Discover the Italian Digital Identity Wallet

@TPAC 2024

Giuseppe De Marco
Open Source Project Leader, Digital Identities
Department for Digital Transformation

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

Hi!

I’m Giuseppe De Marco

+25 years in IT
+15 years in Software Development
+10 years in Research and Education
+7 years in Digital Identities (SAML2, OIDC …)
+4 years in Governative implementation profiles
+3 years in Gov eID Wallet developments

TODAY I TALK ABOUT IT-WALLET, IN PARTICULAR

- → National Regulatory References
- → Architectural Overview
- → Point of interest for implementers
- → Trust Infrastructure
- → Specific Protocols
- → Technical Milestones

picture: freepik.com

THE ROOT OF THE IT-WALLET FRAMEWORK

National Regulation

1. Decree-Law No. 19 of March 2, 2024, subsequently converted into law

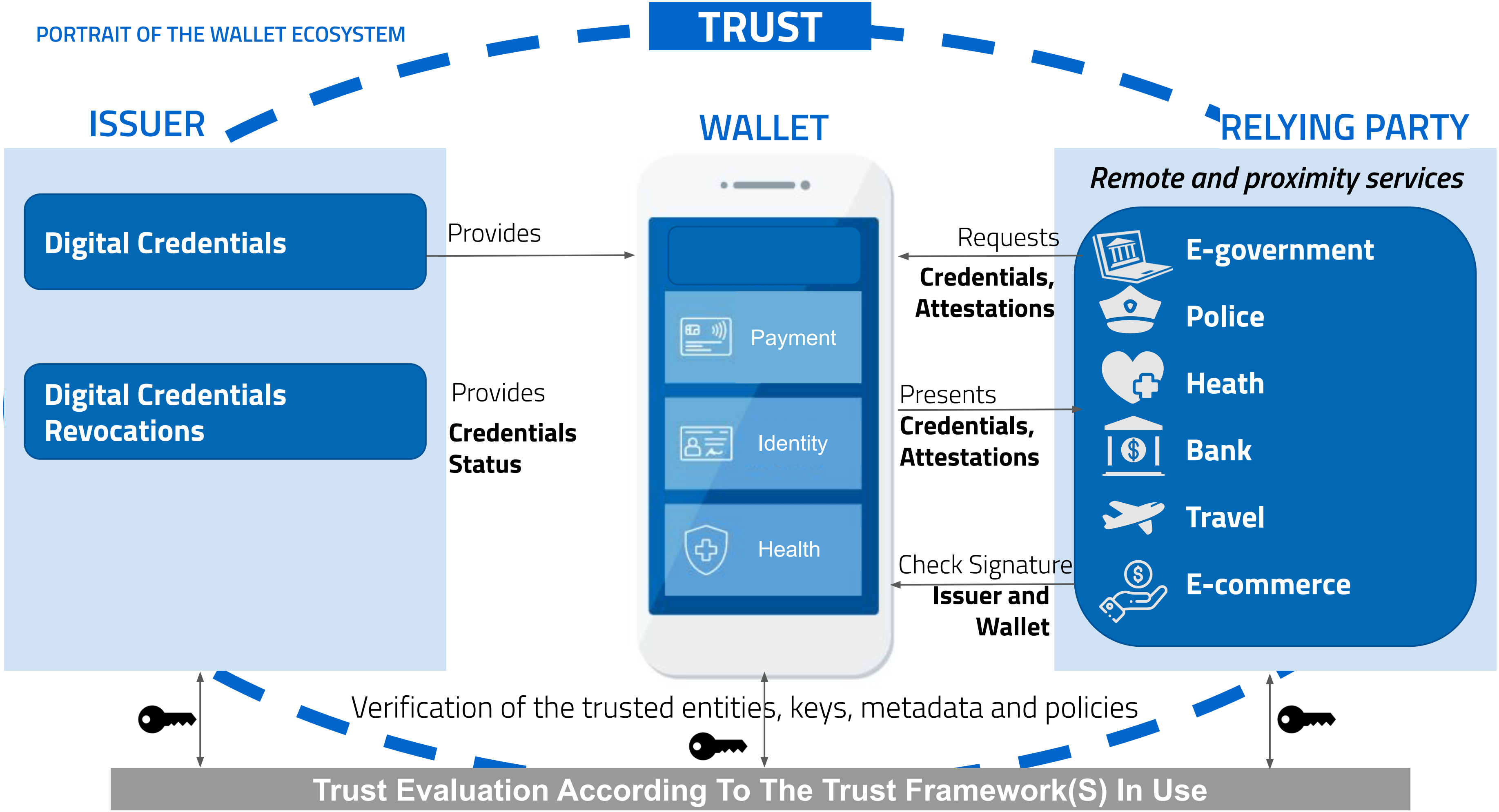
2. Two implementing decrees are expected to be issued with more technical details, providing guidance to all the parties and stakeholders of the National Wallet ecosystem

IT-WALLET IS

Product, Platform and Framework

1. **Product.** Public National Wallet Solution integrated in the Mobile App that facilitates interactions between the Users and the Public Services (the Mobile App is AppIO and it is produced by PagoPA)
2. **Platform**. Digital Identity Scheme along with an IT infrastructures to allow participants get registered to issue and request Users Digital Credentials, and offering private sector Wallet Solutions as well.
3. **Framework**. National regulations, guidelines and technical specification allowing private and public sectors to use the fundamental building blocks to build their services and reduce the costs.

PORTRAIT OF THE WALLET ECOSYSTEM



TRUST

ISSUER

Digital Credentials

Digital Credentials Revocations

Provides

Provides **Credentials Status**

WALLET

Payment

Identity

Health

RELYING PARTY

Remote and proximity services

Requests **Credentials, Attestations**

Presents **Credentials, Attestations**

Check Signature **Issuer and Wallet**

E-government

Police

Heath

Bank

Travel

E-commerce

Verification of the trusted entities, keys, metadata and policies

Trust Evaluation According To The Trust Framework(S) In Use

WALLET ECOSYSTEM IS NOT A PIECE OF CAKE, IT IS AN ENTIRE STACKED CAKE!

How To Approach The … Cake.

- Better to divide the components by specific contexts, **assign the components to experts in specific domains**.
- LoA High must not be only an assumption. Security and reliability of Personal Devices is challenging.
- Several UX challenges as well. Multiple documents, multiple ecosystems, multiple Wallet Solutions, multiple privacy regulations.
- External Hardware Tokens and Smartcards, remote HSM.
- In the past, SAML2 or OIDC used a single data format … now things are changed.

TRUST IS AT THE BASE

Trust from a Technical Perspective

- **Trust Model** is a model, quite abstract and it might be:
  - Direct
  - Third Party mediated
  - Decentralized (it may mix direct and third parties too)

- **Trust Framework** is rules and tools, needs implementations

- **Trust Infrastructure** must be interoperable and transparent

- … **How to check** if participants are compliant to the framework?

REQUIREMENTS FOR LARGE SCALE DEPLOYMENTS USING A TRUSTED THIRD PARTY

Trust that scales

In small-scale and static deployments, it’s possible to keep **a list of the trusted participants** and their metadata

However, **in large-scale and dynamic deployments, that doesn’t scale**

This needs **multilateral relationships**, rather than **bilateral**

Public domain picture: Dreamstime.com

Different Kinds of Ecosystem Participants

- online or in proximity organizational entities:
  - legal persons, systems and cloud services in unsupervised flows
- natural or legal persons:
  - human beings in control of their personal devices
    - on their own
    - on behalf or another person (natural or legal)

picture: freepik.com

Ok, Technically: Elements That Matters

- Entity Identifiers
- Metadata and Cryptographic Material:
    - Online: Remote Endpoints
    - Offline: Verifiable Attestations (such as X.509 Certificates)

WELL-KNOWN ENDPOINT BUT IN A DIFFERENT WAY

Ok, Technically: We Made It More Flexible

eg: two deployments of a Verifiable Credential Issuers can consequently use the FQDN **mario.example.it** and appear as separate entities, these are

- https://mario.example.it/idp/1
- https://mario.example.it/vci

the well-known of idp/1 will therefore be found on **https://mario.example.it/idp/1/.well-known/openid-federation**

OPENID FEDERATION SIGNIFICANTLY REDUCES THE AMOUNT OF SPARSE WELL-KNOWN ENDPOINTS AND METADATA

A Single Entity Configuration Containing All Metadata

.well-known/openid-federation

a JWT signed and self-issued by the entity, which publishes what it prefers in relation to itself

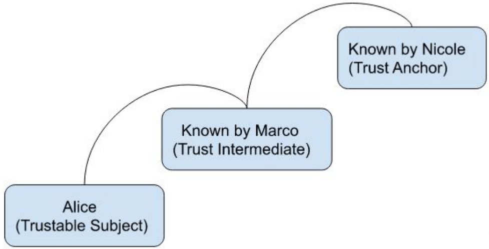
can also contain Trust Marks

one well-known multiple metadata about each role played in the ecosystem

HOW IS TRUST VERIFIED AND ESTABLISHED WITH AN ENTITY?

Thanks to A Trusted Third Party

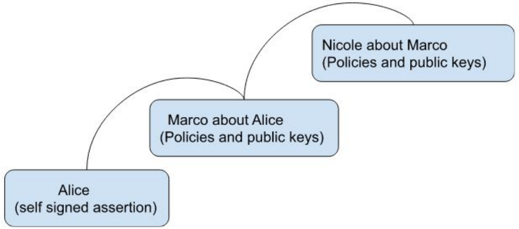
1. In a large ecosystem, direct and indirect relationships exist.
2. Trust with the Trusted Lists and the Trust Anchors is directly established.
3. Trust with **Accreditation Bodies, Issuers**, **Wallet Providers**, **RPs** and **Verifiers**, **may be indirectly established**, thanks to their links to the Trust Anchors.



Known by Nicole (Trust Anchor)

Known by Marco (Trust Intermediate)

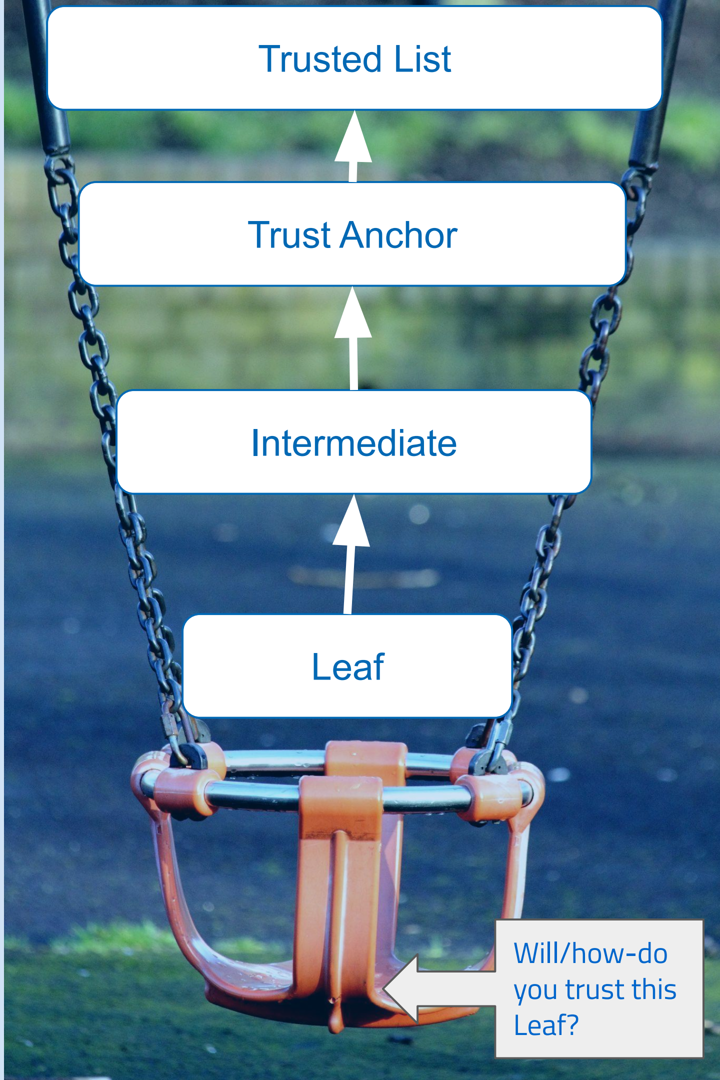
Alice (Trustable Subject)



Nicole about Marco (Policies and public keys)

Marco about Alice (Policies and public keys)

Alice (self signed assertion)



Trusted List

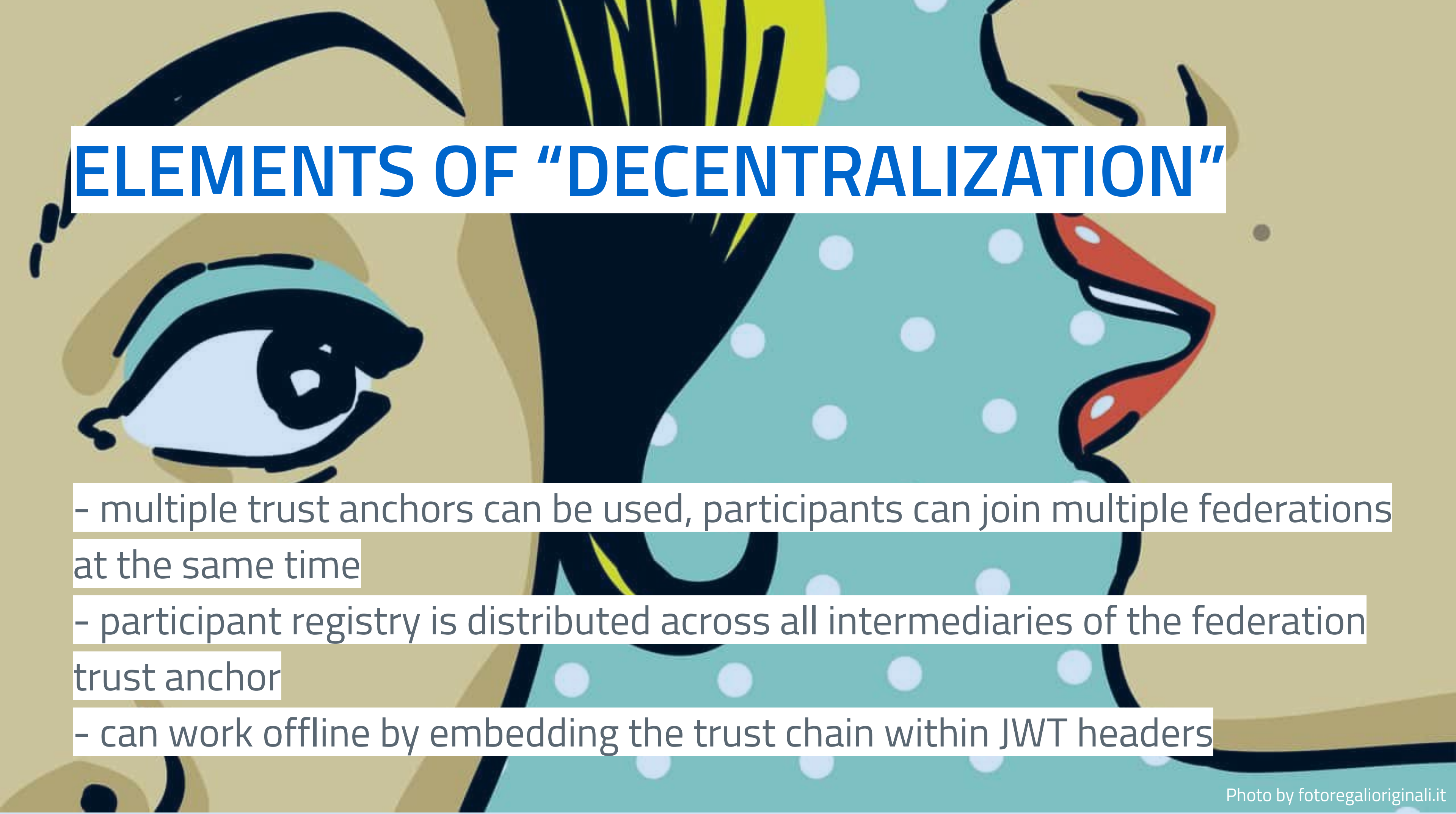
Trust Anchor

Intermediate

Leaf

Will/how-do you trust this Leaf?

ELEMENTS OF “DECENTRALIZATION”

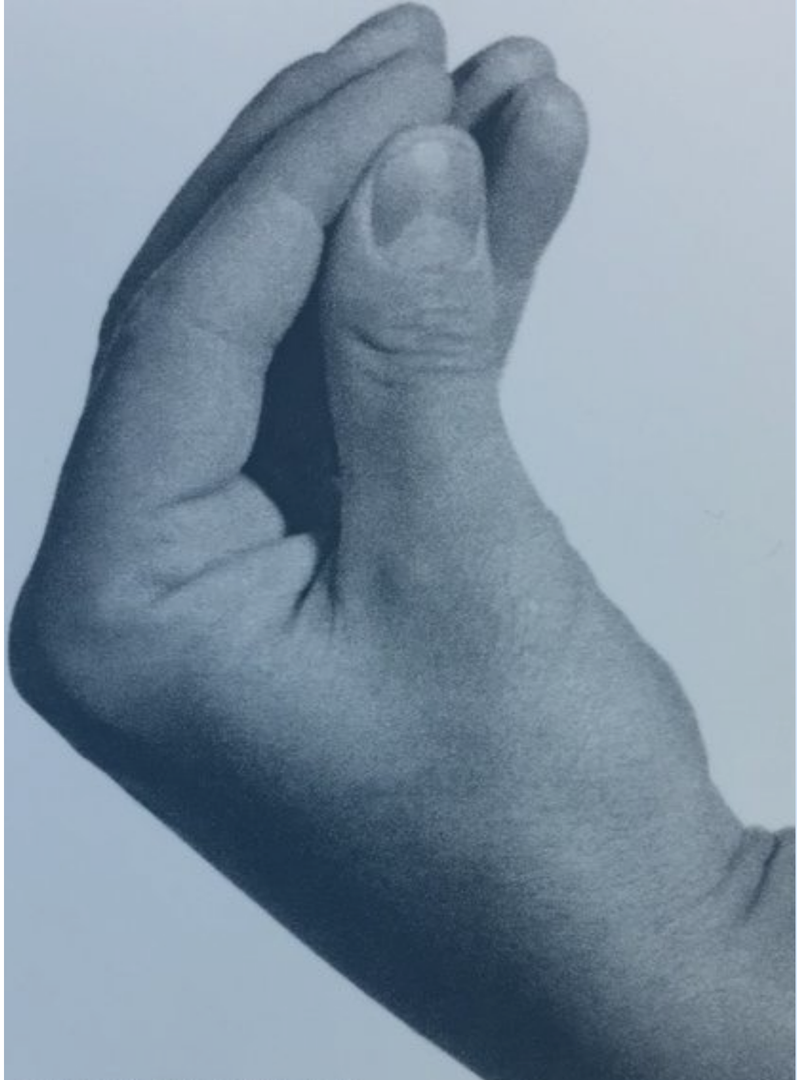


- multiple trust anchors can be used, participants can join multiple federations at the same time
- participant registry is distributed across all intermediaries of the federation trust anchor
- can work offline by embedding the trust chain within JWT headers

Photo by fotoregalioriginali.it

Do you really think that in Italy the whole world must necessarily use OpenID Federation?

No.



CONFLICTS REDUCTION MEANS HARMONIZATION - THE X.509 CASE

X.509 With OpenID Federation 1.0

Federation API can distribute X.509 certificates using the parameter x5c within the JWKs

We do this, once we have the public keys of an entity we automatically export them in both json (JWK) and X.509 (x5c within the JWK).

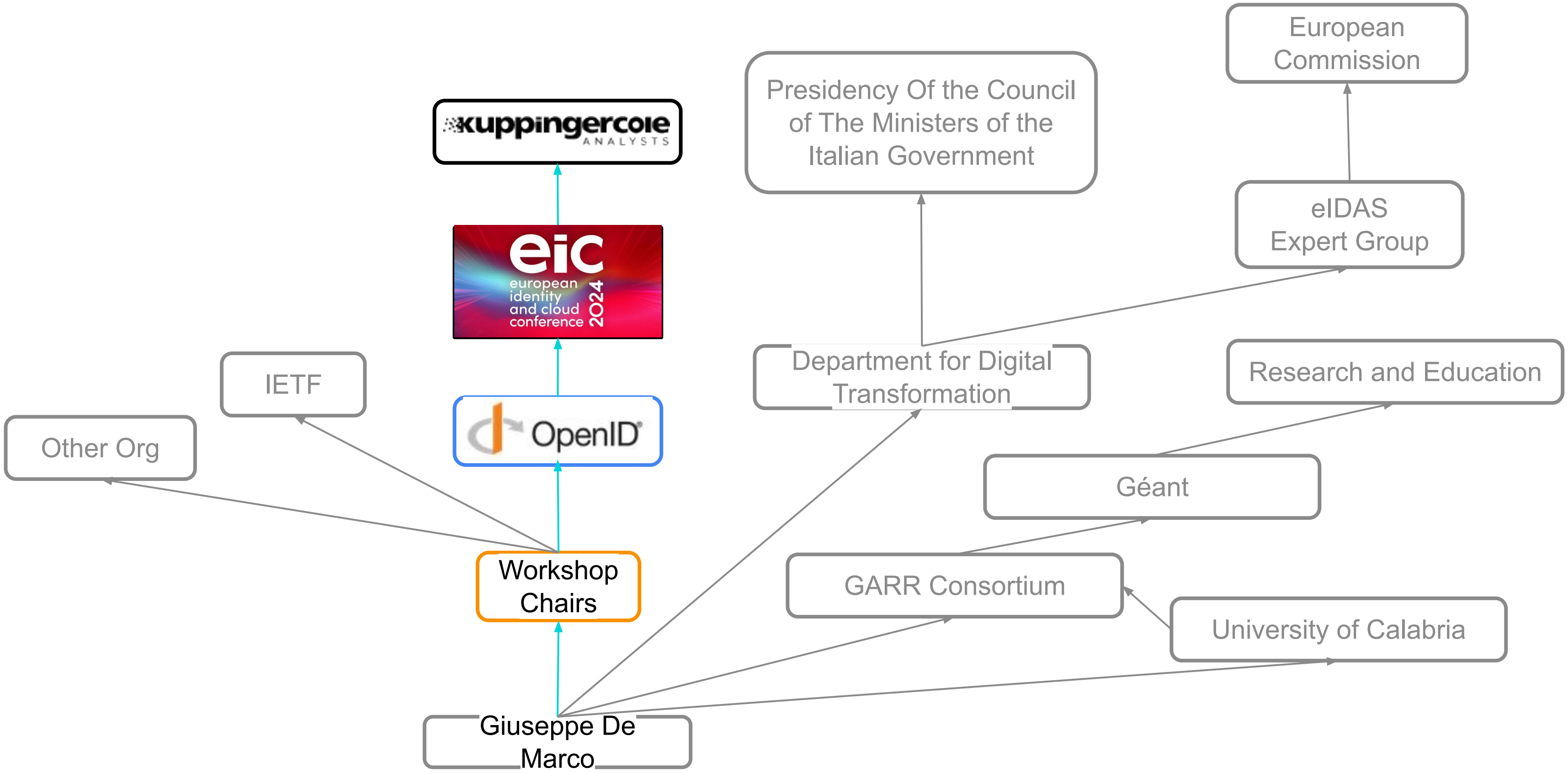
DID and Scalability

My name is Giuseppe De Marco and not

Well-Known:OpenIDFederation:GiuseppeDeMarco

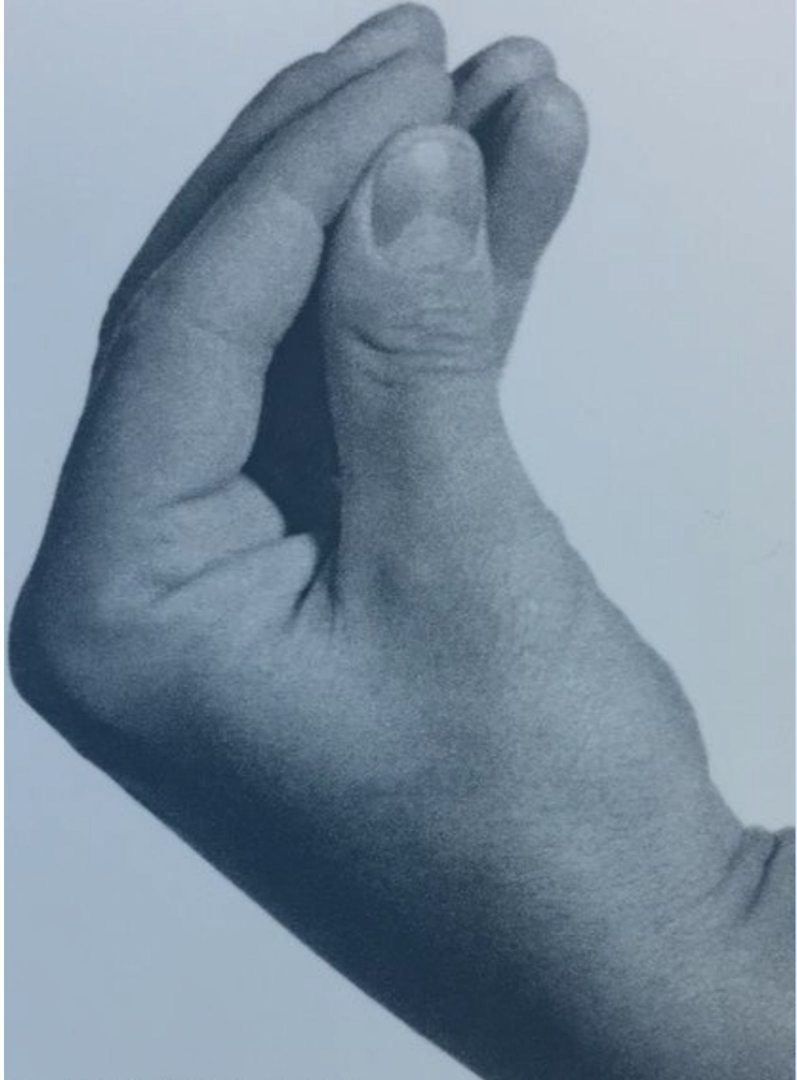
We distinguish my name from the mechanism you might use to establish trust with me

Several Paths To Resolve the Trust



Ok, OpenID Federation for organizational entities with cloud deployments.

And what about Holders, such as natural persons, identifiers and metadata?



THE PATH TO THE TRUST

Trust Resolution and Trust Chain building

REQUIREMENTS

1. All the Trust Anchors URLs/public keys must be taken from the Trusted Lists.
2. The Trust Anchors public keys published on their own MUST match the ones obtained from the Trusted Lists -> double check (don't rely entirely on TLS!)

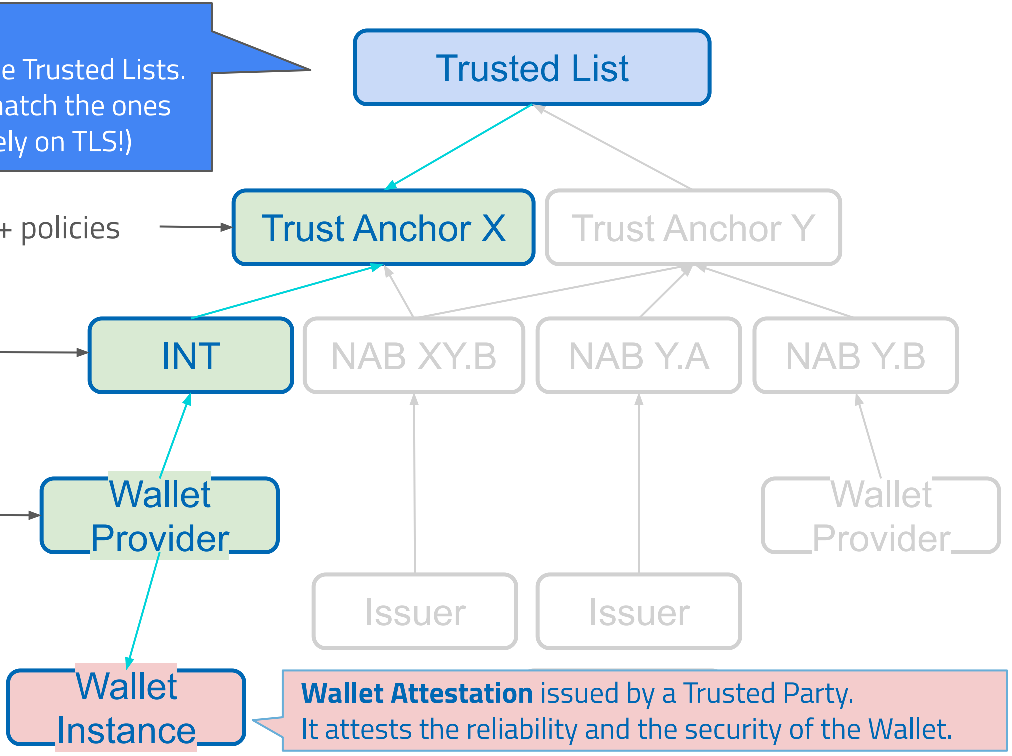
3. Get information/keys about the Intermediate from the TA + policies

2. Get information from the Leaf's Superior (Intermediate)
   What the Intermediate says about the Leaf
   The Leaf's key to verify the Leaf's information + policies
   What the Intermediate says about itself.

1. Get information from the Leaf
   What the Leaf says about itself.

OUTPUT

1. Trust Chain
2. **Final metadata** according to the processed policies
3. Verified **Trust Marks**

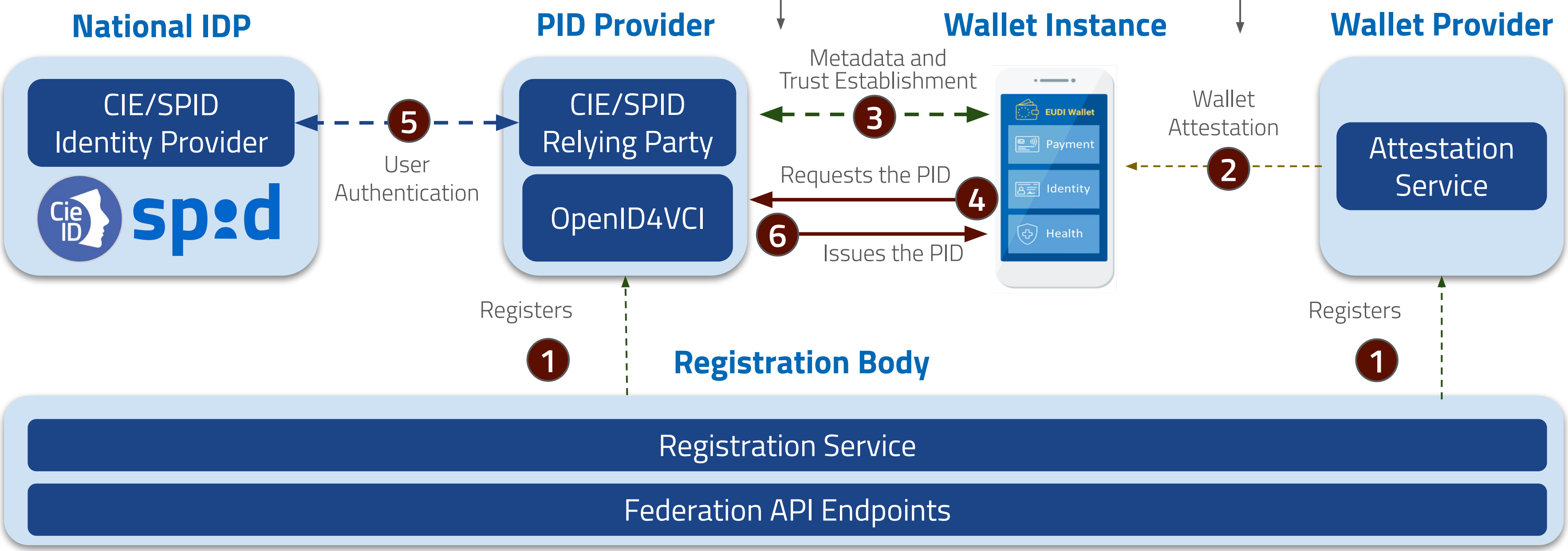


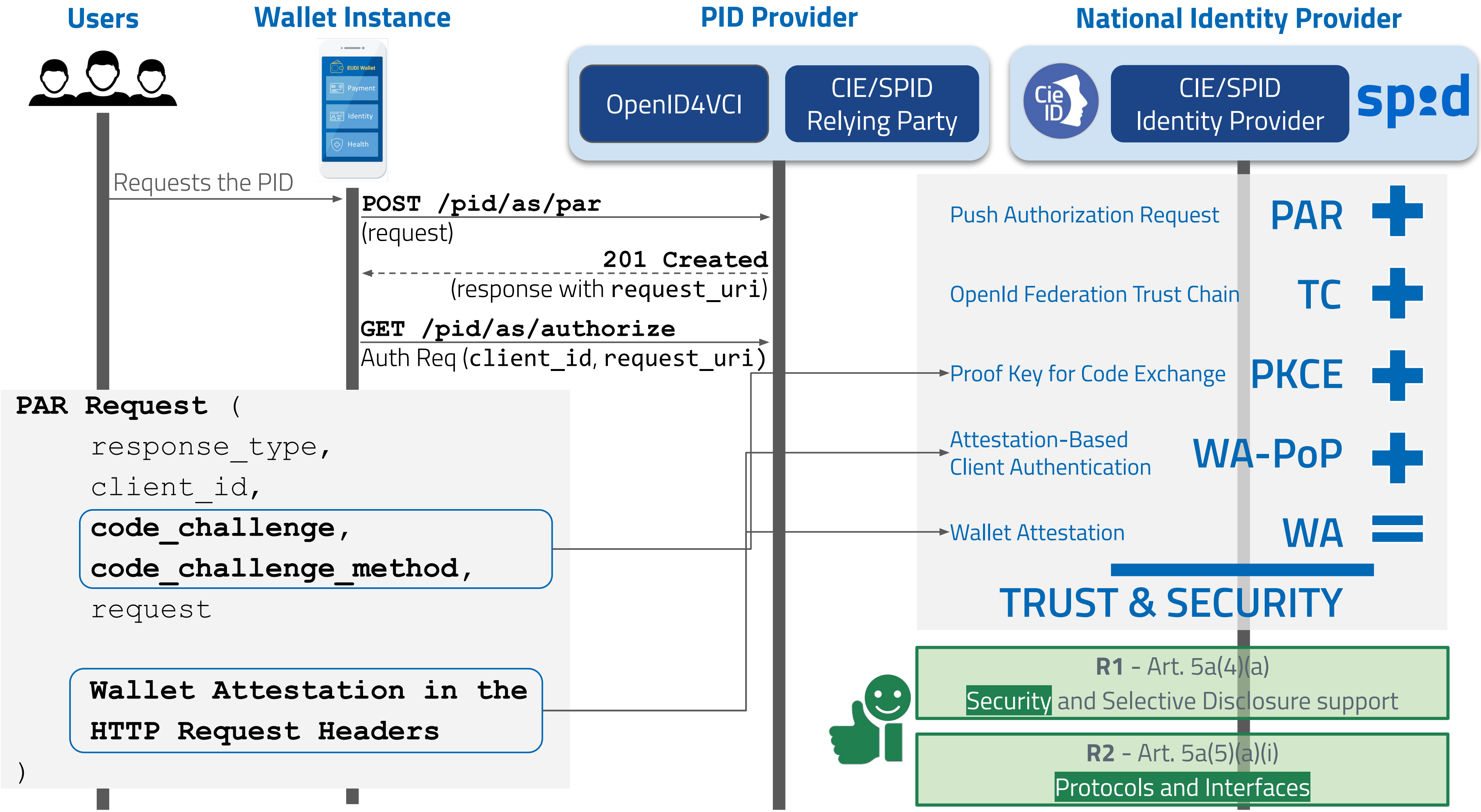
Wallet Attestation issued by a Trusted Party.
It attests the reliability and the security of the Wallet.

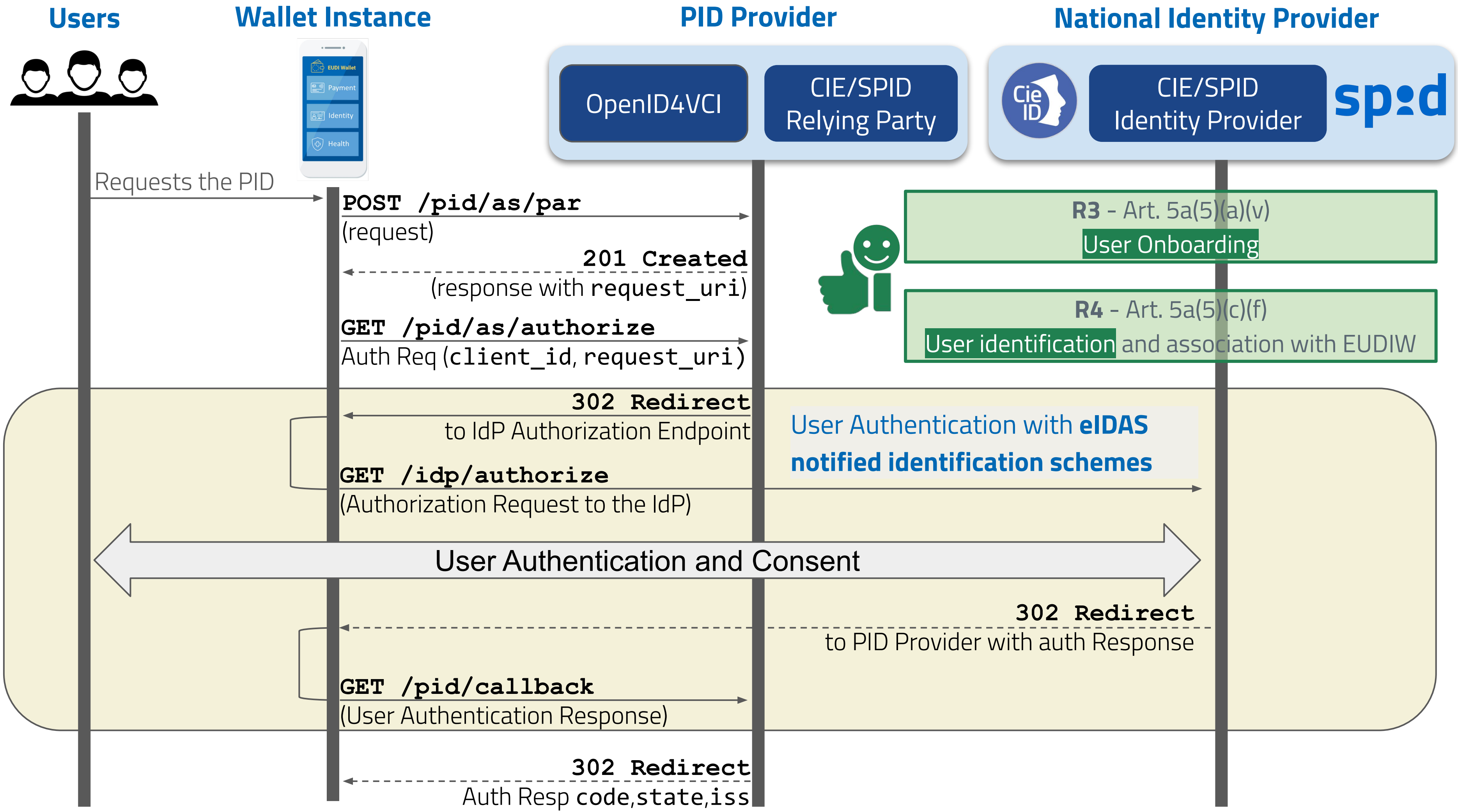
PID Issuance - High Level Flow

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







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)

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

User Authentication with **eIDAS notified identification schemes**

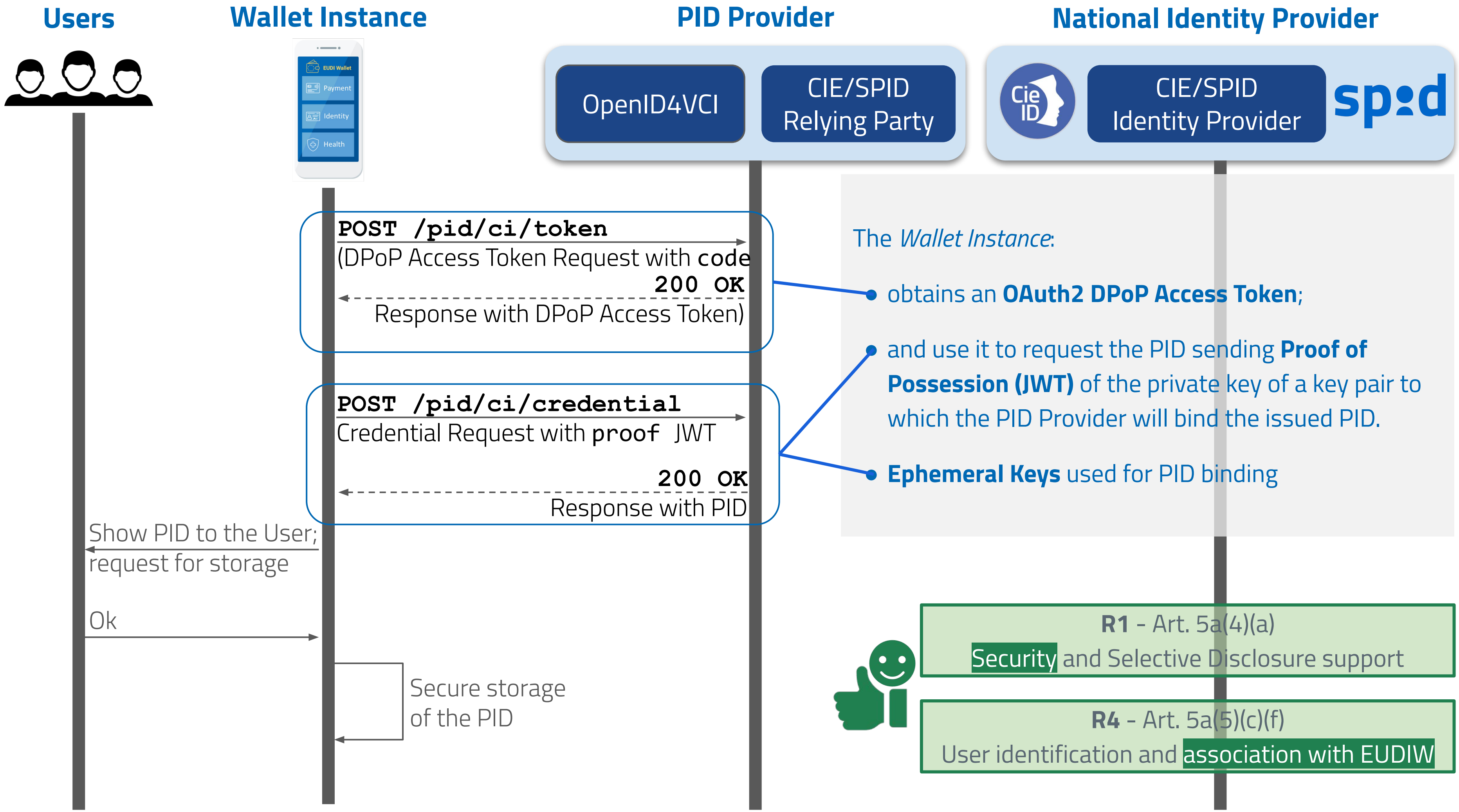
GET /idp/authorize
(Authorization Request to the IdP)

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

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/

WELL-KNOWN ENDPOINT BUT IN A DIFFERENT WAY

Digital Credential Presentation

OpenID4VP for remote flows
ISO 18013-5 for proximity flows

the Wallet Instance must present the Wallet Instance Attestation to the RP.

> Using OpenID4VP this should be nothing more than a common credential provided to the RP within the VP Token array.
>
> Using ISO: multiple documents within a mdoc, and using deviceSigned as proof of possession.

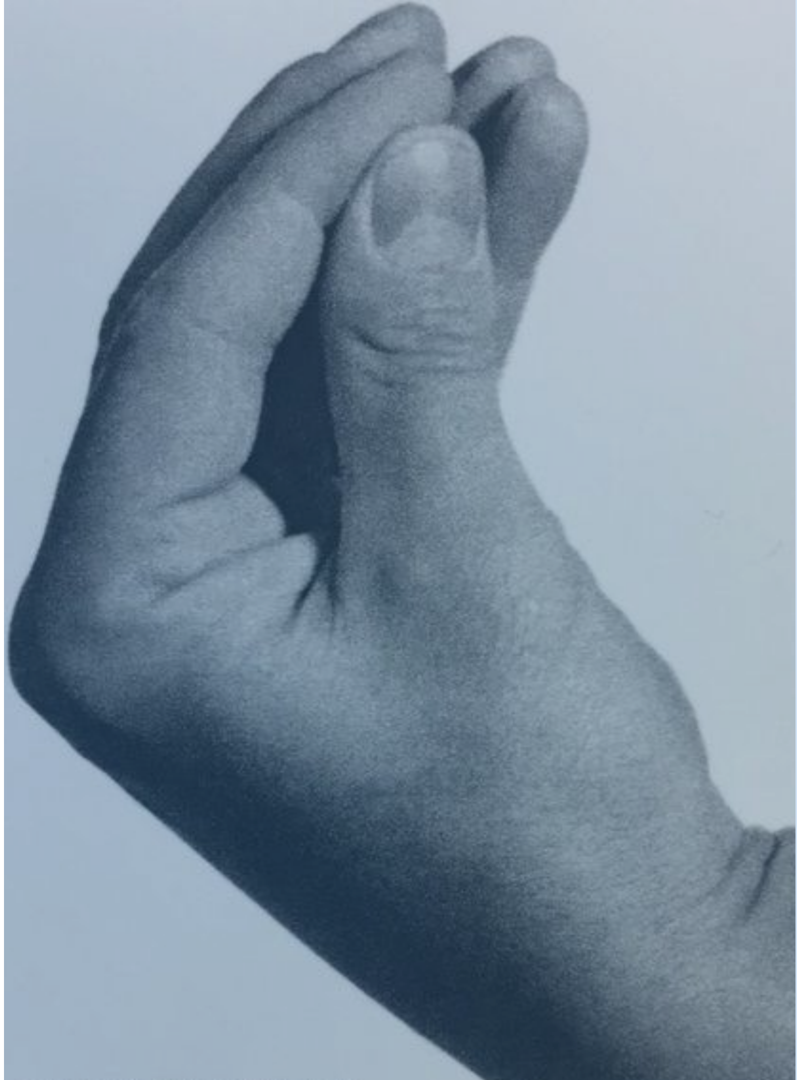
WELL-KNOWN ENDPOINT BUT IN A DIFFERENT WAY

Credential Revocations Check Mechanisms

OAuth Status List are good but …An RP can monitor the status of a credential outside the scope of the successful authentication of the user (monitoring it over time).

We use OAuth Status Assertions (still an I-D draft).

Why don’t you use ZKP, AnonCreds and or Bls Signatures?



HONEST... I RAN OUT OF GAS!
--I HAD A FLAT TIRE!
I DIDN'T HAVE ENOUGH MONEY FOR CAB FARE!
MY TUX DIDN'T COME BACK FROM THE CLEANERS!
AN OLD FRIEND CAME IN FROM OUT OF TOWN!
SOMEONE STOLE MY CAR!
THERE WAS AN EARTHQUAKE!
A TERRIBLE FLOOD!
LOCUSTS!
IT WASN'T MY FAULT, I SWEAR TO GOD!!!

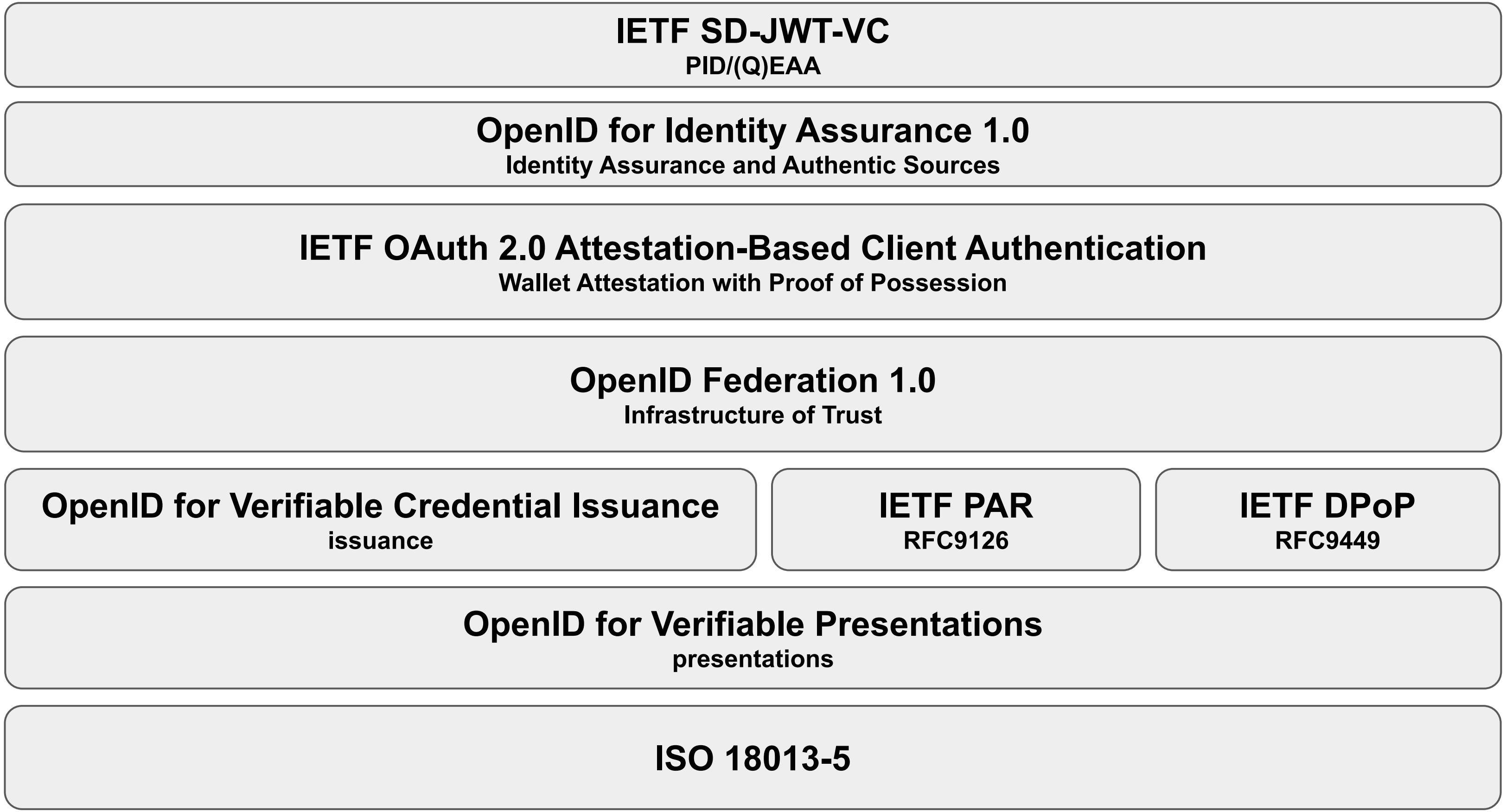
BACKUP & RESTORE

Exporting data containing the identifier of the VCI and the type of credential issued, such that the import of this into another device requires the user to authenticate once for the activation of the new device and a particularly fast mechanism for requesting and obtaining all the other credentials.

two requirements:

- be online, because today national VCIs are remote
- have a little patience to allow the acquisition of each individual credential

Using IETF, OpenID and ISO



IETF SD-JWT-VC
PID/(Q)EAA

OpenID for Identity Assurance 1.0
Identity Assurance and Authentic Sources

IETF OAuth 2.0 Attestation-Based Client Authentication
Wallet Attestation with Proof of Possession

OpenID Federation 1.0
Infrastructure of Trust

OpenID for Verifiable Credential Issuance
issuance

IETF PAR
RFC9126

IETF DPoP
RFC9449

OpenID for Verifiable Presentations
presentations

ISO 18013-5

Milestones

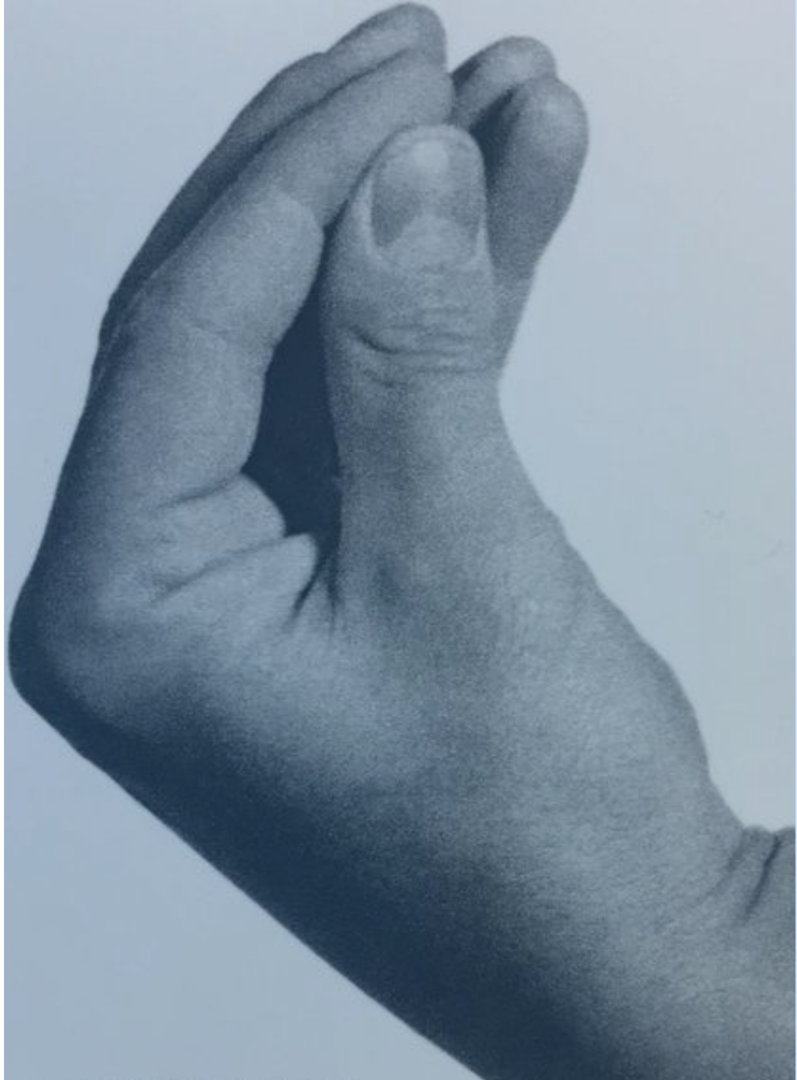
Technical Reference

https://github.com/italia/eudi-wallet-it-docs

Current Milestone

https://github.com/italia/eudi-wallet-it-docs/milestone/9

Hey … What about W3C Credential API?



MILESTONE 0.9 - 2025 Q1

Credential API

Security and Privacy requirements first:

- user-agents must not be able to track credential types and usage
- malevolent add-ons and user education represent a risk:
  - Are user-agents certifiable according the national and european regulation?

Trust Framework Interop

- user-agents might not be able to support whatever trust framework:
  - specialized trust evaluation mechanisms should be handled by specialized wallet solutions

OpenID Federation 1.0 compatibility:

- we are focused on using OpenID4VP to have this assurance at this level of integration.

THANK YOU FOR YOUR ATTENTION

May we have some conversation?

Giuseppe De Marco, gi.demarco@innovazione.gov.it

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