2-01: W3C-VC EU-QEAA shall include within the `type` array, one element whose value shall be the URI defined in requirement EU-QEAA-4.2.2.3-02 (`urn:etsi:eaa:eu:qualified`).

8.2.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-8.2.2.3-01: W3C-VC EU-EAA-PubA shall include within the `type` array, one element whose value shall be the URI defined in requirement EU-EAA-PubA-4.2.2.4-02 (`urn:etsi:eaa:eu:pubA`).

8.2.3 EAA identifier

EAA-8.2.3-01: The `id` component shall implement the semantics specified in clause 4.2.3 of the present document.

EAA-8.2.3-02: A W3C-VC EAA shall incorporate the `id` component.

EAA-8.2.3-03: In a W3C-VC EAA the contents of the `id` component shall be as specified in Verifiable Credentials Data Model v2.0, [1], clause 4.2.

8.2.4 EAA issuer identifier

8.2.4.1 General requirements

EAA-8.2.4.1-01: The `issuer` component shall implement the semantics specified in clause 4.2.4 of the present document.

EAA-8.2.4.1-02: A W3C-VC EAA shall incorporate the `issuer` component.

EAA-8.2.4.1-03: In a W3C-VC EAA the contents of the `issuer` component shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 4.5.

8.2.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed

8.2.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed

8.2.5 EAA and attribute subject identifiers and pseudonyms

8.2.5.1 The EAA subject identifier

EAA-8.2.5.1-01: In Electronic Attestations of Attributes implemented according to the W3C Verifiable Credentials, which do not incorporate a pseudonym for the EAA subject, and whose `credentialSubject` array has more than one element, the `id` field of one of these array elements shall contain the EAA identifier.

EAA-8.2.5.1-02: In Electronic Attestations of Attributes implemented according to the W3C Verifiable Credentials, which do not incorporate a pseudonym for the EAA subject, and whose `credentialSubject` array has only one element, its `id` field shall contain the EAA subject identifier.

NOTE: This is so because in Verifiable Credentials Data Model v2.0 [1] this is the only component defined for including identifiers of both the EAA subject identifier or attribute subject identifiers.

8.2.5.2 The EAA subject pseudonym

Editor's Note: Verifiable Credentials Data Model v2.0 [1] does not include any data element for a pseudonym. If this profile has also to cover this case, it is required to define new data elements. To be completed.

8.2.5.3 The attribute subject identifier

EAA-8.2.5.3-01: In Electronic Attestations of Attributes implemented according to the W3C Verifiable Credentials, which do not incorporate any pseudonym for any of the attribute subjects, and whose `credentialSubject` array has more than one element, the `id` field of one of these array elements shall contain the identifier of the EAA subject, and the `id` fields of the other elements in `credentialSubject` array shall contain identifiers of other attribute subjects.

8.2.5.4 The attribute subject pseudonym

Editor's Note: Verifiable Credentials Data Model v2.0 [1] does not include any data element for a pseudonym. If this profile has also to cover this case, it is required to define new data elements. To be completed.

8.2.5.5 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed.

8.2.5.6 Requirements for Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed.

8.2.6 EAA issuance time

EAA-8.2.6-01: The `issuedAt` component shall implement the semantics specified in clause 4.2.6 of the present document.

EAA-8.2.6-02: A W3C-VC EAA may incorporate the `issuedAt` component.

EAA-8.2.6-03: Its contents shall be a string value of a combined date-time string as specified in W3C Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes" [15] clause 3.3.7.

EAA-8.2.6-04: Its content shall meet the requirements specified in clause 4.2.6.2 of the present document.

8.2.7 EAA validity period

EAA-8.2.7-01: The `validFrom` component shall implement the semantics of the first instant time specified in clause 4.2.7 of the present document.

EAA-8.2.7-02: The `validUntil` component shall implement the semantics of the second instant time specified in clause 4.2.7 of the present document.

EAA-8.2.7-03: A W3C-VC EAA shall incorporate the `validFrom` and `validUntil` components.

EAA-8.2.7-04: The content of `validFrom` and `validUntil` shall be a string value of a combined date-time string as specified in W3C Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes" [15] clause 3.3.7.

EAA-8.2.7-05: The contents of `validFrom` and `validUntil` shall meet the requirements specified in clause 4.2.6.2 of the present document.

8.2.8 Components constraining the usage of EAA

8.2.8.1 EAA audience

EAA-8.2.8.1-01: The `aud` component shall implement the semantics specified in clause 4.2.8.2 of the present document.

EAA-8.2.8.1-02: A W3C-VC EAA may incorporate the `aud` component.

EAA-8.2.8.1-03: Its contents shall be as specified in IETF RFC 7519 [5], clause 4.1.3.

8.2.8.2 Signal of one-time use

EAA-8.2.8.2-01: The `oneTime` component shall implement the semantics specified in clause 4.2.8.3 of the present document.

EAA-8.2.8.2-02: A W3C-VC EAA may incorporate the `oneTime` component.

Editor's Note: to be completed.

8.2.9 Attributes evidence

EAA-8.2.9-01: The `evidence` component shall implement the semantics specified in clause 4.2.9 of the present document.

EAA-8.2.9-02: A W3C-VC EAA may incorporate the `evidence` component.

EAA-8.2.9-03: Its contents shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 5.7 of the present document.

8.2.10 EAA status service

8.2.10.1 General requirements

EAA-8.2.10.1-01: The `credentialStatus` component shall implement the semantics specified in clause 4.2.10 of the present document.

EAA-8.2.10.1-02: A W3C-VC EAA may incorporate the `credentialStatus` component.

Below follows the definition of `credentialStatus` component, as defined within the definitions section in the JSON Schema file whose location is detailed in Annex C, and is copied below for information:

```
"credentialStatus": {"$ref": "#/definitions/service"}
```

Below follows the definition of `service` JSON type, which shall be defined within the definitions section in the JSON Schema file whose location is detailed in Annex C, and is copied below for information.

```
"service": {
    "type": "object",
    "properties": {
        "id": {"type": "string", "format": "uri-reference"},
        "type": {"type": "string"}
    },
    "required": ["id","type"],
    "additionalProperties": false
}
```

EAA-8.2.10.1-03: Within this JSON object, `id` member shall contain an URI reference referencing the service that provides the EAA status information.

EAA-8.2.10.1-04: Within this JSON object, `type` member shall contain the name of the protocol to be used for requesting the EAA status information to the service.

8.2.10.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: To be completed. For EU-QEAA the presence of the EAA status service will be mandatory.

8.2.10.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: To be completed. For EU-EAA-PubA, the presence of the EAA status service will be mandatory

8.2.11 EAA refresh service

EAA-8.2.11-01: The `refreshService` component shall implement the semantics specified in clause 4.2.11 of the present document.

EAA-8.2.11-02: A W3C-VC EAA may incorporate the `refreshService` component.

Below follows the definition of `refreshService` component, as defined within the definitions section in the JSON Schema file whose location is detailed in Annex C, and is copied below for information:

```
"refreshService": {"$ref": "#/definitions/service"}
```

EAA-8.2.11-03: Within this JSON object, `id` member shall contain an URI reference referencing the service able to refresh the EAA.

EAA-8.2.11-04: Within this JSON object, `type` member shall contain the name of the protocol to be used for requesting the EAA refreshing to the service.

8.2.12 EAA verification schema service

EAA-8.2.12-01: The `credentialSchema` component shall implement the semantics specified in clause 4.2.12 of the present document.

EAA-8.2.12-02: A W3C-VC EAA may incorporate the `credentialSchema` component.

EAA-8.2.12-03: Its contents shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 5.4 for data verification schemas.

8.2.13 EAA encoding schema

EAA-8.2.13-01: The `credentialSchema` component shall implement the semantics specified in clause 4.2.13 of the present document.

EAA-8.2.13-02: A W3C-VC EAA may incorporate the `credentialSchema` component.

EAA-8.2.13-03: Its contents shall be as specified in Verifiable Credentials Data Model v2.0 [1], clause 5.4 for data encoding schemas.

8.3 Attested Attributes

EAA-8.3-01: An attested attribute within the `credentitalSubject` component may contain an `id` member as specified in Verifiable Credentials Data Model v2.0 [1], clauses 4.2 and 4.4.

8.4 Attested Attributes metadata

8.4.1 Introduction

Editor's Note: To be completed

8.4.2 Support to selective disclosure of attested attributes

8.4.2.1 Introduction

Editor's Note: to be completed.

8.4.2.2 Disclosure schema identifier

Editor's Note: to be completed.

8.4.2.3 Disclosure

Editor's Note: to be completed.

8.4.2.4 Disclosure reference

Editor's Note: to be completed.

8.4.2.5 Disclosure algorithm identifier

Editor's Note: to be completed.

8.5 EAA digital signature

8.5.1 General requirements

Editor's Note: to be completed.

8.5.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed.

8.5.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed.

8.5.4 Requirements for the signing certificate

8.5.4.1 General requirements

Editor's Note: to be completed.

8.5.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed. Either the certificate is within the EU-QEAA (in the signature, for instance) or the EU-QEAA has data indicating from where the certificate can download it free of charge.

8.5.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed. Either the certificate is within the EU-EAA-PubA (in the signature, for instance) or the EU-EAA-PubAhas data indicating from where the certificate can download it free of charge.

9 Implementation of EAA based on X.509 Attribute Certificates (X.509-AC)

9.1 General requirements

Clause 9 of the present document defines a realization of EAA based on X.509 Attribute certificates as specified in RFC 5755: "An Internet Attribute Certificate Profile for Authorization" [10].

The EAAs implemented according to clause 9 of the present document, will be designated as X.509-AC EAA hereinafter.

Editor's Note: to be completed

9.2 EAA metadata

9.2.1 EAA Context

9.2.1.1 General requirements

EAA-9.2.1.1-01: A X.509-AC EAA shall have its `version` field set to v2. This will explicitly set the EAA context as follows:

- All the information about the issuer shall be derived from the values of the following members: `issuer` field, `issuerUniqueID` field, `authorityKeyIdentifier` extension, `authorityInfoAccess` extensions, and `crlDistributionPoints` extension.

NOTE: RFC 5755 [10] specifies extensions as optional components in an Attribute Certificate.

- All the information required about the subject shall be derived from the values of the following members: `holder` field.

9.2.1.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: To be completed.

9.2.1.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: To be completed.

9.2.2 EAA type

9.2.2.1 General requirements

EAA-9.2.2.1-01: X.509-AC EAA which are neither X.509-AC EU-QEAA nor X.509-AC EU-EAA-PubA, shall not have any component indicating its type.

NOTE 1: Any X.509 Attribute Certificate is an EAA per se. X.509-AC EU-QEAA and X.509-AC EU-EAA-PubA need this data for signalling precisely that they are EU-QEAA and EU-EAA-PubA, respectively. But the rest of X.509-AC EAA does not need it.

Editor's Note: feedback is required on whether the former requirements on X.509-AC EAA which are neither X.509-AC EU-QEAA nor X.509-AC EU-EAA-PubA, are OK or they should include an extension identifying them as such objects.

9.2.2.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-9.2.2.2-01: A X.509-AC EU-QEAA shall incorporate the extensión `qeaaStatements`, which is defined as in the ASN.1 module included within file ASN1_FILE_IN_ETSI_FORGE, whose location is detailed in Annex A and is copied below for information.

```
id-etsi-qeaas-x509AC-prof-identifiers       OBJECT IDENTIFIER ::= { itu-t(0)
identifiedorganization(4) etsi(0) id-qeaas-profile(194721) 1 }

etsi-qeaaStatements  EXTENSION ::= {
          SYNTAX              QEAAStatements
          IDENTIFIED BY       id-qeaa-qaaStatements }

id-qeaas-qaaStatements     OBJECT IDENTIFIER ::= { id-etsi-qeaas-x509AC-prof-identifiers 1 }

      QEAAStatements ::= SEQUENCE OF QEAAStatement
      QEAAStatement ::= SEQUENCE {
          statementId   QEAA-STATEMENT.&Id({SupportedStatements}),
          statementInfo QEAA-STATEMENT.&Type
          ({SupportedStatements}{@statementId}) OPTIONAL }

      SupportedStatements QEAA-STATEMENT ::= { esi-qaaStatement-1, esi-eaaPubAStatement-1}
```

EU-QEAA-9.2.2.2-02: The `qeaaStatements` extension shall not be marked as critical.

EU-QEAA-9.2.2.2-03: A X.509-AC EU-QEAA shall incorporate the `QEAA-Statement` that is defined as in the ASN.1 module included within file ASN1_FILE_IN_ETSI_FORGE, whose location is detailed in Annex A, and is copied below for information.

```
esi-qaaStatement-1 QEAA-STATEMENT ::= { IDENTIFIED BY id-etsi-eqaas-EUqeaaCompliance }

id-etsi-eqaas-EUqeaaCompliance::= { id-qeaas-qaaStatements 1}
```

9.2.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-9.2.2.3-01: A X.509-AC EU-EAA-PubA shall incorporate the extension `qeaaStatements` specified in clause 9.2.2.2 of the present document.

EU-EAA-PubA-9.2.2.3-02: The `qeaaStatements` extension shall not be marked as critical.

EU-EAA-PubA-9.2.2.3-03: A X.509-AC EU-EAA-PubA shall incorporate the `QEAA-Statement` that is defined as in the ASN.1 module included within file ASN1_FILE_IN_ETSI_FORGE, whose location is detailed in Annex A, and is copied below for information.

```
esi-eaaPubAStatement-1 QEAA-STATEMENT ::= { IDENTIFIED BY id-etsi-eaaPubA-EUeaaPubACompliance }

id-etsi-eaaPubA-EUeaaPubACompliance::= { id-qeaas-qaaStatements 2}
```

9.2.3 EAA identifier

EAA-9.2.3-01: A X.509-AC EAA shall contain the `serialNumber` field, whose value, with the value of the `issuer` field, shall identify the EAA itself.

9.2.4 EAA issuer identifier

9.2.4.1 General requirements

EAA-9.2.4.1-01: A X.509-AC EAA shall contain the `issuer` field as specified in RFC 5755 [10].

EAA-9.2.4.1-02: Its value shall be a distinguished name (`dNSName` choice of `GeneralNames` type as specified in IETF RFC 5280: "PKIX Certificate and CRL Profile" [14]) within `v2Form` choice of `AttCertIssuer` type.

EAA-9.2.4.1-03: A X.509-AC EAA may contain the `issuerUniqueID` field, as specified in RFC 5755 [10], clause 4.2.8.

9.2.4.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed

9.2.4.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed

9.2.5 EAA and attribute subject identifiers and pseudonyms

9.2.5.1 EAA subject identifier

EAA-9.2.5.1-01: A X.509-AC EAA shall contain only the EAA subject identifier.

EAA-9.2.5.1-02: The EAA subject identifier shall be present in the `holder` field. Its contents shall be as specified in RFC 5755 [10], clause 4.2.2.

EAA-9.2.5.1-03: In a X.509-AC EAA the `holder` field shall include the `objectDigestInfo` field, which in turn, shall have the `publickeycert` value as specified in RFC 5755 [10] clause 7.3.

9.2.5.2 EAA subject pseudonym

Editor's Note: to be completed.

9.2.5.3 The attribute subject identifier

EAA-9.2.5.3-01: In a X.509-AC EAA all the attributes shall refer to the EAA subject attribute. Therefore, there shall not be any specific component for containing identifiers for different attribute subjects.

9.2.5.4 The attribute subject pseudonym

Editor's Note: to be completed.

9.2.5.5 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed.

9.2.5.6 Requirements for Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed.

9.2.6 EAA issuance time

EAA-9.2.6-01: A X.509-AC EAA shall not contain an indication of the instant when the EAA was generated.

9.2.7 EAA validity period

EAA-9.2.7-01: A X.509-AC EAA shall contain the EAA validity period within the `attrCertValidityPeriod` field. Its contents shall be as specified in RFC 5755 [10], clause 4.1.2.5.

EAA-9.2.7-02: The contents of `notBeforeTime` and `notAfterTime` fields of `attrCertValidityPeriod` shall meet the requirements specified in clause 4.2.6.2 of the present document.

9.2.8 Components constraining the usage of the EAA

9.2.8.1 EAA audience

EAA-9.2.7-01: A X.509-AC EAA shall identify the set of relying parties the EAA is intended for within the `id-ce-targetInformation` extension specified in RFC 5755 [10], clause 4.3.2.

9.2.8.2 Signal of one-time use

9.2.8.2.1 General requirements

EAA-9.2.8.2.1-01: If a X.509-AC EAA needs to indicate that the EAA shall be used only once, and that it shall not be retained for future use, it shall include the `oneTimeUse` extension.

EAA-9.2.8.2.1-02: The `oneTimeUse` extension shall be defined as in the ASN.1 module included within file ASN1_FILE_IN_ETSI_FORGE, whose location is detailed in Annex A, and is copied below for information.

Editor's Note: to be completed.

```
-- Extension for oneTimeUse certificate

id-etsi-qeaas-extensions ::= { id-etsi-qeaas-x509AC-prof-identifiers 2 }

id-etsi-qeaas-ext-oneTimeUse        OBJECT IDENTIFIER ::= { id-etsi-qeaas-extensions 1 }

etsi-qeaas-ext-oneTimeUse-certs     EXTENSION ::= { IDENTIFIED BY id-etsi-qeaas-ext-oneTimeUse }
```

EAA-9.2.8.2.1-03: If the X.509-AC EAA contains this extension then it shall not contain the `id-ce-cRLDistributionPoints` extension specified in in RFC 5755 [10], clause 4.3.5.

EAA-9.2.8.2.1-04: If the X.509-AC EAA contains this extension then it shall contain the `id-ce- noRevAvail` extension specified in in RFC 5755 [10], clause 4.3.6.

9.2.8.2.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: X.509-AC EU-QEAA will have indication of the status service. Therefore the two last requirements of 9.2.8.2 do not apply. To be completed

9.2.8.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: X.509-AC EU-EAA-PubA will have indication of the status service. Therefore the two last requirements of 9.2.8.2 do not apply. To be completed

9.2.9 Attributes evidence

EAA-9.2.9-01: A X.509-AC EAA shall not include this component.

9.2.10 EAA status service

9.2.10.1 General requirements

EAA-9.2.10.1-01: If a X.509-AC EAA provides to the relying party the information or location of the services that can be used to enquire about the validity status of the EAA, it shall place this information either within the extension identified by the OID `id-pe-authorityInfoAccess` (specified in IETF RFC 5280 [14], clause 4.2.2.1) with the `accessMethod` field set to `id-ad-ocsp`, or the within the extension identified by the OID `id-ce-cRLDistributionPoints` (specified in IETF RFC 5280 [14], clause 4.2.1.13), or in both.

EAA-9.2.10.1-02: If a X.509-AC EAA does not provide to the relying party the information or location of the services that can be used to enquire about the validity status of the X.509-AC EAA, it shall include within the X.509 Attribute Certificate the extension identified by the OIS `id-ce-noRevAvail` specified in RFC 5755 [13], clause 4.3.6.

EAA-9.2.10.1-03: The extension identified by the OID `id-pe-authorityInfoAccess` X.509-AC EAA may contain one instance of type `AccessDescription` with its `accessMethod` field set to `id-ad-caIssuers`, and with its `accessLocation` field pointing to the certificate of the EAA Issuer for supporting the validation of the signature of the EU-EAA.

9.2.10.2 Requirements for EU Qualified EAA (EU-QEAA)

EU-QEAA-9.2.10.2-01: A X.509-AC EU-QEAA shall contain the extension identified by the OID `id-pe-authorityInfoAccess`.

EU-QEAA-9.2.10.2-02: In a X.509-AC EU-QEAA the extension identified by the OID `id-pe-authorityInfoAccess` shall contain one instance of type `AccessDescription` as with its `accessMethod` field set to `id-ad-caIssuers`, and its `accessLocation` field shall point to the certificate of the EU-QEAA Issuer for supporting the validation of the signature of the EU-QEAA.

NOTE: The requirement on the value of `accessMethod` field is included for meeting the requirements defined in eIDAS 2.0 annex V.

9.2.10.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

EU-EAA-PubA-9.2.10.3-01: A X.509-AC EU-EAA-PubA shall contain the extension identified by the OID `id-pe-authorityInfoAccess`.

EU-EAA-PubA-9.2.10.3-02: In a X.509-AC EU-EAA-PubA the extension identified by the OID `id-pe-authorityInfoAccess` shall contain one instance of of type `AccessDescription` with its `accessMethod` field set to `id-ad-caIssuers`, and its `accessLocation` field shall point to the certificate of the EU-EAA-PubA Issuer for supporting the validation of the signature of the EU-EAA-PubA.

NOTE: The requirement on the value of `accessMethod` field is included for meeting the requirements defined in eIDAS 2.0 annex VII.

9.2.11 EAA refresh service

Editor's Note: to be completed.

9.2.12 EAA verification schema service

EAA-9.2.12-01: A X.509-AC EAA shall not include this component.

NOTE: The OID of each attribute within the Attribute Certificate shall identify the schema that that attribute has to be verified against.

9.2.13 EAA verification schema service

EAA-9.2.13-01: A X.509-AC EAA shall not incorporate this component.

9.3 Attested attributes

9.3.1 General requirements

EAA-9.3.1-01: A X.509-AC EAA shall incorporate each individual Attested Attribute as an instance of the `Attribute` type specified in clause 4.2.7 of RFC 5755 [10].

EAA-9.3.1-02: A X.509-AC EAA shall place the individual Attested Attributes in the `attributes` field.

EAA-9.3.1-03: The present document specifies two implementations for including attested attributes within in the `attributes` field, namely: as JSON tokens (X.509 AC/JSON implementation) or as instances of ASN.1 types (X.509 AC/ASN.1 implementation).

9.3.2 Attested attributes for X509 AC/JSON implementation

EAA-9.3.2-01: A X.509-AC EAA conformant to the X.509 AC/JSON implementation, shall place the attributes within one instance of `JSONEncodedAttribute`.

EAA-9.3.2-02: `JSONEncodedAttribute` shall be defined as in the ASN.1 module included within file ASN1_FILE_IN_ETSI_FORGE, whose location is detailed in Annex A, and is copied below for information.

```
-- Attribute for JSON encoded attribute

id-etsi-qeaas-attributes ::= { id-etsi-qeaas-x509AC-prof-identifiers 3 }

id-etsi-qeaas-ext-jsonattr      OBJECT IDENTIFIER ::= { id-etsi-qeaas-attributes 1 }

etsi-qeaas-ext-jsonattr     ATTRIBUTE ::= {SYNTAX JSONEncodedAttribute IDENTIFIED BY id-etsi-qeaas-
ext-jsonattr }

JSONEncodedAttribute  ::= UTF8String        -- The set has only ONE element, with the JSON string
UTF-8 encoded.
}
```

The set in the attribute value shall contain only one element, whose value shall be a JSON claim.

9.3.3 Attested attributes for X509 AC/ASN.1 implementation

EAA-9.3.3-01: Within a X.509-AC EAA conformant to the X.509 AC/ASN.1, each attribute shall be a DER-encoded instance of a specific ASN.1 type, and shall be placed within the `attributes` sequence as specified in RFC 5755 [10], clause 4.2.7.

9.4 Attested attributes metadata

9.4.1 Implementation of support to selective disclosure of Attested Attributes

EAA-9.4.1-01: A X.509-AC EAA can achieve selective disclosure through atomic EAAs, i.e. X509 Attribute Certificates attesting only one attribute.

EAA-9.4.1-02: EAAs Issuer issuing X.509-AC EAA should support the selective disclosure with the issuance of atomic X.509 ACs.

9.5 EAA digital signature

9.5.1 General requirements

EAA-9.5.1-01: A X.509-AC EAA shall be signed with the private key of the issuer as defined in RFC 5755.

Editor's Note: to be completed.

9.5.2 Requirements for the signing certificate

9.5.2.1 General requirements

Editor's Note: to be completed.

9.5.2.2 Requirements for EU Qualified EAA (EU-QEAA)

Editor's Note: to be completed. Either the certificate is within the EU-QEAA (in the signature, for instance) or the EU-QEAA has data indicating from where the certificate can download it free of charge.

9.5.2.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (EU-EAA-PubA)

Editor's Note: to be completed. Either the certificate is within the EU-EAA-PubA (in the signature, for instance) or the EU-EAA-PubA has data indicating from where the certificate can download it free of charge.

10 Implementation of Hybrid EAA

Editor's Note: Hybrid EAAs are objects that contain two parts: a machine-readable EAA part, implemented using one of the implementations specified by the present document in clauses 5 to 9, and a human-readable part. Both parts are generated by the EAA issuer, which seals their combination.

Editor's Note: To be completed

11 Requirements on EAA components not specified in the present document

EAA-11-01: Any component of an EAA that is not specified in the present document may be ignored.

Annex A (normative): ASN.1 files

The file at ASN1_FILE_IN_ETSI_FORGE_LINK (ASN1_FILE_IN_ETSI_FORGE) contains the definitions of the ASN.1 types and elements defined in the present document.

Annex B (normative): CBOR schema files

The file at CBOR_FILE_IN_ETSI_FORGE_LINK (CBOR_FILE_IN_ETSI_FORGE) contains the definitions of the CBOR types and defined in the present document.

Annex C (normative): JSON schema files

The file at JSON_FILE_IN_ETSI_FORGE_LINK (JSON_FILE_IN_ETSI_FORGE) contains the definitions of the JSON types and defined in the present document.

Annex D (informative): Support to requirements of Annexes V and VII of eIDAS

Table 1 below shows which components in the TS 119 472-1 define requirements for EU Qualified EAA and for EAA issued by or on behalf of a public body responsible for an authentic source.

Table 1: components specified in TS 119 472-1 that define requirements for Annexes V and VII of eIDAS 2.

Component	QEAA Annex V requirement	EAA PubA AnnexVII requirement
EAA context	(f): indication of scheme of attestations	(f): indication of scheme of attestations
EAA type	(a)	(a)
EAA identifier	(f) attestation identity code	(f) attestation identity code
EAA issuer identifier	(b)	(b)
EAA subject identifier / EAA subject pseudonym	(c)	(c)
Attribute subject identifier / Attribute subject pseudonym	(c)	(c)
EAA status service	(i)	(i)
EAA digital signature	(g)	(g)
EAA Signing certificate	(h)	(h)
Validity period	(e)	(e)
Attested attributes	(d)	(d)

Annex E (informative): TS development status

Table 2 shows the status of TS 119 472-1 as per 2024/12/16

The following legend is used in its cells:

TBD – To be Developed (nothing done yet)
TBC – To Be Completed (there is material but not complete)
D – Done

Table 2: Status of TS 119 472-1 as per 2024/12/12.

Component	EU QEAA / EU EAAPubA / General requirements	Data model - semantics	SD-JWT VC	ISO 18013-5	W3C VC	X.509 Attr Cert	SD-JWT VC DM	Hybrid EAA
EAA context	EU QEAA	D	D	TBD	TBD	TBC	TBD	TBD
	EU EAAPubA	D	D	TBD	TBD	TBC	TBD	TBD
	General requirements	D	D	TBD	D	D		
EAA type	EU QEAA	D	D	D	D	D	TBD	TBD
	EU EAAPubA	D	D	D	D	D	TBD	TBD
	General requirements	D	D	D	D	D	TBD	TBD
EAA identifier	EU QEAA	D	D	TBC	TBD	TBC	TBD	TBD
	EU EAAPubA	D	D	TBC	TBD	TBC	TBD	TBD
	General requirements	D	D	D	D	D	TBD	TBD
EAA issuer identifier	EU QEAA	D	D	D	TBD	TBD	TBD	TBD
	EU EAAPubA	D	D	D	TBD	TBD	TBD	TBD
	General requirements	D	D	D	D	D	TBD	TBD
EAA subject identifier	EU QEAA	D	D	TBC	TBC	TBC	TBD	TBD
	EU EAAPubA	D	D	TBC	TBC	TBC	TBD	TBD
	General requirements	D	D	D	D	D	TBD	TBD
EAA subject pseudonym	EU QEAA	D	D	TBD	TBD	TBD	TBD	TBD
	EU EAAPubA	D	D	TBD	TBD	TBD	TBD	TBD
	General requirements	D	D	TBD	TBD	TBD	TBD	TBD

Component	EU QEAA / EU EAAPubA / General requirements	Data model - semantics	SD-JWT VC	ISO 18013-5	W3C VC	X.509 Attr Cert	SD-JWT VC DM	Hybrid EAA
Attribute subject identifier	EU QEAA	D	D	TBC	TBC	TBC	TBD	TBD
	EU EAAPubA	D	D	TBC	TBC	TBC	TBD	TBD
	General requirements	D	TBD	TBC	D	D	TBD	TBD
Attribute subject pseudonym	EU QEAA	D	D	TBC	TBD		TBD	TBD
	EU EAAPubA	D	D	TBC	TBD		TBD	TBD
	General requirements	S	TBD	D	TBD		TBD	TBD
EAA issuance time		D	D	D	D	D	TBD	TBD
EAA validity period		D	D	D	D	D		
EAA audience		D	D	D	D	D	TBD	TBD
Signal of one-time-use		D	D	TBD	D	TBC	TBD	TBD
Attributes evidence		D	D	D	D	D	TBD	TBD
EAA status service	EU QEAA	D	D	D	TBC	D	TBD	TBD
	EU EAAPubA	D	D	D	TBC	D	TBD	TBD
	General requirements	D	D	D	D	D	TBD	TBD
EAA refresh service		D	D	D	D	TBD	TBD	TBD
EAA verification schema		D	D	TBD	D	D	TBD	

Component	EU QEAA / EU EAAPubA / General requirements	Data model - semantics	SD-JWT VC	ISO 18013-5	W3C VC	X.509 Attr Cert	SD-JWT VC DM	Hybrid EAA
EAA encoding schema		D	D	D	D	D	TBD	
Attestted attributes		D	D	D	D	D	TBD	
Support to selective disclosure		D	D	D	TBD	D	TBD	
EAA digital signature	EU QEAA	D	TBC	TBD	TBD	TBD	TBD	
	EU EAAPubA	D	TBD	TBD	TBD	TBD	TBD	
	General requirements	TBC	TBD	TBD	TBD	TBC	TBD	
Requirements for signing certificate	EU QEAA	D	D	TBD	TBD	TBD	TBD	
	EU EAAPubA	D	D	TBD	TBD	TBD	TBD	
	General requirements	TBC	TBD	TBD	TBD	TBD		

Annex F (informative): Change History

Date	Version	Information about changes
TBC	0.0.1	TBC
TBC	0.0.2	TBC
TBC	0.0.3	TBC
TBC	0.0.4	TBC
29/10/2023	0.0.5	Specified the semantics of components for supporting selective disclosure of Electronic Attributes. Included a clause for implementation of (Q)EAA to ISO/IEC 18013-5 / ISO/IEC23220. Included implementation of components for supporting slective disclosure of Electronic Attributes to MSO. Reworked former JWT/JWS implementation. No longer as one of the profiles associated to W3C Verifiable Credentials: versión 2.0 has dropped the JWT serialization for the moment. Now the JWT/JWS implementation has been converted to SD-JWT VC for incorporating selective disclosure of Electronic Attributes. Included implementation of components for supporting selective disclosure of Electronic Attributes to SD-JWT. In X.509 AC: . Requirement of caIssuers extension. . Inclusion of support of selective disclosure: EAA Issuer issues atomic X-509 ACs . Inclusion of missing Signature component . ASN.1 definition of JSONEncodedAttribute for X.509 AC/JSON implementation: an ASN.1 sequence for containing JSON-encoded Electronic Attributes
30/10/2023	0.06	Added two missing clauses in v0.0.5 Added Disclosure component in semantics. Added implementation to Disclosure component in SD-JWT implementation
Hereinafter follow the versions of the document as draft TS 119 472-1		
5/2/2024	0.0.1	Initial version of the document as part 1 of TS 119 472
1/5/2024	0.0.2	Completed first version of Implementation according to SD-JWT VC. Dropped uncomplete implementation based on W3C Verifiable Credentials. Dropped Semantics and Implementation of EAAs Presentations, which have been moved to TS 119 472-2
29/5/2024	0.0.3	Re-structured contents of semantics and implementations clauses as follows: AA Metadata, Attested Attributes, Attested Attributes metadata, Signature Re-structured Implementation with SD-JWT VC. Implemented agreements reached at the SD-JWT VC implementation editorial meeting conducted on 2/5/2024. Implemented first version of Implementation based on ISO/IEC 18013-5 Re-introduced Implementation based on W3C Verifiable Credentials (aligned with version 1.0; to be reviewed) Re-structured Implementation based on X.509 Attribute Certificates.
16/12/2024	0.0.4	Defined a complete notation for identifying EAAs implementations. Incorporated requirements for Qualified EAAs and EAAs issued by or on behalf of a public body responsible for an authentic source, including proposals for identifiers of issuers (both legal and natural persons). Inserted new realization of W3C Verifiable Credentials 2.0 Inserted placeholders for realization of SD-JET VC DM and for Hybrid EAAs.
23/12/2024	0.0.5	Editorial changes. Assigned identifiers to all the requirements. Some considerations added in realizations where there are issues for meeting the reuquirements for EU-QEAA and EU-EAA-PubA

Date	Version	Information about changes
13/01/2025	0.0.6	Scope includes mention to support to section 4 of Annex I of Implementing Act 2024/2977. Clause 3.3 fixes a wrong wording for general requirements applicable to any EAA and make it clear that the majority of requirements applicable to QEAA and EAA-PubA, (as in Annex V and VII) are based on generally applicable requirements. Some requirements that are mandatory for EU-QEAA and EU-EAA-PubA have been made optional for any EAA. Reworded requirements on presence of components, reworded to meet the ETSI Drafting Rules. Fixed editorial issues identified by ESI TO.

History

Document history		
<Version>	<Date>	<Milestone>