ETSI TS 119 471 V1.1.1 (2025-05)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services

Reference

DTS/ESI-0019471

Keywords

digital identity, EAA, EUDI wallet, identity,
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

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to
the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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).

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.

Introduction

The present document provides detailed policy and security requirements for Electronic Attestation of Attributes (EAA) services and EAA service providers, which play a critical role under the eIDAS Regulation [i.1].

The eIDAS Regulation [i.1] aims to enhance trust in electronic transactions within the internal market by providing a common foundation for secure electronic identification and trust services. One of the key components of this regulation is the concept of EAA, which enables the verification and validation of specific attributes of natural persons, legal persons and objects in an electronic form.

The present document specifies the policies and security requirements for EAA service providers offering EAA services. It includes comprehensive requirements for the verification of attributes, the issuance of attestations, and the validation services required to ensure the integrity and reliability of the EAA lifecycle.

Key aspects covered in the present document include policy and security requirements:

- guidelines on how trust service providers should verify and generate electronic attestations of attributes, ensuring that all processes are secure and reliable;
- attributes verification: requirements for verifying the identity and specific attributes of individuals or entities requesting attestations, ensuring unequivocal certainty;
- issuance and validation of EAAs: requirements on protocols for the secure issuance and validation of electronic attestations, including the use of privacy-preserving techniques to protect user data;
- risk management: comprehensive risk assessment procedures to identify and mitigate potential threats to the security and integrity of EAA services;
- compliance and auditability: requirements for maintaining detailed logs and records of all transactions and operations related to the issuance of EAAs to support auditability and transparency.

1 Scope

The present document specifies policy and security requirements for electronic attestation of attributes trust service providers and the attestation of attributes services they provide.

More specifically the present document specifies policy and security requirements on attributes issuance and validation of EAA by the trust service provider.

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] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

NOTE: The eIDAS regulation as amended by 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.2] ISO/IEC TS 23220-2:2024: "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 systems".

[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] OpenID for Verifiable Credential Issuance.

[i.5] EU Architectural Reference Framework.

[i.6] ISO/IEC 15408-1:2022: "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security".

[i.7] ISO/IEC 19790:2025: "Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules".

[i.8] FIPS 140-2: "Security Requirements for Cryptographic Modules".

[i.9] FIPS 140-3: "Development".

[i.10] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

[i.11] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.12] ISO/IEC 18013-5:2021 "Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [1] and the following apply:

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

NOTE: As per eIDAS definition [i.1].

attestation of attributes validation: process of verifying and confirming that an attestation of attributes is valid

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

authentication: electronic process that enables the electronic identification of a natural or legal person to be confirmed, or the origin and integrity of data in electronic form to be confirmed

NOTE: As per eIDAS definition [i.1].

authentic source: repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person and is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice

NOTE 1: As per eIDAS definition [i.1].

NOTE 2: This include any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to provide attributes about a natural or legal person.

Electronic Attestation of Attributes (EAA): attestation in electronic form that allows the authentication of attributes

NOTE: As per eIDAS definition [i.1].

electronic attestation of attributes policy: set of rules that indicates the applicability of an EAA to a particular community and/or class of application with common requirements

NOTE 1: See clause 4.2.2 of ETSI EN 319 411-1 [i.11] for further explanation.

NOTE 2: This refers to a sector or service specific policies (i.e. banking, age verification).

electronic attestation of attributes practice statement: statement of the practices that an EAASP employs in providing a trust service

NOTE: As per ETSI EN 319 401 [1] definition [1].

electronic attestation of attributes service policy: set of rules that indicates the applicability of EAA service with common controls and security requirements

NOTE: See ETSI EN 319 401 [1] trust service policy definition note.

Electronic Attestation of Attributes Service Provider (EAASP): natural or legal person who provides one or more EAA services either as a qualified or as a non-qualified trust service provider

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

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

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

electronic attestation of attributes trust service: electronic service which supports the issuance and/or validation of electronic attestation of attributes

electronic identification: process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a natural or legal person

NOTE: As per eIDAS definition [i.1].

electronic identification means: material and/or immaterial unit containing person identification data and which is used for authentication to an online service or, where appropriate, to an offline service

NOTE: As per eIDAS definition [i.1].

European digital identity wallet: electronic identification means, which allows the user to securely store, manage and validate identity data and electronic attestations of attributes, to provide them to relying parties and to other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals

NOTE: As per eIDAS definition [i.1].

Person Identification Data (PID): set of identity attributes that uniquely identifies a natural or legal person in the context of the EEA provisioning

NOTE: eIDAS requires PID to be issued in accordance with EU or national law and within the context of a (notified) eID scheme.

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

NOTE: As per eIDAS definition [i.1].

Qualified Electronic Attestation Of Attributes Services Provider (QEAASP): electronic attestation of attributes services provider who is granted the qualified status by an EU National Supervisory Authority

NOTE: As per eIDAS definition [i.1].

relying party: natural or legal person that relies upon an electronic identification, European Digital Identity Wallets or other electronic identification means, or a trust service

NOTE: As per eIDAS definition [i.1].

wallet unit: specific setup of the wallet solution for an individual user

NOTE: As described in CIR (EU) 2024/2977 Article 2.2 [i.3].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [1] and the following apply:

ARF	EU Architectural Reference Framework
CIR	Commission Implementing Regulation
EAA	Electronic Attestation of Attributes
EAAP	Electronic Attestation of Attributes Policy
EAAS	Electronic Attestation of Attributes Service
EAASP	Electronic Attestation of Attributes Service Provider
EAASPol	Electronic Attestation of Attributes Service Policy
EAASPS	Electronic Attestation of Attributes Services Practice Statement
EAL	Evaluation Assurance Level
EQ	Electronic Qualification
EUDIW	European Union Digital Identity Wallet
HSM	Hardware Security Module
ISO	International Organization for Standardization
JWT	JSON Web Token
LoA	Level of Assurance
mDL	mobile Driving License
OpenID4VCI	OpenID for Verifiable Credential Issuance
PID	Person Identification Data
PIM	Person Identification Means
QEAA	Qualified Electronic Attestation of Attributes
QEAAS	Qualified Electronic Attestation of Attributes Service
QEAASP	Qualified Electronic Attestation of Attributes Service Provider
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
SD-JWT	Selective Disclosure JSON Web Token
TSP	Trust Service Provider
VC	Verifiable Credentials
VI	Video Identification
WSCA	Wallet Secure Cryptographic Application
WSCD	Wallet Secure Cryptographic Device
WUA	Wallet Unit Attestation

3.4 Notation

Each requirement is identified as follows:

REQ-EAASP-< the clause number>-<2-digit number - incremental> identifies requirements referred to the non-qualified service provider.

REQ-QEAASP-< the clause number>-<2-digit number - incremental> identifies requirements referred to the qualified service provider.

REQ-EAAS-< the clause number>-<2-digit number - incremental> identifies requirements referred to the service.

4 EAA trust services

4.1 Overview

An EAASP is a trusted entity that issues and/or validates attributes referred to attributes' subject. The EAASP acts as a reliable and trusted third-party authority that vouches for the accuracy and validity of the information provided in the EAA. The EEASP is responsible for ensuring the truthfulness, validity, and timeliness of the attributes and data provided by the authentic or other source, the EAA Subject, and the EAA Subscriber.

4.2 EAA Issuance services

4.2.1 Initiation

4.2.1.1 General

REQ-EAASP-4.2.1.1-01: When issuing an EAA, the EAASP shall verify the identity, along with specific attributes where applicable, of the EAA Subject and/or EAA Subscriber to whom it is issued in accordance with the EAAS and EAASPol.

REQ-EAASP-4.2.1.1-02: The EAASP shall verify that the request contains all necessary information for creating the EAA. The EAASP shall collect and verify the following:

a) That the EAA subject is identical to the EAA Subscriber;

b) When the EAA subject differs from the EAA Subscriber, the EAA Subscriber identity, any additional information required for verification; and

c) That the attribute and attribute subject correspond to the EAA Subject.

REQ-EAASP-4.2.1.1-03 [CONDITIONAL]: If the requested EAA Subject is not the EAA Subscriber then the EEASP shall obtain and verify evidence (electronic or otherwise) that confirms the right to act on behalf of the EAA Subject.

REQ-EAASP-4.2.1.1-04 [CONDITIONAL]: If validation of the attributes is against authentic source, the EAASP shall verify the identity of the authentic source used to verify attributes.

EXAMPLE: Verification of identity can be based on a qualified electronic signature or qualified electronic seal.

REQ-EAASP-4.2.1.1-05 [CONDITIONAL]: When the EAA Subscriber requests the issuance of an EAA for attributes listed in Annex VI that requires consultation of an authentic source, and provided that national authorities have established a secure access system, the EAASP should be able to verify the authenticity of the attribute(s) by at least electronic means.

4.2.1.2 EUDIW specific

In addition, when the EAA is issued to a EUDIW the following requirements apply:

REQ-EAASP-4.2.1.2-01 [CONDITIONAL]: If the EAASP is supporting OpenID4VCI [i.4], the EAASP should support an attestation issuance interface compliant with the OpenID4VCI protocol or an equivalent to issue EAAs to Wallet Units, enabling interoperability between trust service providers and Wallet Unit holders.

REQ-EAASP-4.2.1.2-02: The EAASP shall implement mechanisms to authenticate Wallet Units before issuing an EAA, verifying that the Wallet Unit comes from a trusted Wallet Provider.

REQ-EAASP-4.2.1.2-03: The EAASP shall validate that the Wallet Secure Cryptographic Device (WSCD) of the Wallet Unit complies with the required security level before issuing an EAA.

NOTE: This can be validated using information, such a certification information, provided by the Wallet Provider.

4.2.2 EAA issuance

4.2.2.1 General

REQ-EAASP-4.2.2.1-01: The EAASP shall request only the minimum data necessary for the issuance of the EAA, in line with the principle of data minimization.

In particular:

REQ-EAASP-4.2.2.1-02: The EAASP shall ensure that the minimum set of attributes required for the issuance of EAA are acquired in accordance with the EAAP.

REQ-EAASP-4.2.2.1-03: The EAASP shall verify attributes against one or more authentic or not authentic source, as stated in EAAP.

REQ-EAASP-4.2.2.1-04: The EAASP shall define the attributes to be verified by the content and nature of the EAA defined in EAAP.

REQ-EAASP-4.2.2.1-05: The EAASP shall not verify identity attributes that are not necessary for the EAA issuance.

NOTE: Necessary attributes are those that will be included in the EAA and possibly further attributes, e.g. unique identity, that are necessary to enable validation of the attributes that will be included in the EEA.

REQ-EAASP-4.2.2.1-06: The EAASP shall issue EAA securely to maintain their authenticity and integrity.

REQ-EAASP-4.2.2.1-07: The EAASP shall take measures against forgery of the EAA.

REQ-EAAS-4.2.2.1-08: The EAAS shall be able to authenticate itself towards the subject of the EAA and towards the means into which the EAA is issued.

REQ-EAASP-4.2.2.1.09: The EAASP shall issue an EAA in conformance with the EAASPol and EAAP they claim conformity against.

REQ-EAASP-4.2.2.1-10 [CONDITIONAL]: If the EAASP supports a status service, EAAS policy shall indicate in EAA revocation information which contains a URL indicating the location where a Relying Party can obtain a status list or revocation list, and an identifier or index for this specific certificate or attestation within that list.

EXAMPLE: e.g. short-term EAA does not require a status service to be supported.

4.2.2.2 Verification of attributes against authentic sources

REQ-QEAASP-4.2.2.2-01: The QEAASP shall verify the authenticity of the attributes requested by EAA Subject or EAA Subscriber for an identified EAA Subject against the relevant authentic source at national level or via designated intermediaries recognised at national level.

REQ-QEAASP-4.2.2.2-02: The verification shall be as required by the EEAP.

REQ-QEAASP-4.2.2.2-03: The verification should, if possible, be carried out electronically.

4.2.2.3 EUDIW specific

In addition, when the EAA is issued to a EUDIW the following requirements apply:

REQ-EAASP-4.2.2.3-01: Before the EAA is issued to a EUDIW, the EAASP shall verify and validate the PID/LPID received from the Wallet Unit.

REQ-EAASP-4.2.2.3-02: The EAASP shall authenticate to the EUDIW instance implementing mutual authentication mechanisms that use an access certificate issued by a qualified Certificate Authority.

REQ-EAASP-4.2.2.3-03: The EAASP shall validate the EUDIW instance, whether the EUDIW instance is revoked or suspended.

REQ-EAASP-4.2.2.3-04 [CONDITONAL]: When the EAA is issued to a EUDIW with wallet binding, the EAASP SHALL verify that:

- the WSCD described in the WUA received from the Wallet Unit has proven possession of the private key corresponding to the public key in the WUA; and
- the WSCD has proven possession of the attestation private key.

REQ-EAASP-4.2.2.3-05 [CONDITONAL]: When the EAA is issued with wallet binding that includes association between two or more public keys protected by the same WSCD, the EAASP should verify the said keys are associated.

REQ-EAASP-4.2.2.3-06 [CONDITIONAL]: When the EAAP specifies that wallet binding is required, the EAASP shall implement device binding, ensuring that the EAA is cryptographically bound to a WSCA used by the EUDI Wallet Unit.

REQ-EAASP-4.2.2.3-07: The EAASP shall:

- verify the authenticity of the Wallet Unit by validating the signature over the Wallet Unit Attestation (WUA);
- accept only the trust anchors in the Wallet Provider Trusted List(s) for the Wallet Solutions they support;
- verify that the EUDIW Provider is present in a Wallet Provider Trusted List;
- authenticate and validate the WUA using the trust anchor(s) registered for the Wallet Provider in the Wallet Provider Trusted List; and
- verify that the Wallet Unit's WUA is not revoked.

REQ-EAASP-4.2.2.3-08 [CONDITIONAL]: When using the OpenID4VCI protocol or equivalent issuance protocol for issuing EAAs to a EUDIW, the EAASP shall include its access certificate in its client metadata.

REQ-EAASP-4.2.2.3-09: The EAASP shall implement measures to mitigate the risk of user linkability, including support for limited-validity attestations or once-only attestations as determined by the EAASP policy.

REQ-EAASP-4.2.2.3-10: The EAASP shall support selective disclosure of attributes in issued EAAs, allowing users to share only specific attributes required by a Relying Party without revealing others.

REQ-EAASP-4.2.2.3-11: The EAASP shall support mechanisms to mitigate the risk of user linkability, including at least one of the following:

a) limited-time attestations that expire after a defined period;

b) once-only attestations that can only be presented once;

c) rotating-batch attestations that can be used in random order; or

d) Per-Relying Party attestations that are unique to specific Relying Parties.

REQ-EAASP-4.2.2.3-12 [CONDITIONAL]: When applicable, the EAASP shall implement mechanisms to bind EAAs to the Wallet Unit's device (device binding), ensuring that EAAs cannot be cloned or used from unauthorized devices.

REQ-EAASP-4.2.2.3-13: The EAASP shall support batch issuance when requested by the Wallet Unit, allowing multiple EAAs with the same content to be issued simultaneously for privacy-preserving presentations.

REQ-EAASP-4.2.2.3-14 [CONDITIONAL]: The EAASP shall ensure that the issued EAA is compatible with both proximity presentation flows (supervised and unsupervised) and remote presentation flows (same-device and cross-device).

REQ-EAASP-4.2.2.3-15: The EAASP may include in the EAA an embedded disclosure policy containing rules determining which types of Relying Party are allowed to receive specific attributes from the attestation.

REQ-EAASP-4.2.2.3-16: The EAASP shall implement mechanisms that allow the re-issuance of the EAA upon request from the Wallet Unit, in case of approaching expiration, attribute value changes, or to maintain privacy protections, consistent with the approach chosen to mitigate Relying Party linkability.

R**EQ-EAASP-4.2.2.3-17:** The EAASP shall ensure that each EAA contains unique, cryptographically independent elements to prevent tracking across multiple presentations.

REQ-EAASP-4.2.2.3-18: The EAASP shall ensure that the technical validity period of EAAs is determined considering both security requirements and privacy implications, particularly the risk of user tracking.

REQ-EAASP-4.2.2.3-19: The EAASP should encode and structure the data element identifier and the attribute value according to the schema specified in the relevant rulebook for the Attestation Type.

NOTE: PID Rulebook and the mDL Rulebook in Annex 3 of the EU Architectural Reference Framework [i.5]. ISO 23220-2 [i.2] specifies further requirements for attribute schemas which should be applied where no rulebook exists.

4.2.3 EAA Usage

4.2.3.1 General

REQ-EAASP-4.2.3.1-01: The EAASP shall include in its practice statement and terms and conditions at least the following EAA Subject's obligations:

a) an obligation to provide the EAASP with accurate and complete information in accordance with the requirements of the present document;

b) an obligation for EAA to be only used in accordance with any limitations notified to the EAA Subscriber and/or the EAA Subject;

c) prohibition of unauthorized use of the EAA.

REQ-EAASP-4.2.3.1-02 [CONDITIONAL]: When the EAA Subscriber acts on behalf of a natural or legal person, the EAASP shall ensure that the EAA Subject has sole control over it, unless national legislation or EAASPol states otherwise.

4.2.3.2 EUDIW Specific

In addition, when the EAA is issued to a EUDIW the following requirement applies:

REQ-EAASP-4.2.3.2-01: The EAASP shall ensure that issued EAAs can be presented in both proximity flows (supervised and unsupervised) and remote flows (same-device and cross-device), according to user needs and Relying Party requirements.

4.2.4 EAA Renewal

4.2.4.1 General

EAA renewal refers to the issuance of a new EAA to the EAA Subscriber without changing the EAA content, except for the validity period, and public key where present, public key where present, salts hashes, and the issuer signature or sealDone.

REQ-EAAS-4.2.4.1-01: Requests for renewal of an EAA issued to an EAA Subscriber shall follow the process set out in the EAAS practice statement.

REQ-EAASP-4.2.4.1-02: The EAASP shall check the validity of the EAA to be renewed and that the information used to verify the identity and attributes of the EAA Subject is still valid.

4.2.4.2 EUDIW Specific

In addition, when the EAA is issued to a EUDIW the following requirement applies:

REQ-EAASP-4.2.4.2-03 [CONDITIONAL]: The EAASP shall enable the initiation by a EUDIW Instance of a secured session for re-issuance of attestations issued to this wallet by this EAASP.

4.2.5 EAA Revocation

4.2.5.1 General

REQ-EAASP-4.2.5.1-01: The EAASP shall follow its policies and practices when revoking an EAA.

REQ-EAASP-4.2.5.1-02: The EAASP shall revoke EAA based on authorized and validated EAA revocation requests as soon as possible and with a delay of no more than 24 hours after the revocation request was received.

REQ-EAASP-4.2.5.1-03: Revocation process shall always be executed under EAASP's control.

REQ-EAASP-4.2.5.1-04: An EAASP issuing short-term EAA shall explicitly describe in the EAAS practice statement which EAA cannot be revoked through a revocation management service and which EAA cannot be revoked even by the EAASP on its own initiative.

REQ-EAASP-4.2.5.1-05: The EAASP shall revoke any non-expired EAA when:

a) in case of any errors, fraud, or at the request of the EAA Subscriber or EAA Subject; or

b) the EAA is no longer compliant with the EAAS practice statement, EAASPol or EAAP under which it has been issued; or

c) the EAASP is aware of changes which impact the validity of the EAA; or

d) the EAASP is aware of a security incident that affects the EAA.

REQ-EAASP-4.2.5.1-06: The EAASP shall inform the EAA Subscriber and the EAA Subject, when possible, of a revoked EAA, of the change of status of the EAA.

NOTE: It may not be possible to inform the EAA Subject for example, when it is an infant, or when is known to be deceased or otherwise not available to be contacted.

REQ-EAAS-4.2.5.1-07: Once an EAA is revoked it shall not be reinstated.

REQ-EAAS-4.2.5.1-08: When an EAA is revoked, the revocation shall apply from that time to all instances of the EAA, whether held by the user or previously provided to a relying party.

4.2.5.2 EUDIW Specific

In addition, when the EAA is issued to a EUDIW the following requirements apply:

REQ-EAASP-4.2.5.2-01: The EAASP shall implement at least one of the following revocation information mechanisms:

- a status list where each bit or group of bits denotes the current revocation status of one EAA, or
- a revocation list containing the identifiers of EAAs revoked by the EAASP

REQ-EAASP-4.2.5.2-02: The EAASP shall maintain and publish the necessary information for Relying Parties to verify the authenticity of issued EAAs, including trust anchors and trusted lists when applicable.

REQ-EAASP-4.2.5.2-03: The EAASP shall provide a mechanism allowing the Wallet Unit to check the revocation status of an EAA without the need to contact the EAASP directly at the time of presentation, in order to maintain user privacy.

REQ-EAASP-4.2.5.2-04 [CONDITIONAL]: If the Wallet Provider has suspended or revoked the Wallet Unit on which that EAA is residing, the EAASP issuing EAAs to EUDIW shall immediately revoke the respective EAAs.

REQ-EAASP-4.2.5.2-05: When the EAA is valid for longer than 24 hours, the EAASP shall include in the EAA.

- a URL indicating the location where a Relying Party can obtain status information, and
- an identifier or index for this specific EAA within that status system.

REQ-EAASP-4.2.5.2-06: For EAAs issued to a EUDIW with a validity period of less than 24 hours, the EAASP may omit revocation information if this is explicitly stated in the EAAS practice statement as per REQ-EAASP-4.2.5-05.

REQ-EAASP-4.2.5.2-07 [CONDITIONAL]: When multiple EAAs of the same type with the same content and validity are issued in a batch to a EUDIW, the EAASP shall ensure that revocation of one EAA from the batch results in the revocation of all EAAs in that batch.

4.3 EAA validation services

4.3.1 General

REQ-EAASP-4.3.1-01 [CONDITIONAL]: If the EAA-policy requires that the EAA supports a status service, the EAASP shall provide information and/or services for checking the validity status of the EAA.

In particular:

- **REQ-EAASP-4.3.1-02:** Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, EAAS or other factors which are not under the control of the EAASP, the EAASP shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the EAAS practice statement.

- **REQ-EAASP-4.3.1-03:** The EAASP shall ensure integrity and authenticity of the validity status information.

- **REQ-EAASP-4.3.1-04:** Revocation status information shall include information on the status of EAA at least until the EAA expires.

- **REQ-EAASP-4.3.1-05:** The EAASP shall make revocation status information publicly and internationally available.

REQ-QEAASP-4.3.1-06: The QEAASP shall have no information regarding the usage of the (Q)EAAs issued when a validity status check is performed.

4.3.2 EUDIW Specific

In addition, when the EAA is issued to a EUDIW the following requirements apply:

REQ-EAASP-4.3.2-01: The EAASP shall publish its trust anchors in a Trusted List that is accessible to Relying Parties to enable signature verification.

REQ-EAASP-4.3.2-02: The EAASP shall support validation of EAAs presented in both proximity flows (supervised and unsupervised) and remote flows (same-device and cross-device).

REQ-EAASP-4.3.2-03: The EAASP shall support at least one of the following attestation formats with their corresponding proof mechanisms:

- ISO/IEC 18013-5 [i.12] with its defined proof mechanisms

- SD-JWT VC (Selective Disclosure for JWT-based Verifiable Credentials) with its defined proof mechanisms

REQ-EAASP-4.3.2-04: The EAASP shall provide the necessary mechanisms to enable Relying Parties to verify device binding of the EAA to ensure it was not copied or replayed from another device.

REQ-EAASP-4.3.2-05: The EAASP shall support mechanisms that enable verification of combined presentations of attributes when multiple EAAs are presented together, including cryptographic verification that the EAAs belong to the same user.

REQ-EAASP-4.3.2-06: The EAASP shall provide validation mechanisms that can verify the WSCD signs them at the required Level of Assurance (LoA).

5 Risk Assessment

REQ-EAASP-5-01: All requirements from ETSI EN 319 401 [1], clause 5 shall apply.

6 General provision on policies and practices

6.1 EAAS practice statement

6.1.1 General

REQ-EAASP-6.1.1-01: All requirements from ETSI EN 319 401 [1], clause 6.1 shall apply.

In addition to that:

- **REQ-EAASP-6.1-02:** EAASP should document the revocation mechanism in the EAAS practice statement.

6.1.2 EUDIW specific

REQ-EAASP-6.1.2-01: The EAASP shall document in its EAAS practice statement how it addresses the risk of Attestation Provider linkability, including measures taken to prevent colluding with Relying Parties to track users.

6.2 Terms and conditions

REQ-EAASP-6.2-01: All requirements from ETSI EN 319 401 [1], clause 6.2 shall apply.

In addition the following particular requirements apply:

- **REQ-EAASP-6.2-02:** The terms and conditions shall include at minimum the elements from ETSI EN 319 401 [1], REQ-6.2-02 and the indication of what constitutes EAA service acceptance.
- **REQ-EAASP-6.2.4-03:** The EAASP shall record the agreement with the EAA Subscriber.
- **REQ-EAASP-6.2.4-04:** The agreement shall involve explicit acceptance of the terms and conditions by a wilful act which can be later supported by evidence.
- **REQ-EAASP-6.2.4-05:** The EAASP shall obtain prior consent from EAA Subscribers and EAA Subject, when possible, before informing clearly how their personal data will be used and stored.

NOTE: It may not be possible to inform to and obtain prior consent from the EAA Subject for example, when it is an object or an infant.

- **REQ-EAASP-6.2.4-06:** The records identified above shall be retained for the period of time as indicated to the EAA Subscriber as part of the terms and conditions.

6.3 Information security policy

REQ-EAASP-6.3-01: All requirements from ETSI EN 319 401 [1], clause 6.3 shall apply.

6.4 EAA policy

An EAAP is a defined set of rules that outlines the applicability of a specific electronic attestation of attributes to a particular community or class of applications. The EAA policy ensures that the attestation of attributes adheres to common requirements regarding security, integrity, and operational controls, providing a trusted framework for the use of attributes in digital environments.

An EAA policy specifies the conditions under which attributes may be attested electronically, ensuring its validity and trustworthiness for use in specific sectors or communities. It establishes the baseline rules that apply to the issuance and usage of attributes.

While EAASP define the mandatory requirements for operating trust services, EAA policies focus specifically on the rules governing the attestation of attributes. In some cases, EAA policies may be included within the broader terms and conditions of a trust service, especially for non-qualified EAA services.

EAA policy may apply to various use cases, setting clear guidelines for the community or application in question, ensuring compliance with the regulatory, operational, and security requirements relevant to each case.

EXAMPLE: Sectors like, banking, healthcare, or age verification, and varying levels, such as baseline EAA policy (Non-QEAAP) and Extended EAA policy (QEAAP). EAA policy may also include information about EAA elements as the following:

- Attribute schema defining the structure, logical organisation, type and namespace(s) of the EAA; and/or
- Additional information such as:
  - information EAA issuer,
  - EAA verification mechanisms,
  - underlying identity assurance,
  - Trust Framework to which the properties are related, and
  - Proof of possession, and/or
- Data formats (e.g. its character sets, encoding and serialisation), and/or
- Proof mechanisms defining the methods used to secure the EAA for integrity and authenticity, including selective disclosure.

7 EAASP management and operation

7.1 Internal organization

7.1.1 Organization reliability

REQ-EAASP-7.1.1-01: All requirements from ETSI EN 319 401 [1], clause 7.1.1 shall apply.

In addition the following particular requirements apply:

- **REQ-EAASP-7.1.1-02:** The parts of the EAASP concerned with EAA issuance and revocation management shall be independent for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable EAAS policies.
- **REQ-EAASP-7.1.1-03:** The senior executive, senior staff and staff in trusted roles, of the EAASP concerned with EAA issuance and revocation management shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.
- **REQ-EAASP-7.1.1-04:** The parts of the EAASP concerned with attestation of attributes issuance and revocation management shall have a documented structure which safeguards impartiality of operations.

7.1.2 Segregation of duties

REQ-EAASP-7.1.2-01: All requirements from ETSI EN 319 401 [1], clause 7.1.2 shall apply.

7.2 Human resources

REQ-EAASP-7.2-01: All requirements from ETSI EN 319 401 [1], clause 7.2 shall apply.

7.3 Asset management

REQ-EAASP-7.3-01: All requirements from ETSI EN 319 401 [1], clause 7.3 shall apply.

7.4 Access control

REQ-EAASP-7.4-01: All requirements from ETSI EN 319 401 [1], clause 7.4 shall apply.

In addition the following particular requirements apply:

- **REQ-EAASP-7.4-02:** The EAASP shall enforce multi-factor authentication for all accounts capable of directly causing EAA issuance.

- **REQ-EAASP-7.4-03:** Continuous monitoring and alarm facilities shall be provided to enable the EAASP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

- **REQ-EAASP-7.4-04:** The EAASP shall monitor and log all authentication attempts and failures in order to detect potential malicious activities.

7.5 Cryptographic controls

7.5.1 General

REQ-EAASP-7.5.1-01: All requirements from ETSI EN 319 401 [1], clause 7.5 shall apply.

7.5.2 Key pair generation and installation

REQ-EAASP-7.5.2-01 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall generate EAASP keys securely, including keys used by revocation and registration services, and shall keep the private key secret. In particular:

- **REQ-EAASP-7.5.2-02:** The EAASP shall undertake the EAASP key pair generation and the subsequent certification of the public key in a physically secured environment by personnel in trusted roles.

- **REQ-EAASP-7.5.2-03:** The EAASP shall create the EAA signing key pair under, at least, dual control.

- **REQ-EAASP-7.5.3-04:** The EAASP shall minimise the number of personnel authorized to carry out EAAS key pair generation, in line with the TSP's practices.

- **REQ-EAASP-7.5.2-05:** The EAASP shall use an algorithm specified in ETSI TS 119 312 [i.10] to perform EAAS key pair generation for the EAA signing purposes.

- **REQ-EAASP-7.5.2-06:** The EAASP shall select a key length and algorithm for the EAAS signing key that is specified in ETSI TS 119 312 [i.10] for EAA signing purposes.

REQ-EAASP-7.5.2-07 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall have a documented procedure for conducting EAAS key pair generation for EAA signing keys for all EAAS.

REQ-EAASP-7.5.2-08 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall produce a report demonstrating that the ceremony, following the procedure defined in **REQ-EAASP-7.5.2-07** above, followed the stated steps and ensured the integrity and confidentiality of the key pair.

REQ-EAASP-7.5.2-09 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall include at least the following information in the report for the key ceremony:

a) roles participating in the ceremony (internal and external from the organisation);

b) functions performed by every role and in which phases;

c) responsibilities during and after the ceremony;

d) evidence collected of the ceremony;

e) the date the ceremony was carried out;

f) an inventory of the keys generated, which includes, at least, the following information for each key:

- a unique identifier for the key;
- algorithm, key size and public key fingerprint (SHA256 minimum);
- the unique identifier and model of the secure cryptographic device (e.g. HSM) used for this generation ceremony; and
- the key generation algorithm and settings configured in the secure cryptographic device during the key ceremony, e.g. operation mode, used random number generator and other cryptographic parameters.

REQ-EAASP-7.5.2-10 [CONDITIONAL]: If the EAASP uses keys generated by another TSP, the EAASP shall ensure that the entire process of key generation and installation complies with the requirements specified in **REQ-EAASP-7.5.2-01** to **REQ-EAASP-7.5.2-09**, as applicable, and shall document this in a report demonstrating that integrity and confidentiality were ensured throughout the process.

7.5.3 EAAS key protection and cryptographic module engineering controls

REQ-EAASP-7.5.3-01 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall generate EAAS key pairs—including those used for revocation and registration services—within a secure cryptographic device that functions as a trustworthy system. In addition to that:

- **REQ-EAASP-7.5.3-02:** The EAASP shall ensure that this system either:

  a) holds an assurance level of EAL 4 or higher under ISO/IEC 15408-1 [i.6], or an equivalent national or internationally recognised IT security evaluation scheme, with a security target or protection profile that meets the requirements of the present document, based on a risk analysis and including physical and other non-technical security measures; or

  b) meets the criteria defined in ISO/IEC 19790 [i.7], FIPS PUB 140-2 [i.8] Level 3, or FIPS PUB 140-3 [i.9] Level 3.

REQ-EAASP-7.5.3-03 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall operate the secure cryptographic device in the configuration described in the relevant certification guidance documentation or in an equivalent configuration that achieves the same security objective.

REQ-EAASP-7.5.3-04 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall store and use the EAAS private signing key within a secure cryptographic device that complies with the requirements of **REQ-EAASP-7.5.3-01** and **REQ-EAASP-7.5.3-03**.

REQ-EAASP-7.5.3-05 [CONDITIONAL]: If EAAS keys are generated on the QSCD delivered by QTSP issuing Qualified Certificate, the EAASP shall verify that the QSCD meets the requirements of **REQ-EAASP-7.5.3-01, REQ-EAASP-7.5.3-02**, and **REQ-EAASP-7.5.3-03**.

REQ-EAASP-7.5.3-06 [CONDITIONAL]: When the EAAS private key is outside the secure cryptographic device, the EAASP shall protect it in a manner that ensures the same level of protection as provided by the secure cryptographic device.

REQ-EAASP-7.5.3-07 [CONDITIONAL]: If the EAASP backs up, stores, or recovers the EAAS private signing key, the EAASP shall ensure that personnel in trusted roles carry out the process using at least dual control in a physically secured environment.

REQ-EAASP-7.5.3-08 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall apply the same or a higher level of security controls to copies of the EAAS private signing keys as to the keys currently in use.

REQ-EAASP-7.5.3-09 [CONDITIONAL]: If the EAASP stores the EAAS private signing keys and any copies in a dedicated secure cryptographic device, the EAASP shall implement access controls to ensure the keys remain inaccessible outside the device.

REQ-EAASP-7.5.3-10 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall ensure that the secure cryptographic device remains protected against tampering during shipment and storage.

REQ-EAASP-7.5.3-11 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall destroy the EAAS private signing keys stored on the secure cryptographic device when retiring the device.

7.5.4 Other aspects of key pair management

REQ-EAASP-7.5.4-01 [CONDITIONAL]: If the EAASP generates keys for the digital signature of EAA, the EAASP shall use the EAAS private signing keys appropriately.

In particular:

- **REQ-EAASP-7.5.4-02:** The EAASP shall stop using the EAAS private signing keys at the end of their life cycle.
- **REQ-EAASP-7.5.4-03:** The EAASP shall use EAAS signing keys only for EAA issuance and issuing revocation status information, and for no other purpose.
- **REQ-EAASP-7.5.4-04:** The EAASP shall use the EAAS signing keys only within physically secure premises.

7.5.5 EUDIW specific

In addition, when the EAA is issued to a EUDIW the following requirements apply:

- **REQ-EAASP-7.5.5-01:** The EAASP shall implement device binding mechanisms that cryptographically bind the EAA to the Wallet Secure Cryptographic Device (WSCD) of the Wallet Unit, ensuring that the EAA cannot be copied or used from another device.
- **REQ-EAASP-7.5.5-02:** The EAASP shall verify that the public key included in the EAA is associated with a private key protected by the WSCD described in the Wallet Unit Attestation (WUA).
- **REQ-EAASP-7.5.5-03:** The EAASP shall implement cryptographic protocols that support selective disclosure of attributes, enabling users to present only specific attributes without revealing others.
- **REQ-EAASP-7.5.5-04:** The EAASP shall ensure that the cryptographic mechanisms used support the verification of combined presentation of attributes from multiple EAAs, including verification that they belong to the same user.
- **REQ-EAASP-7.5.5-05:** The EAASP shall implement cryptographic controls that mitigate the risk of Relying Party linkability and Attestation Provider linkability.

EXAMPLE: Using different key pairs for different EAAs issued to the same user.

- **REQ-EAASP-7.5.5-06:** The EAASP shall maintain controls that ensure its access certificate and associated private keys remain secure, including implementing proper key management procedures.
- **REQ-EAASP-7.5.5-07:** When supporting batch issuance, the EAASP shall support the use of cryptographically independent EAAs within a batch to enhance privacy protection.

7.6 Physical and environmental security

REQ-EAASP-7.6-01: All requirements from ETSI EN 319 401 [1], clause 7.6 shall apply.

7.7 Operation security

REQ-EAASP-7.7-01: All requirements from ETSI EN 319 401 [1], clause 7.7 shall apply.

In addition the following particular requirement applies:

- **REQ-EAASP-7.7-02:** EAASP shall monitor capacity demands and projections of future capacity requirements in order to ensure that adequate processing power and storage are available.

7.8 Network security

REQ-EAASP-7.8-01: All requirements from ETSI EN 319 401 [1], clause 7.8 shall apply.

In addition the following particular requirements apply:

- **REQ-EAASP-7.8-02:** The EAASP shall maintain and protect all systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and security perimeters.

- **REQ-EAASP-7.8-03:** The EAASP shall configure all systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the EAAS operations.

- **REQ-EAASP-7.8-04:** The EAASP shall use secure, encrypted channels for the transmission of attribute data to protect against unauthorized access and data breaches.

7.9 Vulnerabilities and Incident management

REQ-EAASP-7.9-01: All requirements from ETSI EN 319 401 [1], clause 7.9 shall apply.

7.10 Collection of evidence for EAASP internal services

REQ-EAASP-7.10-01: All requirements from ETSI EN 319 401 [1], clause 7.10 shall apply.

In addition, the following particular requirements apply:

- **REQ-EAASP-7.10-02:** Evidence of the EAA issuance process shall be collected and securely archived.

- **REQ-EAASP-7.10-03:** All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and system access attempts.

- **REQ-EAASP-7.10-04:** All events related to registration including requests for EAA renewal shall be logged.

- **REQ-EAASP-7.10-05:** The EAASP shall document how the information recorded is accessible.

- **REQ-EAASP-7.10-06:** The EAASP shall log all events relating to the EAA life-cycle.

- **REQ-EAASP-7.10-07:** The EAASP shall log all requests and reports relating to revocation, as well as the resulting action.

- **REQ-EAASP-7.10-08:** The EAASP shall precisely document the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan.

7.11 Business continuity management

7.11.1 General

REQ-EAASP-7.11.1-01: All requirements from ETSI EN 319 401 [1], clause 7.11 shall apply.

In addition the particular requirements from the following clauses 7.11.2 and 7.11.3 apply.

7.11.2 Back up

REQ-EAASP-7.11.2-01: EAASP's systems data necessary to resume operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the EAASP to timely go back to operations in case of incident/disasters.

REQ-EAASP-7.1.1.2-02: Back-up copies of essential information and software should be taken regularly.

REQ-EAASP-7.11.2-03: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

REQ-EAASP-7.11.2-04: Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

REQ-EAASP-7.11.2-05: Backup and restore functions shall be performed by the relevant trusted roles.

7.11.3 Crisis management

REQ-EAASP-7.11.3-01: Following a disaster, the EAASP shall, where practical, take steps to avoid repetition of a disaster.

REQ-EAASP-7.11.3-02: The EAASP shall inform to the following of the compromise: all EAA Subscribers and/or EAA Subjects, when possible, and other entities with which the EAASP has agreements or other form of established relations, among which relying parties and others TSPs.

REQ-EAASP-7.11.3-03: The EAASP shall revoke any EAA it has issued when the EAASP is informed of the compromise.

7.12 EAASP and EAAS termination and termination plans

REQ-EAASP-7.12-01: All requirements from ETSI EN 319 401 [1], clause 7.12 shall apply.

In addition the following particular requirement applies:

- **REQ-EAASP-7.12-02:** The EAASP shall retain the following records after any EAA based on these records ceases to be valid:

  a) log of all events relating to the EAA life cycle; and

  b) attributes attestations data issuance evidence.

REQ-EAASP-7.12-03: The retention period shall be defined by the EAASP in accordance with national legislation.

7.13 Compliance

REQ-EAASP-7.13-01: All requirements from ETSI EN 319 401 [1], clause 7.13 shall apply.

In addition the following particular requirements apply:

REQ-EAASP-7.13-02: The EAASP shall enable privacy-preserving techniques to maintain the privacy of EAA Subject and EAA Subscriber personal data. In addition:

- **REQ-EAASP-7.13-03:** The EAASP shall protect confidentiality and integrity of registration data, especially when exchanged with the EAA Subject or between distributed EAASP's system components.

- **REQ-EAASP-7.13-04:** The EAASP shall implement data minimization principles in the design of the EAA Policy, ensuring that only necessary attributes are included in each specific type of EAA.

- **REQ-EAASP-7.13-05:** The EAASP shall not track, link, correlate, or otherwise obtain knowledge of transactions or EAA Subject behaviour post-issuance of the EAA unless explicitly authorized by the EAA Subject.

- **REQ-EAASP-7.13-06:** The EAASP shall keep logically separate attributes and metadata related to EAA Subject and/or EAA Subscribers relating to the provision of EAAS from other data held.

- **REQ-EAASP-7.13-07:** The EAASP shall, outside of the issuing of EAA, not export personal data to other services, whether provided by the EAASP itself or by other actors, unless explicitly authorized by EAA Subject and/or EAA Subscriber.

- **REQ-EAASP-7.13-08:** The EAASP shall ensure that its systems are designed to log minimal information about EAA issuance and usage, sufficient for security and management purposes, to meet statutory requirements and to support auditability and transparency requirements, but not enabling tracking of user activities.

7.14 Supply chain

REQ-EAASP-7.14-01: All requirements from ETSI EN 319 401 [1], clause 7.14 shall apply.

History

Document history		
V1.1.1	May 2025	Publication