ETSI TR 119 479-1 V1.1.1 (2026-05)

TECHNICAL REPORT

Electronic Signatures and Trust Infrastructures (ESI); Technological Solutions for the EU Digital Identity Framework; Part 1: Foundational EAA Concepts and Architectural Models

Reference
DTR/ESI-0019479-1

Keywords
attribute attestation, digital identity, EAA, EUDI wallet, policies, 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 Report (TR) 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 Technological Solutions for the EU Digital Identity Framework, as identified below:

Part 1: "Foundational EAA Concepts and Architectural Models";

Part 2: "EAA Extended Validation Services Framework and Application";

Part 3: "Support for EAA within AdES signatures;

Part 4: "Hybrid EAA".

Modal verbs terminology

In the present document "**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

An Electronic Attestation of Attribute (EAA) is a digital statement that confirms specific information about a person or object, such as their age, qualification, or membership in an organization. In simple terms, it acts like a digital certificate or proof that can be securely shared online or in person to prove facts about the subject without having to show physical documents. For example, an EAA could confirm that the subject is over 18, holds a particular professional licence, or is a registered student at a university. These attestations are trusted because they are issued and validated by authorized service providers, making them reliable for use in various digital services and transactions.

eIDAS2 [i.1] introduced EAA issuance as a new trust service and mentions the inclusion of EAA in European Digital Identity Wallets (EUDIWs). However, it does not state that the EUDIW is the only way that EAA can be used. The eIDAS 2 Architectural Reference Framework (ARF) [i.4] only speaks about the use of EAA with the EUDIW, but that is because the ARF [i.4] is created only to elaborate the EUDIW concept. This is quite one sided and as a result it influences standardization to only treat EAA for use with EUDIWs, which threatens to lead to a lot of lost potential. The present document is intended to investigate the use of EAA within but also beyond the EUDIW to see how standards can be improved so that EAA can fulfil their potential better.

eDIAS2 [i.1] has the following provisions that relate to EAA:

- Article 3 (43, 44, 45, 46) - definitions of EAA
- Article 3 (47) - definition of authentic source
- Article 5a, 4 (a) - functionality of European Digital Identity Wallet to request, obtain, select, combine, store, delete, share and present EAA
- Article 24 - requirements for qualified trust service providers
- Article 45b - Legal effects of electronic attestation of attributes
- Article 45c - Electronic attestation of attributes in public services
- Article 45d - Requirements for qualified electronic attestation of attributes
- Article 45e - Verification of attributes against authentic sources
- Article 45f - Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source
- Article 45g - Issuing of electronic attestation of attributes to European Digital Identity Wallets
- Article 45h - Additional rules for the provision of electronic attestation of attributes services

Executive Summary

Electronic Attestations of Attributes (EAA) were introduced by the amended eIDAS-Regulation [i.1] to provide trustworthy, verifiable digital statements about natural persons, legal persons, or objects. The present document analyses the foundational concepts, actors, and architectural models required for the issuance, validation, dissemination, and lifecycle management of Electronic Attestations of Attributes (EAA) within and beyond the European Digital Identity Wallet ecosystem. It clarifies that EAAs may be delivered through multiple channels (including wallets, vaults, signature containers and direct file distribution) and are not limited to EUDIW use.

The present document defines the trust framework for EAAs, describing the roles of service providers, subscribers, attribute subjects, authentic and authoritative sources, relying parties, and intermediaries. It further outlines the core service components such as registration, identity proofing, attribute collection, issuance, dissemination, and status management.

A central part of the present document is the definition of EAA Policies, which specify attribute schemas, data formats, binding mechanisms, lifecycle rules, and verification requirements, ensuring consistent trust and interoperability.

The present document also identifies technical considerations including multi-subject attestations, wallet and certificate binding, support for hybrid formats, long-term preservation, and status verification. It concludes by outlining the implications for future ETSI standardization activities to enable reliable and interoperable use of EAAs across diverse public- and private-sector applications.

1 Scope

The present document aims to look at concepts and models around EAA that include but also go beyond the use of EAA with European Digital Identity Wallets, for instance EAA used as Digital Product Passport, Hybrid EAA or in the context of the European Business Wallet (EUBW). The concepts and models in the present document also take into account entities that are involved in the ecosystems like Relying Party Intermediaries and Vaults and the impact of those on the EAA ecosystem. It also considers the possibility for EAA to be distributed not via EUDIWs but issued to Vaults, issued to EUBWs or delivered as a file (to be downloaded or mailed).

The present document is conceptual and aims to support the further development of standards regarding EAA Services for the issuance, validation or preservation of qualified EAA, non-qualified EAA, and EAA issued by the public sector. If not specified, the service description, its components and the service requirements consider all types of EAAs.

In terms of operations, the development of the trust service is carried out based on the provisions of ETSI EN 319 401 [i.5], which defines the basic requirements for the operation of trust services. The issuance service for Electronic Attestation of Attributes is specified in ETSI TS 119 471 [i.6] Policy and Security requirements for Providers of Electronic Attestation of Attribute Services. The present document is intended to support further work on ETSI standardization in the context of EAA Service operations and policy requirements. It aims to support the European Digital Identity Wallet Architecture and Reference Framework [i.4] while considering a broader scope of provisioning EAA Services not only to the EU Digital Identity Wallet.

From a technological perspective, the present document remains at a high level and does not delve into the detailed requirements arising from technical standards that define data formats and protocols. The present document is intended to describe trust service components that can be used for any profile specified within the detailed ETSI TS 119 472-1 [i.7], ETSI TS 119 472-2 [i.8] standards. Additionally, the present document allows for meeting the requirements for creating a service that issues EAAs in accordance with the standards referenced by the eIDAS 2 [i.1] Commission Implementing Regulations.

Many standards and specifications regarding the functioning of attribute attestations draw their experience from the Self-Sovereign Identity (SSI) model, which allows for creating Verifiable Credentials like those specified in W3C VC DM [i.15], securing them in a wallet, and sharing them with verifying parties. The SSI model does not specify special conditions for attribute issuers, generally indicating that any entity with electronic attributes can issue Verifiable Credentials. The eIDAS regulation imposes legal requirements and restrictions on the functioning of trust service providers, which, according to the Regulation, includes the issuers of EAAs.

NOTE: The issuance of electronic attestations of attributes is included in the list of trust services in the definition in article 3 (16) of eIDAS2 [i.1], which means that it recognizes issuers of EAAs as TSP. This means that in the EU anyone creating a digital data that contains attributes for natural persons, legal persons or objects, and that allows to authenticate it, becomes a TSP. This also means that these parties will be subject to all requirements for TSPs (for which an Implementing Act will be issued, but that at least means that they become subject to NIS2).

Trust Service Providers need to provide **technical and organizational** guarantees that the service they provide is trustworthy. Therefore, the model presented by SSI without additional requirements on EAA issuers cannot be adopted. The process of issuing attributes is related to both the identification of actors, the operation of individual components of the EAA Service, and the maintenance of evidence from the conducted processes. In order to guarantee trustworthiness, all of these components need to be part of a trust framework. The present document is intended to clarify that trust framework.

The present document limits the scope to EAA as defined in the eIDAS2 regulation [i.1]. There are potentially other credentials that might use similar technologies for ensuring trust, but if those do not fit the eIDAS2 [i.2] definition of an EAA, they are out of scope of the present document. An example of such credentials are bearer tokens without a natural person, legal person or object as subject, such as concert tickets, vouchers, etc. that allow for an access or reduction to the bearer whoever it is. Since the eIDAS2 [i.3] definition says that the attributes of EAA are always related to a natural or legal person or of an object, such bearer credentials are out of scope of the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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) 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] 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.

[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] Architecture and Reference Framework (ARF).

NOTE: The ARF is a document that is undergoing frequent changes. As any references to the content of the ARF might have become outdated at the time of reading the present document.

[i.5] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.6] ETSI TS 119 471: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services".

[i.7] ETSI TS 119 472-1: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements".

[i.8] ETSI TS 119 472-2: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 2: Profiles for EAA/PID Presentations to Relying Party".

[i.9] ETSI TS 119 472-3: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 3: Profiles for issuance of EAA or PID".

[i.10] 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".

[i.11] ETSI TS 119 461: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.12] ETSI EN 319 132-1 (V1.3.1) (2024-07): "Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.13] ETSI EN 319 142-1 (V1.2.1) (2024-01): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.14] ETSI EN 319 162-1 (V1.1.1) (2016-04): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.15] W3C® Recommendation: "Verifiable Credentials Data Model".

[i.16] IETF RFC 5755: "An Internet Attribute Certificate Profile for Authorization".

[i.17] ISO 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 systems".

[i.18] Commission Implementing Regulation (EU) 2025/1566 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.

[i.19] ETSI TS 119 479-2: "Electronic Signatures and Trust Infrastructures (ESI); Technological Solutions for the EU Digital Identity Framework; Part 2: EAA Extended Validation Services Framework and Application".

[i.20] ETSI TS 119 411-8: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 8: Access Certificate Policy for EUDI Wallet Relying Parties".

[i.21] ETSI TS 119 475: "Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorization decisions".

[i.22] ETSI TS 119 482-3: "Electronic Signatures and Trust Infrastructures (ESI); Additional wallet interfaces; Part 3: Interfaces and formats for the catalogue of Attestation Rulebooks and attributes".

[i.23] 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".

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 [i.5] and the following apply:

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

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

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

attribute(s) subject: natural, 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 eIDAS2 definition [i.1].

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

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

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

authoritative evidence: evidence that is presented by the applicant or authoritative source, holds attribute(s), and is trusted for the binding of these attributes to the applicant

authoritative source: any source irrespective of its form that can be relied upon to provide data, information and/or evidence that can be used to prove identity; or provide attributes about a natural or legal person, according to a quality level that respond to the requirements of the use case

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

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

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

NOTE: As per ETSI EN 319 401 [i.5] definition.

electronic attestation of attributes recipient: any entity that receives the EAA after its issuance

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 [i.5] trust service policy definition note.

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: See clause 4.2.2 of ETSI EN 319 411-1 [i.23] for further explanation.

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

electronic attestation of attributes trust service provider: 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 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 eIDAS2 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 eIDAS2 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 eIDAS2 definition [i.1].

person identification data: set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person

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

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

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

qualified electronic attestation of attributes services provider: electronic attestation of attributes services provider who is granted the qualified status by an EU National Supervisory Authority

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

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [i.5] and the following apply:

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
EUDIW	European Union Digital Identity Wallet
OpenID4VCI	OpenID for Verifiable Credential Issuance
PID	Person Identification Data
QEAA	Qualified Electronic Attestation of Attributes
QEAAS	Qualified Electronic Attestation of Attributes Service
QEAASP	Qualified Electronic Attestation of Attributes Service Provider

4 Conceptual considerations

4.1 Source of attributes

The eIDAS Regulation does not mandate that every EAA be validated based on an authentic source, but it requires trust service providers to ensure its quality and correctness. Wherever attributes rely on authentic sources within the public sector, attribute attestations issued have to be validated against those authentic sources. Annex 6 of the Regulation also specifies the minimal set of attributes that Member States should allow qualified EAA Service Providers to verify from against the authentic sources.

A good practice for every issued EAA is to indicate the authentic sources or authoritative sources based on which the attribute was verified and is compliant with the adopted TSP policy and EAA Policy.

For this study, it is assumed that the source of attributes can be the following sources:

a) Authentic source

1) Public (e.g. Civil registry, TAX registry)

2) Private (e.g. Bank's customer database, Employment register)

b) Authoritative source

1) Physical ID documents

2) Paper documents

3) Electronic documents (e.g. sealed documents)

4) Evidence obtained via a process

4.2 EAA distribution

The eIDAS Regulation does not require that EAAs be issued only to the EUDIW. The purpose of the Regulation is to enable the issuance of digital attestations that can replace physical documents. To this end, the Regulation introduces legal presumptions related to QEAA, which should be treated as the equivalent of a physical document. Therefore, it should be assumed that EAAs can be issued to:

- a EUDIW;
- another type of Wallet;
- a EUBW;
- an application that will include it in a signature;
- to a file (that can be downloaded from the website of the EAASP or e-mailed, …);
- in the form of data transmitted to an authorized party;
- …

In some cases it might even not make sense to issue an EAA to a EUDIW. This will for instance be the case for a lot of EAA with objects as attribute subjects. An EAA could even be issued to several distribution channels.

4.3 Multiple subjects

Several attestation formats, a.o. the W3C Verifiable Credentials Data Model [i.15] and ISO 23220-2 [i.17] allow for multiple attribute subjects in one attestation. The eIDAS2 regulation does not specify if attribute attestation can contain multiple subjects with each their own assigned attributes or not. The flexibility found in the mentioned standards allows a single attestation to present a relationship between two or more attribute subjects. For some use cases this is exactly what is required and attestation formats that do not allow multiple attribute subjects pose limitations for such use cases.

The present document specifies that EAAs issued by the EAA Service may have more than one attribute subject, and multiple attributes can be assigned to each attribute subject. In the present document, it is assumed that the number of Subjects is specific to the type of EAA.

EXAMPLE: An attribute attestation for a power of attorney includes both the attributes and rights of the attorney and the characteristics and information about the principal. The issued attribute attestation should specify both. It is important to note that if an EAA with a power of attorney is issued to the attorney's wallet, the attribute provider should perform the wallet binding as described below.

4.4 Binding

4.4.1 Identity Binding

Paper documents bind attributes to the subject based on identity identifiers of the Attribute Subject. Often this includes the names, birthdate and / or birth place of the Attribute Subject (if a natural person) and in other cases this might also be done via a national citizen identification number or other recognized number that can be used as an identifier (e.g. the LEI or VAT number to identify a company or the Vehicle Identification Number (VIN) to identify a car). It is also perfectly possible to do this in EAAs and allows to match the attributes with the Attribute Subject, when the Relying Party already has knowledge of the same identifiers via another source (e.g. from an internal DB or from the session authentication from the PID). This form of binding does not allow to proof the attribute fully anonymously, so for use cases where anonymity and privacy are important, this form of binding is not ideal. However, there are plenty of use cases (e.g. an EAA with an ISO 27k certificate for a company) where anonymity and privacy are not required or even not wanted. In those use cases, Identity Binding is the best option.

4.4.2 Wallet Binding

If an attribute is issued to a wallet, one of the potential purposes of storing the attribute in the wallet is to enable the wallet holder to confirm that the attribute belongs to them. When EAA has multiple attribute subjects, then the binding should specify what subject is concerned to mitigate the risk that one attribute subject could claim the attributes of another subject. That means that the structure of the EAA should allow to link the attestation key to the specific subject or even to specific attributes. Linking the wallet to the Subject is achieved through Wallet binding. This process involves verifying the identity of the wallet holder by the EAA Service and including information regarding a wallet public attestation key or its identifier in the EAA when an EAA is to be linked to the wallet owner. Performing Wallet binding later allows the wallet owner to prove in the EAA presentation process that the specified attributes are assigned to them. Wallet binding confirms that the EAA Subject is the owner of the wallet.

NOTE 1: Wallet binding only makes sense where the EUDIW holder is also the subject of the attestation. Wallet holders might also want to store attestation in their EUDIW in which they are not the subject. For instance, a (Q)EAA that replaces the car registration, should be possible to be transferred to the EUDIW of any driver, independent whether that driver is the owner of the car or not, so that the driver can present the car registration EAA to a police officer in case of a police check. Certainly if the driver is only using the car once, it makes no sense to request a new car registration EAA that is bound to the wallet of that one time driver.

NOTE 2: Even if the subject is the wallet holder, it can also be possible to authenticate the subject of an attestation with other means than a wallet binding (e.g. the EAA might contain a social security number of the subject that the subject can proof via another wallet bound attestation). In some cases (for instance when the EAA should also be able to be used outside of a EUDIW), this might be a good approach even if this discloses the social security number to the relying party.

4.4.3 Certificate binding

Attributes can be important for the trust in a signature. EAA can be used to link attributes to the identity of the signer. This requires to be able to link the EAA to a sign/seal to allow to prove that the attribute stored in the signed document belongs to the signer. Linking the signer certificate to the attribute subject can be achieved through certificate binding. This process involves the verification of the identity of the sign/seal certificate subject by the EAA Service and including information regarding the sign/seal certificate in the EAA. Performing sign/seal certificate binding allows the certificate subject to prove that the specified attributes are applicable to him.

NOTE 1: Certificate binding only makes sense where the certificate holder is also the subject of the attestation. If the EAA bound to a certificate contains multiple subjects the EAA needs to identify what attributes of what subject are linked to what certificate.

NOTE 2: Based on IETF RFC 5755 [i.16], it was previously possible to issue attribute attestations for signing certificates. This is also supported by the signature container standards (CADES [i.15], XADES [i.12], PADES [i.13], ASIC [i.14]). At least one TSP has been offering this service since 2018.

NOTE 3: Certificate binding is not necessarily limited to Attribute Certificates. Other EAA formats could be used for this purpose as well, but this would require additional standardization efforts.

4.5 EAA Policy and EAA Service Policy

Trusted service providers deliver services based on an adopted and published Trust Service Policy that defines the scope of services provided, specific requirements, and the safeguards in place to meet the legal and standardization requirements of the service provided. For the purpose of issuing EAA, establishing requirements in the trust service policy may be insufficient; therefore, in the present document, optional model for establishing the EAA Policy is introduced.

The model presented in the present document assumes that an EAA Policy will define the specific requirements for issuing a specific attestation type (e.g. diploma, mobile drivers licence, …). The law, particular sectors, standards or the EAA Service Provider itself can establish such policies. A detailed description of EAA Policies is included in clause 5.4.3.

EAA Policies need to contain all information that is required to allow any party involved with the EAA (see clause 5.2) to assess whether the EAA type will respond to their legal, compliance and business needs.

EXAMPLE: Let us take the example of an EAA that says that a certain person is a candidate-notary. The relying party needs to know how it has been created to know if it responds their needs. If it was created based on the authentic source of the Belgian Royal Federation of Notaries, then it will probably fit their needs. If it was created by a single Notary Office (the employer of the candidate-notary), the RP might or might not want to trust the EAA, depending in what they need the EAA for and whether they trust the given Notary Office. If the Subject was identified at Assurance Level (AL) High when the EAA was created they might trust it. If the identification was only at AL Low, they might not.

EAA Service Policies need to contain all information that is required to allow any party involved with the EAA (see clause 5.2) to assess whether the Service is operated in a manner that they can trust.

Both EAA Policies and EAA Service Policies are required to be able to execute a conformity assessment that covers the verification that the EAAs issued fulfil the requirements from the actors involved.

4.6 Vaults

In some countries there are service providers or governments that are offering users a "digital vault" or "digital safe" to receive and store important documents. For instance in Belgium the federation of notaries is offering a platform for storing a.o. deeds and documents related to wills and testaments, A private company is offering a platform that allows companies to deliver documents to their customers (like invoices, salary slips, etc.) and the Belgian federal government offers a Vault where citizens can receive and store documents issued by the government to them (like pension statement, tax documents, fines, etc.). Such Vaults can be seen as tools that offer a subset of the functionality of wallets, limited to receiving, storing and presenting digital data, but that do not have an authentication capability towards relying parties (they only allow users to authenticate to the Vault itself with userid / PW or with existing strong authentication mechanisms from other solutions). Currently these Vaults are mainly focussed on unstructured documents like PDFs, but several of them are looking into adopting EAA as well.

Probably natural persons will be able to chose to have certain EAA delivered to and accessible from their vault on top of the documents that will remain in unstructured format coming from the same sources. In that case the Vault Holder will also be the EAA recipient.

In the example of the notary platform, the kind of data that is present in the Vault is typically data that needs to remain available and trustworthy for the long to very long term (several decades). If some of these documents will be transformed into EAA, these EAA will need to be verifiable after all that time. This means that (unlike a wallet that stores EAA only for current use) Vaults might need to also provide for EAA preservation.

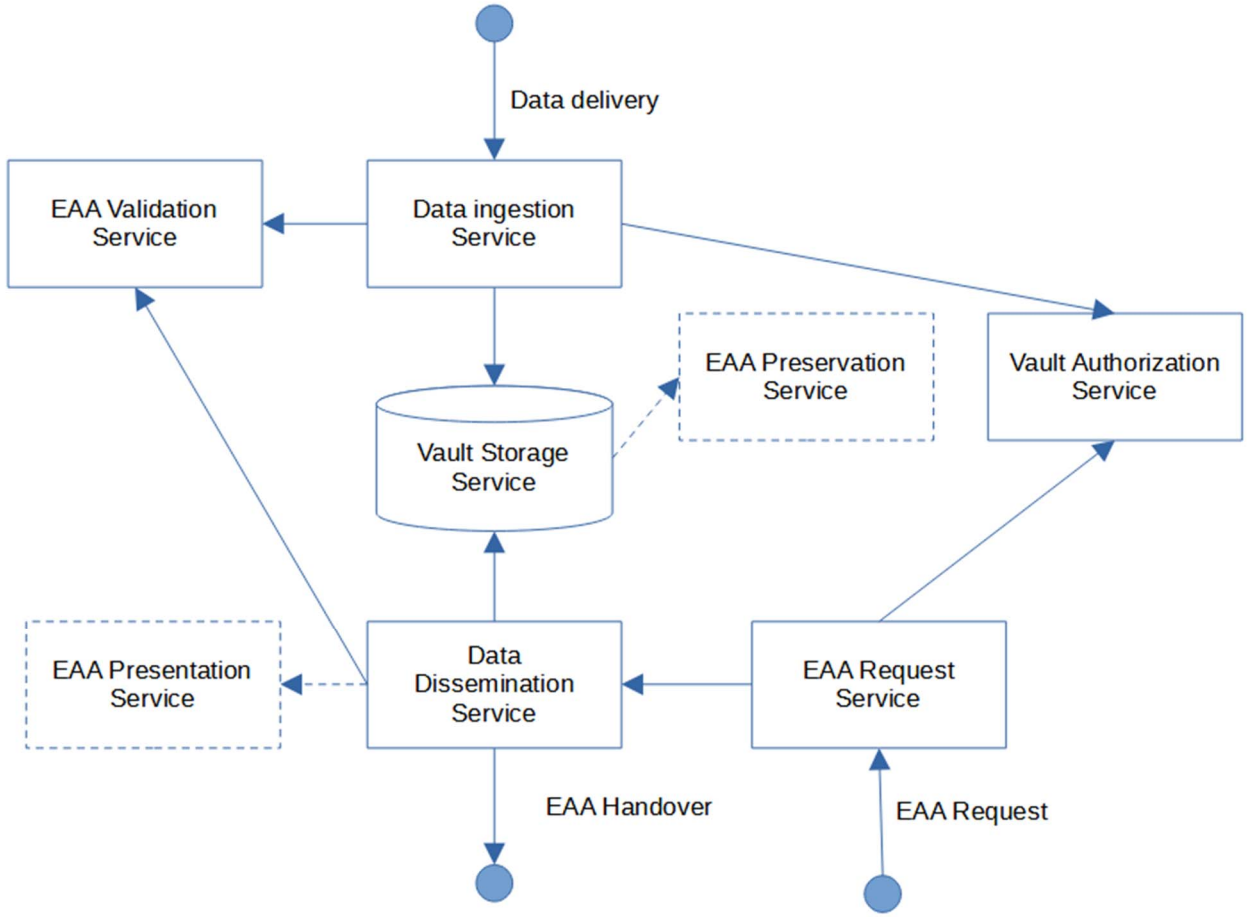

Figure 1: Vault EAA components

4.7 Hybrid EAA

In some use cases it will not always be possible to count on the presence of software that can visualize structured formats for EAA. There will be a number of cases where no EUDIW is involved and EAA are sent via email for instance. In that case a W3C VC or other structured format might be unusable. Also when dealing with entities outside of the EU that have not adopted eIDAS EAA, there will be a need to be able to communicate attributes while the recipient does not possess tools to visualize EAA in structured data format. To avoid staying stuck with paper processes in those use cases, one can use signed or sealed PDFs. Since those also allow to authenticate the attributes, they still respect the legal requirements for EAA, simply unstructured EAA. The reason however that structured EAA are preferred is that it allows for automating processes. To keep the benefits of the structured EAA but also allow parties without specialized tools to be able to trust the attributes, the hybrid EAA format was proposed: When a hybrid EAA is issued, both an unstructured PDF document containing the attributes and a structured EAA containing exactly the same attributes are created, the structured EAA is attached within the PDF document and both are sealed in a way that binds them together. This allows human readability with a simple PDF viewer capable to validate the signature or seal and allows entities that want to use the EAA in automated processes to parse the structured EAA and use the attributes from the structured EAA.

At this moment it is not yet foreseen that the EUDIW will support hybrid EAA. It is probable that Hybrid EAA will have a lot of relevance for the European Business Wallet. There will be no obligation to support structured EAA. Entities that want to benefit from structured EAA (typically bigger organizations that are early adopters), but that deal with parties that are less likely to support them (small organizations or organizations that are slow to adopt novelties), will benefit from the hybrid approach. It might be impossible to introduce EAA for a lot of use cases otherwise.

5 EAA trust service overview

5.1 Attestations in eIDAS

Article 3 point 16(g) of eIDAS2 specifies the issuance of electronic attestations of attributes as a trust service. Based on ARF [i.4], within the European Digital Identity Wallet ecosystem, the Regulation distinguishes four legal categories of attestations, which are defined as follows:

- **Person Identification Data (PID):** A set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.
- **Qualified Electronic Attestation of Attributes (QEAA):** An electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V of the Regulation.
- **Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA):** An 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 the Regulation.
- **Non-Qualified EAA:** An EAA which is not QEAA or PuB-EAA.

These types of attestation differ only in legal terms and do not necessarily differ from a technical perspective. For example, a diploma may be a QEAA or a non-qualified EAA. Similarly, an mDL (mobile Driving Licence) may be issued as a PuB-EAA, a QEAA, or a non-qualified EAA, using the exact same technology, but according to different policies for the issuance of the EAA.

5.2 EAA Service actors

5.2.1 Overview

Figure 2 presents actors of the processes and services described by the present document.

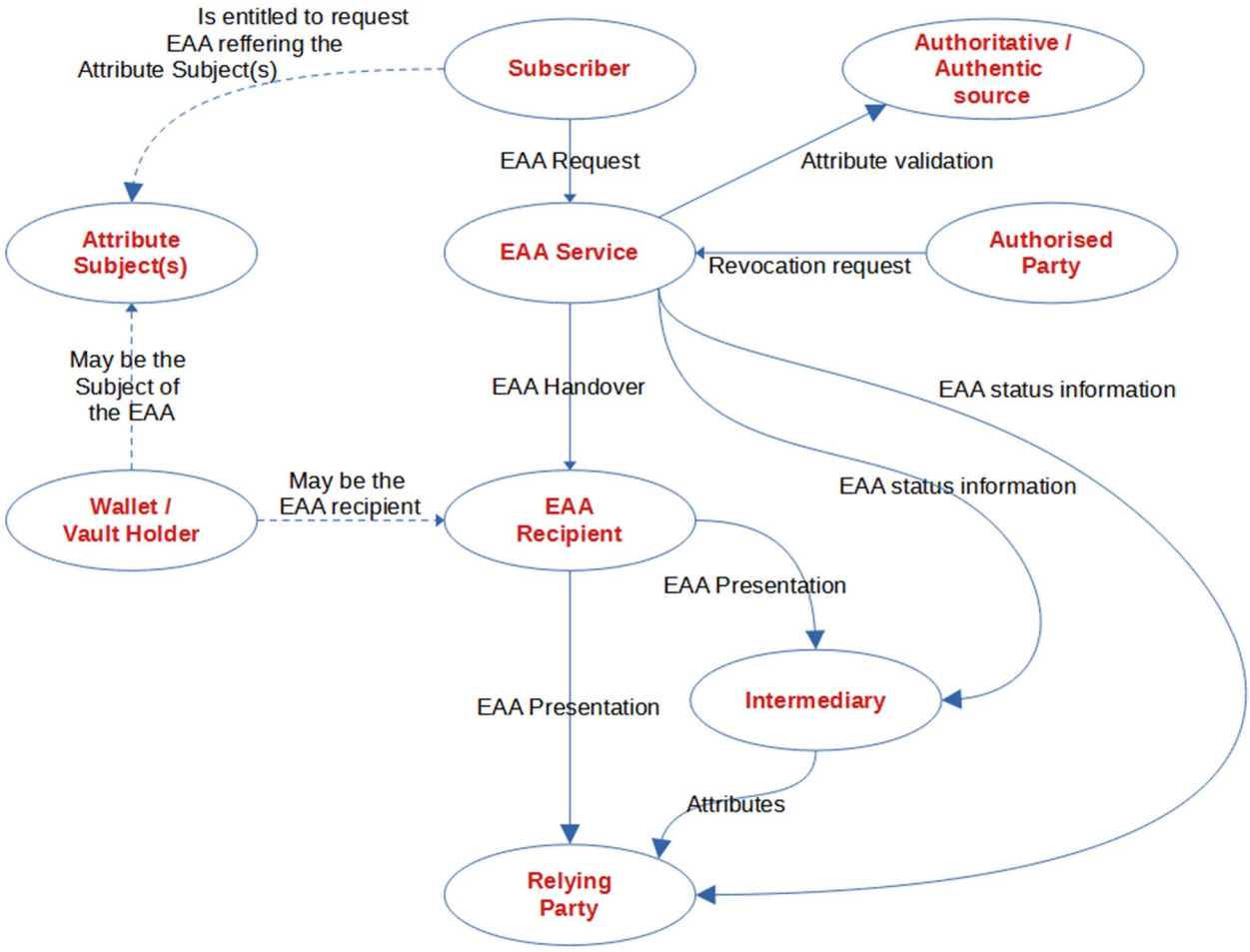

Figure 2: EAA Service actors

5.2.2 EAA Service Provider

A trusted entity that issues and validates electronic attestations of attributes. The EAA service provider acts as a reliable and trusted third-party authority that confirms for the accuracy and validity of the information provided by an authoritative source. The EAASP vouches that it has followed the criteria as set in the EAA Policy and EAA (Schema), but it cannot guarantee more. If for instance the authoritative source contains errors (which unfortunately is often the case, even in authentic sources), the EAASP will probably not even have the possibility to detect this and will most likely not have the ability to correct that. As long as it has followed the agreed upon policy it still did a correct job.

An EAA Service may be composed from other services like i.e. external identity proofing service or attribute registration service.

There is always an EAA Service Provider, but this role can be combined with other roles, e.g. the Authoritative source could issue themselves the EAA and thus also be the EAA Service Provider.

NOTE: Sometimes, the EAASP will serve as a "factory" for another entity. The user requests the EAA from that entity, which then instructs the EAASP to issue it. The EAASP's role is mainly to ensure compliance. For qualified EAAs the EAASP is responsible to pass a positive conformity assessment. Even if another entity handles some conformance tasks and interacts with EUDIWs, users, or other parties, the EAASP retains ultimate responsibility for meeting all conformance requirements.

5.2.3 Subscriber

A Subscriber is a natural or legal person, or a natural person representing a natural or legal person, entering in a legal relationship with the EAASP for the issuance of EAA. If there is payment involved for the issuance of the EAA, then it is the Subscriber that will perform this payment. The Subscriber can be the entity that requests the issuance of an electronic attestation of attributes or can be a source of attributes of a natural or legal person.

EXAMPLE 1: An employer might have EAA issued with the role of the employee. In that case the employer is the entity that has contracted the EAASP for the issuance of the EAA and it is the Subscriber. The request for the issuance of the EAA could be made by the employer that then delivers the EAA to the employee, or it could be made by the employee.

A Subscriber is authorized to possess the attribute data or to transfer them to the TSP for the issuance of an attestation. These authorizations may include, but are not limited to:

- The data pertains to him personally (i.e. the Subscriber is an Attribute Subject)
- There is a connection to the Subject

EXAMPLE 2: A parent that requests an EAA for a minor child.

- The Subscriber is the owner of the data and, in particular, may be the source of the data

EXAMPLE 3: A federation of notaries requesting an EAA to attest that the subject is indeed a notary.

NOTE: Although the Subscriber requests the EAA, it will not necessarily receive the EAA. For instance, the parent will probably receive the EAA about his child, but the EAA of the notary might be provided directly to the notary.

5.2.4 Attribute subject(s)

Entity to which the attested attributes are referring to. The subject can be the same entity as the Subscriber or:

- another natural person;
- another legal person;
- another natural person representing a natural or legal person; or
- an object.

Although the EAA might be issued to the Attribute Subject it can also be issued to another entity. This means that the EAA Recipient might be an Attribute Subject, but it might also not be. Typically, when the Attribute Subject is an object the EAA Recipient will not be the Attribute Subject. When an EAA is issued to a EUDIW, most often the EAA Recipient that is then the Wallet Holder will also be the Attribute Subject.

NOTE: The model described in the present document assumes that the attestation of an attribute can include more than one Attribute Subject. However, when issuing an EAA with multiple Attribute Subjects that includes wallet binding, it is important that the binding will identify the Attribute Subject that is the Wallet Holder to avoid identity theft.

EXAMPLE: An EAA that lists family composition can have multiple Attribute Subjects. Each family member is an Attribute Subject. However, if wallet binding is applied, in order for a family member to be able to pass for another member of the family, either the identity should be verified separately (e.g. from the EUDIW PID) and matched with the Attribute Subject in the family composition EAA (no use of wallet binding), or the wallet binding should identify which of the family members mentioned in the EAA is the Wallet Holder.

5.2.5 Source

5.2.5.1 Authentic source

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

NOTE 1: In some cases authentic sources can provide identity data (schema specific/sector specific) which EAA Services can rely on. If data comes from a public registry, EAA Services might rely on them without additional proofing of subject identity.

NOTE 2: Data incorporated in an authentic source can have joint ownership as well (for example address data for citizens is in some cases jointly owned by a ministry + a local government entity at the same time).

EXAMPLE: A lot of authentic sources can be found in government and the most well know are population registers and driver's license registers. But an employee register from the HR department of a company is also an authentic source. And for a person's favourite colour that person is the primary source of information, so that person is the authentic source himself.

Sometimes the authentic source has incentives in giving wrong data (e.g. green washing). In order to prevent that the EAASP will create attestations with wrong data, the EAASP (as the party that needs to offer trust guarantees about the attributes in the EAA) should take measures to prevent this. These measures should minimally cover liability clauses in a contract with the authentic source but could include audit obligations, penalties, etc. The extend to which measures need to be taken depends on the use case (could the authentic source benefit from wrong data, reputation, etc.).

5.2.5.2 Authoritative source

Any source irrespective of its form that can be relied upon to provide data, information and/or evidence that can be used to prove identity; or provide attributes about a natural or legal person, according to a quality level that responds to the requirements of the use case. Not all use cases for EAA will require the highest level of quality for attributes. In some cases a lower level of quality might still be "good enough". It will be in the EAA Policy that the acceptable level will be defined. Most probably the authoritative sources that are acceptable for the issuance of the EAA type will be listed in the EAA Policy.

NOTE: The level of trust of an authoritative source can be the same as that of an authentic source if the authoritative source has a process to guarantee that the data is exactly the same as from the authentic source (e.g. and eID card that is created with information that comes directly from the national register with ID data).

An authentic source can always be relied upon, meaning that the authentic source for attributes is always as well an authoritative source. Further in the present document the term authentic sources will only be used where the meaning needs to be limited to authentic sources and other authoritative sources do not apply.

EXAMPLE: An identity card that contains an exact copy of the data that is present in the population register can be considered an authoritative source. The HR database of a company might be an authoritative source on bank accounts of their employees (it needs a correct bank account to transfer the salary towards).

The concept of an authoritative source is not included in eIDAS 2 [i.1] or the ARF [i.4], but builds on the definition from ETSI TS 119 461 [i.11] which is referenced in CIR 2025/1566 [i.18].

Sometimes the authoritative source has incentives in giving wrong data (e.g. green washing). In order to prevent that the EAASP will create attestations with wrong data, the EAASP (as the party that needs to offer trust guarantees about the attributes in the EAA) should take measures to prevent this. These measures should minimally cover liability clauses in a contract with the authoritative source but could include audit obligations, penalties, etc. The extend to which measures need to be taken depends on the use case (could the authoritative source benefit form wrong data, reputation, etc.).

5.2.6 Wallet Holder

A Wallet Holder refers to a user of a wallet that can identify and authenticate the user and that can store EAA. Most often, the wallets referred to in the context of the ETSI standards will be EUDI Wallets. However, other wallets could deliver the same functionalities.

Specifically, Wallet Holders can:

- Receive: Obtain and store various digital credentials and identification documents in their wallet;
- Store: Securely hold these credentials within the wallet for future use;
- Present: Provide or display these credentials when needed, for example, to prove their identity;
- Authenticate themselves;
- Optionally: sign data.

A Wallet can also offer the functionality of Wallet Binding that allows the Wallet Holder to proof that an attribute is valid for him without disclosing any other information. However, not all types of wallet have this functionality (the EUDIW does). And for some EAA or use cases this is not possible (e.g. when the Wallet Holder is not the Attribute Subject of the EAA). In those cases Identity Binding is commonly used.

NOTE 1: EAA can be issued to the wallet and potentially be bound to the specific Wallet holder (when it is also an Attribute Subject of the attestation) or issued outside of the wallet.

NOTE 2: The ARF [i.4] uses the term User of Wallet Unit. Since the concept of a Wallet Unit is specific to the ARF and the EUDIW, and the present document wants to be open for other types of wallets, that term was not used in the present document. A User of a Wallet Unit is one type of Wallet Holder.

5.2.7 Vault Holder

A Vault Holder refers to a user of a Vault to store EAA and other data.

Specifically, Vault Holders can:

- Receive: Obtain and store various digital credentials and unstructured documents in their Vault.
- Store: Securely hold these credentials and documents within the Vault for future use, even long term.
- Present: Provide or display these credentials or other documents when needed, for example, to prove a status (student status) or characteristic (earning more than x amount per month).

NOTE: Since a Vault is not capable of authenticating the user towards third parties and does not have a mechanism to securely manage keys on behalf of the user, no key binding of the EAA is possible. This means that EAA issued to a Vault always need to contain an identification of the Attribute Subject. This can for instance be the combination of [Last Name + First Name(s) + birth date] or a national number or any other identifier that can match the attributes to a key that is known to the Relying Parties that allows the Relying Parties to match the Attributes with the Attribute Subject.

5.2.8 EAA Recipient

Any entity that receives EAA after its issuance by the EAASP. The reception of an EAA can be via different means:

- Via a EUDIW
- Via another type of wallet
- Download directly from a webpage of the EAASP
- Via any other secure means

Since there is not always necessarily a wallet involved, the entity that receives the EAA after issuance is not always a Wallet Holder. Only when the EAA is issued to a wallet, then the EAA Recipient is also the Wallet Holder.

NOTE 1: In some use cases, EAA can be very useful, but the use of a wallet is not. Typically EAA that are related to objects or in cases where one person needs to treat EAA of a lot of others.

EXAMPLE 1: The attestations related to a car (car registration, insurance, certificate of conformity) are not related to one Wallet Holder. Any driver of the car should be able to present them. Since most cars today have computers with GUI build in, one could easily imagine that these EAA would be stored in the car itself instead of in the wallet of the driver.

EXAMPLE 2: The leaders of a youth camp need to have information about medical conditions of the children participating to the youth camp. They need to be able to present this medical information in case one of the children needs medical care. It does not make sense that every leader of the camp will store all of the EAA of all the children in their personal wallet.

EXAMPLE 3: When goods are produced for which certain characteristics need to be tracked (e.g. for regulatory reasons), it would make sense to create EAA for these objects. However, as long as there is no final owner of the object yet (object is still in a production or distribution facility), it makes no sense to store the EAA in the wallet of a natural person.

The EAA recipient may have other roles in the EAA ecosystem on top of EAA recipient.

In particular, it can be a:

- Attribute Subject
- Wallet Holder
- Subscriber
- Relying Party
- Another recipient authorized to receive EAA

NOTE 2: In the case of Sign / Seal certificate binding, the EAA recipient is the signer and thus also the Sign / Seal certificate Holder.

5.2.9 Authorized Party

Any entity authorized to submit EAA revocation requests. The Subject, Subscriber and the source (Authentic or Authoritative, depending on the attestation type) are always Authorized Parties. Depending on the attestation type, other parties could also be Authorized Parties. That should be clarified in the EAA Policy.

5.2.10 RP Intermediary

A party that provides a service to Relying Parties related to the handling of the interaction with wallets (a.o. EUDIWs) or other solutions for identification, authentication or attribute attestation of persons.

NOTE: This role is mentioned in the eIDAS 2 regulation [i.4] in Article 5b 10. It has been further described in the ARF [i.4]. At the time of writing the present document this could be found in section 3.11 Relying Parties and intermediaries.

Although RP intermediaries (Relying Party Intermediaries) are not required for the ecosystem to be functional, they are important for the speed of the adoption of the EUDIW and EAA. The EUDIW and EAA are new concepts with a lot of complexity. There is already a lack of cybersecurity specialists and a lot of organizations do not have the means to hire one of them. As a result, those organizations will have a hard time to adopt these new technologies unless they can outsource this task to specialized companies that take the complexity of such adoption out of their hands. That is what RP intermediaries do. Currently there are already a lot of organizations that use eIDAS electronic identification means via an RP intermediary (in the market these RP intermediaries are often called identity brokers). If those RP intermediaries can add the EUDIW then organizations already using the services of RP intermediaries will be able to reap the benefits with minimal friction.

RP intermediaries will have the following positive effects on the EAA ecosystem:

- Inclusion: Mainly the SMEs that do not have a lot of IT specialists, let alone identity specialists, will not be able to use the EUDIW and EAA without help. If they cannot outsource to an RP intermediary, they risk not to have access to the benefits of EUDIWs and EAA. Therefore, the presence of an RP intermediary will lead to a much higher level of inclusiveness for relying parties with lower IT savviness. The lack of RP intermediaries would increase the digital divide between companies with lots of IT capacities and companies will little IT capacities.

- Speed of adoption: The lack of specialists will lead to a waiting line for help with the implementation of the EUDIW and EAA for organizations that do not have in house specialists. This will slow down adoption for the whole EUDIW ecosystem, including adoption by wallet users as they will have less incentive to start using EUDIWs (chicken and egg problem). All the organizations that are already integrated with an RP intermediary will be able to start using them from the moment the RP intermediary has added them to the eIM portfolio.

- Cost: If every organization needs to build their own interfaces and configurations for the 27+ EUDIWs, that will require a lot of effort, which means a high cost. If they can use the EUDIW via their RP intermediary, they can save those costs and use the budget for something more useful.

- Security and privacy: Seen the lack of identity specialists, companies (certainly those legally obliged to adopt the EUDIW by a certain deadline), might be required to have the implementation executed by people that do not have the best knowledge and skills. This could lead to security and privacy issues. RP intermediaries will have the specialists, which means that companies that use such RP intermediaries will be able to use proven procedures that will follow the highest security and privacy standards and will get expert advice.

RP intermediaries will treat a high amount of privacy sensitive information. According to eIDAS 2 [i.5] they are not allowed to store that data, however, if uncontrolled, there could be actors that do not use state of the art solutions. Poor implementations might become a risk to the trust in the EUDIW / EAA ecosystem. That is why Security and Policy Requirements for these RP intermediaries are needed. Ideally all RP intermediaries would be subject to a conformity assessment, so that as well the Relying Parties that use RP intermediary services as the Attribute Subjects and Wallet Holders can be ensured that the data and services are treated in a decent way.

Where the RP intermediary also validates the PID and EAA for the RP, the PID or EAA presentation does not necessarily need to be provided to the RP. If the RP intermediary provides guarantees to the RP to only provide attributes with a positive validation result, the attributes can be provided to the RP in any form that suits the RP and the RP intermediary.

5.2.11 Relying party

A Relying Party is a natural or legal person that relies upon attributes attested in an EAA. Typically, they will take decisions in a business process based on these attributes they rely upon.

5.3 EAA Service Provider components

Figure 3 presents general overview of TSP components:

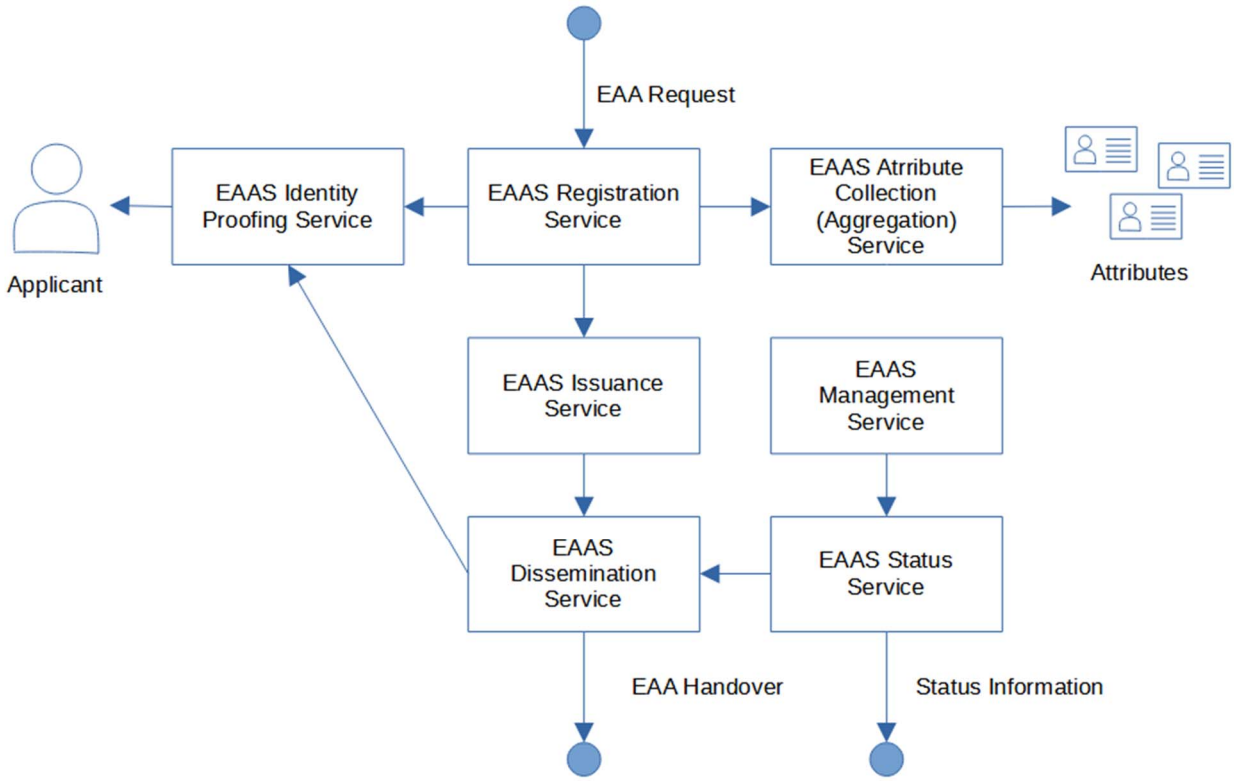

Figure 3: EAA Service components

Table 1 lists the components and indicates their primary roles in the functioning of EAA services.

Table 1: Components description

EAAS component name	Main roles
Registration Service	• Receives request for new EAA issuance from Subscriber • Performs all required verifications as per the applicable EAA Policy: – Authenticates the Subscriber – Verifies that the Subscriber is authorized to request an EAA for the Subject – Collects consent from Subscriber if required – Initiates if required the Subject's identity proofing – Initiates attribute validation against authentic or authoritative source – Collects authoritative evidence • In case of key or certificate binding, collects the public key or certificate data to be included in the EAA
Identity Proofing Service	• Service that performs the process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes • Validates identity of all required applicants: Subscriber, Subject, Wallet holder
Attribute Collection (Aggregation) Service	• Validates attributes against authentic or authoritative source • Creates secured channel with authoritative source • Authenticates the authoritative source • Performs automatic or manual process of the attribute collection
Issuance Service	• Generates EAA • Validates consistency against the EAA Policy • Protects signing or sealing keys • Signs or seals EAA
Dissemination service	• Hands over EAA to EAA recipient • Initiates if required Wallet Holder's identity proofing • Wallet holder authentication if required
Management Service	• Manages attribute life cycle • Receives and authenticates revocation requests • Verifies attribute validity against authoritative source if required • Issues and signs EAA status lists or revocation lists
Status Service	• Provides information about EAA status

Although the EAASP can outsource one or more of these components to other organizations, the EAASP remains the final responsible for compliance with legislation, standards and the EAA Policy that is applicable to the attestation type being issued.

5.4 EAA Policy

5.4.1 Context

The ARF [i.4] describes the concept of an Attestation Rulebook. For each type of attestation, an mDL, a diploma, an e-prescription, and so on, an Attestation Rulebook specifies the attribute scheme, data format and proof mechanisms of that attestation, and, when required, the trust mechanisms for authentication and authorization. It also defines the unique identifiers, syntax/encodings, and semantics of all attributes that can be part of that attestation.

An Attestation Rulebook also makes some choices regarding the protocol(s) for presentation that has to be supported by the relevant attestations. Attestation Rulebooks are defined by different organizations:

- Some rulebooks already have been defined by the European Commission, in consultation with the eIDAS Expert Group. This concerns the PID Rulebook, the mDL Rulebook and the Pseudonym Rulebook. These can be found in Annex 3 of the ARF [i.4].

- The rulebook for an attestation intended to be used across organizations and/or across borders can be defined by an organization in which, insofar possible, all stakeholders are represented. This will prevent multiple attestation rulebooks being defined for the same type of attestation, for example, diplomas. It will also prevent unnecessary differences in the syntax and semantics between similar attestations. It is possible that an individual attestation provider needs to include attributes in an attestation that have not been specified in the relevant sectoral or EU-wide namespace. An example of this are attributes that only have a meaning within the Member State in which the attestation provider resides. To allow such domestic attributes, an attestation provider can define a custom namespace to specify attributes that are specific to this provider and are not included in the EU-wide or sectoral namespace.

- The rulebook for an attestation intended to be used only within an organization, will be defined by that organization.

A lot of the content of these rulebooks is information that in Trust Services usually is taken up in a policy (e.g. certificate policy, signature validation policy, etc.). Consistent with other ETSI standards, ETSI TS 119 471 [i.6] has defined EAA Policies. This will avoid confusion with TSPs, CABs and SBs that already are used to the ETSI terminology from other trust services.

The question arises on the relationship between the ARF term Rulebook and the ETSI term EAA Policy. The intention and a lot of the content of the Rulebooks are similar to what would be expected from EAA Policies. However, it does not completely follow the usual content and mechanisms that are found in policies from ETSI standards for other trust services. There are also some gaps in the content required to guarantee trust (it does for instance have no requirement about the source of the data to be included in the EAA, which is crucial to the trustworthiness of the attributes). And finally the ARF is only written with the EUDIW ecosystem in mind. ARF Annex 2 Topic 12 includes specific requirements on the rulebooks regarding the EUDIW, which makes it impossible to create rulebooks for non-EUDIW bound attestations.

The rulebooks that have been issued so far (PID, mDL) are rulebooks that allow for EU wide interoperability. However, as a consequence, they lack a level of detail that is required for ensuring trust that is depending on member state level situations. As such the rulebook can serve as an overarching legal set of requirements that, if it does contain all the information required, could be used as an EAA policy. But if it is too high level to be used as an EAA policy, separate EAA policies should be created that are compliant with the rulebook. The EAA Policy will contain everything that the rulebook needs to contain. So, if there is no high level rulebook already existing, the EAA Policy can be sufficient and no separate rulebook should be created.

There is merit to have Rulebooks and EAA Policies as separate concepts. The EAA Policies need to be specific enough to make sure it contains all information to guarantee trust. This is sometimes not possible at a wider scale (e.g. pan-European). If a higher level rule set is required to guarantee interoperability and mutual recognition at the wider scale, it makes sense to have a Rulebook as a separate document that the specific EAA Policies can refer to. If that higher level is not required, then a separate document is not required and the EAA Policy can also act as the Rulebook.

Some examples for illustration:

- The European Commission has for instance issued the Rulebook for the mDL. That describes the common minimal rules for mDLs throughout the EU but does not give any detail regarding the specific situation in a member state. Every member state has its own situation and will need to define their own EAA policy, a.o. describing the Source where the data comes from etc. (in some countries this data is in the communes, in others it is in a member state central DB, the rules will be very different for each member state). A member state should issue an EAA Policy in line with the mDL rulebook that specifies what authoritative sources in that member state should be used, what specific rules apply towards ID proofing that is required based on the way that the driver's license database of that member state allows for binding the citizen with the driver's license, etc.

- The aviation sector could create its own EAA policy for EAAs for boarding cards. That would be immediately sufficiently specific to contain all elements to guarantee trust, so that all airlines use the same EAA Policy and no separate Rulebook is required anymore. Every airline can select its own EAASP (or become an EAASP itself) that will implement this general Boarding Card EAA Policy.

5.4.2 EAA policy governance model

Figure 4 presents a general model for EAA Policy governance.

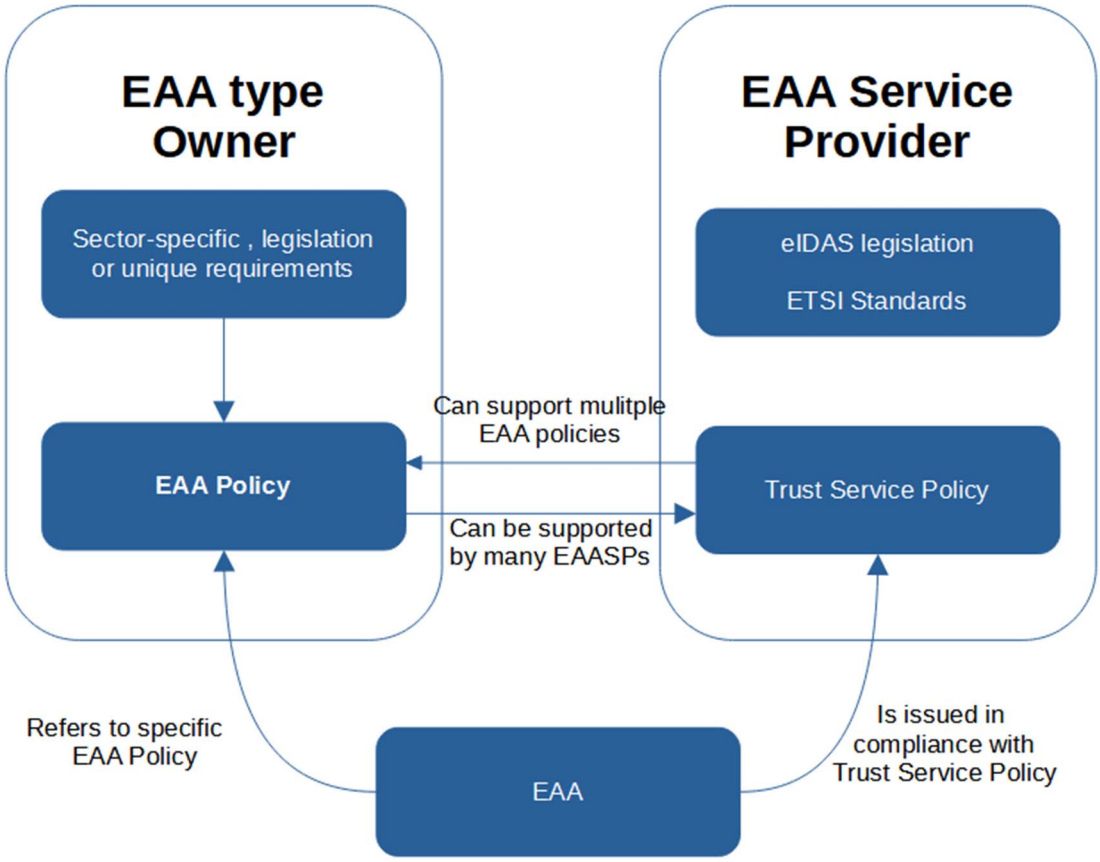

Figure 4: EAA (Schema) model

- The EAA Policy serves as an intermediary layer, enabling various institutions and entities to establish attribute requirements that can be easily adopted by multiple EAASPs. This allows for the straightforward creation of EAA requirements at an intermediate level.
- The EAA Policy can be prepared, published and maintained by various entities (EAA Type Owners), including professional associations, government ministries, sports leagues, standardization bodies, or even private companies. It should be a simple component that many TSPs issuing EAAs can reference. Complexity should be avoided to ensure broad usability.
- It is essential to acknowledge that the differences in implementation between TSPs often prevent them from adopting a single trust service policy. Therefore, the EAA Policy should be agnostic to the infrastructure and processes of the EAASP, ensuring that it can be combined with different trust service policies of different TSPs.
- The use of a separate EAA Policy document is not mandatory. When the issuance of a specific EAA is established solely by one trust service policy without reference to a shared EAA Policy, the issuance rules (the EAA Policy) can also be defined within the service policy document adopted by the TSP. However, it has to be possible to still reference the individual EAA Policy (e.g. by identifying each EAA Policy in the EAA Service Policy with a separate OID). A RP should be able to whitelist the EAA types that it trusts. One EAASP could create EAAs for the same attributes that comply with different EAA Policies of different quality. It is thus not a good idea to whitelist EAA Services, the whitelisting should be possible at the level of the EAA type, meaning the EAA Policy.
- The EAA Policy represents the issuance and presentation requirements for a specific type of EAA. These requirements are stakeholder-approved, simple to create, and serve as inputs to trust service policies, with TSPs declaring which types of EAA they issue.

EXAMPLE 1: Issuance of the Qualified Electronic Attestation of attributes confirming the Attribute Subject home address is specified by national Polish law in EAA Policy. The EAA Policy presents the required data in the EAA and the issuance requirements to provide identity proofing of the Attribute Subject and address validation against a national register of citizens' addresses. This EAA Policy can be different in other countries (e.g. Germany does not have such central register).

EXAMPLE 2: A football league wants to have a uniform model for tickets to enter stadiums. As an EAA Type Owner, it creates, publishes and maintains an EAA Policy that defines the rules for issuing such EAAs and the data structure. This EAA Policy is implemented by a few TSPs in their Policies, which meet a range of additional conditions - typical for providing trust services. Since the EAA Policy is issuance implementation agnostic, it can be implemented by two, three, or five TSPs with different service policies. But all refer to the same model, same recognition, same identification requirements as specified in the EAA Policy.

Different attestation types and schemas can exist for different use cases in different communities. Any party that wants to define an attestation type is recognized as EAA Type Owner. The EAA Type Owner should create an EAAP for this attestation type, so that EAASPs that wish to issue EAA of that type can have its compliance with that policy audited. This is required for the community to be assured that the EAA was created in a way that they can trust. Of course the EAAP should be in line with legal requirements and declared technical standards.

EAA Policies, in principle, can be defined by various sectors such as banking, local or European legislation, technical standards, and the EAASPs themselves. The EAAP should possess the attribute of durability, meaning that once an EAA Policy (in a specific version) is published, it should not be altered, and all issued attributes should refer to it to ensure interoperability and unambiguous interpretation. It is expected that EAAPs will follow a commonly recognized template, specified by standardization.

EAAPs may be established by:

- Standards organizations
- EU and local legislation
- Public sector bodies
- Sector organizations
- Companies willing to issue specific EAAs
- Trust service providers issuing EAAs

5.4.3 Establishing EAA Policies

Compliance with EAA Policies is crucial in order to create EAAs that can be trusted by all parties in the ecosystem. If Relying parties cannot assess whether the identity proofing, collection of attributes, quality of the attribute sources, etc. meet the requirements of their use cases, they cannot trust the EAA for their use case. This means that the EAA Policy should contain all information about all factors that could have an impact on the trust in an EAA.

NOTE 1: For the same attributes, different EAA Types with different EAA Policies can exist (e.g. different source for the attributes). One might be acceptable by all use cases and another only by a subset of use cases.

In order to be complete enough to guarantee trust, EAA Policies should include:

- Information about the EAAP:
  - Type name and URI (e.g. OID or namespace) that allows to identify the attestation type.
  - EAAP version.
  - Attribute schema defining the structure, logical organization and type.
  - Whether the EAA has to be qualified or whether it is also allowed to issue this type of attestation non-qualified.

NOTE 2: Some attestation types will not be possible to meet the requirements for qualified EAA. For an attestation type that can meet the requirements, depending on the EAASP that issues the EAA, the EAA might still be non-qualified or qualified.

- Identification of the EAAP owner.

- The requirements regarding registration, including:
  - requirements on ID proofing, authentication and authorization of the different actors involved;
  - requirements on which consent is required from whom;
  - requirements related to attribute collection;
  - additional statements that should be collected when issuing the EAA;
  - if wallet binding is applied:
    - requirements related to the proof of possession of attestation keys to be included in the EAA;
    - conditions for performing wallet binding;
  - if sign/seal certificate binding is applied:
    - requirements related to the proof of possession of sign/seal certificate references to be included in the EAA;
    - conditions for performing sign/seal certificate binding.
- Requirements regarding the issuance:
  - What data formats to be used (Data formats define the way data in an attestation is formatted, e.g. its character sets, encoding and serialization).

NOTE 3: At the time of writing of the present document, the ARF only foresees mDL, W3C VC DM 2.0 and SD-JWT VC and the CIR 2024/2977 [i.3] only requires support for mDL and W3C VC DM 1.1. However, the ARF and CIR scopes are limited to the EUDIW ecosystem. Other formats could be used outside of that scope. For instance, ETSI has already decided to standardize a Hybrid format that combines a human readable PDF with one or more of the previous mentioned formats.

NOTE 4: The EAAP could specify that the EAA should be offered by the EAASP to the EAA Recipient in more than one format (e.g. Hybrid, SD-JWT and mDL).

  - If not already defined by the data format, the proof mechanisms that should be used (Proof mechanisms define the methods used to secure the attestations for integrity and authenticity, including for selective disclosure).
  - The attestation profile to be used (Attestation Profiles define the structure and semantics of the attributes, including definitions of each attribute).
  - Indication if, and if so what, embedded disclosure policy that should be present in the EAA.
- Requirements regarding the dissemination of the EAA to the EAA Recipient:
  - Requirements on the means for the dissemination (e.g. can only be disseminated to a EUDIW).
  - Requirements related to acceptance of the EAA.
  - Requirements related to proof of possession of a private key linked to a public key / certificate reference contained in the EAA (if present).
- Requirements regarding EAA verification mechanisms.
- Requirements on the lifecycle management of EAA:
  - Requirements regarding the validity period of the EAA.

- Who is authorized for requesting revocation.
- Under what conditions EAAs should be revoked.
- Responsibilities regarding revocation.
- Whether Status Lists or Revocation Lists should be supported.
- Requirements to the revocation system (maximum delay of publication of the revocation information, uptime, ID proofing and authentication requirements for the party requesting the revocation, …).
- Under what conditions EAAs may be renewed.
- Responsibilities regarding renewal.
- Requirements on renewal (ID proofing and authentication requirements for the party requesting the renewal, …).

- Information important to third parties (Relying parties, application builders, …):
  - The attestation stylesheets (Attestation Stylesheets define how the contents of the attestation should be presented to a human in a way that the human viewer can easily understand but that the viewer cannot be mistaken on the meaning of the attributes and their values).

NOTE 5: In practice stylesheets might need to be translated to local languages. These translations can be included in the EAAP or can be left to application developers.

- Limitations on who is allowed to implement the EAAP.
- Special conditions for validating the EAA.
- Required level of assurance for EAA to be presented.

5.5 Business processes

5.5.1 Overview

This clause presents the business processes that occur within the EAA service. Figure 5 presents the main relations between actors and components in the EAA issuance process.

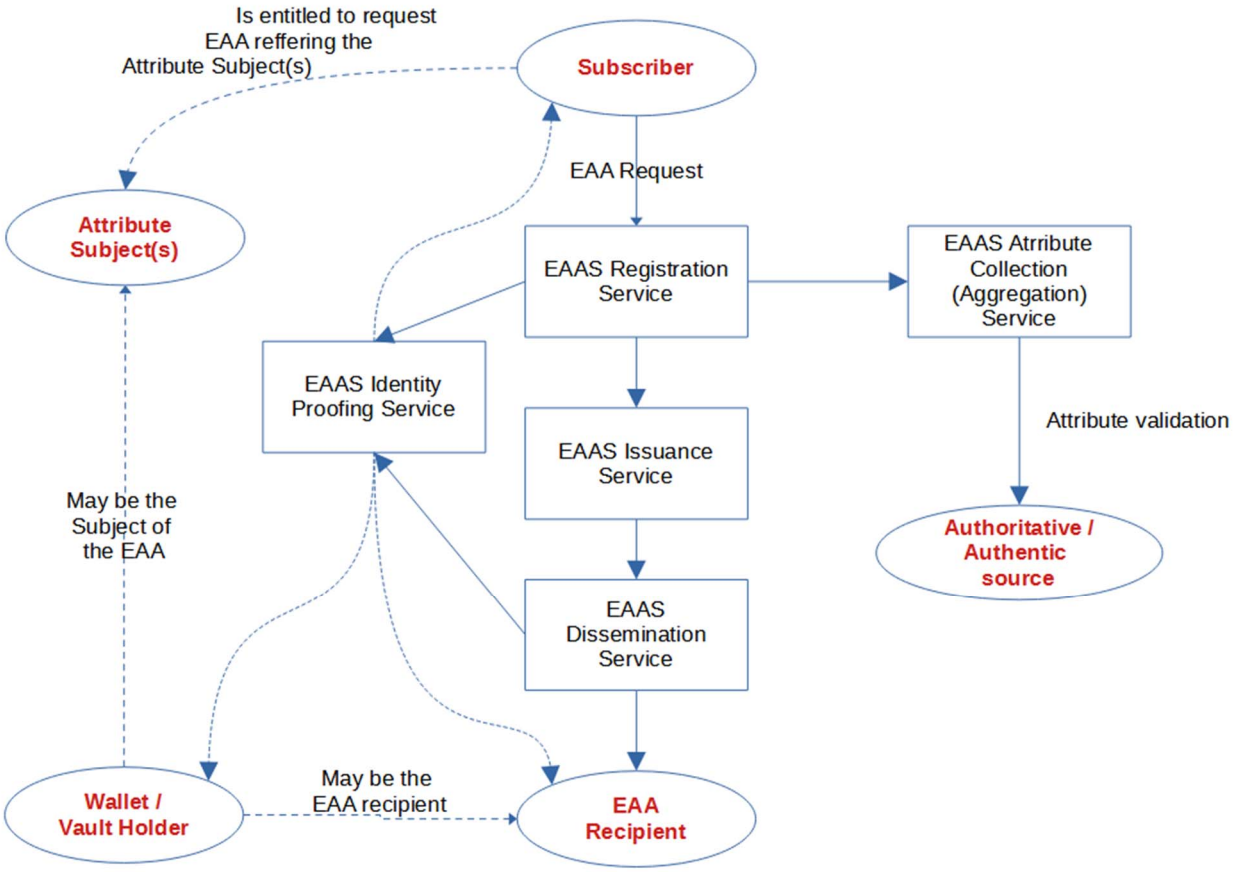

Figure 5: EAA Issuance by EAA Service

5.5.2 EAA registration

Purpose:

The purpose of the EAA registration process is to receive a request for EAA issuance, collecting all necessary evidences from the sources of attributes and identity proofing. The request is received from an authenticated Subscriber.

Input:

- Request form submitted by Subscriber
- Authorization evidence of the Subscriber
- Validation against authentic and authoritative sources
- Additional authorizations if needed on the next steps of the process
- Identity Proofing evidence

Output:

- EAA request registered
- Registration evidence
- Optional: Attribute values

NOTE: There are two possible ways to obtain authentic attributes from an authoritative source: Either the attributes can be requested from the source and the source will deliver the attributes or the attributes will need to be already know by the Subscriber that requests the attestation and the source will only confirm that they are valid. The choice of the mechanism is up to the source. Although there is less risk for data leakage with the second mechanism (verification of known attributes), it might not always be practically possible. For attributes that are more complex (e.g. a diploma that contains details about courses followed) the attribute subject might not be able or willing (too much effort) to provide the exact information (that needs to be fully correct and complete). Or the Subscriber might itself not even know the attributes yet and cannot offer it for verification.

- EAA issuance service process initiation

EAA Service component:

Registration Service

Flow:

1) The request is submitted by the authenticated Subscriber. If the identity of the Subscriber needs to be verified, identity proofing will be conducted each time or based on a previously established agreement. The request can be submitted directly to the TSP or through an interface provided by the Subscriber or attribute source (e.g. a bank).

2) If the EAA Policy requires so, the process initiates subscriber authorization, subject identity proofing and collects evidence.

3) Attributes are obtained from or validated against the source of the attributes. Authoritative evidences are collected.

4) Process validates all evidence and attributes against the EAA Policy.

5) Process initiates the EAA issuance service.

5.5.3 Identity proofing

Purpose:

Verification of the identity of an applicant. An entity is designated as applicant by the process requesting identity proofing (i.e. Subscriber, Attribute Subject, Wallet Holder).

Input:

Request for identity proofing including required level of confidence defined by the EAA Policy.

Output:

Proof of identity

Component:

Identity Proofing Service

Flow:

Identity Proofing process based on ETSI TS 119 461 [i.11].

5.5.4 Collection from or verification against Authoritative source(s)

Purpose:

The purpose of this process against authoritative sources is to obtain accurate and authentic subject attributes. This process follows the requirements stated in the EAA Policy related to quality of the attributes.

Input:

Request for verification

Output:

Verified attributes

Component:

Attribute Collection (Aggregation) Service

Flow:

1) The TSP establishes a secure communication channel with the authoritative source to ensure that the data transfer is protected against any unauthorized access.

2) The TSP authenticates the authoritative source to confirm its legitimacy and to ensure that the data being received is from a trusted entity.

3) The TSP requests or validates the attributes against the data provided by the authoritative source. This involves cross-referencing the submitted information with the data held by the authoritative source to ensure accuracy and authenticity.

5.5.5 EAA Issuance

Purpose:

EAA generation, sealing or signing.

Input:

Registration evidence

Output:

Issued EAA

Component:

Issuance Service

Flow:

Process uses cryptography to create EAA and seal the EAA

5.5.6 Wallet/key binding

Purpose:

Associating the EAA with the Attribute Subject's wallet. This ensures that the EAA is protected and can only be accessed or used by the authorized Attribute Subject. This requires the verification of the binding of the identity of the Wallet Holder with the Attributes in question and to request a proof of possession of the wallet private key.

If the Attestation format does not allow to match the binding from the Wallet Holder to the Attributes on attribute level, but only at attestation level, Wallet binding cannot be allowed for attestations with multiple attribute subjects. Otherwise the Wallet Holder could claim attributes for which he is not the Attribute Subject without a way for the Relying Party to detect (using selective disclosure and pseudonymous attestation presentations for instance).

Input:

Wallet public key

Output:

EAA is bound to the Attribute Subject's wallet.

Component:

Dissemination service

Flow:

EAA is securely linked to the Attribute Subject's cryptographic keys associated with his/her wallet.

5.5.7 Sign/seal certificate binding

Purpose:

Associating the EAA with the Attribute Subject's sign/seal certificate. This ensures the binding of the identity of the Sign/seal certificate Subject with the Attributes in question.

Input

Sign/seal certificate

Output

EAA is bound to the Attribute Subject's Sign/seal certificate.

Component:

Dissemination service

Flow:

EAA is securely linked to the Attribute Subject's Sign/seal certificate.

5.5.8 Handover

Purpose:

The purpose of the handover process is to securely transfer the EAA from the TSP to wallet holder or EAA recipient.

Input:

EAA

Output:

EAA upload to a wallet, downloaded by EAA recipient, other secure means of data exchange.

Component:

Dissemination service

Flow:

The flow depends on the distribution mechanism that is used for the EAA type in question:

1) Option 1: The TSP ensures the Wallet of the EAA Recipient to import the EAA to his/her wallet.
2) Option 2: The TSP ensures that the EAA recipient can download the EAA in a specific format (e.g. Hybrid PDF document).
3) Option 3: The TSP sends the EAA via e-mail to the EAA Recipient.
4) Option 4: The TSP delivers the EAA into the Vault of the EAA Recipient.
5) Other.

5.5.9 Revocation request

Purpose:

The purpose of the EAA revocation request process is to invalidate an EAA that is no longer valid or should not be used. This ensures that any compromised, or otherwise invalid attestations (e.g. the attribute value has changed in the meantime) are securely revoked.

Input:

Revocation request

Output:

EAA revoked in EAASP internal database

Component:

Management Service

Flow:

1) Initiation of a Revocation Request by Authorized Party.
2) Verification of the revocation request by the TSP.
3) Updating the EAA status by the TSP.

5.5.10 EAA Status information

Purpose:

Providing EAA status information to the Relying Party ensures that entities intending to rely on an EAA can verify its current status and validity.

Input:

Status internal database

Output:

Published status result

Component:

Status Service

Flow:

Not specified

6 EAA trust ecosystem

6.1 Scope

This clause discusses what is required for all parties in the ecosystem to be able to have trust in the EAAS and resulting EAA. It is possible that these lead to requirements to be added in ETSI specifications.

6.2 General provision on policies and practices

1) The EAASP should check that its service meets the requirements of the EAA Policy. When changes are applied to the service, that cause the service not to meet those requirements anymore, the EAASP should not issue that type of EAA anymore.

6.3 EAA Policy trust

Without the EAA Policy it is not clear what the minimal guarantees are on the attributes one can find in the EAA. This means that the EAA Policy is crucial for the trust in the EAAs:

1) In order to make sure that the correct EAA Policy can be found back, it has to be possible to reference the EAA Policy via a unique identifier (e.g. OID, URI, …).

2) This unique reference should be included in the EAA, so that during verification the link to the correct EAAP can be made. In order to be able to automate the verification, a URL should be included where the EAAP can be downloaded.

3) It is important that the EAAP remains available over time. For some EAA it could be that a validation of the EAA and the trust value of that EAA is required over the very long time (e.g. long term contracts that have the EAA embedded in a signature, compliance sensitive use cases where evidences of authorizations proven with EAA are required for the long term, etc.). Therefore, there should be a responsible that guarantees that availability of the EAAP for the long term. That can be either the EAA Type Owner, or the EAASP can host a copy of the EAAP, while the EAA Type Owner still has the control over the contents and versioning. In that latter case, if the copy hosted by the EAASP is the version of which the availability will be guaranteed for the long term, the URL where that copy can be found should be the one taken up in the EAA itself.

4) Since all EAA need to be issued according to the EAAP they refer to, the EAASP needs to make sure that it will meet all the requirements of the EAAP. This needs to be the case when initially starting to issue such type of EAA, but it also needs to remain the case later on. This means that if there are changes applied in the EAAP, the EAASP might need to make changes to its configurations or processes to meet the changes requirements of the EAAP. But it also means that if the EAAS is changed that the EAASP needs to verify for each of the EAA types that it issues that the requirements of all the EAAPs are still respected.

5) In order for relying parties to be able to verify this, all of this should be documented in trustworthy documentation. Since the trust in the EAA is guaranteed via the seal on the EAA created by the EAASP, it is logical that this would be in EAASP documents like EAA Service Policy or the practice statement of the EAASP.

6.4 Registration of EAA request

1) For privacy reasons not anyone should be able to obtain an EAA on certain Attribute Subjects. However, for some EAA the Subscriber that might request the EAA will not be the Attribute Subject.

   EXAMPLE 1: A legal representative could request an EAA for the Company it represents.

   EXAMPLE 2: A natural person might request an EAA on an object (e.g. car registration certificate).

   EXAMPLE 3: A natural or legal person can request an EAA for another person (e.g. a parent requesting an EAA with medical data of an infant).

   The EAASP will need to verify that the Subscriber and the EAA recipient (could be another entity than the Subscriber) are both authorized to request and receive the EAA respectively. Part of the authorization verification will be to authenticate these entities.

   The exact authorization requirements for this type of EAA will need to be defined by the EAA Type Owner and documented in the EAA Policy.

2) The request from the Subscriber needs to identify the exact EAA Type that is requested (this can be done by reference to the EAA Policy unique identifier).

3) It is possible that the request needs several types of information in order for the EAAS to be able to execute (e.g. Attribute Subject(s), …). The EAAS will need to verify it has all the information required, and give feedback on that to the Subscriber.

4) Information about the request should be logged as evidence for in case of future disputers on the issuance of the EAA.

6.5 Attributes aggregation

1) In order for the Relying Party to be sure that the attribute quality meets their needs, it needs to be clear what Authoritative Sources are accepted. This should be defined by the EAA Type Owner, documented in the EAA Policy and respected by the EAASP.

2) In order to make sure no rogue entities can pretend to be EAASP, the authoritative source should authenticate and authorize the EAASP and a secure communication channel should be used. Whether this is on an individual basis or for instance based on the registration certificate of the EAASP is a decision to be made by the Authoritative Source.

3) To avoid that a rogue entity would pretend to be the Authoritative source, the EAASP has to authenticate the Authoritative source.

4) The EAAS will need to check the binding of the attributes with the Attribute Subject(s) to avoid mixing attributes and identities. If attributes of the same attestation need to be gathered from more than one source, care needs to be taken not to mix attributes intended for different attestations into one.

5) It is possible that some checks should be done on the received attributes or that they need to be processed in some way before including them into the attestation (e.g. converting non standard country codes into ISO country codes). Only the checks and processing that is specified by the EAA Type Owner should be performed. The EAASP should make sure to do the checks and processing defined by the EAA Type Owner in the EAA Policy, but nothing else.

6) In case the Authoritative Source does only verify attributes already known, the TSP needs to validate the attributes against the data provided by the authoritative source. This involves cross-referencing the submitted information with the data held by the authoritative source to ensure accuracy and authenticity.

6.6 Identity proofing & authorization

1) For the different entities that interact with the EAASP, the EAASP needs to make sure that they are who they pretend to be and whether they are authorized to fulfil the role they have. These entities are:

   a) Subscriber

   b) Any or all of subjects

   c) Wallet holder

   d) EAA Recipient

   e) Authorized -party - for revocation

2) The EAA Policy needs to provide information about level of confidence for identity proofing. But in general:

   a) Identity proofing for QEAA and Pub-EAA have to be on high level of confidence (Extended Level of Identity Proofing as per ETSI TS 119 461 [i.11])

   b) Identity proofing for non-qualified EAA has to be on Baseline level of Identity Proofing as per ETSI TS 119 461 [i.11]) or higher

3) The verifications that have to be performed regarding authorizations and the allowed evidences to base the authorization decision on, should be described in the EAA Policy.

6.7 EAA Issuance

1) The EAASP is responsible for the EAA to be issued according to the requirements in the EAA Policy.

2) The seal of the EAASP on the EAA is a confirmation by the EAASP that he has assumed the responsibility from point 1).

3) The Seal certificate used for sealing EAA should remain valid during the whole lifetime of the EAA that it seals. I.e. the seal certificate should not expire before the last EAA expiry for all EAA it has sealed.

6.8 EAA Dissemination

1) The EAASP will deliver EAA only to the authorized party.

2) If the EAA Policy has this as a requirement:

   a) the EAAS will only deliver this to a wallet (potentially only a EUDIW might be allowed) of a party authorized as an EAA Recipient;

   b) the EAAS will request the wallet for a public key and proof of possession of the private key to be able to do key binding.

NOTE: Key binding can only be done when the wallet holder is also the Attribute Subject of the attributes that will be key bound. If the EAA format does not allow to do key binding on only a subset of attributes, this means that key binding can only be allowed for EAA with only one Attribute Subject.

6.9 EAA Lifecycle management

1) The EAASP is responsible to provide reliable and timely revocation services. An exception should exist for short lived EAA (e.g. EAA for one time use that have to be requested each time even if the attribute does not change, for attributes that are only valid for a very brief period of time).

2) The revocations will be executed as per the requirements of the EAA Policy.

3) Renewal of EAAs to extend their validity, can only be done after insurance was obtained that all attributes remain accurate and current.

4) Revocation is final and cannot be reversed, not even by the EAASP.

5) It is the responsibility of the EAAS to keep track of all events related to the lifecycle of the EAA:

   a) Revocation

   b) Renewal

   c) Validity

   d) Any updates to the EAA

6) When the EAASP receives information that requires a status of an EAA to be updated, it will do so without delay.

6.10 Embedded disclosure policy

eIDAS 2 [i.2] and the ARF [i.4] both specify the use of embedded disclosure policies. They indicate that the use for embedded disclosure policies is not mandatory. Embedded disclosure policies need a tool that will reinforce them. This can be the EUDIW, another wallet, an intermediary, etc. However, in use cases where there is not such tool in play (e.g. the EAA Recipient receives the EAA via e-mail and delivers to the Relying Party by uploading it to its website), an embedded disclosure policy cannot be enforced and thus makes no sense.

6.11 Longevity of EAA

6.11.1 Short lived

Short lived EAA have a lifetime that is lower than 24 hours. Such EAA have no need for revocation verification. There can be several reasons for the issuance of short lived EAA:

- commercial benefit for the EAASP: the EAASP gets paid per transaction;
- less linkability risk (the risk that a profile will be created by one or several entities putting together transactions where the same EAA was used);
- no need for revocation and status services.

6.11.2 Long Lived

Long lived EAA can have a fixed lifetime duration (e.g. 3 years) or the lifetime can be linked to an event (e.g. a known date that a subscription ends). Revocation might not be needed if the attribute cannot be changed before the event (e.g. subscription was paid completely upfront) but might be if not (e.g. subscription is paid on monthly basis and can be stopped by the user before the end of the term).

For EAA where there is the possibility that attributes might change or become invalid before the expiration date of the EAA, a possibility is required to update the EAA (compared to certificates, attributes change much more frequently than the identity in the certificate). This means that in such case revocation and status services have to be available.

6.11.3 Impact on revocation technology

There are use cases where the validity of an EAA at a certain point in time still needs to be able to be verified in the future. Some examples are EAA embedded in signatures and EAA used in processes that need to be auditable (e.g. part of a process subject to compliance requirements). mDL status lists do not allow to see what the status of an EAA was in the past, only at the moment itself. The only way to know whether an EAA was valid a certain point in the past, is to check the status list that was valid at that moment. This means that it has to be possible to retrieve the status list from that moment and that the status list indicates that it was indeed valid at that moment. This requires that the status list not only contains the issuance or publication date, but also the nectUpdate (in the IETF RFC this is optional). If the RP has not retrieved and stored the status list at the time of reception of the EAA, it will only be able to do that if the EAA issuer will provide access to the status lists of the past and not only the current one. This should be a best practice to avoid situations where the status list was not stored and that it turns out that at a point in the future there is a need to verify the EAA status.

6.11.4 Timestamping of EAA

In some use cases it might be needed to be able to proof the validity of an EAA at a point in the past. EAA might be crucial for authorization decisions, and where these decisions have long term consequences, it might be required to be able to proof the EAA for the long term. To avoid that at the time of (re)validation the EAA has in the meantime become invalid or indetermined (expired, revoked, cryptographic algorithm that has become weak) timestamping of the EAA when it is still valid is a solution. When the EAA is included in a signature, the signature format timestamps should cover the EAA as well. I.e. the EAA should then be part of the data to be signed, or at least be covered by the signature timestamps. However, when an EAA is used for authorizing access or transactions directly where there is no signature present, a format for long term validation might be beneficial.

NOTE 1: It might be that ASiC could be suitable for this purpose, but that should be further investigated.

NOTE 2: Keeping a (qualified) validation report of the EAA that is sealed and timestamped is a solution as well, but makes every relying party with such use case dependent on a validation service that issues such reports and then the EAA itself and the report should be kept together which might bring its own challenges.

Annex A:
Example use cases

A.1 Scope

This clause contains a number of use cases to illustrate the different potential implementations of EAA, especially cases that are not the standard use cases that are commonly discussed. The goal is to create an understanding of the requirements of such use cases to which our standards might not cater for at this moment.

A.2 Digital Product Passport (DPP)

A.2.1 Description of the use case

The Digital Product Passport (DPP) is an Electronic Attestation of Attributes (EAA) designed to store and convey essential information about a product throughout its lifecycle. In this context, the EAA can include attributes such as product origin, composition, sustainability certifications, repair history, and ownership changes. The DPP facilitates transparency and traceability, enabling stakeholders (manufacturers, distributors, retailers, and consumers), to access verified product data. The EAA may be exchanged during transactions such as sales, recycling, or regulatory checks, supporting compliance with environmental and market standards.

A.2.2 Trust Service Actors

- **Subscriber:** The **manufacturer** typically acts as the EAA issuer by creating the initial Electronic Attestation of Attributes (EAA) for the product and updating its attributes when necessary. However, in certain circumstances, a **distributor** or **retailer** can also assume this role if they introduce new product attributes, for example, during repackaging or refurbishment.
- **EAA Recipient:** The **distributor** and **retailer** both serve as EAA Recipients as the product progresses through the supply chain. The **consumer** becomes the EAA Recipient once they purchase the product. Each of these entities may request updates or transfer the EAA as ownership changes.
- **Relying Party:** The **consumer** is the primary relying party, depending on the EAA's authenticity and accuracy when acquiring the product. Additionally, **regulatory authorities** may act as relying parties during compliance checks, and **distributors** or **retailers** may rely on EAAs received from upstream entities.
- **EAASP:** The **EAASP** ensures the integrity and authenticity of the EAA throughout its lifecycle, including issuance, updates, validation, and timestamping. In certain models, a manufacturer or regulatory authority may also operate as an EAASP, particularly if they provide in-house attestation or validation services.

NOTE: It is important to note that a single entity, such as a retailer, might fulfil multiple roles (e.g. EAA holder, EAA issuer upon product modification, EAA relying party when accepting goods, and EAA verifier during internal quality control). Similarly, a given role, such as EAA verifier, can be fulfilled by several different parties depending on the stage of the product lifecycle and regulatory requirements.

A.2.3 Business processes

- **Issuance:** The manufacturer generates a DPP EAA for each product, embedding key attributes.
- **Update:** Attributes are updated by authorized parties (e.g. after repair or ownership transfer), with the EAA reflecting the current state.
- **Verification:** Distributors and regulatory bodies verify the EAA during logistics, market entry or compliance checks.

- **Transfer:** The EAA is transferred to the new owner during sales, with updates to ownership attributes.
- **Archival and End-of-Life:** The final status of the product is recorded in the EAA before recycling or disposal.

A.2.4 Technical implications

- **Multiple attribute subjects:** The DPP may need to cover several components or sub-products within a single EAA.
- **Graphical content:** Inclusion of images (e.g. product photos, QR codes) may be required for identification and verification.
- **Interoperability:** The EAA format has to support integration with various supply chain and compliance platforms.
- **Lifecycle management:** Mechanisms for updating, revoking, or archiving attributes have to be robust and secure, with audit trails. The EAA formats used have to allow for updating existing EAA (can be by not modifying existing content, but by adding additional content, e.g. when the product is sold, to the EAA data is added with the date of the transfer and the identity of the new owner which is signed by the old owner).
- **Privacy and security:** Sensitive product or owner data have to be protected according to relevant regulations.

A.3 Mandate of natural person on European Business Wallet (EUBW)

A.3.1 Description of the use case

This use case involves the issuance and management of an EAA that represents the mandate or authority of a natural person to operate a European Business Wallet (EUBW) on behalf of a business entity. The EAA includes attributes such as the person's identity, role, scope of authorization, validity period, and conditions. Such a mandate is essential for digital transactions, document sealing, regulatory filings, and other activities requiring proof of authorization to activate the according functionalities of the EUBW. Although the EUBW could also use other authorization mechanisms, EAA would be very beneficial if the EUBW is composed of multiple (trust) services from different providers. The mandating business entity can then issue one EAA for the mandate, which can be relied upon by the different component providers of the EUBW solution.

A.3.2 Trust Service Actors

- **Subscriber:** The mandating business entity that authorizes the natural person and requests the issuance of the EAA.
- **Attribute Subject:** The natural Person that will be mandated to act on behalf of the business.
- **Relying Party:** The EUBW components (for the mandating business entity) that verifies the mandate EAA when a EUBW transaction or process is initiated by the EAA Attribute Subject.

A.3.3 Business processes

- **Mandate creation:** The business entity initiates the process, specifying the scope and validity of the mandate.
- **EAA issuance:** The TSP validates the request and issues the EAA to the natural person's EUBW.
- **Mandate presentation:** The natural person presents the EAA when engaging in EUBW transactions.

- **Verification:** The EUBW component providers check the EAA's validity and scope before accepting actions or signatures.
- **Modification/revocation:** The business entity or TSP updates or revokes the EAA in case of role changes, expiry, or termination.

A.3.4 Technical implications

- **Multiple attribute subjects:** Mandates may cover multiple roles or business entities, requiring the EAA to support complex attribute sets.
- **Revocation and status services:** Given the dynamic nature of business roles, robust mechanisms for real-time revocation and status checks are essential.
- **Interoperability:** The EAA format has to be compatible with various digital wallets, document signing platforms, and regulatory systems across Europe.
- **Privacy and security:** The EAA has to protect sensitive identity and mandate data, comply with GDPR, and provide clear audit trails.

A.4 EAA included in a signature

A.4.1 Description of the use case

In this use case, an Electronic Attribute Attestation (EAA) is embedded within the digital signature of a document or transaction. The EAA serves as a verifiable proof of specific attributes, such as the signatory's role, their authority, or the context under which the signature is made. This approach is particularly relevant for legal, financial, or regulatory documents where it is essential to not only confirm the identity of the signer but also their eligibility, mandate, or permissions at the time of signing. For instance, a company director signing a contract may include an EAA confirming their directorial status and the scope of their authority. The EAA is exchanged between parties as part of the signature verification process, ensuring that both the signature and the underlying attributes are trusted and auditable. This enhances accountability and compliance in cross-border or multi-party transactions, as well as streamlines due diligence.

The business context for this use case covers scenarios such as contract execution, regulatory filings, financial approvals, or any transaction where proof of role and authority is as critical as proof of identity.

A.4.2 Trust Service Actors

The key actors involved in this use case are:

- **EAA Attribute Subject:** Signatory
- **EAA Subscriber:** The organization or legal entity that grants the authority or mandate to the signatory.
- **EAA Relying Party:** The recipient or verifier of the signed document who checks both the signature and the embedded EAA for authenticity and relevance.

A.4.3 Business processes

The practical implementation of business processes for this use case may include:

1) **Mandate and attribute definition:** The mandating entity defines the attributes to be included in the EAA, such as role, scope, and validity period.
2) **EAA issuance:** The TSP validates the request and issues the EAA to the signatory, binding it to their identity and mandate.

3) **Signature creation:** When the signatory creates the digital signature he delivers the EAA presentation to the signing service which embeds the EAA into the signature data structure (e.g. as part of a qualified electronic signature or advanced electronic signature).

NOTE: Probably at this stage the signing service will check the validity of the EAA and whether the correct role is indicated by the EAA before allowing the signature to be created.

4) **Document exchange:** The signed document, containing the EAA, is sent to the relying party.

5) **Verification:** The relying party verifies both the digital signature and the EAA, ensuring the signatory's authority and attribute validity at the time of signing.

6) **Revocation/Update:** If the signatory's mandate changes or expires, the EAA has to be revoked or updated, and subsequent signatures have to reflect the current status.

A.4.4 Technical implications

Embedding EAAs in signatures introduces several technical considerations:

- **Interoperability:** EAAs embedded in signatures have to be compatible with various signature formats and the different signature creation and validation solutions should be able to treat each other's signatures with embedded EAA.
- **Revocation and status checks:** Real-time mechanisms for revoking or updating EAAs are essential, as mandates can change frequently.
- **Privacy and security:** Sensitive attribute data has to be protected in accordance with GDPR and other regulations, with clear audit trails for compliance.

A.5 Vehicle documents

A.5.1 Description of the use case

Vehicle documents such as car registration certificates, certificates of conformity, and insurance proofs are essential for legal compliance and day-to-day vehicle operation. These documents often need to be presented to public authorities, law enforcement, car workshop, or other third parties. In practice, vehicles may be used by multiple individuals (family members, rental customers, or professional drivers) who all require the ability to present these documents when necessary.

The digitalization of these documents as EAAs enables easier sharing and verification. However, the solution should not bind the document to a single person's wallet, otherwise casual drivers would be unable to present them. Therefore, EAAs for vehicle documents have to be easily transferable between different European Digital Identity Wallets (EUDIWs) or accessible from the car itself (e.g. QR code in the glove compartment giving access to an online copy or stored within the car computer), ensuring flexibility for real-world usage. For example, a rental car's registration and insurance documents should be available to any legitimate driver, not just the primary rental company.

A.5.2 Trust Service Actors

The main actors for this use case include:

- **EAA Recipient:** The person or entity legally responsible for the vehicle and its documents.
- **Subscriber:** Government agency or insurance company issuing the official vehicle documents as EAAs.
- **Relying Party:** Law enforcement, car workshop, or any third party that needs to validate the authenticity and validity of the vehicle documents.

A.5.3 Business processes

The practical implementation of business processes for vehicle documents includes:

1) **Issuance:** The document issuer (e.g. government or insurance company) creates and issues the vehicle document as an EAA, associating it with the vehicle rather than a specific person.

2) **Distribution:** The EAA is made available to the vehicle owner and any casual drivers, typically via secure sharing mechanisms or accessible digital platforms.

3) **Presentation:** Any authorized driver can present the EAA to law enforcement or other relying parties as proof of compliance.

4) **Verification:** The relying party verifies the authenticity and validity of the EAA, checking its attributes and ensuring it matches the vehicle in question.

Update/Revocation: When the vehicle's status changes (e.g. sold, insurance updated), the EAA has to be updated or revoked and replaced with a new attestation.

Annex B:
Impact on standardization

B.1 Impact on ETSI Standards

- Clause 5.4 proposes how Rulebooks and EAA Policies can co-exist and how the relationship between them can be seen. Further discussion and alignment with the European Commission is required regarding definitions of and the relationship between rulebooks, EAA Policies, EAA Schemes or Schemas and catalogues. This should take into account EAA used in a non-EUDIW context to avoid that rulebooks, EAA Policies, EAA Schemes or Schemas and catalogues can only be used for EAA used with the EUDIW.

  Standards potentially impacted: ETSI TS 119 471 [i.6], ETSI TS 119 472 series (if references to those objects / documents need to be included in the EAA), future ETSI TS 119 482-3 [i.22].

- In all standards ETSI should make sure that the RP Intermediary role is considered and that the implementation of the RP Intermediary role will be:

  - As easy and efficient as possible;
  - Will not reduce the trust guarantees for any of the parties involved; and
  - Will not negatively impact security.

  Standards potentially impacted: ETSI TS 119 471 [i.6], ETSI TS 119 412-6 [i.10], ETSI TS 119 472 series (for instance related to the embedded disclosure policy that needs to take into account the Intermediary), ETSI TS 119 476 series (ZKP should be possible via the intermediary), ETSI TS 119 479-2 [i.19], future ETSI EN 319 486 (Intermediaries also need to be able to register, Intermediaries need to be able to register for the RPs that are their customers), ETSI TS 119 411-8 [i.20], ETSI TS 119 472-2 [i.8], ETSI TS 119 472-3 [i.9] (issuance of EAA should also be possible via an intermediary, see for instance the SCA certificates from ARF [i.4] TS12), ETSI TS 119 475 [i.21].

- Currently in ETSI standards there seems to be no policies for making available status information about EAA. Standardization should be foreseen for the formats to be used for status lists or revocation lists, lifecycle management of status lists, availability over time of status lists, etc.

- Certificate binding (see clause 4.4.3) requires some specific verifications related to this binding. Policy and security requirements for this should be specified (as conditional requirements in ETSI TS 119 471 [i.6]).

- Potential update to the standards regarding EAA formats to include the binding of specific attributes or attribute subjects with wallets or certificates in the case of multi subject EAA.

  Standards potentially impacted: ETSI TS 119 471 [i.6], ETSI TS 119 472 series, ETSI TS 119 482-3 [i.22].

B.2 Impact on standards related to the European Business Wallet

NOTE 1: The EUBW will have to deal with a lot of different type of EAA of which a lot will not necessarily be distributed via a EUDIW. As a consequence all changes to standards that are required to go beyond the use of EAA with a EUDIW, are relevant to the EUBW.

- Several of the topics in the present document have importance for the European Business Wallet, a.o.:

  - EAA distribution
  - Multiple subjects
  - Identity Binding vs. Wallet Binding vs. Certificate Binding

- Vaults (if this concept will be adopted by the EUBW)
- Hybrid EAA

- The present document has proposed some concepts and terminology that are important for non-EUDIW bound EAA.
  - It should be verified in all other standards related to EAA, that their implementation is not blocked by those standards (e.g. registration certificates should not make the implementation of a RP Intermediary impossible).

EXAMPLE 1: REQ-EAASP-7.13-04 of ETSI TS 119 471 [i.6] says: "*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*". => This requirement does not take into account that the EAA Policy might be administrated by another entity and that multiple EAASPs can implement one and the same EAA Policy.

EXAMPLE 2: REQ-EAASP-4.2.2.3-11 of ETSI TS 119 471 [i.6] says: "*The EAASP shall support mechanisms to mitigate the risk of user linkability, including at least one of the following …*". This assumes that unlinkability is important for all EAA types. That is not the case. There is no need for unlinkability for a Digital Product Passport (DPP) for instance. Imposing an issuer of a DPP to implement unlinkability measures will add to the cost of DPPs, so DPP issuers will have an unnecessary threshold to issue DPPs in compliance with ETSI TS 119 471 [i.6] or issue them as QEAA.

- These concepts and terms should be consistently reused in other ETSI standards that are related to EAA.

Standards potentially impacted: ETSI TS 119 471 [i.6], ETSI TS 119 472 series

- Clause 5.4.3 contains an overview of content for an EAA Policy that is important to ensure trust in the EAA. This should be added to ETSI TS 119 471 [i.6]. That should include an indication of what of these elements of the EAA Policy should be mandatory and what optional. This will be different for non-qualified EAA and Qualified EAA. ETSI TS 119 471 [i.6] does not give any requirements for Pub-EAA. So, probably this does not have to be added for Pub-EAA.

- Clauses 5.3 and 5.5 decompose the EAAS infrastructure and business processes respectively. This allows to see where issues might arise and to define what requirements might be missing in ETSI TS 119 471 [i.6].

- Topic 12 in Annex 2 of the ARF contains a list of requirements regarding attestation rulebooks. This is written for the EUDIW ecosystem and cannot be implemented as such for EAA that are not (only) intended for use within the EUDIW ecosystem. Some of these requirements exclude the use without EUDIW. Some of the requirements are not valid for EAA that will not be used with a EUDIW. However, a list with the minimal requirements to be included in Rulebook / EAA Policies should be created also for other types of EAA, so that it is clear to the TSP what he should include to be compliant with legislation and best practices.

NOTE 2: Clause 5.4.3 of the present document gives a high level overview of the requirements that should be included, but a detailed list like in the ARF Topic 12 should be added to an ETSI specification (potentially with conditional statements regarding the use in the EUDIW ecosystem or not).

B.3 Other impact on existing standards

- Potential update of the signature format standards to specify that any included EAA should be part of the data to be signed, or at least that it should be covered by the signature timestamps (see clause 6.11.4).

- Potential update of the ASiC standard if it would not suffice to allow for archival timestamping of an EAA included in the ASiC.

B.4 Suggested new work items

Since the RP intermediaries have an important trust role, they should be considered similar in nature as a Trust Service Provider. In order to provide best practices that could be adopted for auditing RP Intermediaries, ETSI should create Security and Policy Requirements for RP intermediaries. This is a new standard to be written for which a new work item should be created.

B.5 Topics requiring further discussion

ETSI TS 119 471 [i.6] and some other ETSI standards use the term EAA subject (defined as: natural or legal person that holds the Electronic Attestation of Attributes). In the present document this term was not used, as the EAA might be received via several channels, by multiple entities that are not necessarily a subject to the EAA. When a natural person receives an AA for an object or where an EUBW receives EAA Related to an employee of the company, it is confusing to call that natural person or the EUBW Holder the EAA Subject. Hence, the present document has used the term EAA Recipient (defined as: Any entity that receives the EAA after its issuance). Further discussion is required if the term EAA Subject should be used for all recipients of EAA (even if they are not a Subject of the EAA) and that the present document should align to the existing standards or that this would make the comprehension of the present document more difficult. It could also be considered that the term EAA Recipient might be adopted by other standards.

Annex C (informative): Bibliography

- Commission Implementing Regulation (EU) 2025/1569 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source.
- ETSI TS 119 478: "Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources".
- OpenIDVCI.

History

Version	Date	Status
V1.1.1	May 2026	Publication