DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO

Bridging Legal Requirements and Technical Solutions

for the European Digital Identity Wallet

2nd International Workshop on Trends in Digital Identity (TDI 2024) - April 9th 2024, Rome

Giuseppe De Marco, gi.demarco@innovazione.gov.it
Francesco Antonio Marino, fa.marino@ipzs.it

Navigating Legal Requirements for EUDI Wallet Development

This presentation aims to:

1. highlight eIDAS regulation articles and annexes relevant for EUDI Wallet implementations.

2. provide a guiding map on the legal requirements for those approaching the development of EUDI Wallet.

How We Have Proceeded

We have collected the delta of changes from the eIDAS Regulation (EU No 910/2014) on 23 July 2014, analyzing:

a. The European Parliament legislative resolution of 29 February 2024.

b. The REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework of 13 March 2024.

Text Structure Overview

1. Recitals

Provide the background, rationale, and objectives behind the eIDAS regulation.
Explain the context and reasons for the provisions that follow.

2. Articles

Outline the obligations, rights, and procedures for Member States, entities, and individuals.

3. Annexes

Include practical details necessary for compliance and operationalization of the regulation.

Recitals

Provide background and explanations about the digital identity Wallets and general eIDAS context. There we found:

1. **One new Recital** at position 67.

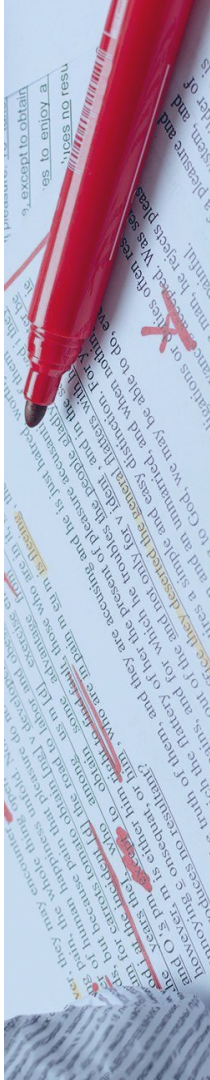
2. **70 updated Recitals** upon 78.

Recitals are considered to be only **informative and not normative**.

Article(s) by Number/Status

1 replaced
2 amended
3 amended
5 replaced
5a, b, c, d, e and 5f inserted
7 amended
8 amended
9 replaced
10 replaced (only Article title)
11a inserted
12 amended
12a and 12b inserted
13, 14, 15 and 16 replaced
17 deleted
18 deleted
19a inserted
20 amended
21 amended
24 amended
24a inserted
25 amended (paragraph 3 deleted)
26 amended
27 amended (paragraph 4 deleted)
28 amended
29 amended
29a inserted
30 amended (paragraph inserted)
31 amended (paragraph replaced)
32 amended
32a inserted
33 amended (par. inserted)
34 amended
35 amended (par. 3 deleted)
36 amended
37 amended (par. 4 deleted)
39a inserted
40a inserted
41 deleted
42 amended
44 amended
45 replaced
45a inserted
45b, c, d, e, f ,g, h, i, j, k and 45l inserted
46a, b, c, d and 46e inserted
47 amended
48a inserted
49 replaced
51 replaced

Summary: 3 deleted, 10 replaced, 24 amended or modified, 33 inserted.



Annexes

ANNEX I, point (i) replaced
ANNEX II, point 3 and 4 deleted
ANNEX III, point (i) replaced
ANNEX IV, points (c)(ca) replaced, point (j) replaced
ANNEX V inserted - REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES
ANNEX VI inserted - MINIMUM LIST OF USER ATTRIBUTES
ANNEX VII inserted - (REQUIREMENTS FOR EAAs ISSUED BY OR ON BEHALF OF A PUBLIC BODY RESPONSIBLE FOR AN AUTHENTIC SOURCE)
ANNEX TO THE LEGISLATIVE RESOLUTION inserted, containing:

- **Statement by the Commission on Article 45** on the occasion of the adoption of Regulation 2024.
- **Statement by the Commission on unobservability** on the occasion of the adoption of Regulation 2024.

Analysis and Classification of Legislative Text By Items

Each Article/Annex contains multiple items.

Analyzing and classifying each item we got two achievements:

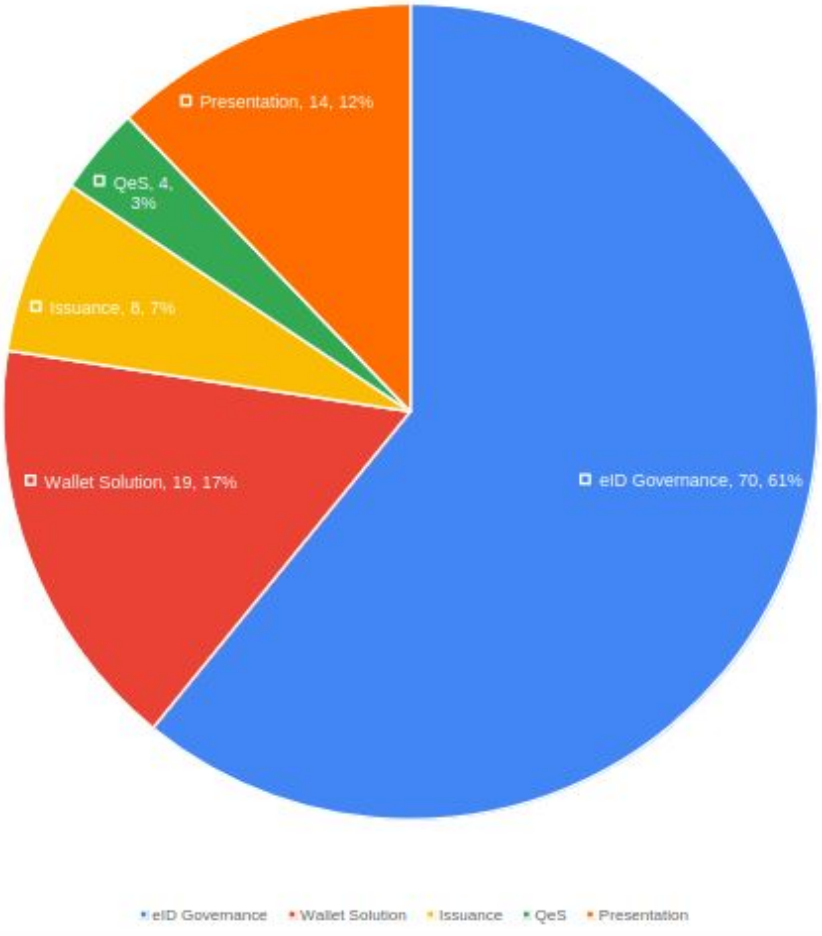
1. Classification of the requirements population.
2. **Self assessment matrix**.

Article Name	Article Text	Subject	Scope
Art. 5a(4)(g)	4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: [...] (g) exercise the user's rights to data portability.	European Digital Identity Wallets	Wallet Solution
Art. 5a(5)(a)(i)	5. European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: [...] (i) for issuance of person identification data, qualified and non qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;	European Digital Identity Wallets	Issuance
Art. 5a(5)(a)(ii)	5. European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: [...] (ii) for relying parties to request and validate person identification data and electronic attestations of attributes;	European Digital Identity Wallets	Presentation

ARTICLES and ANNEXES ITEMS - GROUPED BY SCOPE

Legal Requirements Population

- eID Governance
    - Certification
    - Accreditation
    - Wallet Provisioning
    - Security Framework ...
- Wallet Solution
- **Issuance** (PID/EAA/Pseudonyms)
- Presentation (PID/EAA/Pseudonyms)
- Qualified Electronic Signature



** all about the trust model is behind the lines of each item*
*** pseudonyms are distributed in both the Issuance and the Presentation items*

HIGHLIGHTED ARTICLES - WALLET SOLUTION

Article Item	Context
Art. 5a(4)(a)	**General features**. What the User shall be able to do using the Wallet.
Art. 5a(4)(c)	**Wallet to Wallet flow**. Data exchange, presentation, between the two Wallets.
Art. 5a(4)(d)	**Historical tracking of RPs** involved in presentations, with possibility to report to data protection authorities.
Art. 5a(4)(e)	**Qualified electronic signatures** or Seal by means of Qualified Electronic Seals capabilities.
Art. 5a(4)(g)	**Data portability**.
Art. 5a(5)(a)(v)	**User onboarding** using an electronic identification means in accordance with Article 5a(24).
Art. 5a(5)(a)(vi)	Support for common Protocols and Interfaces for **interaction between two persons' EUDI Wallets**.
Art. 5a(5)(a)(ix)	Support for common Protocols and Interfaces for **requesting a Relying Party the erasure of personal data**.
Art. 5a(5)(a)(x)	Support for common Protocols and Interfaces for **reporting a Relying Party to the competent national authority**.
Art. 5a(7)	**Optional additional features are possible**, including interoperability with existing national electronic identification means.
Art. 5a(8)(a)	Authenticity and validity of European Digital Identity Wallets can be verified with free-of-charge mechanisms.
Art. 5a(9)	**Revocation** circumstances: user decision, security issue or death of the user or cease of activity of the legal person.
Art. 5a(10)	Users can easily **request technical support and report technical problems** or any other incidents.
Art. 5a(11)	EUDI Wallet shall be **provided under an electronic identification scheme with assurance level high**.
Art. 5a(13)	The issuance, use and revocation of the European Digital Identity Wallets shall be **free of charge to all natural persons**.
Art. 5a(14)	The **Wallet Provider shall not collect personal information** about the usage of the Wallet by the User.
Art. 5a(21)	**Accessible** for use, by persons with disabilities.

HIGHLIGHTED ARTICLES - CREDENTIAL (PID/EAA/PSEUDONYMS) PRESENTATION

Article Item	Context
Art. 5a(5)(a)(ii)	support common protocols for Relying Parties to request and validate PID and electronic attestations of attributes
Art. 5a(5)(a)(iii)	support common protocols and interfaces for the sharing and **presentation to relying parties of person identification data**, **electronic attestation of attributes or of selectively disclosed related data online and**, where appropriate, **in offline mode**
Art. 5a(5)(a)(iv)	support common protocols and interfaces for the user to allow interaction with the EUDI Wallet and display EUDI Trust Marks
Art. 5a(5)(a)(vii)	support common protocols and interfaces for **authenticating and identifying relying parties by implementing authentication mechanisms** in accordance with Article 5b
Art. 5a(5)(a)(viii)	support common protocols and interfaces for **Relying Parties to verify the authenticity and validity of European Digital Identity Wallets**
Art. 5a(5(c)	**Relying Parties can be authenticated and identified by implementing authentication mechanisms** in accordance with Article5b
Art. 5a(8)(b)	allow Users to verify the authenticity and validity of the identity of Relying Parties registered with free-of-charge validation mechanisms
Art. 5b(8)	Where **Relying Parties** intend to rely upon European Digital Identity Wallets, they **shall identify themselves to the User**
Art. 5b(9)	**Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required** by Union or national law
Art. 5b(10)	Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.
Art. 5f(2)	Private Relying Parties, with the exception of micro enterprises and small enterprises, shall also accept EUDI Wallets
Art. 11a(1)	Relying Parties for cross-border services shall ensure unequivocal identity matching for natural persons

HIGHLIGHTED ARTICLES - CREDENTIAL (PID/EAA/PSEUDONYM) ISSUANCE

Article Item	Context
Art. 5a(4)(b)	Wallet shall enable the user to **generate pseudonyms and store them encrypted and locally** within the Wallet
Art. 5a(5)(a)(i)	**Issuance of person identification data, qualified and non qualified electronic attestations of attributes** or qualified and non-qualified certificates to the European Digital Identity Wallet
Art. 5a(5)(e)	Possibility of implementing **electronic attestation of attributes with embedded disclosure policies** to be applied when interacting with RPs (the Wallet must support)
Art. 5a(5)(f)	Person Identification Data (PID) uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet
Art. 5a(16)(a)	**PID/EAA Providers are not allowed in tracking user behaviour or knowledge of transactions of the user**
Art. 5a(16)(b)	privacy preserving techniques which ensure **unlinkability, where the attestation of attributes does not require the identification of the user**

PID Issuance - the legal framework

ID	Context	Text	References
R1	Security and Selective Disclosure support	European Digital Identity Wallets shall enable the user, [...], to **securely request, obtain**, [...], **under the sole control of the user**, person identification data [...], while **ensuring that selective disclosure of data** is possible	Art. 5a(4)(a)
R2	Protocols and Interfaces	European Digital Identity Wallets shall **support common protocols and interfaces for issuance** of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;	Art. 5a(5)(a)(i)
R3	User Onboarding	European Digital Identity Wallets shall support common protocols and interfaces to **securely onboard the user** by using an electronic identification means in accordance with Article 5a(24)	Art. 5a(5)(a)(v)
R4	User identification and association with EUDIW	European Digital Identity Wallets shall **ensure that the person identification data**, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, **uniquely represents the natural person,** legal person or the natural person representing the natural or legal person**, and is associated with that European Digital Identity Wallet**	Art. 5a(5)(c)(f)

SELECTIVELY DISCLOSABLE VERIFIABLE CREDENTIAL EXAMPLE

SD-JWT-VC PID Data Model

For instance, the Italian PID is issued using Selective Disclosure JWT format as specified in [SD-JWT-based Verifiable Credentials 02].

```
{
  "iss": "https://pidprovider.example.org",
  "sub": "NzbLsXh8uDCcd7noWXFZAfHkxZsRGC9Xs",
  "iat": 1683000000,
  "exp": 1883000000,
  "status": {
    "status_attestation": {
      "credential_hash_alg": "sha-256"
    }
  },
  "vct": "PersonIdentificationData",
  "unique_id": "xxxxxxxx-xxxx-xxxx-xxxx-xxx",
  "given_name": "Mario",
  "family_name": "Rossi",
  "birth_date": "1980-01-10",
  "tax_id_code": "TINIT-XXXXXXXXXXXXXXXX"
}
```

```
{
  "_sd": [
    "7WG4nT6K26_R3975zcwnVwgoHA7b988_3-vJzbZf6Yc",
    "NOxVzjUJg667iBdeDwmr6tZ46X-jchKwIVxMAfv43yc",
    "TK2RguPYoXzCx0vv5hbN9u5M2mHlWBt41qGWlLXCNu8",
    "UHChpGtNF2bj1FvAfBby1rnf7WXkxelFJ5a4vSj2FO4",
    "q6Tqnxau97tu-MqUDg0fSAmLGZdSuMUMk6a2s3bcsC0",
    "wyfxVqq9BosPT7tN4SHOI4E48P19aVA1ktW5Zf0E-fc"
  ],
  "exp": 1883000000,
  "iss": "https://pidprovider.example.org",
  "sub": "NzbLsXh8uDCcd7noWXFZAfHkxZsRGC9Xs",
  "status": {
    "status_attestation": {
      "credential_hash_alg": "sha-256"
    }
  },
  "vct": "PersonIdentificationData",
  "_sd_alg": "sha-256",
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu3OHF4j4W4vfSVoHIP1ILilDls…",
      "y": "ZxjiWWbZMQGHVWKVQ4hbSIirsVfuecCE6t4j…"
    }
  }
}
```

SD-JWT-VC PID Data Model

A minimum data set:

- ➔ uniquely identifies the User
- ➔ selectively disclosable per attribute (iat included!)
- ➔ bound to a specific Wallet Instance (Holder):
  - ◆ cryptographic key binding for possession proofing during the presentations

R1 - Art. 5a(4)(a)
Security and Selective Disclosure support

R4 - Art. 5a(5)(c)(f)
User identification and association with EUDIW

Image from https://www.freepik.com/

How is the PID provided to the User?

Image from https://www.freepik.com/

PID Issuance - High Level Flow

1. The PID Provider checks that
   a. the Wallet Instance is authentic and valid;
   b. the Wallet Provider is a trusted entity.
2. The Wallet Instance checks that the PID Provider is a trusted entity

Wallet Provider checks the authenticity and genuinity of the Wallet Instance and the compliance with the security requirements related to both the Hardware and the Software

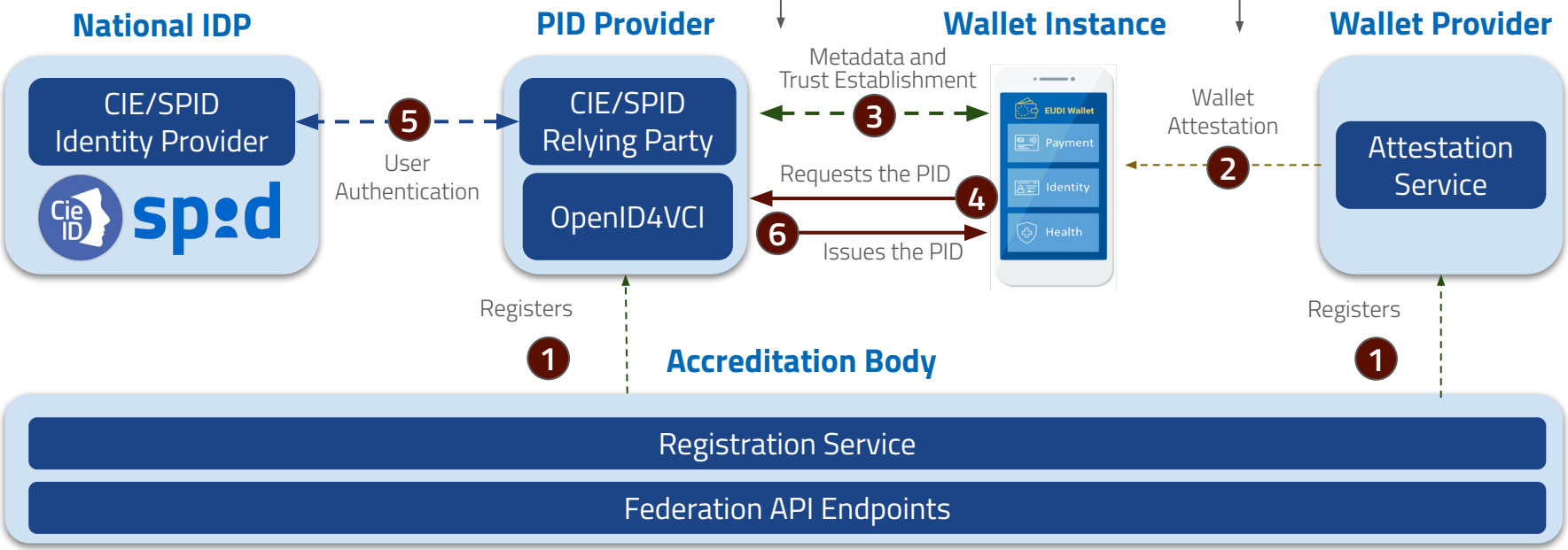
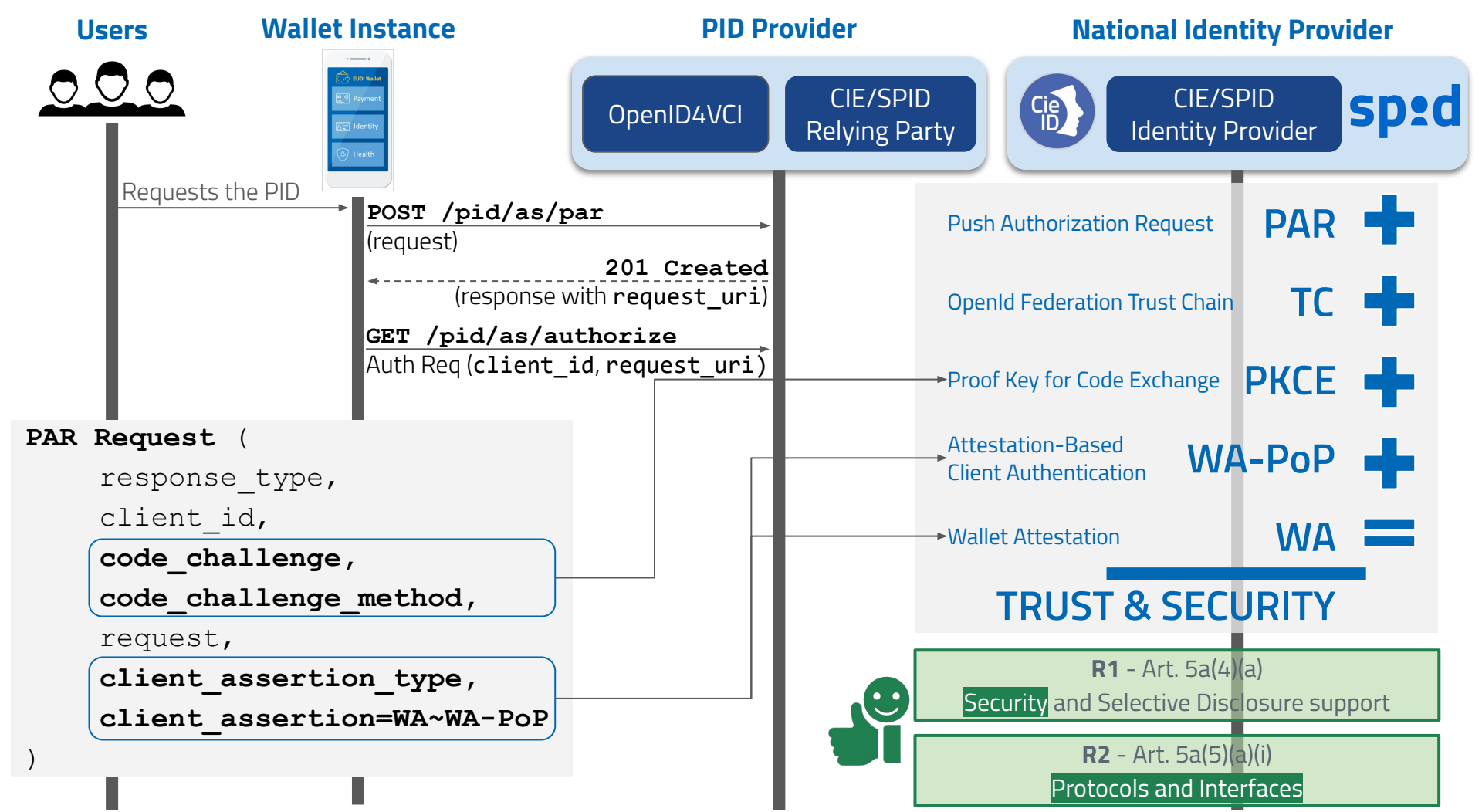


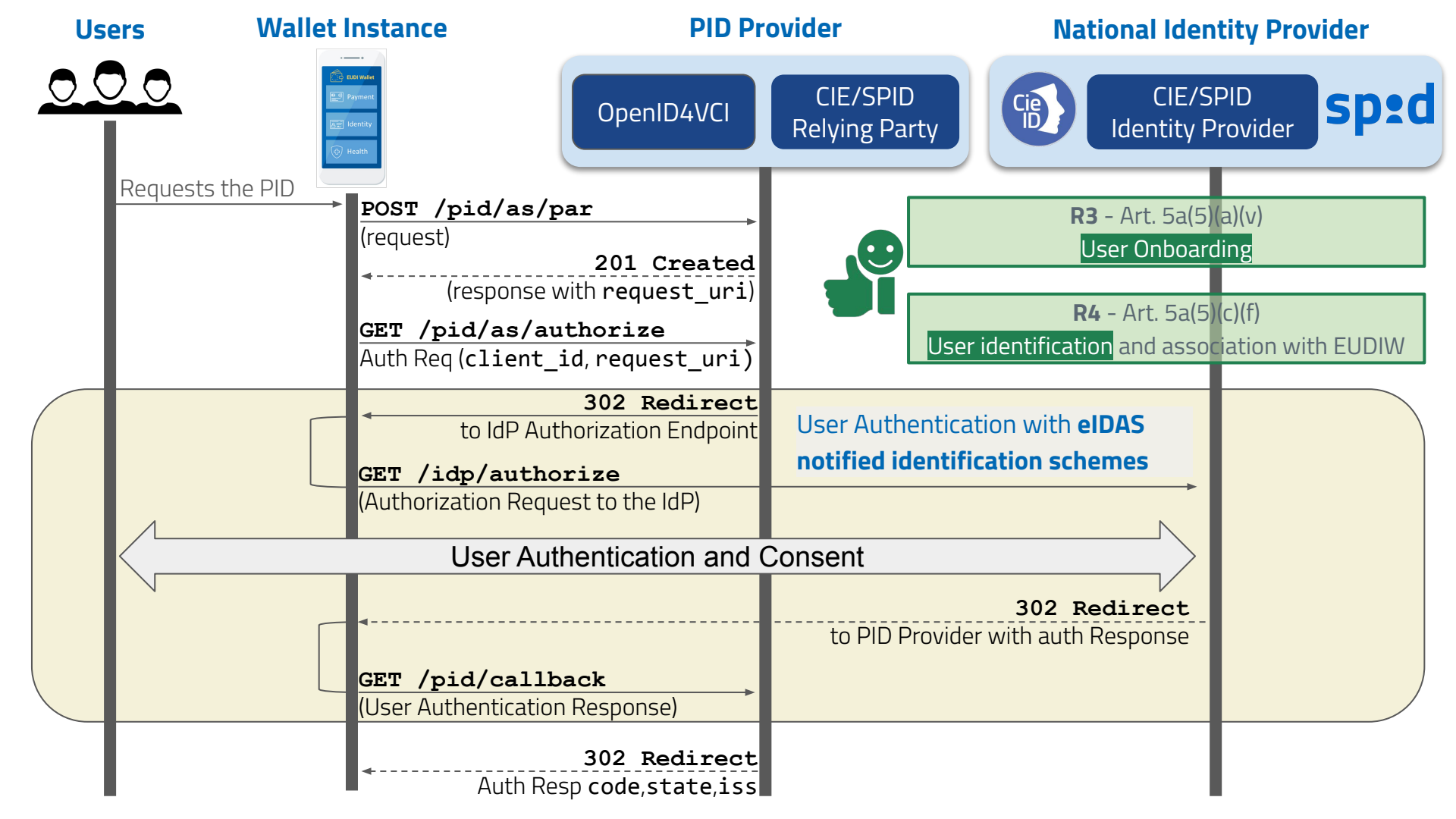
Image from https://www.freepik.com/

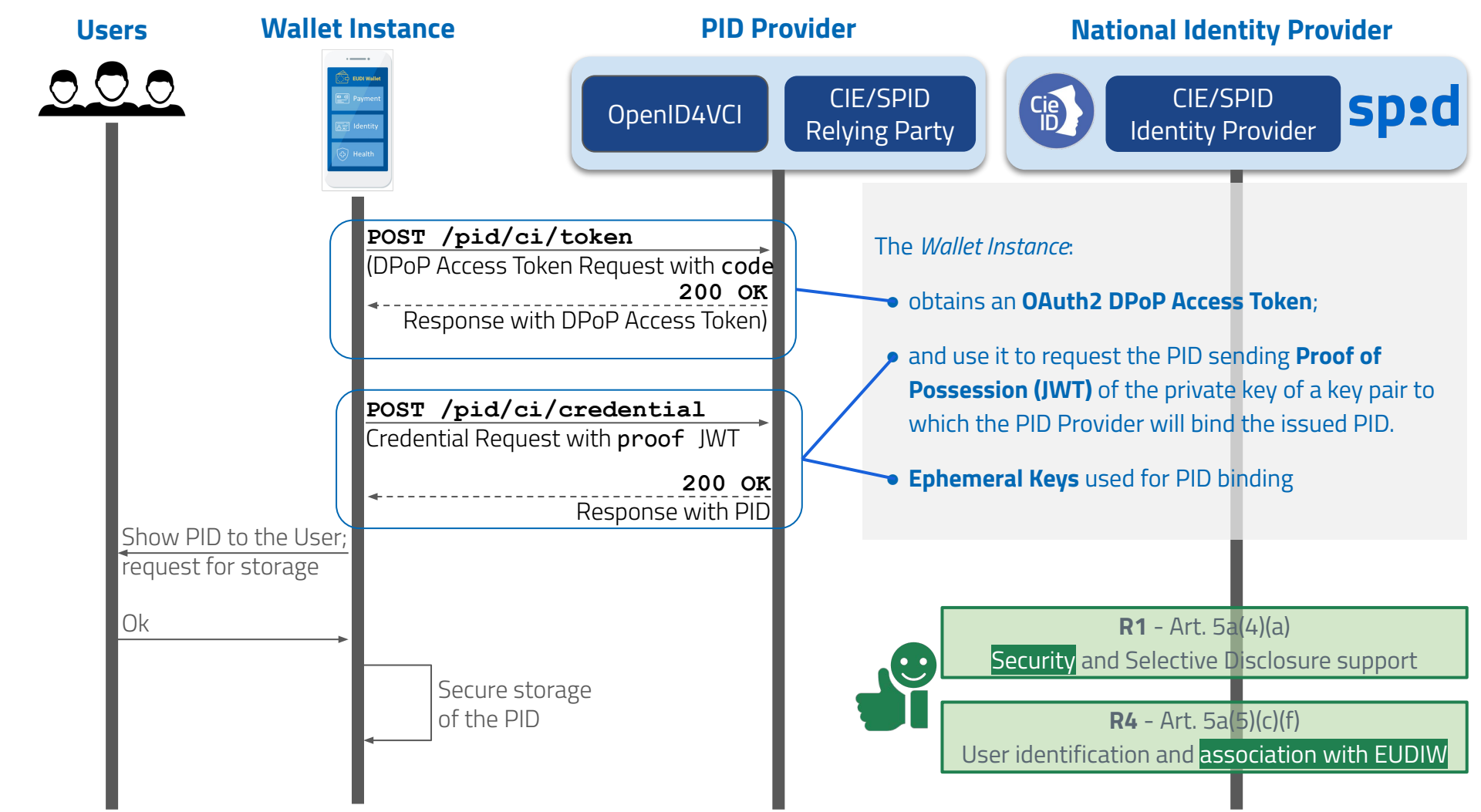
PID Issuance

- The Trust is established using **OpenID Federation 1.0**
- The PID is issued according to **OpenID4VCI Specification**
- The security is ensured by using:
  - **DPoP** Access Tokens;
  - **OAuth 2.0 Attestation-Based Client Authentication** Specification with Wallet Attestation checks;
  - **Proof of Possession** within the JWT proof enabling **Cryptographic Holder Binding** (during the future Presentations);

Image from https://www.freepik.com/


Users
Wallet Instance
PID Provider
National Identity Provider
OpenID4VCI
CIE/SPID Relying Party
CIE/SPID Identity Provider
Requests the PID
POST /pid/as/par
(request)
201 Created
(response with request_uri)
GET /pid/as/authorize
Auth Req (client_id, request_uri)
PAR Request (
response_type,
client_id,
code_challenge,
code_challenge_method,
request,
client_assertion_type,
client_assertion=WA~WA-PoP
)
Push Authorization Request
PAR
OpenId Federation Trust Chain
TC
Proof Key for Code Exchange
PKCE
Attestation-Based Client Authentication
WA-PoP
Wallet Attestation
WA
TRUST & SECURITY
R1 - Art. 5a(4)(a)
Security and Selective Disclosure support
R2 - Art. 5a(5)(a)(i)
Protocols and Interfaces


Users
Wallet Instance
PID Provider
National Identity Provider
EUDI Wallet
Payment
Identity
Health
OpenID4VCI
CIE/SPID Relying Party
Cie ID
CIE/SPID Identity Provider
spid
Requests the PID
POST /pid/as/par
(request)
201 Created
(response with request_uri)
GET /pid/as/authorize
Auth Req (client_id, request_uri)
R3 - Art. 5a(5)(a)(v)
User Onboarding
R4 - Art. 5a(5)(c)(f)
User identification and association with EUDIW
302 Redirect
to IdP Authorization Endpoint
GET /idp/authorize
(Authorization Request to the IdP)
User Authentication with eIDAS notified identification schemes
User Authentication and Consent
302 Redirect
to PID Provider with auth Response
GET /pid/callback
(User Authentication Response)
302 Redirect
Auth Resp code,state,iss


Users
Wallet Instance
PID Provider
National Identity Provider
OpenID4VCI
CIE/SPID Relying Party
CIE/SPID Identity Provider
POST /pid/ci/token
(DPoP Access Token Request with code
200 OK
Response with DPoP Access Token)
POST /pid/ci/credential
Credential Request with proof JWT
200 OK
Response with PID
Show PID to the User; request for storage
Ok
Secure storage of the PID
The Wallet Instance:
obtains an OAuth2 DPoP Access Token;
and use it to request the PID sending Proof of Possession (JWT) of the private key of a key pair to which the PID Provider will bind the issued PID.
Ephemeral Keys used for PID binding
R1 - Art. 5a(4)(a)
Security and Selective Disclosure support
R4 - Art. 5a(5)(c)(f)
User identification and association with EUDIW

Mapping requirements

Id	R1	R2	R3	R4
References	Art. 5a(4)(a)	Art. 5a(5)(a)(i)	Art. 5a(5)(a)(v)	Art. 5a(5)(c)(f)
Context	**Security and Selective Disclosure support**	**Compliance with standards**	**User Onboarding**	**User identification and association with EUDIW**
Technical Mechanisms	Security, Trust and Privacy ➔ PKCE ➔ client auth based on WA+WA-PoP, ➔ DPoP Access Token ➔ Proof JWT ➔ Trust Framework based on OpenID Federation 1.0 ➔ SD-JWT & SD-JWT-VC	➔ OpenID4VCI ➔ OpenID Federation 1.0 ➔ SD-JWT & SD-JWT-VC ➔ Attestation-Based Client Authentication ➔ OAuth2 DPoP	➔ National eID schemes notified eIDAS ➔ Trust Framework based on OpenID Federation 1.0	➔ National eID schemes notified eIDAS ➔ Wallet Attestation ➔ Client Auth based on WA-PoP ➔ Cryptographic Holder Binding (HB)

THANK YOU FOR YOUR ATTENTION

A special thanks to those who supported and contributed to this work:

Wallet team at Dipartimento per la trasformazione digitale and in particular Giulio “the-legal” Messori. IPZS, PagoPA and FBK.

For any further clarification, idea, proposal or discussion, please reach us at:

Giuseppe De Marco, gi.demarco@innovazione.gov.it
Francesco Antonio Marino, fa.marino@ipzs.it

See you soon for the analysis of the Implementing Act!

Image from https://www.freepik.com/