ETSI TR 119 479-2 V1.1.1 (2025-07)

TECHNICAL REPORT

Electronic Signatures and Trust Infrastructures (ESI); Technological Solutions for the EU Digital Identity Framework; Part 2: EAA Extended Validation Services Framework and Application

Reference

DTR/ESI-0019479-2

Keywords

attribute attestation, digital identity, EAA,
encryption, 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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

The present document is part 2 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.

Executive summary

The present document proposes an advanced attestation validation schema managed by the European Union Digital Identity (EUDI) Wallet and the introduction of new policy, the "pricing_policy". The proposed protocol preserves Users' privacy and unlinkability while allowing direct privacy-preserving communication between the Attestation Provider and Relying Party (RP).

The proposed protocol is composed of two parts:

- The first one consists of refreshing the attestation before presenting it, to guarantee its validity and that it has not expired nor been revoked, without the need for the RP to undertake additional controls at presentation time, except those related to the integrity of the attestation.
- The second phase, referred to as Cyphered Attestation Presentation, encrypts the attestation carrying out a JWE and Hierarchical Deterministic Key Derivation. This ensures that the RP interacts with EUDI Wallet to retrieve the JWE and the Attestation Provider to obtain the JWE decryption key, which is obtained using the Hierarchical Deterministic key Derivation process performed by the Attestation Provider. This process prevents the RP from accessing any user's attestation information without direct communication with the Attestation Provider and User, while maintaining privacy for the User. The communication takes place without sharing any info related to the User. This mechanism enables the development of a pricing policy for attestations that facilitate the effective large-scale adoption of the EUDI Wallet.

Introduction

EU Regulation 2024/1183 (also termed here "eIDAS 2.0") [i.12] provides the legal framework for the European Digital Identity (EUDI) Wallet, designed to allow citizens and businesses (from both public and private sectors) to store, manage and present their attestations, such as identity credentials (name, date of birth, tax number, nationality, etc.), certificates, diplomas, professional credentials and more, securely in online, offline, national and cross-border use cases, and electronically sign or seal documents as an individual, as a legal person or as a representative thereof.

To build an interoperable system, the European Commission, through its Architecture and Reference Framework (ARF) and the EUDI Wallet Toolbox, provides a structured approach to the design, implementation and operation of the EUDI Wallet. The Framework itself represents the core architecture that defines the technical specifications, guidelines and architectural principles to ensure consistency and interoperability across different EUDI Wallet implementations.

To put in practice the vision of eIDAS 2.0 and of the ARF, the digital identity ecosystem revolves around three pivotal roles, namely the Attestation Providers, the Wallet User, and the Relying Party.

At the core of this framework, there are two foundational technical properties focused on preserving security and privacy of the EUDI Wallet Users, namely selective disclosure and unlinkability. The former means that a User should be able to share only specific attributes from their credential, instead of revealing it in its entirety, ensuring data minimization and enabling them to prove necessary information without exposing unrelated personal data. The latter means that transactions of the same User cannot be linked or tracked, for more information refer to clause 3 in ETSI TR 119 476 [i.3] for unlinkability definition.

According to the current state of art, RPs rely on credential status list or revocation status list, as described in ARF [i.4], maintained by Attestation Providers to validate attestations. However, this approach compromises unlinkability and User privacy. In clause 8 of ETSI TR 119 476 [i.3] several methods to guarantee privacy-preserving revocation schemas and status check are discussed, but none provide a suitable validity status mechanism that is both simple and matches unlikability requirements.

The proposed solution introduces a simplified validity status mechanism, reducing the burden on RPs by eliminating the need for additional validity checks on presented attestation. However, the primary focus is the introduction of a new policy, the "pricing_policy", applied to attestation. This pricing policy is independent of any revocation or validity check methods. Furthermore, it opens up possibilities for new use cases based on the pricing policy. For instance, in alignment with the proposed extended validation service, Attestation Providers could have the ability to count the number of verification requests made by RPs, maintaining User's privacy and unlinkability.

1 Scope

The present document proposes an extended validation mechanism leveraging on the existing OID4VP protocol. Its primary aim is to support the secure and interoperable validation of electronic attestations by identifying standardization needs in the context of the attestation rulebook and attribute catalogues.

Key focus areas include:

- introduction of attestation refreshing and attestation encryption mechanisms;
- description of embedded disclosure policies and support for pricing policies;
- further considerations on the extension of attestation metadata structures to include policy-related parameters.

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] BIP-0032.

[i.2] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

[i.3] ETSI TR 119 476 (V1.2.1): "Electronic Signatures and Trust Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes".

[i.4] European Digital Identity Wallet Architecture and Reference Framework v1.8 (ARF).

[i.5] IETF draft-demarco-oauth-status-assertions-03: "OAuth Status Assertions".

[i.6] IETF draft-ietf-oauth-sd-jwt-vc-09: "SD-JWT-based Verifiable Credentials (SD-JWT VC)".

[i.7] IETF RFC 7516: "JSON Web Encryption (JWE)".

[i.8] ISO/IEC 18013-5: "Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application".

[i.9] NIST SP 800-56A Rev. 3: "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography".

[i.10] OpenID Foundation: "OpenID for Verifiable Credential Issuance - draft 15", 2024.

[i.11] OpenID Foundation: "OpenID for Verifiable Presentations - draft 24", 2025.

[i.12] 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.13] SOG-IS Crypto Working Group: "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms".

[i.14] W3C® Recommendation 3 March 2022: "Verifiable Credentials Data Model v1.1".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in [i.4], [i.12], [i.14] and the following apply:

attestation provider: natural or legal person who provides QEAA, PuB-EAA, or (non-qualified) EAA issuance services

attribute: feature characteristic or quality of a natural or legal person or of an entity, in electronic form

Electronic Attestation of Attributes (EAA): attestation in electronic form that allows attributes to be authenticated

Electronic Attestation of Attributes issued by or on behalf of a Public sector body (PuB-EAA): electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources

EU Digital Identity (EUDI) Wallet: initiative by the European Union aimed at providing citizens and businesses with a secure and convenient way to manage and use their digital identities

NOTE: The EU Digital Identity Wallet allows users to store and control their personal data in a digital format, enabling them to prove their identity and other attributes in various online and offline situations.

Person Identification Data (PID): 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

PID provider: natural or legal person responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a Wallet Unit

presentation: data derived from one or more attestations, issued by one or more Attestation Providers, that is shared with a specific verifier

Qualified Electronic Attestation of Attributes (QEAA): electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V of European Digital Identity Wallet Architecture and Reference Framework [i.4]

Relying Party (RP): natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service

(Wallet-) Relying Party: Relying Party that intends to rely upon Wallet Units for the provision of public or private services by means of digital interaction

selective disclosure: capability enabling the user to present a subset of the attributes included in a PID or attestation

unlinkability: lack of information required to connect the user's selectively disclosed attributes beyond what is disclosed

NOTE: The unlinkability definition has different shapes, refer to clause 3 of ETSI TR 119 476 [i.3] for further information.

user: natural or legal person, or natural person representing another natural person or legal person, that uses trust services or electronic identification means provided in accordance with Regulation (EU) 2024/1183 [i.12]

(Wallet) User: user who is in control of the Wallet Unit

Wallet Solution: combination of software, hardware, services, settings, and configurations, including Wallet Instances, one or more Wallet Secure Cryptographic Applications, and one or more Wallet Secure Cryptographic Devices

Wallet Unit: unique configuration of a Wallet Solution that includes Wallet instances, Wallet Secure Cryptographic Applications, and Wallet Secure Cryptographic Devices provided by a Wallet Provider to an individual Wallet User

3.2 Symbols

Void.

3.3 Abbreviations

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

ARF	Architecture and Reference Framework
CRQC	Cryptographically Relevant Quantum Computers
EAA	Electronic Attestation of Attributes
ECC	Elliptic Curve Cryptography
EUDI	European Union Digital Identity
HD	Hierarchical Deterministic
JWE	JSON Web Encryption
KID	Key IDentifier
OID4VCI	OpenID for Verifiable Credential Issuance
OID4VP	OpenID for Verifiable Presentation
PID	Personal Identification Data
QEAA	Qualified Electronic Attestation of Attribute
RP(s)	Relying Party(-ies)
URL	Uniform Resource Locator
VP	Verifiable Presentation

4 Extended Validation Service(s)

4.1 Overview

The present clause presents an extension to the digital attestation validation framework.

This advancement enables the development of diverse business models associated with attestations, encompassing issuance, validation, and unrestricted free usage. At present, only issuance and free usage are achievable without the proposed approach.

The proposal discussed in the present document does not require changes to the existing attestation issuance process. It is format-agnostic, maintaining compatibility with all the available.

The concept involves two steps:

1) **Attestation Refreshing:** the attestations are refreshed before being presented, to guarantee their validity without the need for the RP to undertake additional controls, except for integrity of the attestations.

2) **Cyphered Attestation Presentation:** the attestations are encrypted by the User's Wallet using a mechanism described later in the present document, before being shared with a RP. The RP can only access the attestation(s) through direct communication with the User and with the Attestation Provider. This communication occurs without revealing any information about the User and allows the Attestation Provider to count the number of verifications performed by each RP.

These two steps are described more thoroughly in the following clauses.

4.2 Attestation Refreshing

Attestation refreshing consists of periodically refreshing attestation(s) by communicating directly with the Attestation Provider. This could be achieved through two different approaches:

- **Linked credentials:** the Attestation Provider provides the User with a Status Assertion [i.5], which is linked to an attestation. This enables the User to present both the attestation and its Status Assertion to RP as a proof of the attestation's validity status.

- **Credential reissuance:** it is based on multiple access to the RP endpoint, as described in clause 13.5 in OID4VCI [i.10]. It is possible to refresh an issued attestation, the Wallet can retrieve an updated attestation using a valid Access Token or refresh it with a valid Refresh Token, without interaction with the User. If the Wallet lacks both a valid Access and Refresh Token, the Attestation Provider should reissue the attestation by initiating the issuance process from the beginning, which requires interaction with the User. Re-issuance means the replacement of a PID or attestation that already exists in a Wallet Unit by a PID or attestation having the same document type. For formal definitions of re-issuance, refer to ARF Topic B [i.4].

- **Batch Issuance:** it means that instead of issuing a single PID or attestation to a Wallet User, a PID Provider or Attestation Provider issues a batch of them. If the original PID or attestation was issued in a batch, then the PID Provider or Attestation Provider re-issues that PID or attestation in a batch as well. For formal definitions of batch issuance, refer to ARF Topic B [i.4].

This Attestation Refreshing could be done when the Wallet starts up, or on demand, or just before presenting the attestation. These approaches should apply only to attestations that require refreshing. For example, it would not be useful for static attestations. RP can implement their own policies based on the type of service provided. For instance, they could accept an attestation refreshed within the last *N* hours or, for more critical services, only accept an attestation refreshed within the last minute.

This ensures for a non-complex validation mechanism, **since the attestation is refreshed** directly by the Attestation Provider, **third parties are not required to validate it**.

4.3 Cyphered Attestation Presentation

The attestation, once refreshed, is encrypted by the User's Wallet. The RP should then contact the Attestation Provider to retrieve the decryption key in order to verify the attestation. This adds an additional layer of security by ensuring that the RP cannot access the attestation directly, without interaction with the Wallet User and the Attestation Provider.

As previously mentioned, the protocol doesn't imply any change to the current attestation issuance process (described in OID4VCI [i.10]). The Attestation Provider creates and signs the attestation, embedding relevant identity or attribute information for the User (e.g. identity, access rights, etc.). Then the attestation is transmitted to the User's Wallet over a secure channel using TLS, as described in OID4VCI [i.10].

The proposed method involves **encrypting the attestation at the time of presentation**, leveraging the properties of Elliptic Curve Cryptography (ECC) and, more specifically, the **Hierarchical Deterministic (HD) Key Derivation**.

In particular, the method takes advantage of the properties of Hierarchical Deterministic structures, where each derived private key is generated in such a way that the corresponding public key can be computed without knowing the private key itself.

When a Wallet initiates the presentation of an attestation (which could be in various formats, such as SD-JWT VC [i.6] or mdoc [i.8]), the attestation is encrypted according to the JSON Web Encryption (JWE) standard [i.7]. The encryption key for the attestation is generated at the time of the new presentation; it is derived from the Attestation Provider's public key.

In order for the RP to decrypt the JWE, the Wallet should also send them additional information along with the JWE. This will be forwarded to the Attestation Provider. Upon receiving the necessary information, the Attestation Provider retrieves the cryptographic material which the RP can use to obtain the attestation.

More in detail, the expected flow of messages is listed below, subdivided into two phases: Refreshing and Presentation.

Refreshing:

1) The Wallet sends the Attestation Provider a request to refresh the attestation, as described in the previous clause.

2) The Attestation Provider sends an updated attestation back to the Wallet, notifying the Wallet in case the attestation is not valid anymore.

Cyphered Attestation Presentation:

1) The Wallet generates a transaction-specific symmetric encryption key *K* which it uses to encrypt the attestation A. The result of the encryption process is denoted here as K(A).

2) The Wallet generates the JWE of the attestation as follows:

   - The JWE contains all the necessary information for decrypting the body of the JWE itself; this includes:

     - X: a concatenation between a timestamp and a random nonce generated by the Wallet;

     - KID: a Key Identifier, needed to identify the correct Attestation Provider and then ask this Attestation Provider to decrypt CP(K) (see below);

     - CP(K), i.e. the key K encrypted using an asymmetric public key CP belonging to the Attestation Provider and derived from a master public key of the same Attestation Provider.

   - The body of the JWE contains K(A), that is the attestation A encrypted using the symmetric key K (see step 1).

3) The RP receives the JWE and sends CP(K) and X to the Attestation Provider, asking the Attestation Provider to use the derived private key linked to X in order to decrypt CP(K).

4) The Attestation Provider retrieves from X which private key to use in order to decrypt CP(K); after doing so, it obtains K and sends K to the RP.

5) The RP uses K to decrypt K(A), thus retrieving A.

Figure 1 below schematizes the above steps 1) - 5) with regards to Cyphered Attestation Presentation.

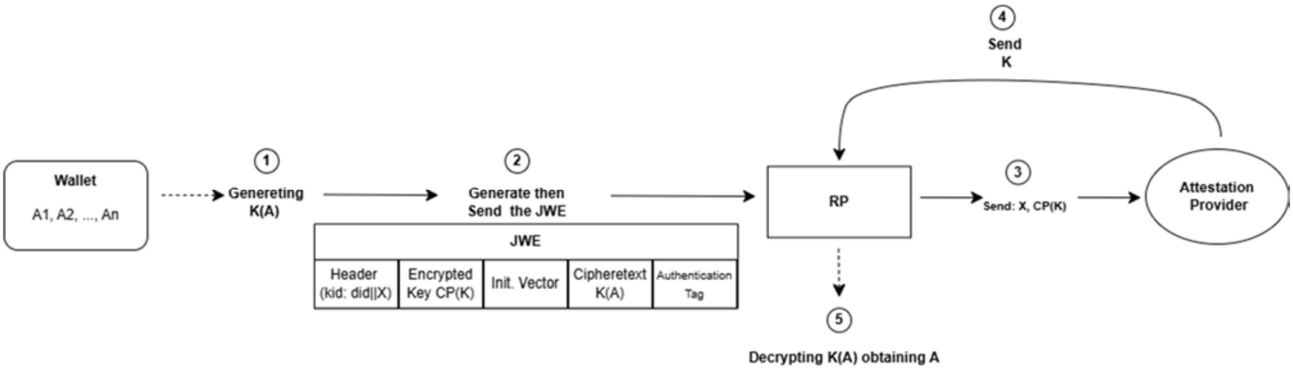


Figure 1: Cyphered Attestation Presentation Scheme

5 Central Rulebook for Attributes

5.1 Overview

The EUDI Wallet ecosystem is governed by a range of policies that address various aspects of user interaction, data security, attestation management and user privacy. These policies are designed to safeguard users' personal information and ensure that the ecosystem functions smoothly across EU boundaries.

The EUDI Wallet is designed to comply with eIDAS 2.0 [i.12], ensuring compliance with strict privacy and security standards. Each interaction of the Wallet undergoes rigorous certification to meet high security requirements.

For instance, the user consent policy guarantees that users retain full control over their data. When a RP requests access to specific attributers, the user should explicitly approve or deny the request. Attestation disclosure policies define which types of RP are allowed by Attestation Provider to access specific attributes from attestation. While these existing policies effectively address user rights, consent, and security, there is a noticeable gap in the area of business-related policies, which are crucial for ensuring the long-term sustainability of the ecosystem. To address this gap, the **Pricing Policy** is introduced in the present document, a guideline that outlines how Service Providers should determine the costs associated with their services or products.

The Pricing Policy would complement existing frameworks by providing clarity and fairness in the pricing of Wallet User's attestation-related services or PID-related services, such as the presentation of attestation. Furthermore, to regulate and organize the market for these attestations, the usage of Attestation Rulebooks catalogue [i.4] is leveraged. This catalogue would serve as a standardized reference for the structure and pricing of different attestations, aligning with broader industry practices and helping to prevent fragmentation in implementation.

The proposed Attestation Cyphered Presentation protocol does not require changes to the existing attestation issuance processes. It is format-agnostic, maintaining compatibility with all available attestation formats. A key advantage of this protocol is its flexibility in supporting various Pricing Policy options. For instance, it enables the selection between various approaches, like:

1) Free-to use attributes

2) Issuance-based fee

3) Verification-based fee

5.2 Attestation metadata extension

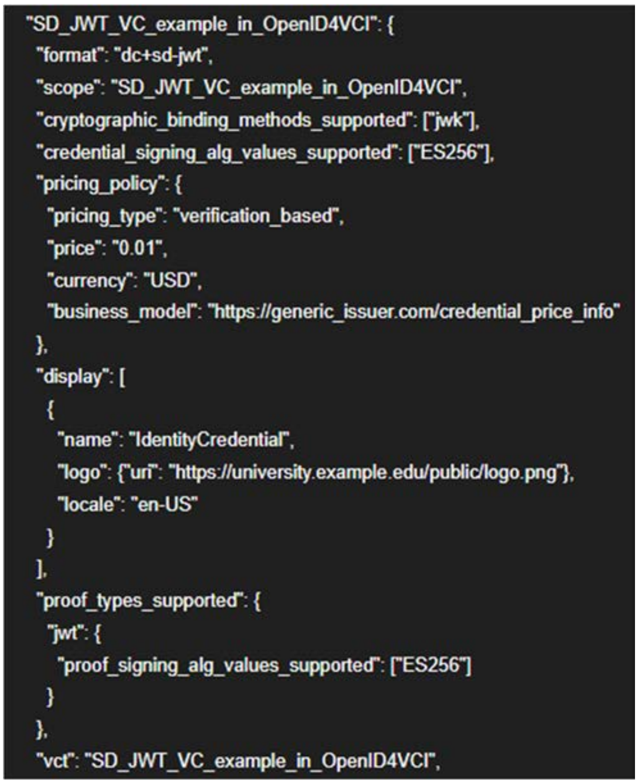
Attestation Providers could utilize the Attestation Rulebooks catalogue to publish their attributes when necessary. This catalogue mitigates the risks of uncontrolled implementation practices that could degrade system quality, increase complexity and maintenance costs. It facilitates the integration of the encrypted attestations approach with verification fees into the **OID4VP** [i.11] protocol. This ensures a more organized, cost-effective, and interoperable ecosystem.

This catalogue would serve as a comprehensive repository of attestation-related information, including **attestation Metadata**, which provides essential details for identifying, verifying, and contextualizing attestations, as well as information on any associated policies. Additionally, a new "**pricing_policy"** parameter could be introduced.

An attestation often includes **embedded disclosure policy**, which consists of a set of rules, embedded in the attestation by its provider, that indicates the conditions that a RP should meet to access the attestation. The pricing policy could originate from the embedded disclosure policy, meaning that the conditions for access to the attestation could include pricing-related criteria.

This pricing policy would allow to specify all relevant details regarding the applied policy, including pricing model, price, currency, and URI linking to the Attestation Provider's detailed policy page.

The following is an example snippet of attestation Metadata, where the metadata for a specific attestation includes a newly proposed parameter "**pricing_policy"**.



```
"SD_JWT_VC_example_in_OpenID4VCI": {
 "format": "dc+sd-jwt",
 "scope": "SD_JWT_VC_example_in_OpenID4VCI",
 "cryptographic_binding_methods_supported": ["jwk"],
 "credential_signing_alg_values_supported": ["ES256"],
 "pricing_policy": {
  "pricing_type": "verification_based",
  "price": "0.01",
  "currency": "USD",
  "business_model": "https://generic_issuer.com/credential_price_info"
 },
 "display": [
  {
   "name": "IdentityCredential",
   "logo": {"uri": "https://university.example.edu/public/logo.png"},
   "locale": "en-US"
  }
 ],
 "proof_types_supported": {
  "jwt": {
   "proof_signing_alg_values_supported": ["ES256"]
  }
 },
 "vct": "SD_JWT_VC_example_in_OpenID4VCI",
```

Figure 2: Attestation Metadata

The proposed solution could also allow to apply different price models:

1) **Static price**, which refers to a pricing strategy where the cost of the service remains unchanged; in practice, a static price is fixed and does not undergo frequent updates. This could be embedded directly into the attribute schema, clearly exposing the unit price per verification. This transparency allows the RP to quickly assess whether they are willing to accept the price or opt not to use the attribute, simplifying decision-making.

2) **Dynamic price**, which refers to a pricing strategy where the cost of the service fluctuates based on various factors. This approach allows businesses to maximize revenue by adjusting prices in real-time or at regular intervals. The affected stakeholders should check a specific URL, periodically updated, where prices are listed. This also allows Attestation Providers to better manage the attributes offering on a daily-basis and/or based on different agreements with several RPs.

The **OID4VP** protocol can be extended to enable interaction with the central registry in the following manner:

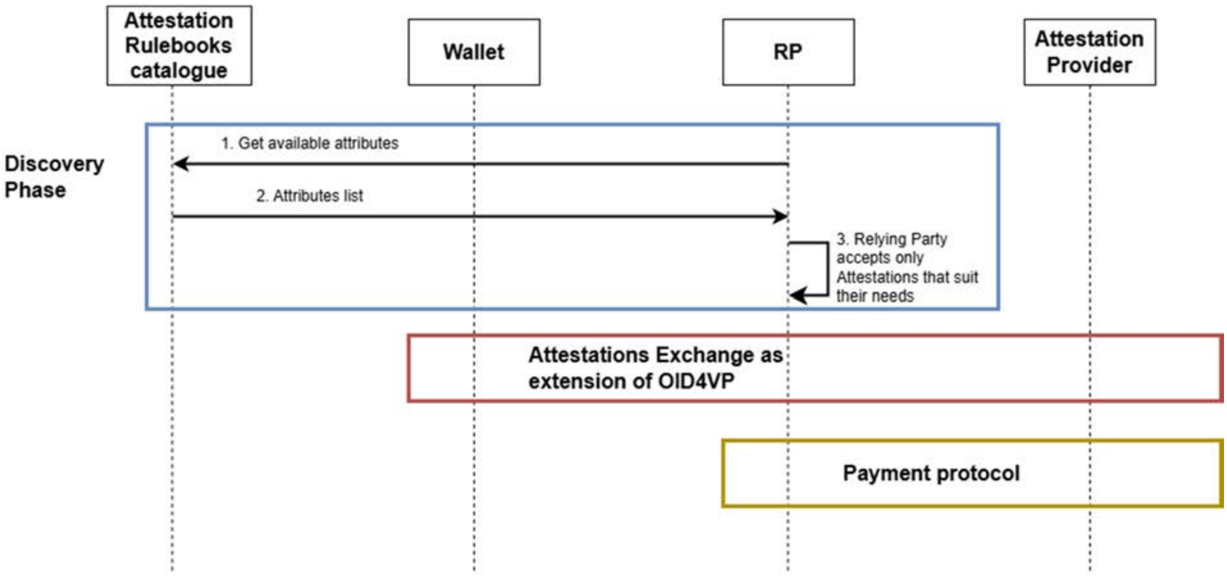

Attestation Rulebooks catalogue
Wallet
RP
Attestation Provider
Discovery Phase
1. Get available attributes
2. Attributes list
3. Relying Party accepts only Attestations that suit their needs
Attestations Exchange as extension of OID4VP
Payment protocol

Figure 3: OID4VP extension for payment scenario

1) **Discovery Phase:** Before a Relying Party (RP) requests a Verifiable Presentation (VP), it queries the central registry to understand the available attributes, Attestation Providers, and associated costs. The RP includes the selected attributes in the request, specifying the willingness to pay associated verification fees.

2) **Attestations Exchange as extension of OID4VP:** Using the Encrypted attestations exchange described in clause 4.3 of the present document.

3) **Verification Cost Exchange:** During the Attestation Provider-RP interaction for decryption and verification, the Attestation Provider verifies whether the payment conditions (if any) are met. A secure payment protocol (e.g. token-based) could be used to process the fee.

6 Security Considerations

1) An overarching issue when dealing with the security of cryptographic systems in use today is the advent of quantum computers, more precisely Cryptographically Relevant Quantum Computers (CRQCs). This kind of computers could break the entire stack on which security is based today, by easily solving the mathematical problems that underpin classical cryptography. This applies both to the well-established RSA scheme and to the Elliptic Curve Cryptography, due to the presence of Shor's Algorithm. Currently this applies to all of the infrastructures providing trust, such as PKIs, and is a general threat that can be faced only through the replacement of the obsolete algorithms used today with quantum-safe ones, such as those approved by NIST in recent times. One well-known attack strategy is the "harvest now, decrypt later", which involves acquiring and stage currently encrypted data within the intention of decrypting it later, once advancements in decryption technology, like the quantum computing, make it accessible. This problem concerns all types of current cryptographic schemes, including the JWE with the cyphered attestation, highlighting the need for a transition to quantum-resistant cryptographic solutions to mitigate these threats.

2) Regardless of considerations about the future advent of quantum computers, a practical security consideration is that only approved curves and parameters should be used, such as those contained in NIST SP 800-56A Rev. 3 [i.9] or other recognized suits are described in ETSI TS 119 312 V1.5.1 [i.2] or in SOG-IS [i.13].

3) The general security of the described mechanism is guaranteed, without taking into account the potential advent CRQCs, by the Discrete Logarithm Problem over Elliptic Curves and by the non-reversibility of the used hash functions.

4) An issue could be the fact that the mechanism of HD keys is not formally standardized (by a formal SDO) but is described in clause 4.4.4.2 of ETSI TR 119 476 [i.3].

5) The mechanism described does not suffer from the well-known weakness of leakage of the private key of the Attestation Provider, as described in BIP 32 [i.1], because this key is never exposed to the public.

7 Privacy Considerations

The mechanism set up so far brings about some considerations regarding privacy, described below:

1) With regard to clause 4.3 about Cyphered Attestation Presentation, it should be highlighted that the Attestation Provider and the RP could collude in order to decrypt the JWE: this is due to the possibility to share the entire JWE with the Attestation Provider.

2) In principle, the Attestation Provider could generate a new private-public key couple for each request of a new attestation. This fact would allow a tracking of the Wallet User's activity by the Attestation Provider, resulting in a concern for the privacy.
Therefore, it would be advisable to control the number of public keys available for the Attestation Provider: if the number of public keys increases over time, this could be an indicator of potentially malicious Attestation Provider's behaviour.

3) The entire mechanism allows for the Users' privacy because:

   - The cryptographic material (e.g. the public key CP in clause 4.3) is not directly generated by the Attestation Provider. It is, instead, derived by the Wallet starting from one of the Attestation Provider's public keys in such a way that the Attestation Provider is not aware of this generation; moreover, several "child" public keys can be generated starting from the same "parent" public key belonging to the Attestation Provider.

   - The Attestation Provider never gets the attestation in plain, unless the RP explicitly shares it with the Attestation Provider, without the User's consent.

4) In the worst-case scenario where the Attestation Provider has issued only one attestation, it would be possible to link the attestation to the Wallet User.

Annex A: Hierarchical Deterministic (HD) Key Derivation

The present clause describes the details of the key derivation already mentioned in clause 4.3 using the well-known "Alice and Bob" scenario, described in clause 4.4.4.2 of ETSI TR 119 476 [i.3].

At first, each of Alice and Bob choose their private-public key pair.
They agree on an elliptic curve of order n over a finite field and with generator G = (G_x, G_y).
Alice has her master private key MS (which is a scalar value) and the corresponding master public key is MP (which is a point on the elliptic curve). The equation that links MS and MP is the following:

$$\mathrm{MP} = \mathrm{MS} \cdot \mathrm{G}$$

where retrieving MS only from MP is deemed to be computationally hard due to the discrete logarithm problem over elliptic curves.

Bob wants to derive "child" public keys CP_1, CP_2, … from MP, without having access to MS and in such a way that Alice can derive the same keys starting from the corresponding "child" private keys CS_1, CS_2, …, each of them derived from MS.

The starting point is the idea, outlined in BIP 32 [i.1], according to which these keys are grouped into a hierarchical structure, for instance a tree, originating from one master key. This applies to private keys and to their public counterparts as well.

More precisely, the mechanism goes as follows:

- The master private key MS is generated in a random way starting from a seed.
- The master public key MP is obtained as mentioned before.
- Child public key CP_1 is obtained from MP in the following way:

$$\mathrm{CP_1} = \mathrm{MP} + \mathrm{HMAC}(\mathrm{MP}, \mathrm{X}) * \mathrm{G}$$

where HMAC is a function that performs hashing through SHA512 algorithm, and successive children CP_2, CP_3, … are derived with the same mechanism but with different values of X, which is a combination of a random nonce produced by Bob and a timestamp;

- Child private key CS_1 is derived from MS using a similar mechanism:

$$\mathrm{CS_1} = \left(\mathrm{MS} + \mathrm{HMAC}(\mathrm{MP}, \mathrm{X})\right) \bmod \mathrm{n}$$

where the only differences with the previous formula are the presence of MS instead of MP and the presence of the modulo operator.

The described mechanism works because CP_1 corresponds to CS_1; in fact:

$$\begin{gathered} \mathrm{CP_1} = \mathrm{MP} + \mathrm{HMAC}(\mathrm{MP}, \mathrm{X}) * \mathrm{G} \\ = (\mathrm{MS} * \mathrm{G}) + \mathrm{HMAC}(\mathrm{MP}, \mathrm{X}) * \mathrm{G} \\ = \left(\mathrm{MS} + \mathrm{HMAC}(\mathrm{MP}, \mathrm{X})\right) * \mathrm{G} \\ = \mathrm{CS_1} * \mathrm{G} \end{gathered}$$

where:

- the second equation derives from the definition of MP;
- the operations in the third equation are performed *mod n*.

The result shows that the public key CP_1 is indeed corresponding to the private key CS_1.

Finally, in order to transpose the described mechanism into the EUDI Wallet ecosystem, it is necessary to recognize that Alice is the Attestation Provider, while Bob is the Wallet User; the RP is a generic third party interested in obtaining Bob's attestations.

The following diagram (Figure A.1) describes the aforementioned entire flow in the EUDI Wallet scenario.

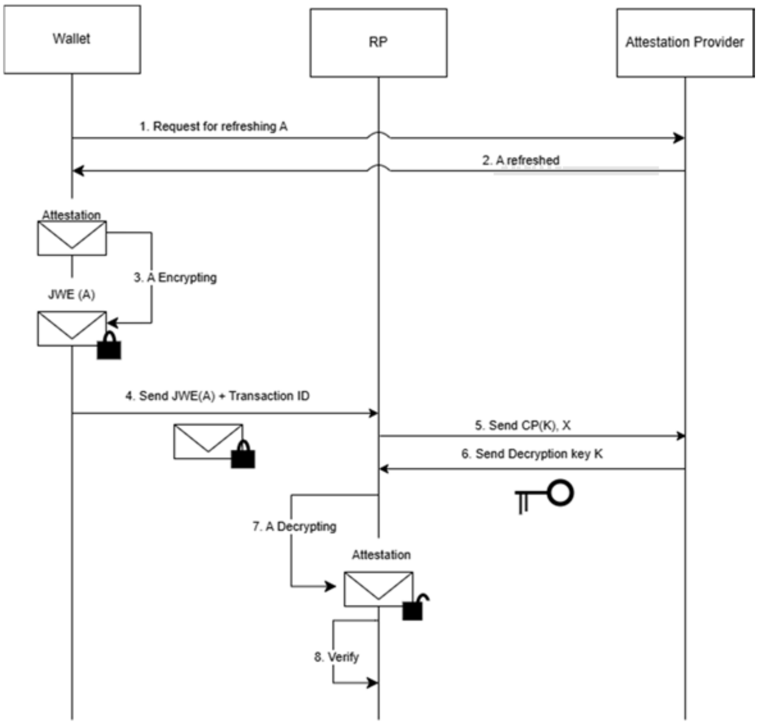


Figure A.1: Attestation Cyphered sequence diagram

History

Document history		
V1.1.1	July 2025	Publication