ETSI TS 119 472-2 V1.1.1 (2025-12)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 2: Profiles for EAA/PID Presentations to Relying Party

Reference

DTS/ESI-0019472-2

Keywords

attribute attestation, digital identity, EUDI Wallet,
trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [5].

Modal verbs terminology

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

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

1 Scope

The present document:

1) Specifies three (3) realizations for Presentations of Electronic Attestation of Attributes (EAAP hereinafter) built on the realizations of Electronic Attestation of Attributes (EAA hereinafter), specified in ETSI TS 119 472-1 [5] namely: SD-JWT VC EAAP, ISO/IEC-mdoc EAAP, and JSON-LD W3C VC EAAP.

NOTE: The realization X509-AC EAAP will be added in the next version of the present document.

2) Specifies two (2) profiles of protocols for allowing Relying Parties (RP hereinafter) to request to the EUDI Wallet EAAPs or Personal Identification Data (PID hereinafter), and the EUDI Wallet to send the requested EAAPs/PIDs to the RP. The profiles are built on the protocols defined in:

   a) ISO/IEC 18013-5 [10].

   b) OpenID4VC-HAIP [11], whose part dealing with presentation of credentials is in turn a profile of OpenID4 VP [7].

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

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

[1] W3C® Recommendation (15 May 2025): "Verifiable Credentials Data Model v2.0".

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

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

[4] IETF RFC 2397: "The 'data' URL scheme". August 1988.

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

[6] IETF RFC 9101: "The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)", August 2021.

[7] OpenID4 VP: "OpenID for Verifiable Presentations 1.0". July 2025.

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

[9] IETF RFC 7516: "JSON Web Encryption (JWE)", May 2015.

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

[11] OpenID4VC-HAIP: "OpenID4VC High Assurance Interoperability Profile 1.0 - draft 04". 19 September 2025.

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

2.2 Informative references

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

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

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

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

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

[i.3] Architecture and Reference Framework (ARF) version 2.4.0.

[i.4] IETF RFC 8152: "CBOR Object Signing and Encryption (COSE)", July 2017.

[i.5] ETSI TS 119 182: "Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[i.6] ETSI TS 119 152-1: "Electronic Signatures and Trust Infrastructures (ESI); CB AdES (CBOR-AdES) digital signatures Part 1: Building blocks and CB-AdES baseline signatures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 119 471 [i.1], ETSI TS 119 472-1 [5], ETSI TR 119 462 [i.2], Architecture and Reference Framework (ARF) version 2.4.0 [i.3] and the following apply:

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

3.2 Symbols

Void.

3.3 Abbreviations

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

CBOR	Concise Binary Object Representation
COSE	CBOR Object Signing and Encryption
DCQL	Digital Credentials Query Language
DM	Data Model
EAA	Electronic Attestation of Attributes
EAAP	Electronic Attestation of Attributes Presentation
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EUDI	European Digital Identity

GEN	General
HAIP	High Assurance Interoperability Profile
HTTP	Hypertext Transfer Protocol
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
JSON-LD W3C VC JOSE	JSON-LD W3C Verifiable Credentials secured with JOSE
JSON-LD W3C VC SD-JWT	JSON-LD W3C Verifiable Credentials secured with SD-JWT
JSON-LD W3C VC	JSON-LD serialized W3C Verifiable Credentials.
JSON-LD W3C VP JOSE	JSON-LD W3C Verifiable Presentations secured with JOSE
JWS	JSON Web Signature
JWT	JSON Web Token
KB	Key Binding
KB-JWT	Key Binding JSON Web Token
LD	Linked Data
mDL	mobile Driving Licence
OIDFVP	OpenID for Verifiable Presentations
PID	Personal Identification Data
REQ	Request
RO	Request Object
RP	Relying Party
SD	Selective Disclosure
SD-JWT VC	Selective Disclosure based JSON Web Token Verifiable Credentials
SD-JWT	Selective Disclosure based on JSON Web Token
SD-JWT+KB	SD-JWT with a Key Binding JWT
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VP	Verifiable Presentation
W3C VC DM	W3C Verifiable Credentials Data Model
WU	Wallet Unit
X509-AC	X.509 Attribute Certificate

4 Implementation of Electronic Attestation of Attributes Presentations

4.1 EAAP implementation based on SD-JWT VC

The present clause specifies a realization of EAAP for the SD-JWT VC EAA defined in clause 5 of ETSI TS 119 472-1 [5].

The EAAPs implemented according to the present clause will be designated as SD-JWT VC EAAP hereinafter.

EAAP-SD-JWT VC-01: If the SD-JWT VC EAA contains the `cnf` claim, the corresponding SD-JWT VC EAAP shall be a SD-JWT+KB as specified IETF SD-JWT [2].

EAAP-SD-JWT VC-02: If the SD-JWT VC EAA does not contain the `cnf` claim, the corresponding SD-JWT VC EAAP shall be a SD-JWT VC EAAP as specified in IETF SD-JWT [2].

EAAP-SD-JWT VC-03: If the SD-JWT VC EAA does not contain the `cnf` claim, the EAA subject binding shall be ensured by other means (e.g. claims-base binding, biometric-base binding).

EAAP-SD-JWT VC-04: A SD-JWT VC EAAP shall be serialized using either the Compact Serialization, as specified in clause 5.2 of IETF SD-JWT [2], or the Flattened JSON Serialization, as specified in clause 8.2 of IETF SD-JWT [2].

EAAP-SD-JWT VC-05: The Key Binding JSON Web Token (KB-JWT) of a SD-JWT VC EAAP (which is a SD-JWT+KB) shall be signed by the EAA subject.

4.2 EAAP implementation based on ISO/IEC-mdoc

The present clause specifies a realization of EAAPs for the ISO/IEC-mdoc EAAs defined in clause 6 of ETSI TS 119 472-1 [5].

NOTE 1: Clause 6 of ETSI TS 119 472-1 [5] defines different requirements for ISO/IEC-mdoc EAAs that are mobile driving licenses (mDL) and ISO/IEC-mdoc EAAs that are NOT mDLs in terms of data elements and their namespaces. See that document for more details.

The EAAPs implemented according to the present clause will be designated as ISO/IEC 18013-5 [10] EAAP hereinafter.

ISO/IEC 18013-5 [10] requires that the mdoc (the EUDI Wallet) builds an instance of type `DeviceResponse` in response to a correct instance of type `DeviceRequest` sent by the mdoc reader/verifier (a Relying Party).

This instance of `DeviceResponse` type can contain the `documents` member, which is an array of instances of type `Document`.

Each element in this array can contain an indication of error if the request of that element was not correctly built or any other problem has occurred during the processing of the request by the mdoc or during the generation of the corresponding document.

EAAP-ISO/IEC-mdoc-01: Each element in the `documents` member of an instance of type `DeviceResponse` as defined in clause 10.3.3 of ISO/IEC 18013-5 [10] that does not contain the `errors` member shall be an ISO/IEC-mdoc EAAP if the mentioned element does not contain the `errors` member.

NOTE 2: As each element in the `documents` member of an instance of type `DeviceResponse` is of type `Document`, an ISO/IEC-mdoc EAAP is an instance of type `Document` that does not contain the `errors` member.

EAAP-ISO/IEC-mdoc-02: The `deviceAuth` member of the `deviceSigned` member of the ISO/IEC-mdoc EAAP shall contain the `deviceSignature` child member.

4.3 EAAP implementation based on JSON-LD W3C VC DM

4.3.1 Introduction

The present clause specifies requirements for generating EAAPs for the JSON-LD W3C VC EAA specified in clause 7 of ETSI TS 119 472-1 [5].

These EAAPs shall be generated as specified in W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [3]. This W3C Recommendation defines how to secure JSON-LD W3C Verifiable Credentials and JSON-LD W3C Verifiable Presentations either with JWS (the W3C Recommendation uses JOSE), or with SD-JWT.

The EAAPs specified in clause 4.3.2 of the present document use JWS signatures as specified in IETF RFC 7515 [8], for generating EAAPs of both JSON-LD W3C VC JOSE EAAs and JSON-LD W3C VC SD-JWT EAAs. These EAAPs will be designated as JSON-LD W3C VP JOSE EAAPs.

4.3.2 JOSE-signed JSON-LD W3C EAAPs for JSON-LD W3C EAAs

The present clause specifies requirements for generating presentations, signed by the EAA subject, of JSON-LD W3C VC JOSE EAAs specified in clause 7.6.4.2 of ETSI TS 119 472-1 [5].

EAAP-JSON-LD W3C VP JOSE-01: A JSON-LD W3C VC JOSE EAAP shall meet the requirements defined in: clause 4.13 of "Verifiable Credentials Data Model v2.0" [1], clause 3.1.2 of W3C Recommendation (15 May 2025): "Securing Verifiable Credentials using JOSE and COSE" [3], and the requirements defined in the present clause.

EAAP-JSON-LD W3C VP JOSE-02: A JSON-LD W3C VC JOSE EAAP shall be a JWS signature generated by the EAA subject.

EAAP-JSON-LD W3C VC JOSE-03: The payload of a JSON-LD W3C VC JOSE EAAP shall be an object meeting the requirements defined in clause 4.13 of "Verifiable Credentials Data Model v2.0" [1].

EAAP-JSON-LD W3C VP JOSE-04: The payload of a JSON-LD W3C VC JOSE EAAP shall have the `verifiableCredential` property.

NOTE 1: The `verifiableCredential` property is defined in clause 4.13 of [1] as an array. Each element of the `verifiableCredential` array encapsulates either a sequence of one or more JSON-LD W3C VC JOSE EAAs or a sequence of one or more JSON-LD W3C VC SD-JWT EAA as specified in clause 7 of ETSI TS 119 472-1 [5].

EAAP-JSON-LD W3C VP JOSE-05: Each element in the `verifiableCredential` array shall have the `type`, `@context`, and `id` properties.

EAAP-JSON-LD W3C VP JOSE-06: The `type` property child of each element in the `verifiableCredential` array shall have the value `EnvelopedVerifiableCredential`.

NOTE 2: This value signals that each element in the `verifiableCredential` array contains signed JSON-LD W3C VC JOSE EAAs and/or JSON-LD W3C VC SD-JWT EAAs as specified in clause 7 of ETSI TS 119 472-1 [5].

EAAP-JSON-LD W3C VP JOSE-07: The `id` property child of each element in the `verifiableCredential` array shall contain one or more data URIs as specified in IETF RFC 2397 [4].

EAAP-JSON-LD W3C VP JOSE-08: Each data URI within the `id` property shall be separated from the next one by the ';' character.

EAAP-JSON-LD W3C VC JOSE-09: If the URI encapsulates a sequence of one or more JSON-LD W3C VC JOSE EAAs then the media type of the `id` property shall be `application/vc+jwt`.

NOTE 3: These values declare that the data URL encapsulates a sequence of one or more JSON-LD W3C VC JOSE EAAs.

EAAP-JSON-LD W3C VC JOSE-10: If the URI encapsulates a sequence of one or more JSON-LD W3C VC SD-JWT EAAs then the media type of the `id` property shall be `application/vc+sd-jwt`.

NOTE 4: These values declare that the data URL encapsulates a sequence of one or more JSON-LD W3C VC SD-JWT EAAs.

EAAP-JSON-LD W3C VP JOSE-11: All the signed JSON-LD W3C VC EAAs in the data part of the data URL of the `id` property shall use the same Serialization, either the Compact Serialization or the base64 encoding of the Flattened JSON.

EAAP-JSON-LD W3C VP JOSE-12: If all the signed JSON-LD W3C VC EAAs in the data part of the data URL of the `id` property are base64 encoding of the Flattened JSON Serialization mentioned before, the string "`;base64,`" shall be inserted between the value of the media type and the data part.

NOTE 5: As a consequence of the former requirements JSON-LD W3C VC EAAs using Compact Serialization and JSON-LD W3C VC EAAs using Flattened JSON Serialization, are placed in different elements of the `verifiableCredential` array.

NOTE 6: Therefore, each object in the `verifiableCredential` array encapsulates a sequence of one or more JSON-LD W3C VC JOSE EAAs or a sequence of one or more JSON-LD W3C VC SD-JWT EAAs as specified in clause 7 of ETSI TS 119 472-1 [5].

4.4 EAAP implementation based on X.509 Attribute Certificates (X509-AC)

NOTE: To be completed in later versions. A possible solution would be to use an enveloping JAdES signature, specified in ETSI TS 119 182 [i.5], with the `srAttrs` header parameter, enclosing the `certified` member containing an array of X.509 Attribute certificates. Also other solutions need to be investigated.

5 ISO/IEC 18013-5 proximity presentation flows

5.1 Introduction

Clause 5 and its subclauses define a profile for a EAAP response/request built on ISO/IEC 18013-5 [10].

5.2 General requirements

ISO/IEC 18013-5-GEN-01: The ephemeral key pair built during the device engagement phase shall be an ECDH-ES agreed elliptic curve key of type P-256.

ISO/IEC 18013-5-GEN-02: This ephemeral key pair built during the device engagement phase shall use the ECDSA algorithm.

ISO/IEC 18013-5-GEN-03: If the present document modifies a requirement in OpenID4VC-HAIP [11], the modified requirement defined by the present document shall prevail.

NOTE: This allows, for instance, that the present document converts in mandatory an optional requirement from OpenID4VC-HAIP [11] or extends mandatory requirements. Note that OpenID4VC-HAIP [11] also defines requirements for presenting ISO/IEC-mdoc EAAs.

EXAMPLE: The present document extends the crypto suite required by OpenID4VC-HAIP [11].

ISO/IEC 18013-5-GEN-04: The EUDI Wallet and the Relying Parties message shall support the A128GCM algorithm and the A256GCM algorithm.

5.3 ISO/IEC-mdoc proximity EAAP Request profile

ISO/IEC 18013-5-REQ-01: The RP shall send to the WU a `DeviceRequest` message as specified in ISO/IEC 18013-5 [10] for requesting the presentation of one or more EAAs.

ISO/IEC 18013-5-REQ-02: The `docRequests` array child member of `DeviceRequest` shall not be empty.

ISO/IEC 18013-5-REQ-03: All the elements of the `docRequests` array shall contain the `readerAuth` member.

NOTE 1: ISO/IEC 18013-5 [10] defines `readerAuth` member as an instance of `ReaderAuth` type, which makes equal to `COSE_Sign1` type defined in IETF RFC 8152 [i.4]. Therefore `readerAuth` is a digital signature.

ISO/IEC 18013-5-REQ-04: The digital signature implemented in the `readerAuth` shall be generated with the ECDSA algorithm using a P-256 elliptic curve.

ISO/IEC 18013-5-REQ-05: The digital signature implemented in `readerAuth` shall be generated with the private key whose corresponding public key is enclosed within the RP access certificate.

NOTE 2: ETSI TC ESI is currently developing ETSI TS 119 152-1 [i.6], a CBOR format for AdES signatures (CB-AdES). Once this document is published, ETSI TC ESI will reassess the suitability of requiring that these signatures are CB-AdES-B-B.

ISO/IEC 18013-5-REQ-06: The digital signature implemented in `readerAuth` shall include the `x5chain` parameter in the unprotected header.

ISO/IEC 18013-5-REQ-07: The `x5chain` unprotected header parameter shall contain the RP access certificate in its first element, and its certificate path up to, but excluding, the trust anchor.

ISO/IEC 18013-5-REQ-08: The instances of type `ItemsRequest`, encapsulated in the elements in the `docRequests` member, shall contain a non-empty `requestInfo` member (which is a CBOR map).

NOTE 3: All the elements in the `docRequests` member are instances of type `ItemsRequest` encapsulated in a CBOR byte string (type `ItemsRequestBytes`).

ISO/IEC 18013-5-REQ-09: The mentioned `requestInfo` member shall contain a member with label "`euWrprc`".

ISO/IEC 18013-5-REQ-10: The member with label "`euWrprc`" shall map the label "`euWrprc`" to a CBOR byte string.

ISO/IEC 18013-5-REQ-11: The CBOR byte string mapped to the "`euWrprc`" label shall contain the serialization of the RP registration certificate.

NOTE 4: This new member is required for incorporating the RP registration certificate(s), which are placed in an extension of the `requestInfo`.

5.4 ISO/IEC 18013-5 proximity EAAP Response profile

ISO/IEC 18013-5-RESP-01: In response to a `DeviceRequest` message sent by the RP, the WU shall generate a `DeviceResponse` message as specified in ISO/IEC 18013-5 [10].

ISO/IEC 18013-5-RESP-02: All the disclosed attested attributes shall be present in the `issuerSigned` member of the `DeviceResponse` message.

ISO/IEC 18013-5-RESP-03: The `deviceSigned` member of the `DeviceResponse` message shall not contain any attested attribute.

NOTE 1: Therefore, the `deviceSigned` member is devoted to contain transaction specific data.

ISO/IEC 18013-5-RESP-04: The `DeviceResponse` message shall be encrypted with either the A128GCM algorithm or the A256GCM algorithm.

NOTE 2: This requirement extends the requirement specified by clause 5 of OpenID4VC-HAIP [11].

ISO/IEC 18013-5-RESP-05: The `deviceAuth` child member of the `deviceSigned` shall contain the `deviceSignature` child member.

NOTE 3: ISO/IEC 18013-5 [10] defines `deviceSignature` as an instance of type `DeviceSignature`, and makes `DeviceSignature` equal to `COSE_Sign1`.

ISO/IEC 18013-5-RESP-06: The signature implemented in `deviceSignature` shall be generated with the private key of the EUDI Wallet user whose associated public key is present in the `deviceKeyInfo` member of the instance of type `MobileSecurityObject` present within the `issuedSigned` member of the `DeviceResponse`.

NOTE 4: This ensures that the EAAP is actually signed by the EAA subject with the private key owned by the EAA subject.

6 Remote presentation flows

6.1 Introduction

Clause 6 and its subclauses define a profile of a protocol that allows Relying Parties (RP hereinafter) to request to the EUDI Wallet EAAPs or Personal Identification Data (PID hereinafter), and the EUDI Wallet to send the requested EAAPs to the RP.

This protocol profile is built on OpenID4VC-HAIP [11], clause 5.1.

6.2 General requirements

GEN-REQ-01: The EUDI Wallet shall implement the profile of the protocol defined in OpenID4VC-HAIP [11], clause 5.1.

GEN-REQ-02: The Relying Parties shall implement the profile of the protocol defined in OpenID4VC-HAIP [11], clause 5.1.

NOTE 1: The present document profiles and adds EUDI Wallet-specific requirements; new requirements are provided only where OpenID4VC-HAIP [11] is silent.

GEN-REQ-03: If the present document modifies a requirement in OpenID4VC-HAIP [11], the modified requirement defined by the present document shall prevail.

NOTE 2: This allows, for instance, that the present document converts in mandatory an optional requirement from OpenID4VC-HAIP [11] or extends mandatory requirements.

EXAMPLE: The present document extends the crypto suite required by OpenID4VC-HAIP [11].

GEN-REQ-04: The EUDI Wallet and the Relying Parties message shall support the A128GCM algorithm and the A256GCM algorithm.

NOTE 3: OpenID4VC-HAIP [11] requires support to P-256 key type and ES256 algorithm to both the EUDI Wallet and the Relying Parties.

6.3 Authorization Request (EAAP request) profile

6.3.1 Common requirements

6.3.1.1 Introduction

Clause 6.3.1 and its subclauses define requirements that apply regardless of the EAA implementation (SD-JWT VC EAA, ISO/IEC-mdoc EAA, and JSON-LD W3C-VC EAA) whose presentation is requested.

6.3.1.2 General requirements

OIDFVP-HAIP_COMMON_GEN_REQ-01: The WU shall support at least a custom URL scheme "`eu-eaap://`" for its `authorization_endpoint`.

OIDFVP-HAIP_COMMON_GEN_REQ-02: The Authorization Request shall use the Client Identifier Prefix `x509_hash`.

OIDFVP-HAIP_COMMON_GEN_REQ-03: The possible values for the `format` claim within the `dcql_query` shall be: "`dc+sd-jwt`", "`mso_mdoc`", "`x509_attr`", "`jwt_vc_json`", and "`vp+jwt`".

OIDFVP-HAIP_COMMON_GEN_REQ-04: For requesting a SD-JWT VC EAAP as specified in clause 4.1 of the present document, the `format` claim shall have the value "`dc+sd-jwt`".

OIDFVP-HAIP_COMMON_GEN_REQ-05: For requesting an ISO/IEC-mdoc EAAP as specified in clause 4.2 of the present document the `format` claim shall have the value "`mso_mdoc`".

OIDFVP-HAIP_COMMON_GEN_REQ-06: For requesting a JWS-signed W3C VC EAAP not using JSON-LD, as specified in clause B.1.3.1 of OpenID4 VP [7], the `format` claim shall have the value "`jwt_vc_json`".

OIDFVP-HAIP_COMMON_GEN_REQ-07: For requesting a JSON-LD W3C VP JOSE EAAP, as specified in clause 4.3 of the present document, the `format` claim shall have the value "`vp+jwt`".

6.3.1.3 Requirements for the Authorization Request message

OIDFVP-HAIP_COMMON_AR_REQ-01: The Authorization Request shall contain the `request_uri` parameter, and therefore shall not contain the Request Object (RO).

NOTE: The Request Object is passed by reference to the WU.

OIDFVP-HAIP_COMMON_AR_REQ-02: The Authorization Request shall contain the `request_uri_method` parameter.

OIDFVP-HAIP_COMMON_AR_REQ-03: The Authorization Request shall contain the `client_id` parameter.

6.3.1.4 Requirements for the Request Object

OIDFVP-HAIP_COMMON_RO_REQ-01: The RO shall be a JWT as specified in IETF RFC 9101 [6] signed with a JWS signature.

OIDFVP-HAIP_COMMON_RO_REQ-02: The RO JWT body shall contain the `response_uri` parameter.

NOTE 1: The value of the `response_uri` parameter is the URI where the WU returns the encrypted Authorization Response.

OIDFVP-HAIP_COMMON_RO_REQ-03: The RO JWT body shall contain the `response_mode` parameter.

OIDFVP-HAIP_COMMON_RO_REQ-04: The value of the `response_mode` parameter shall be "`direct_post.jwt`".

NOTE 2: The WU returns the encrypted Authorization Response including the EAAP sending an HTTP POST Request. The response is encrypted using JWS.

OIDFVP-HAIP_COMMON_RO_REQ-05: If required, the `verifier_info` parameter shall be placed within the RO JWT body.

OIDFVP-HAIP_COMMON_RO_REQ-06: If the RP has a registration certificate, the `verifier_info` parameter shall be present within the RO JWT body.

OIDFVP-HAIP_COMMON_RO_REQ-07: The element in the `verifier_info` array enclosing the registration certificate shall be a JSON Object which shall not contain the `credential_ids` member.

OIDFVP-HAIP_COMMON_RO_REQ-08: The value of the `format` member of the element in the `verifier_info` array enclosing the registration certificate shall be: "`registration_cert`".

OIDFVP-HAIP_COMMON_RO_REQ-09: The value of the `data` member of the element in the `verifier_info` array enclosing the registration certificate shall be the base64url encoding of the serialized RP registration certificate.

OIDFVP-HAIP_COMMON_RO_REQ-10: The RO JWT body shall contain the `client_metadata` parameter.

OIDFVP-HAIP_COMMON_RO_REQ-11: The `client_metadata` parameter shall contain the `jwks` member.

OIDFVP-HAIP_COMMON_RO_REQ-12: The `jwks` member shall contain the `kid` and `use` parameters for identifying the key and the use of the identified key, respectively.

OIDFVP-HAIP_COMMON_RO_REQ-13: The `kid` parameters shall univocally identify one key.

NOTE 3: Clause 6.2 specifies the key types and the algorithms for the present profile.

OIDFVP-HAIP_COMMON_RO_REQ-14: The RO JWT body shall contain the `nonce` parameter.

OIDFVP-HAIP_COMMON_RO_REQ-15: The RO JWT body shall contain the `client_id` parameter.

OIDFVP-HAIP_COMMON_RO_REQ-16: The RO JWT body should contain the `state` parameter.

OIDFVP-HAIP_COMMON_RO_REQ-17: The RO JWT body shall contain the `dcql_query` parameter.

OIDFVP-HAIP_COMMON_RO_REQ-18: The Authority Key Identifier (aki)-based Trusted Authority Query(trusted_authorities) for DCQL shall use the ETSI trusted Lists mechanism as specified in ETSI TS 119 612 [12].

OIDFVP-HAIP_COMMON_RO_REQ-19: The RO shall be signed by the RP using the private key whose corresponding public key is enclosed within the RP access certificate.

OIDFVP-HAIP_COMMON_RO_REQ-20: The JWS Protected Header of the JWS signature on the RO, shall incorporate the `x5c` header parameter.

OIDFVP-HAIP_COMMON_RO_REQ-21: The x5c header parameter in the JWS Protected Header of the JWS signature on the RO shall contain the RP access certificate in its first element, and its certificate path up to, but excluding, the trust anchor.

OIDFVP-HAIP_COMMON_RO_REQ-22: The JWS Protected Header of the JWS signature on the RO shall incorporate the iat header parameter.

OIDFVP-HAIP_COMMON_RO_REQ-23: The RO JWT body shall contain the aud parameter.

6.3.2 Specific requirements when requesting ISO/IEC 18013-5 EAAP

OIDFVP-HAIP-ISO/IEC_18013_5_REQ-01: The requirements specified in OpenID4 VP [7], Appendix B.2, shall apply, unless stated otherwise by requirements in the present clause.

6.3.3 Specific requirements when requesting W3C VC EAAP

OIDFVP-HAIP-W3C_VC_REQ-02: The requirements specified in OpenID4 VP [7], Appendix B.1, shall apply.

6.4 Authorization Response (EAAP response) profile

6.4.1 Common requirements

OIDFVP-HAIP_COMMON_RESP-01: The WU shall encrypt the authorization response.

OIDFVP-HAIP_COMMON_RESP-02: The authorization response shall include the vp_token parameter, as specified in clause 8 of OpenID4 VP [7].

OIDFVP-HAIP_COMMON_RESP-03: The vp_token parameter, shall contain one or more EAAPs.

OIDFVP-HAIP_COMMON_RESP-04: The authorization response may include other parameters, as specified in clause 8.1 of OpenID4 VP [7].

OIDFVP-HAIP_COMMON_RESP-05: All the EAAPs included in the authorization response shall be signed by the EAA subject.

OIDFVP-HAIP_COMMON_RESP-06: The authorization response shall be encrypted using IETF RFC 7516 [9] as specified in clause 8.3 of OpenID4 VP [7].

OIDFVP-HAIP_COMMON_RESP-07: The encrypted authorization response shall be sent via an HTTP POST request to the endpoint whose URI is the value of the parameter response_uri of the authorization request.

OIDFVP-HAIP_COMMON_RESP-08: If the RP successfully process the EAAP returned in the authorization response, the RP shall respond to the wallet with an HTTP POST response with status code 200, Content-type parameter set to the value application/json, and a JSON Object in its body, which shall have the redirect_uri member.

OIDFVP-HAIP_COMMON_RESP-09: The value of the redirect_uri member of the JSON Object present in the HTTP POST response with status code 200 shall be an URI, where the wallet shall redirect the user agent.

7 Security considerations

The security considerations in clause 14 of OpenID4 VP [7] apply.

Annex A (normative): Transaction data for authorization

A.1 Introduction

The present annex specifies transaction data for managing authorization of the EUDI Wallet user to a RP to either execute a payment (clause A.2) or to generate an electronic signature, Qualified Electronic Signature or Advanced Electronic Signature, for instance (clause A.3).

A.2 Payment authorization

NOTE: This will be completed in the next version.

A.3 Electronic signature authorization

NOTE: This will be completed in the next version.

Annex B (informative): Change history

Date	Version	Information about changes
29/7/2025	0.0.1	First version July 2025.
31/7/2025	0.0.2	Added ISO/IEC 18013-5 proximity presentation flows. Added Annex A on Transaction Data for authorization (empty annex for the moment) Added requirements on transaction data to OpenID4VP authorization request profile.
29/9/2025	0.0.3	This version builds one of the protocols directly on HAIP without repeating its requirements (dropped requirements defined in HAIP). Implemented dispositions to comments raised to version v0.0.2.
6/10/2025	0.0.4	Final version for RC after dealing with all the comments raised to v0.0.3.

History

Document history		
V1.1.1	December 2025	Publication