PID Rule Book

for the EUDI Wallet ecosystem

v1.0.0

This is a working document that holds no legal value and does not reflect any common agreement or position of the co-legislators. It presents a state-of-play of ongoing work of the eIDAS Expert Group. This document is being continuously updated and should not be considered final.

1 Introduction

1.1 Scope

This document is the Person Identification Data (PID) Rule Book. It contains requirements specific to the PID use case within the EUDI Wallet. These requirements hold in addition to the requirements in the Architecture Reference Framework (ARF), see [ARF]. Requirements in the ARF hold **for all** use cases in the EUDI Wallet.

This PID Rule Book contains the following topics:

- Chapter 2 specifies the PID attribute schema. This describes the structure, the type, the entity identifiers, and the logical organization of the mandatory and optional attributes of the PID. It also describes how Member States can specify any possible national attributes. Two encodings for these attributes are specified, one compliant with [ISO18013-5], the other compliant with [SD-JWT].
- Chapter 3 specifies the Wallet Instance attestation schema, which describes the same information for the Wallet Instance attestation signed by the Wallet Provider for each Wallet Instance. This information will be moved to another document in the future.
- Chapter 4 specifies details about the trust infrastructure necessary for PID attestations, for both ISO/IEC 18013-5-compliant and SD-JWT-compliant encodings. This information may be moved to another document in the future.

Further topics will be added if and when they are identified.

1.2 Key words

This document uses the capitalized key words ‘SHALL’, ‘SHOULD’ and ‘MAY’ as specified in [RFC 2119], i.e., to indicate requirements, recommendations and options specified in this document.

In addition, ‘must’ (non-capitalized) is used to indicate an external constraint, i.e., a requirement that is not mandated by this document, but, for instance, by an external document such as [ARF]. The word ‘can’ indicates a capability, whereas other words, such as ‘will’, and ‘is’ or ‘are’ are intended as statements of fact.

1.3 Terminology

This document uses the terminology specified in [ARF].

2 PID attribute schema

2.1 Overview

This chapter describes the structure, type, data element identifiers and logical organisation of the mandatory and optional attributes of the PID attestation within the EUDI Wallet, as well as the PID metadata:

- Section 2.2 specifies the document type and namespace(s) for a PID attestation:
  - Section 2.2.1 specifies the PID document type, as well as the EU-wide PID namespace within which the PID data elements defined in this document are specified.
  - Section 2.2.2 describes how Member States can specify national attributes by defining a domestic PID namespace.
- Section 2.3 specifies the set of data elements covering the PID attributes specified in [ARF].
- Section 2.4 similarly specifies the set of data elements covering the PID metadata.
- Section 2.5 specifies two different encodings for these data elements. The first encoding uses Concise Binary Object Representation (CBOR) and complies with ISO/IEC 18013-5:2021 [ISO18013-5]. The second encoding uses JSON and complies with [SD-JWT] and [OpenID4VP].

2.2 Document type and namespace

2.2.1 EU-wide document type and namespace for PID attestation

The concepts of document type and namespace, and the way in which they are used, are specified in ISO/IEC 18013-5. These concepts are used in the same way in OpenID for Verifiable Presentations [OpenID4VP].

PID Providers SHALL use the document type “eu.europa.ec.eudi.pid.1” for PID attestations. This value follows the recommendation in ISO/IEC 18013-5 to use the general format [Reverse Domain].[Domain Specific Extension]. Since the European Commission controls the domain ec.europa.eu, this document type value will not collide with any document type potentially defined by other organisations. The version number “1” in this document type MAY be used to distinguish between the first version of the ISO-compliant PID attribute (defined in this document) and any future version.

Similarly, PID Providers SHALL use the value “eu.europa.ec.eudi.pid.1” for the namespace of the first version of the PID attributes and PID metadata specified in sections 2.3 and 2.4[1]. This namespace clearly indicates that any data elements defined within it are Person Identification Data specified in the context of the EUDI Wallet. Again, the version number “1” allows for future extension(s) or change(s) of the PID data elements defined the next section.

PID Providers SHALL use this document type and namespace for the ISO/IEC 18013-5 compliant data element encoding specified in section 2.5.2 and for the SD-JWT-compliant encoding in section 2.5.3.

[1] Note that the document type and namespace have the same value. This is allowed according to ISO/IEC 18013-5.

2.2.2 Domestic PID namespaces for national attributes

ISO/IEC 18013-5 specifies a mechanism called **domestic namespaces**, allowing PID Providers to issue such national attributes to an EUDI Wallet. To do so, a PID Provider SHALL define a domestic PID namespace. Within that namespace, the PID Provider is free to define any attribute it needs, for example, a national social security number or taxpayer identification number (TIN).

If a PID Provider chooses to define a domestic namespace, it SHALL append the applicable ISO 3166-1 alpha-2 country code or the ISO 3166-2 region code, separated by a period, to the EU-wide PID namespace, excluding the version number. The PID Provider MAY include a version number in the domestic namespace.

EXAMPLE: The first domestic PID namespace for Germany could be “eu.europa.ec.eudi.pid.de.1”.

PID Providers SHALL use the same domestic namespace for both ISO/IEC 18013-5-compliant PIDs and SD-JWT-compliant PIDs, see section 2.5.

A PID Provider that defines a domestic namespace SHALL publish the namespace, including all data element identifiers, their definition, presence and encoding format, on a website that is publicly available. A central registry for such domestic namespace definitions MAY be established in the future.

2.3 PID attributes

2.3.1 Introduction

Data elements corresponding to the PID attributes specified in [ARF] are defined in Table 1 in section 2.3.2. Data elements corresponding to the PID metadata specified in [ARF] are defined in Table 2 in section 2.4.1.

Note that the metadata data elements defined in section 2.4.1 are handled by PID Providers, PID Users and Relying Parties in exactly the same way as the data elements corresponding to the PID attributes in Table 1. There is no technical difference between these data elements. The only reason to distinguish between PID attributes and PID metadata is because the ARF makes this distinction.

Table 1 and Table 2 contain the following information:

- The first column of both tables lists all PID attributes and PID metadata (respectively) specified in section 5.1.1.1 of [ARF].
- For each of these attributes and metadata, the second column specifies the identifiers of one or more corresponding data elements. In case more than one data element is specified for a single PID attribute or metadata, the reasons for this are explained in the subsection referenced in the first column. The data element identifiers in the second column SHALL be used in requests and responses according to [ISO18013-5] or [OpenID4VP], as applicable. There SHALL be at most one data element with the same data element identifier in each PID attribute.

  NOTE: Data element values MAY be multi-value. If so, this is clearly indicated.
- The third column describes the meaning of the data element.

- The fourth column specifies whether the presence of the element in a PID attribute is mandatory (M), or optional (O).

  NOTE: If Table 1 or Table 2 indicates a data element as mandatory, this solely means that the PID Provider SHALL ensure that this element is present in the PID. It does not imply that a Relying Party is required to request such a data element when interacting with the Wallet Instance. Neither does it imply that the PID User cannot refuse to release a mandatory data element if requested.

  > The detailed process for identity matching, especially for cross-border use cases will be detailed in a future version of ARF. The Presence property (M/O) of each attribute in Table 1 will be revisited.

- The fifth column indicates how the data elements SHALL be encoded, using the CDDL representation types defined in [RFC 8610]. Section 2.5. specifies how these representation types SHALL be serialized into CBOR and JSON data structures, respectively. Note the following:
  - `tstr`, `uint`, `bstr`, `bool` and `tdate` are CDDL representation types defined in [RFC 8610].
  - All data elements having encoding format `tstr` SHALL have a maximum length of 150 characters.
  - This document specifies `full-date` as `full-date = #6.1004(tstr)`, where tag 1004 is specified in [RFC 8943].
  - In accordance with [RFC 8949], section 3.4.1, a `tdate` data element shall contain a `date-time` string as specified in [RFC 3339]. In accordance with [RFC 8943], a `full-date` data element shall contain a `full-date` string as specified in [RFC 3339].
  - The following requirements SHALL apply to the representation of dates in data elements, unless otherwise indicated:
    - Fractions of seconds SHALL NOT be used;
    - A local offset from UTC SHALL NOT be used; the `time-offset` defined in [RFC 3339] SHALL be to “Z”.

2.3.2 Overview

PID attribute in [ARF]	Corresponding data element identifier(s)	Definition	Presence	Encoding format
Current Family Name				
	family_name	Current last name(s) or surname(s) of the PID User.	M	tstr
Current First Names				
	given_name	Current first name(s), including middle name(s), of the PID User.	M	tstr
Date of Birth (See section 2.3.3)				
	birth_date	Day, month, and year on which the PID User was born. [2]	M	full-date
	age_over_18	Attesting whether the PID User is currently an adult (true) or a minor (false).	O	bool
	age_over_NN	Additional current age attestations, NN <> 18.	O	bool
	age_in_years	The current age of the PID User in years.	O	uint
	age_birth_year	The year when the PID User was born. [3]	O	uint
Family Name at Birth				
	family_name_birth	Last name(s) or surname(s) of the PID User at the time of birth.	O	tstr
First Names at Birth				
	given_name_birth	First name(s), including middle name(s), of the PID User at the time of birth.	O	tstr

[2] Please note that the current specification does not yet foresee a solution for the situation when the date of birth of the User is incomplete or unknown. Work is ongoing to find a solution to this scenario, in alignment with current implementation of eIDAS nodes.

[3] See footnote 2.

PID attribute in [ARF]	Corresponding data element identifier(s)	Definition	Presence	Encoding format
Place of Birth (See section 2.3.4)				
	`birth_place`	The country, state, and city where the PID User was born.	O	`tstr`
	`birth_country`	The country where the PID User was born, as an Alpha-2 country code as specified in ISO 3166-1.	O	`tstr`
	`birth_state`	The state, province, district, or local area where the PID User was born.	O	`tstr`
	`birth_city`	The municipality, city, town, or village where the PID User was born.	O	`tstr`
Current Address (See section 2.3.5)				
	`resident_address`	The full address of the place where the PID User currently resides and/or can be contacted (street name, house number, city etc.).	O	`tstr`
	`resident_country`	The country where the PID User currently resides, as an Alpha-2 country code as specified in ISO 3166-1.	O	`tstr`
	`resident_state`	The state, province, district, or local area where the PID User currently resides.	O	`tstr`
	`resident_city`	The municipality, city, town, or village where the PID User currently resides.	O	`tstr`
	`resident_postal_code`	Postal code of the place where the PID User currently resides.	O	`tstr`
	`resident_street`	The name of the street where the PID User currently resides.	O	`tstr`
	`resident_house_number`	The house number where the PID User currently resides, including any affix or suffix.	O	`tstr`

PID attribute in [ARF]	Corresponding data element identifier(s)	Definition	Presence	Encoding format
Gender				
	`gender`	PID User's gender, using a value as defined in ISO/IEC 5218.	O	`uint`
Nationality / Citizenship (See section 2.3.6)				
	`nationality`	Alpha-2 country code as specified in ISO 3166-1, representing the nationality of the PID User.	O	`Nationality`, see section 2.3.6

Table 1 PID attributes and corresponding data elements

2.3.3 Date of birth-related data elements

[ARF] specifies 'Date of Birth' as a mandatory data element in a PID attribute. This document defines the following data elements related to this PID attribute:

• `birth_date`	(mandatory)
• `age_birth_year`	(optional)
• `age_in_years`	(optional)
• `age_over_18`	(optional)
• `age_over_NN`, NN <> 18	(optional)

Having multiple data elements instead of a single one allows having different levels of granularity for requests and responses, and thus allows issuers and Relying Parties to practice data minimization. For example, in some use cases, a Relying Party only needs to establish that the PID User is not a minor. In that case, requesting `age_over_18` suffices. Releasing more specific information, such as the PID User's age in years or birth year, would then constitute an unnecessary infringement of the User's privacy.

This document specifies `age_over_18` and other `age_over_NN` data elements as optional data elements. PID Providers are free to add more `age_over_NN` data elements.

The requirements in clause 7.2.5 of ISO/IEC 18013-5 SHALL be applicable for the `age_over_18` and `age_over_NN` data element in the PID set. This document affirms that issuing more (rather than fewer) `age_over_NN` data elements in a PID is beneficial for the PID User's privacy. Note that the usage of the `age_over_NN` data element is more complicated than it may look at first sight. The examples in ISO/IEC 18013-5 Annex D.2.2 will help to understand how the `age_over_NN` data element is to be used and interpreted.

2.3.4 Place of birth-related data elements

[ARF] specifies 'Place of Birth' as an optional data element in a PID attribute. This document defines the following data elements related to this PID attribute:

• `birth_place`	(optional)
• `birth_country`	(optional)
• `birth_state`	(optional)
• `birth_city`	(optional)

Having multiple data elements instead of a single one allows having different levels of granularity for requests and responses, and thus allows issuers and Relying Parties to practice data minimization.

2.3.5 Address-related data elements

[ARF] specifies 'Current Address' as an optional data element in the PID set. This document defines a number of current address-related data elements:

• `resident_address`	(optional)
• `resident_country`	(optional)
• `resident_state`	(optional)

• `resident_city`	(optional)
• `resident_postal_code`	(optional)
• `resident_street`	(optional)
• `resident_house_number`	(optional)

Having multiple data elements instead of a single one allows different levels of granularity for requests and responses, and thus allows issuers and Relying Parties to practice data minimisation. For example, in some contexts a RP must verify only that the PID User is a resident of a certain country. Releasing more specific address information such as state, city or postal code would then constitute an unnecessary infringement of the User's privacy.

Note that in most cases requesting a PID User's resident street and house number will not make sense without simultaneously requesting at least the resident city, as there will be many duplicate street names and house numbers in a given country. These data elements have been added primarily to assist in, for example, automated form filling.

2.3.6 Nationality / Citizenship

The ARF specifies 'Nationality / Citizenship' as a possible additional optional data element in the PID set and notes that this is potentially a multi-valued attribute, because a citizen can have more than one nationality.

This document defines a data element `nationality` taking as its value a single Alpha-2 country code. This implies that any additional nationality of the PID User must be added by the respective Member State as a domestic data element, see section 2.2.2. This possibility is also recognized in [ARF].

2.4 PID metadata

2.4.1 Overview

Section 5.1.1 of [ARF] says: "Metadata associated with the PID may additionally detail the date of issuance and/or expiration, the issuing authority and/or Member State, information necessary to perform holder binding and/or proof of possession, the information or location of the services that can be used to enquire about the validity status of and potentially more information."

The first column of Table 2 contains all the PID metadata identified in the quote above. The meaning of the remaining columns is explained in section 2.3.1.

PID metadata in [ARF]	ISO-compliant data element identifier	Definition	Presence	Encoding format
Date of issuance				
	`issuance_date`	Date (and possibly time) when the PID was issued.	M	`tdate` or `full-date`
Date of expiration				
	`expiry_date`	Date (and possibly time) when the PID will expire.	M	`tdate` or `full-date`
Issuing authority				
	`issuing_authority`	Name of the administrative authority that has issued this PID instance, or the ISO 3166 Alpha-2 country code of the respective Member State if there is no separate authority authorized to issue PIDs.	M	`tstr`
	`document_number`	A number for the PID, assigned by the PID Provider.	O	`tstr`
	`administrative_number`	A number assigned by the PID Provider for audit control or other purposes.	O	`tstr`
Member State				
	`issuing_country`	Alpha-2 country code, as defined in ISO 3166-1, of the PID Provider’s country or territory.	M	`tstr`
	`issuing_jurisdiction`	Country subdivision code of the jurisdiction that issued the PID, as defined in ISO 3166-2:2020, Clause 8. The first part of the code SHALL be the same as the value for issuing_country.	O	`tstr`

PID metadata in [ARF]	ISO-compliant data element identifier	Definition	Presence	Encoding format
Validity status location information		**To be decided**		

Table 2 PID metadata and corresponding data elements

2.4.2 Validity status information

PID revocation will be further detailed in a future version of ARF. Probably validity status information will not be included in the PID metadata, but rather in the cryptographic proof structures, i.e., the MSO for ISO-compliant PIDSs and the SD-JWT for SD-JWT-compliant PIDs.

2.5 PID data element encodings

2.5.1 Introduction

Requirement 6 in section 5.1.2 of the ARF specifies that PID attestation must be issued in accordance with both the data model specified in ISO/IEC 18013-5:2021 [ISO18013-5] and the W3C Verifiable Credentials Data Model 1.1. Requirements 7 and 8 make clear that for the latter encoding, Selective Disclosure JSON Web Tokens (SD-JWT), as specified in [SD-JWT], must be used, and that consequently, data elements must be encoded in JSON. For the former, data elements must be encoded in CBOR.

This section therefore specifies two separate encodings for the PID data model, an ISO/IEC 18013-5-compliant encoding in CBOR, and a SD-JWT-compliant encoding in JSON.

2.5.2 ISO/IEC 18013-5-compliant encoding

2.5.2.1 Encoding rules

If data elements specified in in Table 1 or Table 2 are encoded with CBOR, they SHALL be encoded as specified in [RFC 8949].

The CDDL representation types used in Table 1 and Table 2 are specified in section 2.3.1. Rules to encode CDDL representation types with CBOR are specified [RFC 8610] and [RFC 8949].

2.5.2.2 Further stipulations

The value of all data elements (both PID attributes and PID metadata) SHALL be valid at the value of the timestamp in the `validFrom` element in the MSO from ISO/IEC 18013-5 clause 9.1.2.4[4].

> NOTE: The value of the `age_over_18`, `age_over_NN` and `age_in_years` data elements, if present, changes whenever the PID User has a birthday. The value of many other data elements will also change over time. It is up to the PID Provider to ensure that the above requirement is complied with. This document does not require that an issuer issues a new PID as soon as it becomes aware of a change in the PID User's data.

The `issue_date` data element (Table 2) SHALL NOT be later than the `validFrom` element in the MSO, as defined in clause 9.1.2.4 of ISO/IEC 18013-5.

If the Relying Party retrieved the `issuing_country` data element (Table 2), it SHALL verify that the value of that element matches the `countryName` element in the Subject field within the Document Signer certificate; see ISO/IEC 18013-5 Annex B.

If the Relying Party retrieved the `issuing_jurisdiction` data element (Table 2), it SHALL verify that the value of that element matches the `stateOrProvinceName` element, if it is present in the Subject field within the Document Signer certificate; see ISO/IEC 18013-5 Annex B.

[4] As explained in [TrustModel], server retrieval, as specified in ISO/IEC 18013-5, SHALL NOT be used for EUDI Wallets.

Data elements in Table 1 and Table 2 SHALL be released only as Issuer Signed Items, as specified in [ISO/IEC 18013-5]. This means that these data elements SHALL be signed by the PID Provider, not by the Wallet Instance.

At the discretion of the PID Provider, domestic data elements (see section 2.2.2) MAY be signed either by the PID Provider or by the Wallet Instance.

2.5.3 SD-JWT-compliant encoding

2.5.3.1 Encoding rules

If data elements are encoded with JSON, they SHALL be encoded as specified in [RFC 8259].

The CDDL representation types used in Table 1 and Table 2 are specified in section 2.3.1. Rules to encode CDDL representation types with JSON are specified in [RFC 8949] section 6.1 Given the CDDL representation types used in the current version of this document, the following rules are relevant:

- A CDDL `uint` (i.e., an unsigned integer) becomes a JSON number.
- A CDDL `bstr` (i.e., a byte string) is encoded in base64url without padding and becomes a JSON string.
- A CDDL `tstr` (i.e., a UTF-8 text string) becomes a JSON string[5].
- A CDDL `bool` (i.e., a Boolean) becomes a JSON false or a JSON true, as applicable.
- A CDDL `tdate` or `full-date` (which is a tagged item or ‘tag’) becomes a JSON string representing the content of the tag; the tag number is ignored.

Although not used in the current version of this document, the following CDDL representation types are frequently used in general, and hence rules to encode them with JSON may become relevant in future versions:

- A CDDL array (i.e., a structure enclosed in square brackets [ ]) becomes a JSON array.
- A CDDL `nint` (i.e., a negative integer) becomes a JSON number.
- A CDDL map (i.e., a structure enclosed in curly brackets { }) becomes a JSON object. Since this is possible directly only if all keys are UTF-8 strings, any CDDL maps defined in future versions of this document SHALL only use keys that are UTF-8 strings.

If other CDDL representation types will be used in future versions of this document, the corresponding rules for encoding them with JSON will be added here.

2.5.3.2 Further stipulations

Data elements in Table 1 and Table 2 SHALL be released only in a VP Token, as specified in [OpenID4VP]. This means that these data elements SHALL be signed by the PID Provider, not by the Wallet Instance.

At the discretion of the PID Provider, domestic data elements (see section 2.2.2) MAY be released in either a VP Token or an ID Token.

[5] Note that JSON requires escaping certain characters ( ): quotation mark (U+0022), reverse solidus (U+005C), and the "C0 control characters" (U+0000 through U+001F). All other characters are copied unchanged into the JSON UTF-8 string.

3 Wallet Instance attestation attribute schema

Note: the information in this chapter does not pertain to the PID directly. It will be included in a separate Wallet Attestation Rulebook, to be detailed in a future version of ARF.

3.1 Introduction

The Trust Model [TrustModel] introduces the concept of a Wallet Instance Attestation issued by the Wallet Provider for each Wallet Instance.

3.2 Document type and namespace

Like any other attestation, a Wallet Instance Attestation needs a document type and a namespace. The document type “eu.europa.ec.eudi.wallet-instance.1” SHALL be used for this purpose, and the namespace “eu.europa.ec.eudi.wallet-instance.1” SHALL be used to identify data elements in this Wallet Instance Attestation.

3.3 Data model

Please note that there currently is no specification of a Wallet Instance Attestation and the attributes in it, either within the context of the EUDI Wallet or in an international standard or specification. Once this is available, a corresponding data model will be added in this section, comparable to the one for the PID in chapter 2.

4 Trust infrastructure details

4.1 Introduction

To trust a signature over a PID attestation, the RP needs a mechanism to validate that the public key it uses to verify that signature is trusted. Both ISO/IEC 18013-5 and OpenID4VP provide such mechanisms. However, in both cases, additional details need to be specified to fully specify these mechanisms for PID attestations within the EUDI Wallet ecosystem.

4.2 ISO/IEC 18013-5-compliant PID attestations

4.2.1 OIDs for use in PID-related certificates

ISO/IEC 18013-5 specifies an X.509-based PKI for the purpose of trusting public keys. This PKI has multiple roots; there is an independent (self-signed) root certificate for every issuer. Annex B of the standard specifies the formats of the X.509 certificates for all participants in the ecosystem.

These certificate formats are mDL-specific, but only because they use the following Object Identifier (OID): `id-mdl OBJECT IDENTIFIER ::= { iso(1) standard(0) 18013 5 }`[6], as well as a number of child OIDs ('arcs') of this OID, see Annex B.1.1 of ISO/IEC 18013-5. All other aspects of these certificate profiles can be used for any type of mobile document complying with the security mechanisms defined in ISO/IEC 18013-5, including a PID attestation within the EUDI Wallet ecosystem.

To make the certificate profiles applicable for PIDs in ISO/IEC 18013-5-compliant EUDI Wallets, this document specifies the following OIDs (in ASN.1 notation):

- `id-eudi OBJECT IDENTIFIER ::= {european-commission 2}`
  `- – arc for EUDI Wallets`
- `id-eudi-iso OBJECT IDENTIFIER ::= {id-eudi 0}`
  `- - arc for ISO/IEC 18013-5-compliant EUDI Wallets`[7]
- `id-eudi-iso-pid OBJECT IDENTIFIER ::= {id-eudi-iso 0} – arc for PID attributes within ISO-compliant EUDI Wallets`
- `id-eudi-iso-pid-kp OBJECT IDENTIFIER ::= {id- eudi-iso-pid 1}`
  `- - arc for extended key purposes within certificates used for PID attributes within ISO-compliant EUDI Wallets`
- `id-eudi-iso-pid-kp-DS OBJECT IDENTIFIER ::= {id-eudi-iso-pid-kp 2}`
  `- - arc for document signer certificates, used by PID Providers`
- `id-eudi-iso-pid-kp-ReaderAuth OBJECT IDENTIFIER ::= {id-eudi-iso-pid-kp 6}`

[6] Note that this notation is incorrect. The http://oid-info.com/ website officially registers this OID as `{iso(1) standard(0) driving-licence(18013) part-5(5)}`. This does not impact the value of the OID.

[7] The presence of this arc allows SD-JWT-compliant implementations of the EUDI Wallet to have their own arc 'next' to this one, if necessary.

`- - arc for mdoc reader authentication certificates, used by Relying Parties requesting PIDs`[8]

- `id-eudi-iso-pid-kp-IACALink OBJECT IDENTIFIER ::= {id-eudi-iso-pid-kp 4}`
  `- - arc for IACA Link certificates, used by PID Providers`
- `id-eudi-iso-pid-kp-IACA OBJECT IDENTIFIER ::= {id-eudi-iso-pid-kp 7}`
  `– - arc for IACA Root certificates, used by PID Providers`

These OIDs SHALL be used in certificates used for PID attributes within the ISO-compliant EUDI Wallet ecosystem, in exactly the same way as the corresponding OIDs specified in ISO/IEC 18103-5 are used within the mobile driving license ecosystem.

Notes:

- The numbers for the various extended key purposes are taken from ISO/IEC 18013-5.
- These new OIDs will have to be officially registered.
- The OID `european-commission` is already registered: `european-commission ::= {iso(1) identified-organization(3) european-commission(130)}`. The respective Registration Authority for this OID will have to be consulted to get approval for the proposed addition of an arc for the EUDI Wallet.

4.2.2 Trusted Issuer List

Section 4.2.2. of [TrustModel] describes the concept of a trusted list of Issuers. This document specifies that for PID attestations, such a trusted list SHALL be used. Relying Parties SHALL only trust PID issuers that are included in a trusted list of PID Providers. Additionally, there SHALL be only a single trusted list of PID Providers, which SHALL be generated and maintained by a yet-to-be-determined party. This list SHALL also contain the (root) certificate(s) of each PID Provider.

Regarding the format of this trusted list, the format specified ETSI TS 119 612 v2.1.1 SHALL be used.

4.3 SD-JWT-compliant PID attestations

Details on the trust infrastructure for SD-JWT and OpenID4VP-compliant PIDs will be detailed in a future version of ARF.

[8] Note that the use of this PID-specific OID implies that an mdoc reader authentication certificate containing this OID cannot be used to perform Relying Party authentication for any other type of attestation within the EUDI Wallet. This is by design, as it seems good for security to separate reader authentication per attestation type. However, decisions regarding Relying Party authentication will be detailed in a future version of ARF.

5 References

[ARF]	The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet Architecture and Reference Framework, November 2023, Version 1.2.0
[ISO18013-5]	ISO/IEC 18013-5, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application, First edition, 2021-09
[SD-JWT]	Selective Disclosure for JWTs (SD-JWT) draft-ietf-oauth-selective-disclosure-jwt-04, 11 April 2023 [9] Retrievable from https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/
[OpenID4VP]	OpenID for Verifiable Presentations – draft 18, 21 April 2023 [10] Retrievable from https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
[2015/1505]	COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[RFC 2119]	RFC 2119 - Key words for use in RFCs to Indicate Requirement LevelsS. Bradner, March 1997
[RFC 3339]	RFC 3339 - Date and Time on the Internet: Timestamps, G. Klyne et al., July 2002
[RFC 8259]	RFC 8259 - The JavaScript Object Notation (JSON) Data Interchange Format, T. Bray, Ed., December 2017
[RFC 8610]	RFC 8610 - Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures, H. Birkholz et al., June 2019
[RFC 8943]	RFC 8943 -Concise Binary Object Representation (CBOR) Tags for Date, M. Jones et al., November 2020
[RFC 8949]	RFC 8949 - Concise Binary Object Representation (CBOR), C. Bormann et al., December 2020
[TrustModel]	Trust Model for the EUDI Wallet Ecosystem – generic for all use cases, version 0.8.1, 2023-05-25

[9] The exact version to be referenced is to be determined. [ARF] references v0.2 of 30 December 2022. v0.4 is the latest version available at the time of writing of this document. The level of interoperability between these versions is not known. As [SD-JWT] is still under development, presumably later versions will become available over time.

[10] The exact version to be referenced is to be determined. [ARF] references v0.14 of 30 December 2022. Draft 18 is the latest version available at the time of writing of this document. The level of interoperability between these versions is not known. As [OpenID4VP] is still under development, presumably later versions will become available over time.