ETSI TS 119 472-1 V1.2.1 (2026-02)

TECHNICAL SPECIFICATION

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

Reference
RTS/ESI-0019472-1v121

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

The present document is part 1 of a multi-part deliverable covering profiles for Electronic Attestation of Attributes, as identified below:

Part 1: "General requirements";

Part 2: "Profiles for EAA/PID Presentations to Relying Party";

Part 3: "Profiles for issuance of EAA or PID".

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 [i.2] 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 Regulation (EU) 2024/1183 [i.2] clause 4.

3) Defines 4 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 Regulation (EU) 2024/1183 [i.2], particularized for the different realizations. Below follows the list of realizations:

   a) SD-JWT VC. Realization based on SD-JWT VC (clause 5). SD-JWT VC is specified in IETF SD-JWT [5].

   b) ISO/IEC-mdoc. Realization based on the structures defined in ISO/IEC 18013-5 [12], suitably extended by the present document, and data elements defined in ISO/IEC 18013-5 [12], ISO/IEC 23220-2 [13], and the present document.

NOTE: ISO/IEC 18013-5 [12] defines a namespace and a set of elements (placed in the mentioned namespace) suitable for EAAs that are mobile driving licenses. ISO/IEC 23220-2 [13] defines another namespace and a set of elements of general use in any type of electronic document, suitable for EAAs that are NOT mobile driving licenses.

   c) JSON-LD W3C-VC. Realization based on JSON-LD serialization of W3C Verifiable Credentials Data Model (clause 7). W3C Verifiable Credentials Data Model is specified in W3C Recommendation (15 May 2025): "Verifiable Credentials Data Model v2.0" [1].

   d) X.509-AC. Realization based on X.509 Attribute Certificates (clause 8). X.509 Attribute Certificates are specified in IETF RFC 5755 [6].

4) Aims to support the Commission Implementing Regulation (EU) 2024/2977 [i.3].

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 in the ETSI docbox.

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® Recommendation (15 May 2025): "Verifiable Credentials Data Model v2.0".

[2] W3C® Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE". (W3C VC_JOSE_COSE).

[3] IETF SD-JWT VC draft-ietf-oauth-sd-jwt-vc-13: "SD-JWT-based Verifiable Credentials (SD-JWT VC)", November 2025.

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

[5] IETF SD-JWT draft-ietf-oauth-selective-disclosure-jwt-22: "Selective Disclosure for JWTs (SD-JWT)", May 2025.

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

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

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

[9] IETF RFC 5280 (May 2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[10] W3C® Recommendation (5 April 2012): "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes".

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

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

[13] 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".

[14] IETF RFC 7800 (April 2016): "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)".

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

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

[17] ETSI TS 119 412-6: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers".

[18] W3C® Recommendation (15 May 2025): "Data Integrity ECDSA Cryptosuites v1.0".

[19] W3C® Candidate Recommendation (3 April 2025): "Data Integrity BBS Cryptosuites v1.0".

[20] IETF RFC 9360 (February 2023): "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates".

[21] JSON Schema Core: "JSON Schema: A Media Type for Describing JSON Documents".

[22] IETF RFC 8610 (June 2019): "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures".

[23] W3C® Recommendation (20 July 2017): "Shapes Constraint Language (SHACL)".

[24] W3C® Recommendation (15 May 2025): "Bitstring Status List v1.0".

[25] IETF draft-ietf-oauth-status-list-13: "Token Status List (TSL)".

[26] W3C® Recommendation (15 May 2025): "Verifiable Credential Data Integrity v1.0".

[27] IETF RFC 5646 (September 2009): "Tags for Identifying Languages".

[28] IETF RFC 6960 (June 2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[29] W3C® Recommendation (16 July 2020): "JSON-LD 1.1. A JSON-based Serialization for Linked Data".

[30] IETF RFC 7517 (May 2015): "JSON Web Key (JWK)".

[31] OpenId Fundation: "OpenID Identity Assurance Schema Definition 1.0", October 2024.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

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

[i.2] 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.

[i.3] 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.4] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.5] EU Architecture and Reference Framework version 2.4.0.

[i.6] EUDI Wallet TS11: "Specification of interfaces and formats for the catalogue of attributes and the catalogue of attestations".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 119 471 [i.1] and the following apply:

EAA administrative validity period: date(s) from and/or up to which the attributes in the EAA are valid, which are represented as attribute(s) in the attestation

NOTE: Definition taken from the ARF [i.5].

EAA technical validity period: dates (and possibly times) from and up to which the EAA is valid

NOTE: Definition taken from the ARF [i.5].

Electronic Attestation of Attributes context: 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 issued by or on behalf of a public body responsible for an authentic source (PuB-EAA): electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII of eIDAS2 Regulation [i.2]

Electronic Attestation of Attributes Presentation (EAAP): tampered-proof presentation of an electronic attestation of attributes built in such a way that the subject of the EAA presented can be trusted through a cryptographic verification

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Attribute Certificate
API	Application Programming Interface
ARF	EU Architecture and Reference Framework
ASN.1	Abstract Syntax Notation 1
CBOR	Concise Binary Object Representation
CIR	Commission Implementing Regulation
COSE	CBOR Object Signing and Encryption
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DID	Decentralized Identifier
EAA	Electronic Attestation of Attributes
EAAP	Electronic Attestation of Attributes Presentation
ECDSA	Elliptic Curve Digital Signature Algorithm
ISO/IEC-mdoc EAA	EAA implemented using the structures of ISO/IEC 18013-5 [12] and the data elements defined in ISO/IEC 18013-5 [12] and ISO/IEC 23220-2 [13] as specified in the present document
ISO/IEC-mdoc PuB-EAA	PuB-EAA implemented using the structures of ISO/IEC 18013-5 [12] and the data elements defined in ISO/IEC 18013-5 [12] and ISO/IEC 23220-2 [13] as specified in the present document
ISO/IEC-mdoc QEAA	QEAA implemented using the structures of ISO/IEC 18013-5 [12] and the data elements defined in ISO/IEC 18013-5 [12] and ISO/IEC 23220-2 [13] as specified in the present document
JOSE	JSON Object Signing and Encryption
JSON-LD W3C VC JOSE	JSON-LD W3C Verifiable Credentials secured with JOSE.
JSON-LD W3C VC SD-JWT	JSON-LD W3C Verifiable Credentials secured with SD-JWT
JSON-LD W3C-VC EAA	EAA implemented with JSON-LD serialization of "Verifiable Credentials Data Model v2.0" [1] as specified in the present document
JSON-LD W3C-VC PuB-EAA	PuB-EAA implemented with "Verifiable Credentials Data Model v2.0" [1] as specified in the present document
JSON-LD W3C-VC QEAA	QEAA implemented with "Verifiable Credentials Data Model v2.0" [1] as specified in the present document
JSON-LD W3C-VC	JSON-LD serialized W3C Verifiable Credentials
JWS	JSON Web Signature
JWT	JSON Web Token
LD	Linked Data
mDL	mobile Driving Licence
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PID	Personal Identification Data
PSB	Public Sector Body
PuB-EAA	Electronic Attestation of Attributes issued by or on behalf of a public body responsible for an authentic source

QEAA	Qualified Electronic Attestation of Attributes
RDF	Resource Description Framework
SD-JWT VC EAA	EAA implemented with IETF SD-JWT VC [3] as specified in the present document
SD-JWT VC PuB-EAA	PuB-EAA implemented with IETF SD-JWT VC [3] as specified in the present document
SD-JWT VC QEAA	QEAA implemented with IETF SD-JWT VC [3] as specified in the present document
SD-JWT VC	Selective Disclosure based JSON Web Token Verifiable Credentials
SD-JWT	Selective Disclosure based JSON Web Token
SHA	Secured Hash Algorithm
SHACL	Shapes Constraint Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
VAT	Value Added Tax
VC	Verifiable Credential
X.509-AC EAA	EAA implemented with IETF RFC 5755 [6] as specified in the present document
X.509-AC PuB-EAA	PuB-EAA implemented with IETF RFC 5755 [6] as specified in the present document
X.509-AC QEAA	QEAA implemented with IETF RFC 5755 [6] as specified in the present document
X.509-AC	X.509 Attribute Certificate
XML	Extensible Markup Language
XSD	XML Schema Definition

3.4 Notation

The present document assigns one identifier for each requirement.

The present document uses the terms "signature" and "digital signature" as defined in ETSI TR 119 001 [i.4], and therefore, they refer to objects that are able to support electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per [i.2].

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 [i.2]. The present document refers to this type of EAAs either as "EU Qualified EAA" or by the abbreviation QEAA.

Some of these specific requirements for 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 (QEAA)".

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

1) The initial string "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.

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 Regulation (EU) 2024/1183 [i.2]. The present document refers to this type of EAAs with the abbreviation PuB-EAA.

Some of the requirements for PuB-EAA 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 (PuB-EAA)".

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

1) The initial string "PuB-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.

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 key binding.
5) Clause 4.6 defines semantics for the digital signature of the EAA and the EAA signing certificate.

4.2 EAA metadata

4.2.1 EAA specification

4.2.1.1 Introduction

The present clause defines requirements for a set of metadata that allow access to the EAA specification details, like the EAA type, all the individual components of the EAA, the inner structure of the EAA, how to handle the EAA, etc.

4.2.1.2 EAA type

EAA-4.2.1.2-01: This component shall indicate the type of the EAA.

EAA-4.2.1.4-02: An EAA shall incorporate the EAA type.

EAA-4.2.1.2-03: The incorporation, value, and placement of the EAA type data shall depend on the specific EAA implementation.

4.2.1.3 EAA context

EAA-4.2.1.3-01: If the components of the EAA have URLs as names, the EAA shall include one or more context components.

EAA-4.2.1.3-02: The EAA context component shall reference a document defining a map between URLs identifying components of an EAA and short-forms aliases for these components.

EAA-4.2.1.3-03: The incorporation, value, and placement of the information of the EAA context components shall depend on the specific EAA implementation.

4.2.1.4 EAA schema

EAA-4.2.1.4-01: The EAA 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-4.2.1.4-02: An EAA may incorporate a sequence of one or more references allowing to retrieve the EAA schema.

EAA-4.2.1.4-03: Each reference in the aforementioned sequence:

1) Shall include a type identifier; and

2) Shall include a URI Reference which references the schema itself.

EAA-4.2.1.4-04: The incorporation and placement of the aforementioned sequence shall depend on the specific EAA implementation.

4.2.2 EAA category

4.2.2.1 General requirements

EAA-4.2.2-01: The EAA category shall be an explicit signal identifying the category of the EAA in the context where the EAA has been issued.

EAA-4.2.2-02: An EAA may include the EAA category.

4.2.2.2 Requirements for EU Qualified EAA (QEAA)

QEAA-4.2.2.2-01: A QEAA shall include the EAA category, signalling its condition of QEAA.

QEAA-4.2.2.2-02: For QEAA realizations using URIs as identifiers of the category, the value of the EAA category shall be the following URN: `urn:etsi:esi:eaa:eu:qualified`.

NOTE: These requirements meet the requirement (a) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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".

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

PuB-EAA-4.2.2.3-01: A PuB-EAA shall include an explicit signal of its condition of PuB-EAA.

PuB-EAA-4.2.2.3-02: For PuB-EAA realizations using URIs as identifiers of the category, this signal shall be the following URN: `urn:etsi:esi:eaa:eu:pub`.

NOTE: These requirements meet the of requirement (a) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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 EAA identifier

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

EAA-4.2.3-02: An EAA may 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 1: The requirements in the present clause meet the first part of requirement (f) in Annex V of Regulation (EU) 2024/1183 [i.2] for QEAA, which requires the presence of *"(f) the attestation identity code, which must be unique for the qualified trust service provider"*.

NOTE 2: The requirements in the present clause meet the first part of requirement (e) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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 may 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 registered.

EAA-4.2.4.1-05: The value of the identifier of an EU Member State shall be the Alpha 2-character country code as specified in ISO 3166-1 [15] 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 built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

NOTE: Note that although these requirements are defined in clause 5.1.4 of ETSI EN 319 412-1 [16] for building strings that are values of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate, the resulting strings can be used as the identifier of an EAA issuer if it is a legal person.

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

EAA-4.2.4.1-09: If both a national Value Added Tax (VAT) 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.

EAA-4.2.4.1-10: If the issuer of the EAA is a natural person, the EAA may include the name of this natural person.

4.2.4.2 Requirements for EU Qualified EAA (QEAA)

QEAA-4.2.4.2-01: A QEAA shall incorporate the EAA issuer identifier.

QEAA-4.2.4.2-02: A QEAA shall include an identifier of the EU Member State, in which the QEAA issuer is registered.

QEAA-4.2.4.2-03: 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.

QEAA-4.2.4.2-04: If the issuer of the QEAA is a legal person, the QEAA shall include a registration identifier as stated in the official records, where such a registration identifier exists.

QEAA-4.2.4.2-05: If the issuer of the QEAA is a legal person, the registration identifier shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

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

QEAA-4.2.4.2-07: If the issuer of the QEAA is a natural person, the QEAA shall include the name of this natural person.

NOTE 1: These requirements meet requirement (b) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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".

QEAA-4.2.4.2-08: A QEAA shall include the download URL of the certificate supporting the digital signature of the QEAA.

NOTE 2: This requirement meets requirement (h) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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".

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

PuB-EAA-4.2.4.3-01: A PuB-EAA shall incorporate the EAA issuer identifier.

PuB-EAA-4.2.4.3-02: A PuB-EAA shall include an identifier of the EU Member State, in which the public body issuing the PuB-EAA is established.

PuB-EAA-4.2.4.3-03: 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.

PuB-EAA-4.2.4.3-04: A PuB-EAA shall include the registration identifier of the public body issuing the PuB-EAA, as stated in the official records, where such a registration identifier exists.

PuB-EAA-4.2.4.3-05: The registration identifier shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

PuB-EAA-4.2.4.3-06: A PuB-EAA shall include the name of the public body issuing the PuB-EAA.

NOTE 1: These requirements meet requirement (b) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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"*.

PuB-EAA-4.2.4.3-07: A PuB-EAA shall include the download URL of the certificate supporting the digital signature of the PuB-EAA.

NOTE 2: This requirement meets requirement (h) in Annex VII of Regulation (EU) 2024/1183 [i.2] for Pub-EAA, 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"*.

4.2.5 EAA issued on behalf

EAA-4.2.5-01: If the EAA is issued on behalf of another entity, the EAA may incorporate an indication of this fact.

EAA-4.2.5-02: The incorporation, value, and placement of this indication shall depend on the specific EAA implementation.

EAA-4.2.5-03: If the EAA is issued on behalf of another entity, the EAA may incorporate an identifier whose value unambiguously identifies the entity on behalf of which the EAA has been issued.

EAA-4.2.5-04: If the EAA has been issued on behalf of another entity, the EAA may include the name of this entity.

EAA-4.2.5-05: If the entity on whose behalf the EAA has been issued is a legal person, the EAA may include a registration identifier of this legal person as stated in the official records, where such a registration identifier exists.

EAA-4.2.5-06: The registration identifier of the legal entity on whose behalf the EAA has been issued may be expressed using the structured character string specified in requirement EAA-4.2.4.1-07.

4.2.6 EAA subject and attribute subject identifiers and pseudonyms

4.2.6.1 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.

4.2.6.2 The EAA subject identifier

EAA-4.2.6.2-01: An EAA may include the EAA subject identifier, or the pseudonym of the EAA subject, or none of them.

NOTE 1: The former requirement implies that there can be EAAs that do not include any identifier or pseudonym of the EAA subject.

NOTE 2: 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-4.2.6.2-02: The incorporation, value, and placement of the EAA subject identifier shall depend on the specific EAA implementation.

4.2.6.3 The EAA subject pseudonym

EAA-4.2.6.3-01: The presence of the EAA subject pseudonym instead of the EAA subject identifier shall be clearly indicated.

EAA-4.2.6.3-02: The mechanism used for incorporating the EAA subject pseudonym within the EAA, shall depend on the specific EAA implementation.

4.2.6.4 The attribute subject identifier

EAA-4.2.6.4-01: The EAA may bind each attribute either to the identifier or to the pseudonym of the entity (attribute subject) that this attribute refers to.

NOTE 1: The former requirement implies that there can be EAAs that do not bind any attribute to any identifier or pseudonym of an entity.

NOTE 2: 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 3: 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-4.2.6.4-02: 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.

4.2.6.5 The attribute subject pseudonym

EAA-4.2.6.5-01: An EAA may incorporate pseudonym(s) for attribute subject(s).

EAA-4.2.6.5-02: The mechanism used for incorporating the pseudonym(s) for attribute subject(s) within the EAA, shall depend on the specific EAA implementation.

EAA-4.2.6.5-03: 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-4.2.6.5-04: 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.

4.2.6.6 Additional requirements

EAA-4.2.6.6-01: If the EAA contains several attribute subject identifiers, one of them shall be the EAA subject identifier.

EAA-4.2.6.6-02: 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.

4.2.6.7 Requirements for EU Qualified EAA (QEAA)

QEAA -4.2.6.7-01: A QEAA shall include either the EAA subject identifier or the pseudonym of the EAA subject.

QEAA-4.2.6.7-02: All the attributes present within a QEAA shall refer to one entity: the QEAA subject.

NOTE: These requirements meet the requirement (c) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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"*.

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

PuB-EAA-4.2.6.8-01: A PuB-EAA shall include either the EAA subject identifier or the pseudonym of the EAA subject.

PuB-EAA-4.2.6.8-02: All the attributes present within PuB-EAA shall refer to one entity: the EAA subject.

NOTE: These requirements meet the requirement (c) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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"*.

4.2.7 EAA issuance

4.2.7.1 General requirements

EAA-4.2.7.1-01: The EAA issuance data shall unambiguously identify either the date, or the date and time instant when the EAA was issued.

EAA-4.2.7.1-02: An EAA may incorporate the EAA issuance data.

EAA-4.2.7.1-03: The incorporation and placement of the EAA issuance data shall depend on the specific EAA implementation.

4.2.7.2 Time indication content

EAA-4.2.7.2-01: A time instant:

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; and
4) Shall not use local offset from UTC.

4.2.8 EAA validity periods

4.2.8.1 Introduction

The present clause specifies requirements for the two types of EAA validity periods, namely: the administrative validity period, and the technical validity period.

4.2.8.2 Common requirements for administrative and technical validity periods

EAA-4.2.8.2-01: A validity period shall be expressed by two instant times in Coordinated Universal Time (UTC).

EAA-4.2.8.2-02: The content of each instant time shall meet the requirements specified in clause 4.2.7.2 of the present document.

EAA-4.2.8.2-03: The incorporation and placement of the information on validity periods shall depend on the specific EAA implementation.

4.2.8.3 Specific requirements for the EAA technical validity period

EAA-4.2.8.3-01: An EAA shall incorporate the EAA technical validity period.

NOTE 1: This requirement meets the requirement (e) in Annex V of Regulation (EU) 2024/1183 [i.2] for QEAA, which requires the presence of *"(e) details of the beginning and end of the attestation's period of validity"*.

NOTE 2: This requirement meets the requirement (e) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, which requires the presence of *"(e) details of the beginning and end of the attestation's period of validity"*.

4.2.8.4 Specific requirements for the EAA administrative validity period

EAA-4.2.8.4-01: An EAA may incorporate the EAA administrative validity period.

4.2.9 Data constraining the usage of EAA

4.2.9.1 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.

4.2.9.2 EAA audience

EAA-4.2.9.2-01: The EAA audience shall identify the set of relying parties the EAA is intended for.

NOTE 1: This restriction is added to the restrictions imposed by any Embedded Disclosure Policy existing for the EAA and the restrictions established for the Relying Parties during their registration.

EAA-4.2.9.2-02: An EAA may incorporate the EAA audience.

EAA-4.2.9.2-03: Presence of the EAA audience shall mean that the EAA is intended only for the relying parties identified in it.

EAA-4.2.9.2-04: The value of EAA audience 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 2: 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-4.2.9.2-05: The values of the identifiers of the relying parties or the groups of relying parties shall depend on the specific EAA implementation.

EAA-4.2.9.2-06: The incorporation and placement of the EAA audience shall depend on the specific EAA implementation.

4.2.9.3 Signal of one-time use

EAA-4.2.9.3-01: An EAA may incorporate the signal of one-time-use within the EAA.

EAA-4.2.9.3-02: 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-4.2.9.3-03: Its absence shall indicate that the aforementioned constraint shall not apply to the EAA.

EAA-4.2.9.3-04: The incorporation, value, and placement of this signal shall depend on the specific EAA implementation.

4.2.10 Attributes evidence

EAA-4.2.10-01: 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 1: 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-4.2.10-02: An EAA may incorporate the attributes evidence.

EAA-4.2.10-03: The attributes evidence shall consist in a sequence of one or more evidence.

EAA-4.2.10-04: Each evidence:

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

NOTE 2: 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-4.2.10-05: The incorporation and placement of attributes evidence shall depend on the specific EAA implementation.

4.2.11 EAA status service

4.2.11.1 General requirements

EAA-4.2.11.1-01: 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-4.2.11.1-02: An EAA may incorporate the EAA status service.

EAA-4.2.11.1-03: An EAA that incorporates the EAA short-lived component (clause 4.2.13 of the present document), shall not incorporate the EAA status service.

EAA-4.2.11.1-04: 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 Recommendation: "Bitstring Status List v1.0" [24].

EAA-4.2.11.1-05: The incorporation, value, and placement of the EAA status service shall depend on the specific EAA implementation.

4.2.11.2 Requirements for EU Qualified EAA (QEAA)

QEAA-4.2.11.2-01: If a QEAA does not contain the EAA short-lived component, it shall include the EAA status service.

NOTE: This requirement meets the requirement (i) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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"*.

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

PuB-EAA-4.2.11.3-01: If a PuB-EAA does not contain the EAA short-lived component, it shall include the EAA status service.

NOTE: This requirement meets the requirement (i) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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"*.

4.2.12 EAA renewal service

EAA-4.2.12-01: The EAA renewal service shall contain details allowing to request to renew the EAA to a renewal service.

EAA-4.2.12-02: An EAA may incorporate EAA renewal service data.

EAA-4.2.12-03: The attestation renewal service data:

1) Shall include a URI to the service.

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

EAA-4.2.12-04: The incorporation and placement of the EAA renewal service shall depend on the specific EAA implementation.

4.2.13 EAA short-lived

EAA-4.2.13-01: An EAA may contain the EAA short-lived component.

EAA-4.2.13-02: The presence of the EAA short-lived component shall indicate that the validity period of the EAA is so short that it shall not be necessary to check its revocation status.

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.

EAA-4.3-02: Each attribute within an EAA shall have a value, whose semantics and inner structure shall depend on the specific Attribute.

EAA-4.3-03: Each attribute within an EAA shall refer to one attribute subject.

NOTE: If all the attributes of the EAA refer to the same entity (the EAA subject), this attribute subject is the same as the EAA subject.

EAA-4.3-04: Each attribute within an EAA may have a component indicating the format used by the attribute identifier.

EAA-4.3-05: Each attribute within an EAA may have a component identifying its type.

EAA-4.3-06: Each attribute within an EAA may have a component where a friendly identifier of the attribute is available.

EAA-4.3-07: Each attribute within an EAA may have a component that allows to individually reference the attribute.

EAA-4.3-08: 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 attested 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 binding 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 data for key binding

EAA-4.5-01: An EAA should incorporate a component proving that a certain public key is in possession of the EAA subject.

NOTE 1: If this component is present within the EAA, the EAA subject can use the private key corresponding to this public key for signing an EAA presentation.

NOTE 2: In some specific cases, the EAA can bind the attested attributes to the EAA subject using claim binding or a direct EAA subject identification data binding, instead of public key binding.

EAA-4.5-02: The value of this component may be either a public key, a certificate, or a reference to one of them.

EAA-4.5-03: If the value of this component is a pointer either to a public key or to a certificate, the EAA shall contain the digest of the referenced object.

EAA-4.5-04: It is recommended that this component is a public key.

NOTE 3: This is for security and privacy reasons.

4.6 EAA digital signature

4.6.1 General requirements

EAA-4.6.1-01: An EAA shall incorporate a digital signature generated by the EAA issuer using its private key.

EAA-4.6.1-02: Where the syntax used for the digital signature makes it possible, the digital signature shall be an AdES-B-B digital signature in that syntax.

EAA-4.6.1-03: If the EAA includes selective disclosures, then the disclosures shall be placed in the container for unsigned attributes.

EAA-4.6.1-04: If the digital signature is an AdES-B-B digital signature, and the EAA includes selective disclosures, then the disclosures shall be placed, if the serialization rules allow it, in the container for unsigned attributes specified in the corresponding AdES specification.

NOTE: The compact serialization for SD-JWT (IETF RFC 7519 [4]) defines its own mechanism for incorporating the disclosures.

EAA-4.6.1-05: The EAA signature may include the signing certificate.

EAA-4.6.1-06: The EAA signature may include certificates in the certification path, except the trust anchor.

EAA-4.6.1-07: The signing certificate shall meet the requirements of the profile EAA specified in ETSI TS 119 412-6 [17].

4.6.2 Requirements for EU Qualified EAA (QEAA)

QEAA-4.6.2-01: The QEAA digital signature shall be a qualified electronic signature or a qualified electronic seal.

NOTE 1: This requirement meets requirement (g) in Annex V of Regulation (EU) 2024/1183 [i.2] for QEAA, which requires the presence of *"(g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider"*.

QEAA-4.6.2-02: The QEAA digital signature shall contain a signed attribute whose value is a reference to the place from where the qualified certificate supporting the QEAA digital signature can be downloaded from, and a signed attribute containing the digest of the mentioned qualified certificate.

NOTE 2: This requirement meets requirement (h) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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"*.

QEAA-4.6.2-03: The QEAA digital signature should contain the qualified certificate supporting the QEAA digital signature.

QEAA-4.6.2-04: The signing certificate shall meet the requirements of the profile QEAA specified in ETSI TS 119 412-6 [17].

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

PuB-EAA-4.6.3-01: The PuB-EAA digital signature shall be a qualified electronic signature or a qualified electronic seal.

NOTE 1: These requirements meet requirement (g) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, which requires the presence of *"(g) the qualified electronic signature or qualified electronic seal of the issuing body"*.

PuB-EAA-4.6.3-02: The PuB-EAA digital signature shall contain a signed attribute whose value is a reference to the place from where the qualified certificate supporting the PuB-EAA digital signature can be downloaded from, and a signed attribute containing the digest of the mentioned qualified certificate.

NOTE 2: This requirement meets requirement (h) in Annex VII of Regulation (EU) 2024/1183 [i.2]for 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"*.

PuB-EAA-4.6.2-03: The PuB-EAA digital signature should contain the qualified certificate supporting the PuB-EAA digital signature.

PuB-EAA-4.6.2-04: The signing certificate shall meet the requirements of the profile **PSB** specified in ETSI TS 119 412-6 [17].

5 Implementation of EAA based on SD-JWT VC

5.1 General requirements

Clause 5 subclauses specify a realization of EAA that implements EAA as a JSON Web Signature as specified in IETF RFC 7515 [8], built on IETF SD-JWT VC [3], which further profiles a Selective Disclosure JSON Web Token as specified in IETF SD-JWT draft-ietf-oauth-selective-disclosure-jwt-22 [5]. The EAAs implemented according to clause 5 of the present document, will be designated as SD-JWT VC EAA hereinafter.

EAA-5.1-01: 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 [3].

5.2 EAA metadata

5.2.1 EAA specification

5.2.1.1 Introduction

Clause 6 of IETF SD-JWT VC [3] defines the SD-JWT VC Type Metadata, how it is associated with a specific SD-JWT VC type, and the methods for its retrieval and processing.

5.2.1.2 EAA type

EAA-5.2.1.2-01: A SD-JWT VC EAA shall include the `vct` claim as specified in IETF SD-JWT VC [3], which shall implement the semantics specified in clause 4.2.1.2 of the present document, and that shall be associated to the SD-JWT VC Type Metadata.

EAA-5.2.1.2-02: The `vct` claim shall point to the SD-JWT VC Type Metadata.

EAA-5.2.1.2-03: A SD-JWT VC EAA shall incorporate the claim `vct#integrity` as specified in IETF SD-JWT VC [3], clause 6.

5.2.1.3 EAA context

The information of the context of a SD-JWT VC EAA can be included in the SD-JWT VC Type Metadata.

5.2.1.4 EAA schema

NOTE: See [i.6], which specifies among other things "a data model for catalogue of attributes, guidance on Attestation Rulebooks, attestation type data models and applicable Application Programming Interface (API) for management of machine-readable attestation schemas".

5.2.2 EAA category

5.2.2.1 General requirements

EAA-5.2.2.1-01: SD-JWT VC EAAs issued by EAAs issuers registered in the European Union, which are neither SD-JWT VC QEAAs nor SD-JWT VC PuB-EAAs, shall not include the `category` claim.

5.2.2.2 Requirements for EU Qualified EAA (QEAA)

QEAA-5.2.2.2-01: An SD-JWT VC QEAA shall include the `category` claim, which shall implement the semantics specified in clause 4.2.2 of the present document.

QEAA-5.2.2.2-02: The value of the `category` claim in a SD-JWT VC QEAA shall be the URN defined in requirement QEAA-4.2.2.2-02 (`urn:etsi:esi:eaa:eu:qualified`).

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

PuB-EAA-5.2.2.3-01: An SD-JWT VC PuB-EAA shall include the `category` claim, which shall implement the semantics specified in clause 4.2.2 of the present document.

PuB-EAA-5.2.2.3-02: The value of the `category` claim in a SD-JWT VC PuB-EAA shall be the URN defined in requirement PuB-EAA-4.2.2.3-02 (`urn:etsi:esi:eaa:eu:pub`).

5.2.3 EAA identifier

EAA-5.2.3-01: The `jti` component specified in IETF RFC 7519 [4], 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 may incorporate the `jti` component.

5.2.4 EAA issuer identifier

5.2.4.1 General requirements

Common requirements to both types of EAA Issuer (natural or legal person)

EAA-5.2.4.1-01: A SD-JWT VC EAA may include the `issuing_authority` claim, specified in CIR (EU) 2024/2977 [i.3], table 5 Annex I, containing the name of the SD-JWT VC EAA issuer.

EAA-5.2.4.1-02: The `issuing_authority` claim shall be a JSON String.

EAA-5.2.4.1-03: A SD-JWT VC EAA shall not incorporate the `issuing_authority` claim if it incorporates the qualified certificate supporting the EAA signature.

EAA-5.2.4.1-04: A SD-JWT VC EAA may incorporate the `issuing_country`, identifying the EU Member where the SD-JWT VC EAA issuer is established.

EAA-5.2.4.1-05: The value of the optional `issuing_country` claim shall be as specified in requirement EAA-4.2.4.1-05 of the present document.

EAA-5.2.4.1-06: The `issuing_country` claim shall be a JSON String.

EAA-5.2.4.1-07: A SD-JWT VC EAA shall not incorporate the `issuing_country` claim if it incorporates the qualified certificate supporting the SD-JWT VC EAA signature.

NOTE 1: According to ETSI TS 119 412-6 [17], the information provided by the `issuing_authority` claim and the `issuing_country` claim is present in the qualified certificate.

Requirements when the EAA Issuer is a legal person

EAA-5.2.4.1-08: Where a registration identifier is applicable, a SD-JWT VC EAA may include the `iss_reg_id` claim.

EAA-5.2.4.1-09: The `iss_reg_id` claim shall be a JSON String.

EAA-5.2.4.1-10: The value of the `iss_reg_id` claim may be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

EAA-5.2.4.1-11: A SD-JWT VC EAA shall not incorporate the `iss_reg_id` claim if it incorporates the qualified certificate supporting the SD-JWT VC EAA signature.

NOTE 2: According to ETSI TS 119 412-6 [17], the information provided by the `iss_reg_id` claim already is present in the qualified certificate.

5.2.4.2 Requirements for EU Qualified EAA (QEAA)

QEAA-5.2.4.2-01: A SD-JWT VC QEAA shall include the name of its Issuer either within the `issuing_authority` claim, or within the qualified certificate supporting its signature.

NOTE: The `issuing_authority` claim is specified in CIR (EU) 2024/2977 [i.3], table 5 Annex I.

QEAA-5.2.4.2-02: A SD-JWT VC QEAA shall include the identifier of the country where its Issuer is established either in the `issuing_country` claim or within the qualified certificate supporting its signature.

QEAA-5.2.4.2-03: If the issuer of the SD-JWT VC QEAA is a legal person and if a registration identifier is applicable, the SD-JWT VC QEAA shall include the registration identifier either in the `iss_reg_id` claim or within the qualified certificate supporting its signature.

QEAA-5.2.4.2-04: The value of the `iss_reg_id` claim shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

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

PuB-EAA-5.2.4.3-01: A SD-JWT VC PuB-EAA shall include the name of its Issuer either within the `issuing_authority`, or within the qualified certificate supporting its signature.

NOTE: The `issuing_authority` claim is specified in CIR (EU) 2024/2977 [i.3], table 5 Annex I.

PuB-EAA-5.2.4.3-02: A SD-JWT VC PuB-EAA shall include the identifier of the country where its Issuer is established either within the `issuing_country` claim or within the qualified certificate supporting its signature.

PuB-EAA-5.2.4.3-03: If the issuer of the SD-JWT VC PuB-EAA is a legal person and if a registration identifier is applicable, then the SD-JWT VC PuB-EAA shall include the registration identifier either in the `iss_reg_id` claim or within the qualified certificate supporting its signature.

PuB-EAA-5.2.4.3-04: The value of the `iss_reg_id` claim shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

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 [4], clause 4.1.2, and further profiled in clause 3.2.2.2 of IETF SD-JWT VC [3], shall implement the semantics specified in clause 4.2.6.2 of the present document.

EAA-5.2.5.1-02: A SD-JWT VC EAA may include the `sub` claim, or the `also_known_as` claim, or none of them.

5.2.5.2 The EAA subject pseudonym

EAA-5.2.5.2-01: The `also_known_as` claim shall implement the semantics specified in clause 4.2.6.3 of the present document.

EAA-5.2.5.2-02: The `also_known_as` claim shall be a JSON String.

5.2.5.3 The attribute subject identifier

EAA-5.2.5.3-01: A SD-JWT VC EAA may contain attributes referring to different entities.

EAA-5.2.5.3-02: In a SD-JWT VC EAA each attribute not associated to the EAA subject shall be associated either to an attribute subject identifier or to an attribute subject pseudonym.

EAA-5.2.5.3-03: An SD-JWT VC EAA may associate a set of attributes to the identifier of an entity different than the EAA subject using the type specified in clause 5.3 of the present document.

5.2.5.4 The attribute subject pseudonym

EAA-5.2.5.4-01: A SD-JWT VC EAA may associate a set of attributes to the pseudonym of an entity different than the EAA subject using the type specified in clause 5.3 of the present document.

5.2.5.5 Requirements for EU Qualified EAA (QEAA)

QEAA-5.2.5.5-01: In a SD-JWT VC QEAA all the attributes shall refer to 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 (PuB-EAA)

PuB-EAA-5.2.5.6-01: In a SD-JWT PuB-EAA all the attributes shall refer to the EAA subject.

5.2.6 EAA issuance

EAA-5.2.6-01: The `iat` claim, specified in IETF RFC 7519 [4] clause 4.1.6, and further profiled in IETF SD-JWT VC [3] clause 3.2.2.2, shall implement semantics specified in clause 4.2.7 of the present document.

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

NOTE: The `NumericDate` value (the value of the `iat` claim), specified in IETF RFC 7519 [4], meets the requirements specified in clause 4.2.7.2 of the present document.

5.2.7 EAA validity periods

5.2.7.1 Specific requirements for the EAA technical validity period

EAA-5.2.7.1-01: A SD-JWT VC EAA shall include the `nbf` claim specified in IETF RFC 7519 [4], clause 4.1.5, and further profiled in IETF SD-JWT VC [3], clause 3.2.2.2.

EAA-5.2.7.1-02: The `nbf` claim shall implement the semantics of the first time instant of the SD-JWT VC EAA technical validity period.

EAA-5.2.7.1-03: A SD-JWT VC EAA shall include the `exp` claim specified in IETF RFC 7519 [4], clause 4.1.5, and further profiled in IETF SD-JWT VC [3], clause 3.2.2.2.

EAA-5.2.7.1-04: The `exp` claim shall implement the semantics of the second time instant of the SD-JWT VC EAA technical validity period.

5.2.7.2 Specific requirements for the EAA administrative validity period

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

EAA-5.2.7.2-02: The `adm_nbf` claim shall implement the semantics of the first time instant of the SD-JWT VC EAA administrative validity period.

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

EAA-5.2.7.2-04: The `adm_exp` claim shall implement the semantics of the second time instant of the SD-JWT VC EAA administrative validity period (the expiration time).

EAA-5.2.7.2-05: A SD-JWT VC EAA either shall contain both the `adm_nbf` and the `adm_exp` claims, or shall not contain any of them.

EAA-5.2.7.2-06: The content of `adm_nbf` and `adm_exp` claims shall be a `NumericDate`, specified in IETF RFC 7519 [4].

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 4.2.9.2 of the present document.

NOTE: The restrictions mentioned in clause 4.2.9.2 of the present document can be imposed by Embedded Disclosure Policy existing for the EAA and the restrictions established for the Relying Parties during their registration.

5.2.8.2 Signal of one-time use

EAA-5.2.8.2-01: The `oneTime` claim shall implement the semantics specified in clause 4.2.9.3 of the present document.

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

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

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` claim shall have the `null` JSON primitive type.

5.2.9 Attributes evidence

EAA-5.2.9-01: A SD-JWT VC EAA may incorporate the `evidence` claim specified in [31] implementing the semantics specified in clause 4.2.10 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 4.2.11 of the present document.

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

EAA-5.2.10.1-03: The `status` component shall be a JSON Object.

EAA-5.2.10.1-04: The `status` JSON Object shall have the `type` member.

EAA-5.2.10.1-05: The `status` JSON Object's `type` member shall be a JSON String.

The following string value is defined for the `type` member of `status`: "`TokenStatusList`": for Token Status List as specified in IETF draft-ietf-oauth-status-list-13 [25].

EAA-5.2.10.1-06: The `status` JSON Object shall have the `purpose` member.

EAA-5.2.10.1-07: The `status` JSON Object's `purpose` member shall be a JSON String, indicating the purpose of the status list.

EAA-5.2.10.1-08: The `status` JSON Object shall have the `index` member.

EAA-5.2.10.1-09: The `status` JSON Object's `index` member shall be a JSON Integer, indicating an index in the status list.

EAA-5.2.10.1-10: The `status` JSON Object shall have the `uri` member.

EAA-5.2.10.1-11: The `status` JSON Object's `uri` member shall be a JSON String, whose value shall be an URL pointing to the status list.

EAA-5.2.10.1-12: The `status` JSON Object may have other members.

5.2.10.2 Requirements for EU Qualified EAA (QEAA)

QEAA-5.2.10.2-01: If a SD-JWT VC QEAA does not contain the `shortLived` claim, it shall include the EAA `status` claim.

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

PuB-EAA-5.2.10.3-01: If a SD-JWT VC PuB-EAA does not contain the `shortLived` claim, it shall include the EAA `status` claim.

5.2.11 EAA renewal service

EAA-5.2.11-01: A SD-JWT VC EAA shall not incorporate any component implementing the semantics specified in clause 4.2.12 of the present document.

5.2.12 EAA short-lived (`shortLived`)

EAA-5.2.12-01: A SD-JWT VC EAA may incorporate the `shortLived` claim implementing the semantics specified in clause 4.2.13 of the present document.

EAA-5.2.12-02: The `shortLived` claim shall have the `null` JSON primitive type.

5.3 Attested Attributes

EAA-5.3-01: If disclosure of attributes are required, the SD-JWT VC EAA shall incorporate the corresponding disclosures as specified in clause 5.4.1 of the present document.

EAA-5.3-02: For associating a set of attributes to one entity different than the EAA subject, the SD-JWT VC EAA shall include the `subAttrs` claim.

EAA-5.3-03: The `subAttrs` claim shall have either the `sub_id` member or the `sub_aka` member.

EAA-5.3-04: The `sub_id` member shall be a JSON String whose value shall be the identifier of the attribute subject, which shall associate the attributes to this attribute subject.

EAA-5.3-05: The `sub_aka` member shall be a JSON String whose value shall be the pseudonym of an attribute subject which shall associate the attributes to this attribute subject.

EAA-5.3-06: The `subAttrs` claim shall have the `attrs` member.

EAA-5.3-07: The `attrs` member shall be a JSON Array whose elements shall be the attributes associated to the attribute subject whose identifier appears in the `sub_id` member or whose pseudonym appears in the `sub_aka` member.

5.4 Attested Attributes metadata

5.4.1 Support to selective disclosure of attested attributes

5.4.1.1 General requirements

EAA-5.4.1.1-01: A SD-JWT VC EAA shall support the selective disclosure of attributes using components specified in IETF SD-JWT VC [3] and IETF SD-JWT [5].

5.4.1.2 Disclosure schema identifier

EAA-5.4.1.2-01: 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.

5.4.1.3 Disclosure

EAA-5.4.1.3-01: A SD-JWT VC EAA shall contain one disclosure for each selectively disclosable attested attribute.

EAA-5.4.1.3-02: When a SD-JWT VC EAA is serialized, the disclosures shall be incorporated in the SD-JWT VC EAA as specified in IETF SD-JWT [5].

5.4.1.4 Disclosure reference

EAA-5.4.1.4-01: 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 [5]), shall include the `_sd` component containing their disclosure digests computed as specified in clause 5.2.4.1 of IETF SD-JWT [5].

EAA-5.4.1.4-02: 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 [5]), 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 [5].

5.4.1.5 Disclosure algorithm identifier (_sd_alg)

EAA-5.4.1.5-01: The `_sd_alg` component, specified in IETF SD-JWT [5], and further profiled in IETF SD-JWT VC [3], shall implement the semantics specified in clause 4.4.2.5 of the present document.

EAA-5.4.1.5-02: If the SD-JWT VC EAA contains one or more disclosures, then the `_sd_alg` component shall be present.

5.5 EAA data for key binding

EAA-5.5-01: A SD-JWT VC EAA should incorporate the `cnf` claim as specified in IETF SD-JWT [5], implementing the semantics specified in clause 4.5 of the present document.

EAA-5.5-02: The `cnf` claim may only contain either a representation of the EAA subject public key or a representation of the EAA subject certificate as specified in IETF RFC 7800 [14].

EAA-5.5-03: For representing the EAA subject certificate, the `cnf` claim may contain the `x5c` parameter containing only the certificate itself, or the `x5t#S256` parameter, or the `x5u` parameter as specified in IETF RFC 7517 [30].

EAA-5.5-04: If the EAA subject certificate is represented by the `x5u` parameter, the `x5t#S256` parameter shall also be present.

EAA-5.5-05: If the EAA subject certificate is represented by the `x5c` parameter, neither the `x5u` parameter, nor the `x5t#S256` parameter shall be present.

EAA-5.5-06: The `cnf` claim should contain a representation of the EAA subject public key.

5.6 EAA digital signature

5.6.1 General requirements

EAA-5.6.1-01: If the SD-JWT VC EAA is not serialized using compact serialization, its digital signature shall be a JAdES digital signature as specified in ETSI TS 119 182-1 [11].

5.6.2 Requirements for EU Qualified EAA (QEAA)

QEAA-5.6.2-01: The digital signature signing a SD-JWT VC QEAA shall be a qualified electronic signature or a qualified electronic seal.

QEAA-5.6.2-02: The Protected Header of the digital signature signing a SD-JWT VC QEAA shall contain the `x5u` and the `x5t#S256` header parameters, specified in IETF RFC 7515 [8].

NOTE 1: This requirement meets requirement (h) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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"*.

NOTE 2: The presence of the `x5t#S256` header parameter is required for security reasons.

QEAA-5.6.2-03: The Protected Header of the digital signature signing a SD-JWT VC QEAA should contain the `x5c` header parameter, specified in IETF RFC 7515 [8].

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

PuB-EAA- 5.6.3-01: The digital signature signing a SD-JWT VC PuB-EAA shall be a qualified electronic signature or a qualified electronic seal.

PuB-EAA-5.6.3-02: The Protected Header of the digital signature signing a SD-JWT VC PuB-EAA shall contain the `x5u` and the `x5t#S256` header parameters, specified in IETF RFC 7515 [8].

NOTE 1: This requirement meets requirement (h) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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".

NOTE 2: The presence of the `x5t#S256` header parameter is required for security reasons.

PuB-EAA-5.6.3-03: The Protected Header of the digital signature signing a SD-JWT VC PuB-EAA should contain the `x5c` header parameter, specified in IETF RFC 7515 [8].

6 Implementation of EAA based on ISO/IEC-mdoc

6.1 General requirements

Clause 6 of the present document specifies a realization of EAA designated as **ISO/IEC-mdoc EAA** hereinafter.

EAA-6.1-01: The data structures of the EAA shall be the data structures defined in ISO/IEC 18013-5 [12], extended with some structures defined in the present document for meeting specific EAA requirements.

EAA-6.1-02: **If the EAA is a mobile driving license (mDL)** (i.e. the document type of the EAA is "org.iso.18013.5.1.mDL"), it:

1) Shall contain data elements defined in section 7.1 of ISO/IEC 18013-5 [12] within the namespace "org.iso.18013.5.1"; and

2) May contain data elements defined in the present document.

EAA-6.1-03: **If the EAA is NOT a mobile driving license**, it:

1) Shall contain data elements defined in section 6.3 of ISO/IEC 23220-2 [13] within the namespace "org.iso.23220.1";

2) May contain data elements defined in the present document; and

3) May contain data elements defined in another document.

EAA-6.1-04: The data elements defined in the present document shall be assigned the namespace "org.etsi.01947201.010101".

NOTE 1: Table A.1 in Annex A shows the namespaces for the data elements addressed in the ISO/IEC-mdoc EAA realization.

EAA-6.1-05: If the ISO/IEC-mdoc EAA is a mDL, the "presence" column of the Table 5 of ISO/IEC 18013-5 [12] shall apply.

NOTE 2: The "presence" Table 5 of ISO/IEC 18013-5 [12] specifies which data elements are mandatory and which ones are optional.

EAA-6.1-06: If the ISO/IEC-mdoc EAA is NOT a mDL, the document defining the ISO/IEC-mdoc EAA type shall specify which data elements are mandatory.

EAA-6.1-07: ISO/IEC-mdoc EAA shall be an instance of `IssuerSigned` type defined in ISO/IEC-mdoc [12], clause 8.3.2.1.2.2, extended as specified in the present document.

EAA-6.1-08: The encoding of any new data element of tstr type defined in clause 6 shall be Unicode unless stated otherwise.

6.2 EAA metadata

6.2.1 EAA specification

6.2.1.1 EAA type

There is no need to define any data element for indicating the type of the ISO/IEC-mdoc EAA. The rationale is explained below.

When the wallet requests the issuance of an ISO/IEC-mdoc EAA, it knows the EAA type, so that when the ISO/IEC-mdoc EAA issuer issues the ISO/IEC-mdoc EAA (an instance of `IssuerSigned` type) the wallet keeps track internally of its type.

When a relying party requests the presentation of a specific type of ISO/IEC-mdoc EAA, the wallet can retrieve the ISO/IEC-mdoc EAA of this type and send it to the relying party.

6.2.1.2 EAA context

There is no need to define any data element for indicating the context because the data elements namespaces appear within the ISO/IEC-mdoc EAA regardless its type.

6.2.1.3 EAA schema

NOTE: See [i.6], which specifies among other things "a data model for catalogue of attributes, guidance on Attestation Rulebooks, attestation type data models and applicable Application Programming Interface (API) for management of machine-readable attestation schemas".

6.2.2 EAA category

6.2.2.1 General requirements

EAA-6.2.2.1-01: ISO/IEC-mdoc EAAs issued by EAAs issuers registered in the European Union, which are neither ISO/IEC-mdoc QEAAs nor ISO/IEC-mdoc PuB-EAAs, shall not include the `category` data element.

NOTE: As the `category` data element is defined in the present document its namespace is "org.etsi.01947201.010101".

EAA-6.2.2.1-02: The `category` data element shall implement the semantics specified in clause 4.2.2 of the present document.

EAA-6.2.2.1-03: The `category` data element shall be of type `tstr` (specified in IETF RFC 8610 [22]).

6.2.2.2 Requirements for EU Qualified EAA (QEAA)

QEAA-6.2.2.2-01: An ISO/IEC-mdoc QEAA shall include the `category` data element, which shall implement the semantics specified in clause 4.2.2 of the present document.

QEAA-6.2.2.2-02: The value of the `category` data element in an ISO/IEC-mdoc QEAA shall be the URN defined in requirement QEAA-4.2.2.2-02 (`urn:etsi:esi:eaa:eu:qualified`).

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

PuB-EAA-6.2.2.3-01: An ISO/IEC-mdoc PuB-EAA shall include the `category` data element, which shall implement the semantics specified in clause 4.2.2 of the present document.

PuB-EAA-6.2.2.3-02: The value of the `category` data element in an ISO/IEC-mdoc PuB-EAA shall be the URN defined in requirement PuB-EAA-4.2.2.3-02 (`urn:etsi:esi:eaa:eu:pub`).

6.2.3 EAA identifier

EAA-6.2.3-01: An ISO/IEC-mdoc EAA shall incorporate the `document_number` data element.

EAA-6.2.3-02: The `document_number` data element shall implement the semantics of clause 4.2.3 of the present document.

EAA-6.2.3-03: If the ISO/IEC-mdoc EAA is a mDL, then the `document_number` data element shall be as specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [12].

EAA-6.2.3-04: If the ISO/IEC-mdoc EAA is NOT a mDL the `document_number` data element shall be as specified in clause 6.3 of ISO/IEC 23220-2 [13].

NOTE: In both cases, the value of the `document_number` data is a number (e.g. a unique serial number).

6.2.4 EAA issuer identifier

6.2.4.1 General requirements

Common requirements to both types of EAA Issuer (natural or legal person)

EAA-6.2.4.1-01: If an ISO/IEC-mdoc EAA is a mDL it shall include the `issuing_authority` component, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [12].

EAA-6.2.4.1-02: The `issuing_authority` data element shall implement the semantics of clause 4.2.4 of the present document.

EAA-6.2.4.1-03: If an ISO/IEC-mdoc EAA is NOT a mDL it shall include the `issuing_authority_unicode` component, specified in clause 6.3 of ISO/IEC 23220-2 [13].

EAA-6.2.4.1-04: The `issuing_authority_unicode` data element shall implement the semantics of clause 4.2.4 of the present document.

NOTE 1: ISO/IEC 23220-2 [13] defines two data elements (each one with its own identifier) with different character sets, namely: latin1 (the character set mandated for `issuing_authority` in ISO/IEC 18013-5 [12]), and Unicode.

EAA-6.2.4.1-05: An ISO/IEC-mdoc EAA may incorporate the `issuing_country`, identifying the EU Member where the ISO/IEC-mdoc EAA issuer is registered.

EAA-6.2.4.1-06: If the ISO/IEC-mdoc EAA is a mDL, then the `issuing_country` data element shall be as specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [12].

EAA-6.2.4.1-07: If the ISO/IEC-mdoc EAA is NOT a mDL the `issuing_country` data element shall be as specified in clause 6.3 of ISO/IEC 23220-2 [13].

EAA-6.2.4.1-08: 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.

Requirements when the EAA is a legal person

EAA-6.2.4.1-09: Where a registration identifier is applicable, an ISO/IEC-mdoc EAA may include the `iss_reg_id` data element.

NOTE 2: As the `iss_reg_id` data element is defined in the present document its namespace is "org.etsi.01947201.010101".

EAA-6.2.4.1-10: The `iss_reg_id` data element shall be an element of the type `tstr` (specified in IETF RFC 8610 [22]).

EAA-6.2.4.1-11: The value of the `iss_reg_id` data element shall be a registration identifier.

EAA-6.2.4.1-12: The value of the `iss_reg_id` data element may be built applying the rules specified in requirements LEG-5.1.4-02 to LEG-5.1.4-08 (both included) in clause 5.1.4 of ETSI EN 319 412-1 [16].

EAA-6.2.4.1-13: An ISO/IEC-mdoc EAA shall not incorporate the `iss_reg_id` claim if it incorporates the qualified certificate supporting the ISO/IEC-mdoc EAA signature.

6.2.4.2 Requirements for EU Qualified EAA (QEAA)

QEAA-6.2.4.2-01: If the issuer of the ISO/IEC-mdoc QEAA is a legal person and if a registration identifier is applicable, an ISO/IEC-mdoc QEAA shall include the registration identifier either in the `iss_reg_id` data element or within the qualified certificate supporting its signature.

QEAA-6.2.4.2-02: The value of the `iss_reg_id` data element shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

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

PuB-EAA-6.2.4.3-01: Where a registration identifier is applicable, an ISO/IEC 18013-5 [12] PuB-EAA shall include the registration identifier either in the `iss_reg_id` data element or within the qualified certificate supporting its signature.

PuB-EAA-6.2.4.3-02: The value of the `iss_reg_id` data element shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

6.2.5 EAA subject and attribute subject identifiers and pseudonyms

6.2.5.1 EAA subject identifier

EAA-6.2.5.1-01: If an ISO/IEC-mdoc EAA requires that the EAA subject (the holder of the mDL) is identified, the ISO/IEC-mdoc EAA shall include the following data elements, specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [12]: `given_name` and `family_name`, and `document_number`.

EAA-6.2.5.1-02: An ISO/IEC-mdoc EAA that is a mDL shall include either the complete set of data elements mentioned in the previous requirement identifying the EAA subject, or the `also_known_as` data element.

NOTE 1: As the `also_known_as` data element is defined in the present document its namespace is "org.etsi.01947201.010101".

EAA-6.2.5.1-03: The `also_known_as` data element shall be an element of the type `tstr` (specified in IETF RFC 8610 [22]).

EAA-6.2.5.1-04: If the ISO/IEC-mdoc EAA is NOT a mDL, and requires that the EAA subject (the holder of the mDoc) is identified, the ISO/IEC-mdoc EAA shall include the following data elements, specified in clause 6.3 of ISO/IEC 23220-2 [13]: `given_name`, `family_name`, and `document_number`.

NOTE 2: Although the identifiers of the data elements are the same in both ISO/IEC 18013-5 [12] and ISO/IEC 23220-2 [13], their namespaces differ, and in addition, `given_name` and `family_name` are encoded in Unicode in ISO/IEC 23220-2 [13], and in latin1 in ISO/IEC 18013-5 [12].

EAA-6.2.5.1-05: An ISO/IEC-mdoc EAA that is NOT a mDL shall include either the complete set of data elements mentioned in the previous requirement identifying the EAA subject, or the `also_known_as` data element.

6.2.5.2 EAA subject pseudonym

EAA-6.2.5.2-01: An ISO/IEC-mdoc EAA may contain the `also_known_as` data element, which shall contain the pseudonym of the EAA, and therefore shall implement the semantics specified in clause 4.2.6.3 of the present document.

6.2.5.3 Attribute subject identifier

EAA-6.2.5.3-01: An ISO/IEC-mdoc EAA may include attributes that refer to entities that are not the EAA subject: the attribute subjects.

EAA-6.2.5.3-02: For each attribute subject, an ISO/IEC-mdoc EAA may include the attribute subject identifier or the attribute subject pseudonym.

EAA-6.2.5.3-03: In an ISO/IEC-mdoc EAA the identifiers of the attribute subjects shall be associated to their corresponding attributes as specified in clause 6.3 of the present document.

6.2.5.4 Attribute subject pseudonym

EAA-6.2.5.4-01: An ISO/IEC-mdoc EAA may include pseudonyms of attribute subjects.

EAA-6.2.5.4-02: In an ISO/IEC-mdoc EAA, the pseudonyms of the attribute subjects shall be associated with their corresponding attributes as specified in clause 6.3 of the present document.

6.2.5.5 Requirements for EU Qualified EAA (QEAA)

QEAA-6.2.5.5-01: In an ISO/IEC-mdoc QEAA all the attributes shall refer to the EAA subject.

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

PuB-EAA-6.2.5.6-01: In an ISO/IEC-mdoc PuB-EAA all the attributes shall refer to the EAA subject.

6.2.6 EAA issuance

EAA-6.2.6-01: An ISO/IEC-mdoc EAA shall incorporate the `issue_date` data element.

EAA-6.2.6-02: The `issue_date` data element shall indicate the issuance date according to the semantics of clause 4.2.7 of the present document.

EAA-6.2.6-03: If the ISO/IEC-mdoc EAA is a mDL, then the `issue_date` data element shall be as specified in Table 5 of clause 7.2.1 of ISO/IEC 18013-5 [12].

EAA-6.2.6-04: If the ISO/IEC-mdoc EAA is NOT a mDL the `issue_date` data element shall be as specified in clause 6.3 of ISO/IEC 23220-2 [13].

6.2.7 EAA validity periods

6.2.7.1 Specific requirements for the EAA technical validity period

EAA-6.2.7.1-01: The `validFrom` member of the `validityInfo` member of the instance of `MobileSecurityObject` type specified in clause 9.1.2.4 of ISO/IEC 18013-5 [12], shall implement the semantics of the start time of the ISO/IEC-mdoc EAA technical validity period.

EAA-6.2.7.1-02: The `validUntil` member of the `validityInfo` member of the instance of `MobileSecurityObject` type specified in clause 9.1.2.4 of ISO/IEC 18013-5 [12], shall implement the semantics of the end type instant of the ISO/IEC-mdoc EAA technical validity period.

EAA-6.2.7.1-03: The `validFrom` and the `validUntil` members shall indicate the UTC time for date and time.

EAA-6.2.7.1-04: The `validFrom` and the `validUntil` members shall have seconds precision.

EAA-6.2.7.1-05: The `validFrom` and the `validUntil` members shall not contain fractions of seconds.

6.2.7.2 Specific requirements for the EAA administrative validity period

EAA-6.2.7.2-01: If the ISO/IEC-mdoc EAA is a mDL, then the `expiry_date` element specified in table 5 of clause 7.1 of ISO/IEC 18013-5 [12], shall implement the semantics of the end date of the ISO/IEC-mdoc EAA administrative validity period.

EAA-6.2.7.2-02: If the ISO/IEC-mdoc EAA is NOT a mDL, then the `expiry_date` element specified in clause 6.3 of ISO/IEC 23220-2 [13], shall implement the semantics of the end date of the ISO/IEC-mdoc EAA administrative validity period.

EAA-6.2.7.2-03: The `issue_date` data element, as specified in clause 6.2.6 of the present document, may be considered, wherever appropriate, to implement the semantics of the start date of the ISO/IEC-mdoc EAA Administrative validity period.

6.2.8 Components constraining the usage of EAA

6.2.8.1 EAA audience

EAA-6.2.8.1-01: An ISO/IEC-mdoc EAA shall not incorporate any data element implementing the semantics specified in clause 4.2.9.2 of the present document.

NOTE: The restrictions mentioned in clause 4.2.9.2 of the present document can be imposed by Embedded Disclosure Policy existing for the EAA and the restrictions established for the Relying Parties during their registration.

6.2.8.2 Signal of one-time use

EAA-6.2.8.2-01: An ISO/IEC-mdoc EAA may incorporate the `oneTime` data element.

EAA-6.2.8.2-02: The `oneTime` data element shall implement the semantics specified in clause 4.2.9.3 of the present document.

NOTE: As the `oneTime` data element is defined in the present document its namespace is "org.etsi.01947201.010101".

EAA-6.2.8.2-03: The `oneTime` data element shall have the `bool` CBOR type.

EAA-6.2.8.2-04: If the `oneTime` data element is present and set to true, it shall indicate that the EAA shall be used only once, and that it shall not be retained for future use.

EAA-6.2.8.2-05: If the `oneTime` data element is present and set to `false` or it is absent, the aforementioned constraint shall not apply to the EAA.

6.2.9 Attributes evidence

EAA-6.2.9-01: An ISO/IEC-mdoc EAA shall not incorporate any data element implementing the semantics specified in clause 4.2.10 of the present document.

6.2.10 EAA status service

6.2.10.1 General requirements

EAA-6.2.10.1-01: An ISO/IEC-mdoc may contain the `status` member within the instance of `MobileSecurityObject`.

EAA-6.2.10.1-02: The `status` member shall implement the semantics specified in clause 4.2.11 of the present document.

EAA-6.2.10.1-03: The `status` member may contain the `status_list` member as specified in clause 6.3 of IETF draft-ietf-oauth-status-list-13 [25].

NOTE: At the moment of writing the present document, ISO/IEC 18013-5 [12] is under revision taking into account the `status` member specified in clause 6 of IETF draft-ietf-oauth-status-list-13 [25]. Clause 6.2.10 of the present document can be updated for referencing the revised ISO/IEC 18013-5 [12].

6.2.10.2 Requirements for EU Qualified EAA (QEAA)

QEAA-6.2.10.2-01: If an ISO/IEC-mdoc QEAA does not contain the `shortLived` data element, it shall contain the `status` member within the instance of `MobileSecurityObject` as specified in clause 6.2.10.1.

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

PuB-EAA-6.2.10.3-01: If an ISO/IEC-mdoc PuB-EAA does not contain the `shortLived` data element, it shall contain the `status` member within the instance of `MobileSecurityObject` as specified in clause 6.2.10.1.

6.2.11 EAA renewal service

EAA-6.2.11-01: An ISO/IEC-mdoc EAA shall not incorporate any component implementing the semantics specified in clause 4.2.12 of the present document.

6.2.12 EAA short-lived

EAA-6.2.12-01: An ISO/IEC-mdoc EAA may incorporate the `shortLived` data element.

EAA-6.2.12-02: The `shortLived` data element shall implement the semantics specified in clause 4.2.13 of the present document.

NOTE: As the `shortLived` data element is defined in the present document its namespace is "org.etsi.01947201.010101".

EAA-6.2.12-03: The `shortLived` data element shall have the `bool` CBOR type.

EAA-6.2.12-04: If the `shortLived` data element is present and set to `true`, it shall indicate that the validity period of the EAA is so short that it shall not be necessary to check its revocation status.

EAA-6.2.12-05: If the `shortLived` data element is present and set to `false` or it is absent, the aforementioned constraint shall not apply to the EAA and it shall be necessary to check its revocation status.

6.3 Attested attributes

EAA-6.3-01: An ISO/IEC-mdoc EAA shall include each attested attribute, regardless it is disclosable or not, in one or more `IssuerSignedItem` component, and shall be incorporated to the ISO/IEC-mdoc EAA as specified in clause 8.3.2.1.2.2 of ISO/IEC 18013-5 [12].

EAA-6.3-02: For associating one attribute to one entity different than the EAA subject, the ISO/IEC-mdoc EAA shall include an instance of the `SubAttr` type (which is defined below) in the `elementValue` member of `IssuerSignedItem`.

```
SubAttr = {
    ("subId" : SubId    ; the subject attribute identifier
    //
    ?"subAka" : tstr); the subject attribute pseudonym
},

SubId = {
```

```
    "family_name" : tstr,   ; The family name of the attribute subject
    "given_name" : tstr,    ; The given name of the attribute subject
    "document_number": tstr ; The number of the personal identification data assigned to
                            ;the attribute subject
}
```

EAA-6.3-03: An instance of `SubAttr` type shall have either the `subId` member or the `subAka` member.

EAA-6.3-04: The `subId` member shall be a CBOR map whose members shall univocally identify the attribute subject.

EAA-6.3-05: The `subAka` member shall be a CBOR String whose value shall be the pseudonym of an attribute subject which shall associate the attributes to this attribute subject.

6.4 Attested Attributes metadata

6.4.1 Support to selective disclosure of attested attributes

6.4.1.1 Introduction

NOTE: ISO/IEC 18013-5 [12] imposes the presence of one instance of the `MobileSecurityObjectType`.

6.4.1.2 Disclosure schema identifier

EAA-6.4.1.2-01: An ISO/IEC-mdoc EAA shall include the `version` component within its `MobileSecurityObject`.

6.4.1.3 Disclosure

EAA-6.4.1.3-01: An ISO/IEC-mdoc EAA containing disclosable attributes, shall include each disclosure in one `IssuerSignedItem` component, and shall be incorporated to the ISO/IEC-mdoc EAA as specified in clause 8.3.2.1.2.2 of ISO/IEC 18013-5 [12].

6.4.1.4 Disclosure reference

EAA-6.4.1.4-01: For an ISO/IEC-mdoc EAA, the `valueDigests` component shall implement the semantics specified in clause 4.4.2.3 of the present document.

EAA-6.4.1.4-02: If an ISO/IEC-mdoc 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 [12] for supporting the semantics specified in clause 4.4.2.3 of the present document.

6.4.1.5 Disclosure algorithm identifier

EAA-6.4.1.5-01: An ISO/IEC-mdoc EAA containing disclosable attributes, shall include the `digestAlgorithm` component within its `MobileSecurityObject`.

6.5 EAA data for Key Binding

EAA-6.5-01: An ISO/IEC-mdoc EAA shall incorporate the `deviceKey` member within the `deviceKeyInfo` member of the instance of `MobileSecurityObject` type, to implement the semantics specified in clause 4.5 of the present document.

EAA-6.5-02: The `deviceKey` member within the `deviceKeyInfo` member of the instance of `MobileSecurityObject` type, shall contain a public key whose private key is in possession of the EAA subject.

6.6 EAA digital signature

6.6.1 General requirements

EAA-6.6.1-01: An ISO/IEC-mdoc EAA shall be signed by a CB-AdES digital signature.

6.6.2 Requirements for EU Qualified EAA (QEAA)

QEAA-6.6.2-01: The CB-AdES digital signature signing an ISO/IEC-mdoc QEAA shall be a qualified electronic signature or a qualified electronic seal.

QEAA-6.6.2-02: The Protected Header of the CB-AdES digital signature signing an ISO/IEC-mdoc QEAA shall contain the `x5u` and the `x5t` header parameters, both specified in IETF RFC 9360 [20].

QEAA-6.6.2-03: The digest algorithm used in the `x5t` header parameter, shall be SHA-256.

NOTE 1: This requirement meets requirement (h) in Annex V of Regulation (EU) 2024/1183 [i.2] for 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".

NOTE 2: The presence of the `x5t` header parameter is required for security reasons.

QEAA-6.6.2-04: The Protected Header of the CB-AdES digital signature signing an ISO/IEC-mdoc QEAA should contain the x5chain header parameter, specified in IETF RFC 9360 [20].

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

PuB-EAA-6.6.3-01: The CB-AdES digital signature signing an ISO/IEC-mdocPuB-EAA shall be a qualified electronic signature or a qualified electronic seal.

PuB-EAA-6.6.3-02: The Protected Header of the CB-AdES digital signature signing an ISO/IEC-mdoc PuB-EAA shall contain the `x5u` and the `x5t` header parameters, both specified in IETF RFC 9360 [20].

NOTE 1: This requirement meets requirement (h) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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".

NOTE 2: The presence of the x5t header parameter is required for security reasons.

PuB-EAA-6.6.3-03: The digest algorithm used in the `x5t` header parameter, shall be SHA-256.

PuB-EAA-6.6.3-04: The Protected Header of the CB-AdES digital signature signing an ISO/IEC-mdoc PuB-EAA should contain the `x5chain` header parameter, specified in IETF RFC 9360 [20].

7 Implementation of EAA based on W3C Verifiable Credentials (JSON-LD W3C-VC)

7.1 General requirements

Clause 7 of the present document specifies a realization of EAA based on the JSON-LD (specified in W3C Recommendation: "JSON-LD 1.1. A JSON-based Serialization for Linked Data" [29]) serialization of W3C Recommendation (15 May 2025): "Verifiable Credentials Data Model v2.0" [1].

Clauses from 7.1 to 7.5 specify the contents of an EAA that has not yet been signed by the EAA issuer. These not-yet-signed EAAs will be designated as JSON-LD W3C-VC EAA hereinafter.

Clause 7.6 specifies different mechanisms for signing JSON-LD W3C-VC EAAs and defines a set of acronyms for designating the different resulting formats of signed JSON-LD W3C-VC EAAs.

EAA-7.1-01: A JSON-LD W3C-VC EAA shall use the JSON-LD syntax for its serialization.

7.2 EAA metadata

7.2.1 EAA specification

7.2.1.1 EAA type

EAA-7.2.1.1-01: A JSON-LD W3C-VC EAA shall incorporate the credential object's `type` property, as specified in "Verifiable Credentials Data Model v2.0" [1], implementing the semantics specified in clause 4.2.1.2 of the present document.

EAA-7.2.1.1-02: In a JSON-LD W3C-VC EAA the `type` property shall be an array of at least two strings.

7.2.1.2 EAA context

EAA-7.2.1.2-01: A JSON-LD W3C-VC EAA shall incorporate the `@context` property, as specified in "Verifiable Credentials Data Model v2.0" [1], implementing the semantics specified in clause 4.2.1.3 of the present document.

EAA-7.2.1.2-02: In a JSON-LD W3C-VC EAA the `@context` property shall be an array of URI values.

EAA-7.2.1.2-03: In a JSON-LD W3C-VC EAA the `@context` shall contain the URI specified in "Verifiable Credentials Data Model v2.0" [1] (https://www.w3.org/ns/credentials/v2), and any other URI referencing a document that maps URLs to short-form aliases required for the EAA.

EAA-7.2.1.2-04: The URL associated to each new property defined in the present document shall be the result of concatenating https://uri.etsi.org/019472010101# and the term used in the definition of the property in the present document.

7.2.1.3 EAA schema

EAA-7.2.1.3-01: A JSON-LD W3C-VC EAA may incorporate the `credentialSchema` property, as specified in "Verifiable Credentials Data Model v2.0" [1], implementing the semantics of clause 4.2.1.4 of the present document.

NOTE 1: The Verifiable Credentials JSON schema specification can be found at https://www.w3.org/ns/credentials/v2.

NOTE 2: [i.6] offers an alternative to the presence of this property within the JSON-LD W3C-VC EAA, as it specifies among other things "a data model for catalogue of attributes, guidance on Attestation Rulebooks, attestation type data models and applicable Application Programming Interface (API) for management of machine-readable attestation schemas".

EAA-7.2.1.3-02: In a JSON-LD W3C-VC EAA the `credentialSchema` property shall be an array of at least one member.

EAA-7.2.1.3-03: In a JSON-LD W3C-VC EAA each member of the `credentialSchema` property shall have two properties, namely: `id`, specified in clause 4.5 of [1], which will point to the document containing the schema, and `type`, which will indicate the type of schema contained in the mentioned document.

The following string values are defined for the `type` child property of `credentialSchema`:

1) "`JsonSchemaCredential`": for schemas defined using JSON schema syntax as specified in JSON Schema Core [21].

2) "`CddlSchemaCredential`": for schemas defined using Concise Data Definition Language as specified in IETF RFC 8610 [22].

3) "`ShaclSchemaCredential`": for schemas defined using SHACL as specified in W3C Recommendation: "Shapes Constraint Language (SHACL)" [23].

NOTE 2: SHACL is able to define schemas for RDF graphs, but it is not able to define schemas for RDF Data Sets. As a VC with embedded proofs a RDF Data set, SHACL will be able to define the schema of the EAA secured with the embedded proofs. Instead, it will be able to define the schema of the EAA without any embedded proof.

EAA-7.2.1.3-04: Additional string values may be defined for the `type` child property of `credentialSchema`, each one identifying a different syntax for defining the JSON-LD W3C-VC EAA schema.

7.2.2 EAA category

7.2.2.1 General requirements

EAA-7.2.2.1-01: If an indication of the category of the EAA (implementing the semantics specified in clause 4.2.2 of the present document) is required, this category shall be indicated in one of the strings in the credential object's `type` array property, specified in "Verifiable Credentials Data Model v2.0" [1].

7.2.2.2 Requirements for EU Qualified EAA (QEAA)

QEAA-7.2.2.2-01: In a JSON-LD W3C-VC QEAA one of the elements of the credential object's `type` array property shall be the URI defined in requirement QEAA-4.2.2.2-02 (`urn:etsi:esi: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 (PuB-EAA)

PuB-EA-7.2.2.3-01: In a JSON-LD W3C-VC PuB-EAA one of the elements of the credential object's `type` array property shall be the URI defined in requirement PuB-EAA-4.2.2.3-02 (`urn:etsi:esi:eaa:eu:pub`).

7.2.3 EAA identifier

EAA-7.2.3-01: The `id` property shall implement the semantics specified in clause 4.2.3 of the present document.

EAA-7.2.3-02: A W3C-VC EAA may incorporate the credential object's `id` property.

EAA-7.2.3-03: In a JSON-LD W3C-VC EAA the contents of the `id` property shall be as specified in "Verifiable Credentials Data Model v2.0" [1], clause 4.2.

7.2.4 EAA issuer identifier

7.2.4.1 General requirements

Common requirements regardless whether the EAA issuer is a natural or a legal person

EAA-7.2.4.1-01: The `issuer` property, specified in Verifiable Credentials Data Model v2.0 [1], shall implement the semantics specified in clause 4.2.4.1 of the present document.

EAA-7.2.4.1-02: A W3C-VC EAA shall incorporate the `issuer` property.

EAA-7.2.4.1-03: In a W3C-VC EAA the `issuer` property shall be an object.

EAA-7.2.4.1-04: In a W3C-VC EAA the `issuer` property shall have the `id` child property, whose value shall be a URI, as specified in "Verifiable Credentials Data Model v2.0" [1].

NOTE: This means that a DID is a valid value for this `id` child property.

EAA-7.2.4.1-05: In a W3C-VC EAA the `issuer` property may include the `issuing_authority` child property.

EAA-7.2.4.1-06: In a W3C-VC EAA the `issuing_authority` child property of the `issuer` property shall be either a JSON String or a JSON Object.

EAA-7.2.4.1-07: If the `issuing_authority` child property of the `issuer` property in a W3C-VC EAA is a JSON String, then it shall contain the name of the W3C-VC EAA issuer.

EAA-7.2.4.1-08: If the `issuing_authority` child property of the `issuer` property in a W3C-VC EAA is a JSON Object, then it shall contain the name of the W3C-VC EAA issuer in several languages.

EAA-7.2.4.1-09: If the `issuing_authority` child property of the `issuer` property in a W3C-VC EAA is a JSON Object, then every key of the map shall be a language code as specified in IETF RFC 5646 [27], and the value mapped to the key shall be the name of W3C-VC EAA issuer in that language.

EAA-7.2.4.1-10: In a W3C-VC EAA the `issuer` property may include the `issuing_country` child property identifying the EU Member where the SD-JWT VC EAA issuer is registered.

EAA-7.2.4.1-11: In a W3C-VC EAA the value of the `issuing_country` property shall be as specified in the requirement EAA-4.2.4.1-05 of the present document.

Requirements when the EAA issuer is a legal person

EAA-7.2.4.1-12: Where a registration identifier is applicable, the `issuer` property may include the `reg_id` child property.

EAA-7.2.4.1-13: The value of the `reg_id` child property shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

7.2.4.2 Requirements for EU Qualified EAA (QEAA)

QEAA-7.2.4.2-01: The W3C-VC QEAA `issuer` property shall include the `issuing_authority` child property.

QEAA-7.2.4.2-02: The W3C-VC QEAA `issuer` property shall include the `issuing_country` child property.

QEAA-7.2.4.2-03: If the issuer of the W3C-VC QEAA is a legal person and if a registration identifier is applicable, the `issuer` property shall include the `reg_id` child property.

QEAA-7.2.4.2-04: The value of the `reg_id` child property shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

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

PuB-EAA-7.2.4.3-01: The W3C-VC PuB-EAA `issuer` property shall include the `issuing_authority` child property.

PuB-EAA-7.2.4.3-02: The W3C-VC PuB-EAA `issuer` property shall include the `issuing_country` child property.

PuB-EAA-7.2.4.3-03: Where a registration identifier is applicable, the W3C-VC PuB-EAA `issuer` property shall include the `reg_id` child property.

PuB-EAA-7.2.4.3-04: The value of the `reg_id` child property shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

7.2.5 EAA issued on behalf

EAA-7.2.5-01: If the W3C-VC EAA is issued on behalf of another entity, the EAA may incorporate the `onBehalf` child property of the `issuer` property, as specified in the present clause.

EAA-7.2.5-02: The `onBehalf` child property shall be a JSON Array of zero or more JSON Objects.

EAA-7.2.5-03: Each JSON Object within the `onBehalf` child property shall have a member id, whose value shall be a URI identifying an entity on whose behalf the EAA has been issued.

EAA-7.2.5-04: Each JSON Object within the `onBehalf` child property may have a member name, whose value shall be the name of an entity on whose behalf the EAA has been issued.

EAA-7.2.5-05: If the entity on whose behalf the EAA has been issued is a legal person, each JSON Object within the `onBehalf` child property may have a member `reg_id`, whose value shall be as specified in the requirement EAA-4.2.4.1-07.

7.2.6 EAA and attribute subject identifiers and pseudonyms

7.2.6.1 General requirements

EAA-7.2.6.1-01: In a W3C-VC EAA each element of the `credentialSubject` array shall contain either the `id` child property or the `pseudonym` child property specified in the present clause.

NOTE 1: If the `credentialSubject` array contains one element, this entity is the EAA subject.

EAA-7.2.6.1-02: In a W3C-VC EAA the `pseudonym` child property of an element of the `credentialSubject` array shall contain a string whose value is the pseudonym of the entity associated to the attributes present in this array element.

NOTE 2: The `id` child property can also be used for keeping the EAA subject anonymous. This can be achieved, for instance, using DIDs or other identifiers that introduce a level of indirection.

EAA-7.2.6.1-03: If a W3C-VC EAA includes a `credentialSubject` array with more than one element, one of these elements shall contain attributes associated only to one specific entity (attribute subject), and one of these entities shall be the EAA subject.

NOTE 3: Note that as it is required that each element of the `credentialSubject` array contains either the identifier or the pseudonym of the entity associated to the attributes within the element, and as one of these entities is the EAA subject, the EAA subject identifier or the EAA subject pseudonym is always present.

7.2.6.2 The EAA subject identifier

EAA-7.2.6.2-01: If the `credentialSubject` array of a W3C-VC EAA has one element, and this element has the `id` child property, this `id` child property shall identify the EAA subject.

NOTE: The `id` child property can have a value that is associated to the real-world identity of the EAA subject, or can have a value that does not reveal their real-world identity. This can be achieved, for instance, using DIDs or other identifiers that introduce a level of indirection, allowing the EAA subject to remain anonymous.

7.2.6.3 The EAA subject pseudonym

EAA-7.2.6.3-01: If the `credentialSubject` array of a W3C-VC EAA has one element, and this element includes the `pseudonym` child property, then the value of this element shall be the pseudonym of the EAA subject.

7.2.6.4 The attribute subject identifier

EAA-7.2.6.4-01: If the W3C-VC EAA includes a `credentialSubject` array that has more than one element, and this element has the `id` child property, this `id` child property shall identify the entity associated to the attributes in this element.

NOTE: The `id` child property can have a value that is associated to the real-world identity of the attribute subject, or can have a value that does not reveal their real-world identity. This can be achieved, for instance using DIDs or other identifiers that introduce a level of indirection, allowing the EAA subject to remain anonymous.

7.2.6.5 The attribute subject pseudonym

EAA-7.2.6.5-01: If the W3C-VC EAA includes a `credentialSubject` array that has more than one element, if one of these elements includes the `pseudonym` child property, then this child property shall contain the pseudonym of the entity associated to these attributes (the attribute subject).

7.2.6.6 Requirements for subject(s) names

EAA-7.2.6.6-01: The elements in the `credentialSubject` array of a JSON-LD W3C-VC EAA may contain the child property `name`.

EAA-7.2.6.6-02: The child property `name` in one element of the `credentialSubject` array of a JSON-LD W3C-VC EAA may be either a JSON String or a JSON Object.

EAA-7.2.6.6-03: If the child property `name` in one element of the `credentialSubject` array of a JSON-LD W3C-VC EAA is a JSON Object, then it shall contain the name of the entity associated with the corresponding attributes in several languages.

EAA-7.2.6.6-04: If the child property `name` in one element of the `credentialSubject` array of a JSON-LD W3C-VC EAA is a JSON Object, then every key of the map shall be a language code as specified in IETF RFC 5646 [27], and the value mapped to the key shall be the name of the entity associated with the corresponding attributes in that language.

7.2.6.7 Requirements for EU Qualified EAA (QEAA)

QEAA-7.2.6.7-01: The `credentialSubject` array of a JSON-LD W3C-VC QEAA shall contain only one element.

QEAA-7.2.6.7-02: The element of the `credentialSubject` array of a JSON-LD W3C-VC QEAA shall contain either the `id` child property or the `pseudonym` child property.

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

PuB-EAA-7.2.6.8-01: The `credentialSubject` array of a JSON-LD W3C-VC PuB-EAA shall contain only one element.

PuB-EAA-7.2.6.8-02: The element of the `credentialSubject` array of a JSON-LD W3C-VC PuB-EAA shall contain either the `id` child property or the `pseudonym` child property.

7.2.7 EAA issuance

EAA-7.2.7-01: The `issuedAt` property shall implement the semantics specified in clause 4.2.7 of the present document.

EAA-7.2.7-02: A JSON-LD W3C-VC EAA may incorporate the `issuedAt` property specified in the present clause.

EAA-7.2.7-03: The content of the `issuedAt` property shall be a `dateTimeStamp` string as specified in W3C Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes" [10], clause 3.3.7.

7.2.8 EAA validity periods

7.2.8.1 Specific requirements for technical validity period

EAA-7.2.8.1-01: A W3C-VC EAA shall incorporate the `validFrom` and `validUntil` properties, specified in "Verifiable Credentials Data Model v2.0" [1].

EAA-7.2.8.1-02: The `validFrom` property shall implement the semantics of the first instant time of the W3C-VC EAA technical validity period.

EAA-7.2.8.1-03: The `validUntil` property shall implement the semantics of the second instant time of the W3C-VC EAA technical validity period.

EAA-7.2.8.1-04: The contents of `validFrom` and `validUntil` shall be `dateTimeStamp` strings as specified in W3C Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes" [10], clause 3.3.7.

7.2.8.2 Specific requirements for administrative validity period

EAA-7.2.8.2-01: A W3C-VC EAA may incorporate the `admValidFrom` and `admValidUntil` properties specified in the present clause.

EAA-7.2.8.2-02: The `admValidFrom` property shall implement the semantics of the first instant time of the W3C-VC EAA administrative validity period.

EAA-7.2.8.2-03: The `admValidUntil` property shall implement the semantics of the second instant time of the W3C-VC EAA administrative validity period.

EAA-7.2.8.2-04: The content of `admValidFrom` and `admValidUntil` shall be a `dateTimeStamp` string as specified in W3C Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes" [10], clause 3.3.7.

7.2.9 Components constraining the usage of EAA

7.2.9.1 EAA audience

EAA-7.2.9.1-01: A JSON-LD W3C-VC EAA shall not incorporate any data element implementing the semantics specified in clause 4.2.9.2 of the present document.

NOTE: The restrictions mentioned in clause 4.2.9.2 of the present document can be imposed by Embedded Disclosure Policy existing for the EAA and the restrictions established for the Relying Parties during their registration.

7.2.9.2 Signal of one-time use

EAA-7.2.9.2-01: The `oneTime` property, specified in the present clause, shall implement the semantics specified in clause 4.2.9.3 of the present document.

EAA-7.2.9.2-02: A JSON-LD W3C-VC EAA may incorporate the `oneTime` property.

EAA-7.2.9.2-03: The `oneTime` property shall have a boolean value.

EAA-7.2.9.2-04: If the `oneTime` property is absent, it shall be considered that its value is `false`.

7.2.9.3 Terms of use

EAA-7.2.9.3-01: A JSON-LD W3C-VC EAA may incorporate the `termsOfUse` property specified in "Verifiable Credentials Data Model v2.0" [1], clause 5.5.

EAA-7.2.9.3-02: The `termsOfUse` property shall be either a JSON Object or a JSON Array of JSON Objects. In both cases, each JSON Object shall contain the details of one set of terms of use.

EAA-7.2.9.3-03: Each JSON Object mentioned in requirement EAA-7.2.9.3-02 shall have the `type` child property identifying its type.

The following string value is defined for the `type` child property of `termsOfUse`:

1) "`embSDPolicy`": for indicating that the `termsOfUse` property contains details on the embedded selective disclosure policy associated to the JSON-LD W3C-VC EAA.

EAA-7.2.9.3-04: If the value of the `type` child property of the JSON Object mentioned in requirement EAA-7.2.9.3-02 is "`embSDPolicy`" then the mentioned JSON Object shall have the `embSDPolicyId` child property whose value shall be a URI identifying the embedded selective disclosure policy associated to the JSON-LD W3C-VC EAA.

7.2.10 Attributes evidence

EAA-7.2.10-01: A JSON-LD W3C-VC EAA may incorporate the `evidence` property.

EAA-7.2.10-02: The `evidence` property, specified in "Verifiable Credentials Data Model v2.0" [1], clause 5.7, shall implement the semantics specified in clause 4.2.10 of the present document.

EAA-7.2.10-03: The `evidence` property shall be a JSON Array whose elements shall be JSON Objects.

EAA-7.2.10-04: Each JSON Object within the JSON Array `evidence` property shall have the `type` child property. The value of the `type` child property shall be a JSON array of one or more elements whose values shall be URIs.

EAA-7.2.10-05: Each JSON Object within the JSON Array `evidence` property may have the `id` child property indicating the type of the evidence.

EAA-7.2.10-04: Each JSON Object within the JSON Array `evidence` property may have other members, whose specification is out of the scope of the present document.

7.2.11 EAA status service

7.2.11.1 General requirements

EAA-7.2.11.1-01: The `credentialStatus` property, specified in "Verifiable Credentials Data Model v2.0" [1], clause 5.6, shall implement the semantics specified in clause 4.2.11 of the present document.

EAA-7.2.11.1-02: A JSON-LD W3C-VC EAA may incorporate the `credentialStatus` object property.

The following string values are defined for the `type` child property of `credentialStatus`:

1) "`BitstringStatusListEntry`": for Bitstring Status List as specified in W3C Recommendation: "Bitstring Status List v1.0" [24].

2) "`TokenStatusList`": for Token Status List as specified in IETF draft-ietf-oauth-status-list-13 [25].

3) "`CRL`": for CRL as specified in IETF RFC 5280 [9].

4) "`OCSP`": for OCSP responses served by an OCSP Server as specified in IETF RFC 6960 [28].

EAA-7.2.11.1-03: If the value of the `type` child property of `credentialStatus` property is "`CRL`" or "`OCSP`" the value of the `statusPurpose` child property shall be present and set to value "`revocation`".

EAA-7.2.11.1-04: If the value of the `type` child property of `credentialStatus` property is "`CRL`" or "`OCSP`" the value of the `statusListCredential` child property shall be present and its value shall be an URL pointing to the revocation status service.

7.2.11.2 Requirements for EU Qualified EAA (QEAA)

QEAA-7.2.11.2-01: If a JSON-LD W3C-VC QEAA does not contain the `shortLived` property, it shall contain the `credentialStatus` property.

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

PuB-EAA-7.2.11.3-01: If a JSON-LD W3C-VC PuB-EAA does not contain the `shortLived` property, it shall contain the `credentialStatus` property.

7.2.12 EAA renewal service

EAA-7.2.12-01: A JSON-LD W3C-VC EAA may incorporate the `refreshService` property.

EAA-7.2.12-02: The `refreshService` property, specified in "Verifiable Credentials Data Model v2.0" [1], clause 5.4, shall implement the semantics specified in clause 4.2.12 of the present document.

EAA-7.2.12-03: The `refreshService` property shall be either a JSON Object or a JSON Array of JSON Objects. In both cases, each JSON Object shall contain the details of one renewal service.

7.2.13 EAA short-lived

EAA-7.2.13-01: The `shortLived` property, specified in the present clause, shall implement the semantics specified in clause 4.2.13 of the present document.

EAA-7.2.13-02: A JSON-LD W3C-VC EAA may incorporate the `shortLived` property.

EAA-7.2.13-03: The `shortLived` property shall have a boolean value.

EAA-7.2.13-04: If the `shortLived` property is absent, it shall be considered that its value is `false`.

7.3 Attested Attributes

EAA-7.3-01: Each element in the `credentialSubject` array property shall contain attested attributes associated to one entity.

7.4 Attested Attributes metadata

EAA-7.4-01: If a JSON-LD W3C-VC EAA has to incorporate selective disclosure of attributes using enveloping proofs, it shall use SD-JWT as specified in W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [2], clause 3.2.1.

EAA-7.4-02: If a JSON-LD W3C-VC EAA has to incorporate selective disclosure of attributes and it uses embedded proofs, it shall use crypto suites that allow this feature, as the one specified in W3C Recommendation (15 May 2025): "Data Integrity ECDSA Cryptosuites v1.0" [18], clause 3.5, or the one specified in W3C Candidate Recommendation (3 April 2025): "Data Integrity BBS Cryptosuites v1.0" [19], for securing the JSON-LD W3C-VC EAA.

7.5 EAA data for key binding

EAA-7.5-01: A JSON-LD W3C-VC EAA secured with SD-JWT should incorporate, in the VC Payload, the `cnf` property as specified in clause 4.1.3 of W3C VC_JOSE_COSE [2], implementing the semantics specified in clause 4.5 of the present document.

EAA-7.5-02: A JSON-LD W3C-VC EAA not secured by using SD-JWT should incorporate, in the VC Payload, the `cnf` property implementing the semantics specified in clause 4.5 of the present document.

EAA-7.5-03: In both cases the `cnf` property may only contain either a representation of the EAA subject public key or a representation of the EAA subject certificate as specified in IETF RFC 7800 [14].

EAA-7.5-04: For representing the EAA subject certificate, the `cnf` property may contain the `x5c` child property containing only the certificate itself, or the `x5t#S256` child property, or the `x5u` child property as specified in IETF RFC 7517 [30].

EAA-7.5-05: If the EAA subject certificate is represented by the `x5u` child property, the `x5t#S256` child property shall also be present.

EAA-7.5-06: If the EAA subject certificate is represented by the `x5c` child property, neither the `x5u` child property nor the `x5t#S256` child property shall be present.

EAA-7.5-07: The `cnf` property should contain a representation of the EAA subject public key.

7.6 EAA digital signature

7.6.1 General requirements

EAA-7.6.1-01: A JSON-LD W3C-VC EAA shall be secured either with embedded proofs or with enveloping proofs.

EAA-7.6.1-02: A JSON-LD W3C-VC EAA that does not have selective disclosures shall be signed by a JWS signature that shall meet the requirements defined in clause 3.1.1 of W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [2], and the requirements defined in clause 7.6.4.2 of the present document.

NOTE 1: These signed EAAs will be designated JSON-LD W3C VC JOSE EAA hereinafter.

NOTE 2: Notice that [2] uses the term JOSE for referring to generate a JWS on the JSON-LD W3C-VC EAA.

EAA-7.6.1-03: A JSON-LD W3C-VC EAA that has selective disclosures shall be signed using SD-JWT, and shall meet the requirements defined in clause 3.2.1 of W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [2], and the requirements defined in clause 7.6.4.3 of the present document.

NOTE 3: These signed EAAs will be designated JSON-LD W3C VC SD-JWT EAA hereinafter.

The expression "signed-with-enveloping-proof JSON-LD W3C-VC" will be used to indistinctly designate both JSON-LD W3C VC JOSE EAA and JSON-LD W3C VC SD-JWT EAA in requirements that are common to both formats.

7.6.2 Requirements for EU Qualified EAA (QEAA)

EAA-7.6.2-01: If the JSON-LD W3C-VC QEAA is secured using embedded proofs, the digital signature shall meet the requirements specified in clause 4.6.2 of the present document.

EAA-7.6.2-02: The digital signature of a signed-with-enveloping-proof JSON-LD W3C-VC QEAA shall be a qualified electronic signature or a qualified electronic seal.

EAA-7.6.2-03: The Protected Header of the digital signature of a signed-with-enveloping-proof JSON-LD W3C-VC QEAA shall contain the `x5u` and the `x5t#S256` header parameters, specified in IETF RFC 7515 [8].

NOTE 1: This requirement meets requirement (h) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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".

NOTE 2: The presence of the `x5t#S256` header parameter is required for security reasons.

EAA-7.6.2-04: The Protected Header of the digital signature of a signed-with-enveloping-proof JSON-LD W3C-VC QEAA should contain the `x5c` header parameter, specified in IETF RFC 7515 [8].

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

EAA-7.6.3-01: If the JSON-LD W3C-VC PuB-EAA is secured using embedded proofs, the digital signature shall meet the requirements specified in clause 4.6.2 of the present document.

EAA-7.6.3-02: The digital signature of a signed-with-enveloping-proof JSON-LD W3C-VC PuB-EAA shall be a qualified electronic signature or a qualified electronic seal.

EAA-7.6.3-03: The Protected Header of the digital signature of a signed-with-enveloping-proof JSON-LD W3C-VC PuB-EAA shall contain the `x5u` and the `x5t#S256` header parameters, specified in IETF RFC 7515 [8].

NOTE 1: This requirement meets requirement (h) in Annex VII of Regulation (EU) 2024/1183 [i.2] for PuB-EAA, 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".

NOTE 2: The presence of the `x5t#S256` header parameter is required for security reasons.

EAA-7.6.3-04: The Protected Header of the digital signature of a signed-with-enveloping-proof JSON-LD W3C-VC PuB-EAA should contain the `x5c` header parameter, specified in IETF RFC 7515 [8].

7.6.4 Requirements the JSON-LD W3C-VC EAA secured with enveloping proofs

7.6.4.1 General requirements

EAA-7.6.4.1-01: If a signed-with-enveloping-proof JSON-LD W3C-VC contains both the `iat` claim in the JOSE headers, and the `issuedAt` property, the time indicated in both components shall be the same.

EAA-7.6.4.1-02: If a signed-with-enveloping-proof JSON-LD W3C-VC contains both the `nbf` claim in the JOSE headers, and the `validFrom` property, the time indicated in both components shall be the same.

EAA-7.6.4.1-03: If a signed-with-enveloping-proof JSON-LD W3C-VC contains both the `exp` claim in the JOSE headers, and the `validUntil` property, the time indicated in both components shall be the same.

EAA-7.6.4.1-04: If a signed-with-enveloping-proof JSON-LD W3C-VC contains both the `jti` claim in the JOSE headers, and the `id` property containing the identifier of the EAA, their values shall be the same.

EAA-7.6.4.1-05: A signed-with-enveloping-proof JSON-LD W3C-VC shall not contain the `status` claim in the JOSE headers.

7.6.4.2 Additional requirements for JSON-LD W3C VC JOSE EAAs

The present clause defines requirements for JSON-LD W3C VC JOSE EAAs in addition to the requirements defined in clause 3.1.1 of W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [2].

EAA-7.6.4.2-01: A JSON-LD W3C VC JOSE EAA shall be serialized using Compact Serialization.

EAA-7.6.4.2-02: The digital signature generated by the EAA issuer shall be a JAdES-B-B.

7.6.4.3 Requirements for JSON-LD W3C VC SD-JWT EAAs

The present clause defines requirements for JSON-LD W3C VC SD-JWT EAAs in addition to the requirements defined in clause 3.2.1 of W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [2].

EAA-7.6.4.2-01: A JSON-LD W3C VC SD-JWT EAA shall be serialized using either Compact Serialization or Flattened JSON Serialization, as specified in IETF SD-JWT [5].

EAA-7.6.4.2-02: If a JSON-LD W3C VC SD-JWT EAA is serialized using Flattened JSON Serialization, the digital signature shall be a JAdES-B-B signature as specified in ETSI TS 119 182-1 [11].

NOTE: IETF SD-JWT [5] Compact Serialization defines a structure that goes beyond JWS Compact Serialization, adding to the JWS Compact Serialization the disclosures separated by '~'.

EAA-7.6.4.2-03: If a JSON-LD W3C VC SD-JWT EAA is serialized using Compact Serialization, the resulting structure shall consist in the Compact Serialization of a JAdES-B-B signature, as specified in ETSI TS 119 182-1 [11], followed by the sequence of disclosures appended as specified in IETF SD-JWT [5].

7.6.4.4 Requirements for EU Qualified EAA (QEAA)

QEAA-7.6.4.4-01: If the digital signature is a JAdES-B-B as specified in ETSI TS 119 182-1 [11], then the requirements specified in clause 5.6.2 shall also apply.

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

QEAA-7.6.4.5-01: If the digital signature is a JAdES-B-B as specified in ETSI TS 119 182-1 [11] then the requirements specified in clause 5.6.3 shall also apply.

7.6.5 Requirements for JSON-LD W3C-VC EAA with embedded proofs

7.6.5.1 General requirements

EAA-7.6.5.1-01: A JSON-LD W3C-VC EAA secured using embedded proofs shall include the `proof` property, as specified in "Verifiable Credentials Data Model v2.0" [1] clause 4.12.

EAA-7.6.5.1-02: The contents of the `proof` property should be as specified in W3C Recommendation: "Verifiable Credential Data Integrity v1.0" [26].

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

8.1 General requirements

Clause 8 of the present document defines a realization of EAA based on X.509 Attribute certificates as specified in IETF RFC 5755 [6].

The EAAs implemented according to clause 8 of the present document, will be designated as X.509-AC EAA hereinafter.

The informative Annex B of the present document contains the details of how to reach the file that contains the ASN.1 definitions for X.509-AC EAAs.

This separate file is a convenience tool and its content is informative. In case of any discrepancy between the definitions of the types and data elements given in the present document and the ones given in the separate file, the definitions given in the present document shall take precedence.

NOTE: The file containing the ASN.1 definitions includes a preamble with, among other parts, import and export sentences, so that its contents can be processed by software.

8.2 EAA metadata

8.2.1 EAA specification

8.2.1.1 EAA type

EAA-8.2.1.1-01: The `etsi-eaaType` extension specified in the present clause shall implement the semantics specified in clause 4.2.1.2 of the present document.

EAA-8.2.1.1-02: An X.509-AC EAA may incorporate the extension `etsi-eaaType`, which is defined below.

```
-- Arc for all the identifiers of the extensions of X.509-AC EAAs
```

```
id-etsi-eaa-x509AC-ext-root OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) id-
qeaas-profile(194721) }

-- Subarc for identifiers of extensions applicable to all EAAs

id-etsi-eaa-x509AC-nqext    OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-ext-root 2 }

-- EAA Type attestation extension

id-etsi-eaa-x509AC-ext-type OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-nqext 1 }

etsi-eaaType  EXTENSION ::= {
    SYNTAX EAAType IDENTIFIED BY id-etsi-eaa-x509AC-ext-type}

EAAType  ::= UTF8String
```

EAA-8.2.1.1-03: The value of the `etsi-eaaType` extension shall be a URI identifying the type of the X.509-AC EAA.

8.2.1.2 EAA context

EAA-8.2.1.2-01: An 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` extension, `crlDistributionPoints` extension, and `EAAType` extension.

NOTE: IETF RFC 5755 [6] 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.

8.2.1.3 EAA schema

EAA-8.2.1.3-01: An X.509-AC EAA shall not have any component implementing the semantics specified in clause 4.2.1.4 of the present document.

NOTE: See [i.6], which specifies among other things "a data model for catalogue of attributes, guidance on Attestation Rulebooks, attestation type data models and applicable Application Programming Interface (API) for management of machine-readable attestation schemas".

8.2.2 EAA category

8.2.2.1 General requirements

EAA-8.2.2.1-01: X.509-AC EAAs issued by EAA Providers registered in the European Union, which are neither X.509-AC QEAAs nor X.509-AC PuB-EAAs, shall not include any extension for signalling a specific category.

8.2.2.2 Requirements for EU Qualified EAA (QEAA)

QEAA-8.2.2.2-01: An X.509-AC QEAA shall incorporate the extension `etsi-qeaaStatements`, which is defined below.

```
-- Subarc for extensions applicable only to QEAA and PuB-EAA

id-etsi-qeaas-x509AC-prof-identifiers   OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-ext-root 1 }

-- QEAA-STATEMENT class definition

QEAA-STATEMENT ::= CLASS {
    &statementId  OBJECT IDENTIFIER UNIQUE,
    &Type OPTIONAL
}
WITH SYNTAX {
    IDENTIFIED BY &statementId
```

```
    [SYNTAX &Type]
}

-- QEAAStatements definition

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

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

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

SupportedStatements QEAA-STATEMENT ::= { etsi-qeaaStatement-1 | etsi-eaaPubAStatement-1}
```

QEAA-8.2.2.2-02: The `etsi-qeaaStatements` extension shall not be marked as critical.

QEAA-8.2.2.2-03: An X.509-AC QEAA shall incorporate the `QEAA-Statement` that is defined below.

```
-- EUqeaaCompliance QEAAStatement definition

id-etsi-qeaas-EUqeaaCompliance OBJECT IDENTIFIER ::= { id-qeaas-qeaaStatements 1}

etsi-qeaaStatement-1 QEAA-STATEMENT ::= { IDENTIFIED BY id-etsi-qeaas-EUqeaaCompliance }
```

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

PuB-EAA-8.2.2.3-01: An X.509-AC PuB-EAA shall incorporate the extension `etsi-qeaaStatements` specified in clause 8.2.2.2 of the present document.

PuB-EAA-8.2.2.3-02: The `etsi-qeaaStatements` extension shall not be marked as critical.

PuB-EAA-8.2.2.3-03: An X.509-AC PuB-EAA shall incorporate the `QEAA-Statement` that is defined below.

```
-- eaaPubA-EUeaaPubACompliance QEAAStatement definition

id-etsi-eaaPubA-EUeaaPubACompliance OBJECT IDENTIFIER ::= { id-qeaas-qeaaStatements 2}

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

8.2.3 EAA identifier

EAA-8.2.3-01: An X.509-AC EAA shall contain the `serialNumber` field, whose value, with the value of the `issuer` field, shall identify the EAA itself.

8.2.4 EAA issuer identifier

8.2.4.1 General requirements

EAA-8.2.4.1-01: An X.509-AC EAA shall contain the `issuer` field as specified in IETF RFC 5755 [6].

EAA-8.2.4.1-02: Its value shall be a distinguished name (`dNSName` choice of `GeneralNames` type as specified in IETF RFC 5280 [9]) within `v2Form` choice of `AttCertIssuer` type.

EAA-8.2.4.1-03: An X.509-AC EAA may contain the `issuerUniqueID` field, as specified in IETF RFC 5755 [6], clause 4.2.8.

Requirements when the EAA issuer is a legal person

EAA-8.2.4.1-04: If the X.509-AC EAA issuer is a legal person, the `issuer` field shall not contain any of the X.509 attributes providing details of natural persons.

EAA-8.2.4.1-05: Where a registration identifier is applicable, the `issuer` field may contain the attribute `organizationIdentifier` attribute.

EAA-8.2.4.1-06: The value of the `organizationIdentifier` attribute may be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the subject field of an X.509 certificate.

Requirements when the EAA issuer is a natural person

EAA-8.2.4.1-07: If the X.509-AC EAA issuer is a natural person, the `issuer` field shall not contain any of the X.509 attributes providing details of legal persons.

8.2.4.2 Requirements for EU Qualified EAA (QEAA)

QEAA-8.2.4.2-01: In an X.509-AC QEAA the `issuer` field shall contain, at least the following X.509 attributes: `country` (C), and `organizationName` (O).

QEAA-8.2.4.2-02: If the issuer of the X.509-AC QEAA is a legal person and if a registration identifier is applicable, the `issuer` field shall contain the attribute `organizationIdentifier` attribute.

QEAA-8.2.4.2-03: The value of one instance of the `organizationIdentifier` attribute shall be built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

QEAA-8.2.4.2-04: In an X.509-AC 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 X.509-AC QEAA issuer for supporting the validation of the signature of the X.509-AC QEAA.

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

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

PuB-EAA-8.2.4.3-01: In an X.509-AC PuB-EAA the `issuer` field shall contain, at least the following X.509 attributes: `country` (C), and `organizationName` (O).

PuB-EAA-8.2.4.3-02: Where a registration identifier is applicable, one instance of the `organizationIdentifier` attribute shall be present and built according to the rules defined in clause 5.1.4 of ETSI EN 319 412-1 [16] to build the value of the `organizationIdentifier` attribute in the `subject` field of an X.509 certificate.

PuB-EAA-8.2.4.3-03: In an X.509-AC PuB-EAA 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 X.509-AC PuB-EAA issuer for supporting the validation of the signature of the X.509-AC PuB-EAA.

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

8.2.5 EAA and attribute subject identifiers and pseudonyms

8.2.5.1 EAA subject identifier

EAA-8.2.5.1-02: In an X.509-AC EAA the EAA subject identifier shall be present in the `holder` field.

EAA-8.2.5.1-03: In an X.509-AC EAA the `holder` field shall include the `objectDigestInfo` field, which in turn, shall have the `publickeycert` value as specified in IETF RFC 5755 [6], clause 7.3.

8.2.5.2 EAA subject pseudonym

EAA-8.2.5.2-01: In an X.509-AC EAA the EAA subject identifier shall be present in the `holder` field.

EAA-8.2.5.2-02: In an X.509-AC EAA the `holder` field shall include the `objectDigestInfo` field, which in turn, shall have the `publickeycert` value as specified in IETF RFC 5755 [6], clause 7.3, which shall be certified in an X.509 certificate issued in such a way that it protects the subject privacy.

8.2.5.3 The attribute subject identifier

EAA-8.2.5.3-01: An X.509-AC EAA may contain attributes referring to different entities.

EAA-8.2.5.3-02: In an X.509-AC EAA each attribute not associated to the EAA subject shall be associated either to an attribute subject identifier or to an attribute subject pseudonym.

EAA-8.2.5.3-03: An X.509-AC EAA may associate a set of attributes to the identifier of an entity different than the EAA subject using one of the types specified in clauses 8.3.2 and 8.3.3 of the present document.

8.2.5.4 The attribute subject pseudonym

EAA-8.2.5.4-01: An X.509-AC EAA may associate a set of attributes to the pseudonym of an entity different than the EAA subject using one of the types specified in clauses 8.3.2 and 8.3.3 of the present document.

8.2.5.5 Requirements for EU Qualified EAA (QEAA)

QEAA-8.2.5.5-01: In an X.509-AC QEAA all the attributes shall refer to the EAA subject.

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

PuB-EAA-8.2.5.6-01: In an X.509-AC PuB-EAA all the attributes shall refer to the EAA subject.

8.2.6 EAA issuance

EAA-8.2.6-01: An X.509-AC EAA shall not contain a component devoted to indicate the instant when the EAA was generated.

8.2.7 EAA validity periods

8.2.7.1 Specific requirements for the EAA technical validity period

EAA-8.2.7.1-01: The `notBeforeTime` field of `attrCertValidityPeriod` specified in clause 4.2.6, shall implement the semantics of the first instant time of the X.509-AC EAA technical validity period.

EAA-8.2.7.1-02: The `notAfterTime` fields of `attrCertValidityPeriod` specified in clause 4.2.6, shall implement the semantics of the second instant time of the X.509-AC EAA technical validity period.

8.2.7.2 Specific requirements for the EAA administrative validity period

EAA-8.2.7.2-01: An X.509-AC EAA may incorporate the X.509-AC EAA administrative validity period.

EAA-8.2.7.2-02: The `notBeforeTime` field of the `etsi-eaaAdmValidityPeriod` extension specified below, shall implement the semantics of the first instant time of the X.509-AC EAA administrative validity period.

EAA-8.2.7.2-03: The `notAfterTime` fields of the `etsi-eaaAdmValidityPeriod` extension specified below, shall implement the semantics of the second instant time of the X.509-AC EAA administrative validity period.

EAA-8.2.7.2-04: The X.509-AC EAA `etsi-eaaAdmValidityPeriod` extension shall be as defined below.

```
-- EAA administrative validity period attestation extension

id-etsi-eaa-x509AC-ext-adm-validityPeriod   OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-nqext 3 }

etsi-eaaAdmValidityPeriod  EXTENSION ::= {
    SYNTAX             AdmValidityPeriod
    IDENTIFIED BY      id-etsi-eaa-x509AC-ext-adm-validityPeriod }

AdmValidityPeriod  ::= SEQUENCE {
    notBeforeTime  GeneralizedTime,
    notAfterTime   GeneralizedTime
}
```

8.2.8 Components constraining the usage of the EAA

8.2.8.1 EAA audience

EAA-8.2.8.1-01: An X.509-AC EAA may identify the set of relying parties the EAA is intended for within the `id-ce-targetInformation` extension specified in IETF RFC 5755 [6], clause 4.3.2.

NOTE: The restrictions mentioned in clause 4.2.9.2 of the present document can also be imposed by Embedded Disclosure Policy existing for the EAA and the restrictions established for the Relying Parties during their registration.

8.2.8.2 Signal of one-time use

EAA-8.2.8.2-01: If an 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 `etsi-eaaOneTimeUse` extension.

EAA-8.2.8.2-02: The `etsi-eaaOneTimeUse` extension shall be as defined below.

```
-- oneTimeUse EAA attestation extension

id-etsi-eaa-x509AC-ext-oneTimeUse       OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-nqext 2 }

etsi-eaaOneTimeUse  EXTENSION ::= { IDENTIFIED BY id-etsi-eaa-x509AC-ext-oneTimeUse }
```

8.2.9 Attributes evidence

EAA-8.2.9-01: An X.509-AC EAA shall not include any component meeting the semantics specified in clause 4.2.10 of the present document.

8.2.10 EAA status service

8.2.10.1 General requirements

EAA-8.2.10.1-01: If an 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 [9], clause 4.2.2.1) with the `accessMethod` field set to `id-ad-ocsp`, or within the extension identified by the OID `id-ce-cRLDistributionPoints` (specified in IETF RFC 5280 [9], clause 4.2.1.13), or within both.

EAA-8.2.10.1-02: If an 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 OID `id-ce-noRevAvail` specified in IETF RFC 5755 [6], clause 4.3.6.

8.2.10.2 Requirements for EU Qualified EAA (QEAA)

QEAA-8.2.10.2-01: If an X.509-AC QEAA contains the `etsi-eaaShortLived` extension, none of the two extensions identified in requirement EAA-8.2.10.1-01 shall be present within the X.509-AC QEAA.

NOTE: The requirement on the value of `accessMethod` field in requirement EAA-8.2.10.1-01 meets the requirements defined in eIDAS 2.0, annex V.

QEAA-8.2.10.2-02: If an X.509-AC QEAA does not contain the `etsi-eaaShortLived` extension, it shall contain one of the two extensions identified in requirement EAA-8.2.10.1-01.

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

PuB-EAA-8.2.10.3-01: If an X.509-AC PuB-EAA contains the `etsi-eaaShortLived` extension, none of the two extensions identified in requirement EAA-8.2.10.1-01 shall be present within the X.509-AC PuB-EAA.

NOTE: The requirement on the value of `accessMethod` field meets the requirements defined in eIDAS 2.0, annex VII.

PuB-EAA-8.2.10.3-02: If an X.509-AC PuB-EAA does not contain the `etsi-eaaShortLived` extension, it shall contain one of the two extensions identified in requirement EAA-8.2.10.1-01.

8.2.11 EAA renewal service

EAA-8.2.11-01: An X.509-AC EAA shall not incorporate any component implementing the semantics specified in clause 4.2.12 of the present document.

8.2.12 EAA short-lived

EAA-8.2.12-01: The `etsi-eaaShortLived` extension shall implement the semantics specified in clause 4.2.13 of the present document.

EAA-8.2.12-02: An X.509-AC EAA may incorporate the `etsi-eaaShortLived` extension.

EAA-8.2.12-03: The `eaashortLived` extension shall be as defined below.

```
-- shortLived EAA attestation extension

id-etsi-eaa-x509AC-ext-shortLived       OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-nqext 4 }

etsi-eaaShortLived  EXTENSION ::= { IDENTIFIED BY id-etsi-eaa-x509AC-ext-shortLived }
```

EAA-8.2.12-04: If the X.509-AC EAA contains this extension then it shall neither contain the `id-ce-cRLDistributionPoints` extension specified in IETF RFC 5755 [6], clause 4.3.5 nor the `id-pe-authorityInfoAccess` with the `accessMethod` field set to `id-ad-ocsp`.

EAA-8.2.12-05: If the X.509-AC EAA contains this extension then it shall contain the `id-ce-noRevAvail` extension specified in IETF RFC 5755 [6], clause 4.3.6.

8.3 Attested attributes

8.3.1 General requirements

EAA-8.3.1-01: An X.509-AC EAA shall incorporate each individual Attested Attribute as an instance of the `Attribute` type specified in clause 4.2.7 of IETF RFC 5755 [6].

EAA-8.3.1-02: An X.509-AC EAA shall place the individual Attested Attributes in the `attributes` field.

The present document specifies two implementations for including attested attributes within the `attributes` field, namely: as JSON tokens (X.509 AC/JSON implementation) or as instances of ASN.1 (defined in Recommendation ITU-T X.680-X.683 [7]) types (X.509 AC/ASN.1 implementation).

8.3.2 Attested attributes for X.509 AC/JSON implementation

EAA-8.3.2-01: An X.509-AC EAA conformant to the X.509 AC/JSON implementation, shall place the attributes within one instance of `JSONEncodedAttribute` type.

EAA-8.3.2-02: `JSONEncodedAttribute` shall be as defined below.

```
-- JSON encoded attestation extension

id-etsi-eaa-x509AC-ext-jsonattr     OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-nqext 5 }


etsi-eaa-ext-jsonattr       ATTRIBUTE ::= {SYNTAX JSONEncodedAttribute IDENTIFIED BY id-etsi-eaa-
x509AC-ext-jsonattr }

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

EAA-8.3.2-03: The set in the attribute value shall contain only one element, whose value shall be a JSON claim.

EAA-8.3.2-04: For associating a set of attributes to one entity different than the EAA subject, the `JSONEncodedAttribute` shall contain the UTF-8 String resulting of encoding an instance of the type `subAttrs`, specified in clause 5.3 of the present document.

8.3.3 Attested attributes for X.509 AC/ASN.1 implementation

EAA-8.3.3-01: Within an 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 IETF RFC 5755 [6], clause 4.2.7.

EAA-8.3.3-02: For associating a set of attributes to one entity different than the EAA subject using the X.509 AC/ASN.1 implementation, the X.509-AC EAA shall use as value of the attribute one instance of the `SubAttrs` type, which is defined below.

```
-- Attribute for associating a sequence of attributes to one attribute subject

id-etsi-eaa-x509AC-ext-subAttrs     OBJECT IDENTIFIER ::= { id-etsi-eaa-x509AC-nqext 6 }


etsi-eaa-ext-subAttrs       EXTENSION ::= {SYNTAX SubjectAttrs IDENTIFIED BY id-etsi-eaa-x509AC-ext-
subAttrs }

SubjectAttrs ::= SEQUENCE{
    subIdOrPseudonym    IdOrPseudonym,
    attrs           Extensions -- the attributes associated to the attribute subject
}

IdOrPseudonym ::= CHOICE{
    subId   [0] IA5String,
    subAka  [1] IA5String,
}
```

EAA-8.3.3-03: The `subId` field of the `subOrPseudonym` CHOICE shall contain the identifier of the attribute subject. The `subAka` field of the `subOrPseudonym` CHOICE shall contain the pseudonym of the attribute subject. The `attrs` field shall contain all the attributes associated to the attribute subject.

8.4 Attested attributes metadata

8.4.1 Implementation of support to selective disclosure of Attested Attributes

An X.509-AC EAA can achieve selective disclosure through atomic EAAs, i.e. X.509 Attribute Certificates attesting only one attribute.

EAA-8.4.1-01: EAAs Issuer issuing X.509-AC EAA should support the selective disclosure with the issuance of atomic X.509 ACs.

8.5 EAA data for key binding

In an X.509-AC EAA the key binding is natively implemented, because the requirement EAA-8.2.5.1-03 states that "the `holder` field shall include the `objectDigestInfo` field, which in turn, shall have the `publickeycert` value as specified in IETF RFC 5755 [6], clause 7.3".

8.6 EAA digital signature

8.6.1 Requirements for EU Qualified EAA (QEAA)

QEAA-8.6.1-01: The requirements specified in clause 4.6.2 shall apply

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

PuB-EAA-8.6.2-01: The requirements specified in clause 4.6.3 shall apply.

Annex A (informative): Data elements and namespaces for ISO/IEC-mdoc EAA realization

Table A.1 specifies the namespaces for the data elements addressed in the ISO/IEC-mdoc EAA realization.

The first column shows the data element identifier.

The second column shows the namespace where the data element is placed when it is a data element of an ISO/IEC-mdoc EAA that is a mDL (document type "org.iso.18013.5.1.mDL").

The third column shows the namespace where the data element is placed when it is a data element of an ISO/IEC-mdoc EAA that is not a mDL (has a different document type).

The fourth column identifies the document that defines the data element. If ISO/IEC 18013-5 [12] and ISO/IEC 23220-2 [13] define a data element with the same identifier, the corresponding cell in the column is divided in two, each one identifying one of these documents.

The fifth column identifies the clause in the document that defines the data element. If ISO/IEC 18013-5 [12] and ISO/IEC 23220-2 [13] define a data element with the same identifier, the corresponding cell in the column is divided in two, each one identifying the clause of the corresponding document where the data element is defined.

Table A.1: Data elements and namespaces for ISO/IEC-mdoc EAA realization

Data element identifier	Namespace for mDL EAA	Namespace for non-mDL EAA	Defining document	Clause(s)
issuing_authority	"org.iso.18013.5.1"	NA	ISO/IEC 18013-5 [12]	7.2.1
issuing_authority_latin1	NA	"org.iso.23220.1"	ISO/IEC 23220-2 [13]	6.2.3
document_number	"org.iso.18013.5.1"	"org.iso.18013.5.1"	ISO/IEC 18013-5 [12]	7.2.1
			ISO/IEC 23220-2 [13]	6.3
issuing_country	"org.iso.18013.5.1"	"org.iso.23220.1"	ISO/IEC 18013-5 [12]	7.2.1
			ISO/IEC 23220-2 [13]	6.3
issue_date	"org.iso.18013.5.1"	"org.iso.23220.1"	ISO/IEC 23220-2 [13]	7.2.1
			ISO/IEC 23220-2 [13]	6.3
expiry_date	"org.iso.18013.5.1"	"org.iso.23220.1"	ISO/IEC 18013-5 [12]	7.2.1
			ISO/IEC 23220-2 [13]	6.3
Schema	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.1.3
category	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.2
iss_reg_id	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.4
also_known_as	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.5
oneTime	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.8.2
status_service	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.10
shortLived	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.2.12
SubAttr	"org.etsi.01947201.010101"	"org.etsi.01947201.010101"	ETSI TS 119 472-1 (the present document)	6.3

Annex B (informative): Location of file with ASN.1 definitions for X.509-AC EAAs

The file `definitions_for_X.509-AC_EAAs.asn1` at https://forge.etsi.org/rep/esi/x19_47201_Profiles_for_EAA/raw/v1.2.1/definitions_for_X.509-AC_EAAs.asn1 contains the ASN.1 definitions for X.509-AC EAAs.

Annex C (informative): Change history

Date	Version	Information about changes
2/12/2025	1.1.2	Implemented agreements reached with the EC team that generated the "EC assessment" document of TS 119 472-1v0.0.11 (the one approved by RC which was the version evolved by editHelp to v1.1.1), generated after the approval by RC of TS 119 472-1v1.1.1. Below follows the list 1. Reference version 13 of SD-JWT VC draft 2. Modified text in 5.2.1.1 (Introduction for SD-JWT VC EAA) for matching the text to actual contents of SD-JWT VC Type Metadata in its version 13 3. Removed schema claim as in SD-JWT VC v13 this claim has been dropped 4. Modified the specification of `status` component in ISO/IEC-mdoc EAA. Added an optional child element `status_list` as specified in draft-ietf-oauth-status-list-12. The other potential child element, defined in second edition draft of ISO/IEC 18013-5 can not be included. 5. Dropped `BitStringStatusListEntry` as a potential content of the status in SD-JWT VC EAA implementation. 6. Fixed error: if a QEAA or PuB-EAA are short-lived, then the mandatory requirement of having a status component has been dropped. Implemented dispositions for some of the comments raised by SPRIND after the approval by RC of TS 119 472-1v1.1.1 1. Reference version 13 of SD-JWT VC draft 2. Removed schema claim as in SD-JWT VC v13 this claim has been dropped 3. Allow EAAs that do not contain neither `sub` nor `also_known_as` 4. Modified the specification of `status` component in ISO/IEC-mdoc EAA. Added an optional child element `status_list` as specified in draft-ietf-oauth-status-list-12. 5. Dropped `BitStringStatusListEntry` as a potential content of the status in SD-JWT VC EAA implementation 6. Two editorial changes 7. Allow any level of JAdES signatures. Implemented some changes in the ASN.1 definitions for X.509-AC EAA implementation.
14/12/2025	1.1.3	Implemented agreements reached by EC team, ESI members, and SPRIND on comments raised by SPRIND that had not been disposed in v1.1.2. Below follows a brief enumeration: 1. EAA identifier made mandatory for QEAA and Pub_EAA in all the implementations. 2. EAA identifier made optional in non-QEAA and non-PuB-EAA for SD-JWT VC EAA, JSON-LD VC EAA. EAA identifier made mandatory in non-QEAA and PuB-E ISO/IEC-mdoc EAA and X.509-AC EAA (their corresponding specifications make document_number and serialNumber mandatory) 3. Requirements on details of issuer: name, country, and registration id modified for taking into account that these details can also be present in the qualified certificate supporting the EAA signature. Also, make them optional in non-QEAA and non-PuB-EAA, in those implementations that allow it (for instance, in ISO/IEC-mdoc EAA ISO 18013-5 forces the presence of some of them even in non-QEAA and non-PuB-EAA) 4. Accepted the optional presence of a component evidence as specified in "OpenID Identity Assurance Schema Definition 1.0" Implemented some fixes in the ASN.1 definitions. A separate file containing the ASN.1 definitions for X.509-AC EAA implementation has been generated and will be made publicly available as a convenience tool for implementors (informative material). Added an informative annex which in its published version shall point to the location of the mentioned file.

Date	Version	Information about changes
16/12/2025	1.1.4	In clause "4.5 EAA data for key binding", the requirement has been changing from "shall" to "should" ''EAA-4.5-01: An EAA should incorporate a component proving that a certain public key is in possession of the EAA subject." NOTE 1 wording has been changed to apply only "In this case" NOTE 2 has been added for providing rationale to this should. The "shall" has also turned into "should" in those implementations that allow it, namely: 5.5 (SD-JWT VC EAA), and 7.5 JSON-LD W3C-VC EAA. For the other implementations: ISO/IEC 18013-5 makes DeviceKey in keyDeviceInfo mandatory in the MSO. X.509-AC EAA, previous requirement EAA-8.2.5.1-03 states that "the holder field shall include the objectDigestInfo field, which in turn, shall have the publickeycert value as specified in IETF RFC 5755 [6], clause 7.3"

History

Version	Date	Status
V1.1.1	December 2025	Publication
V1.2.1	February 2026	Publication