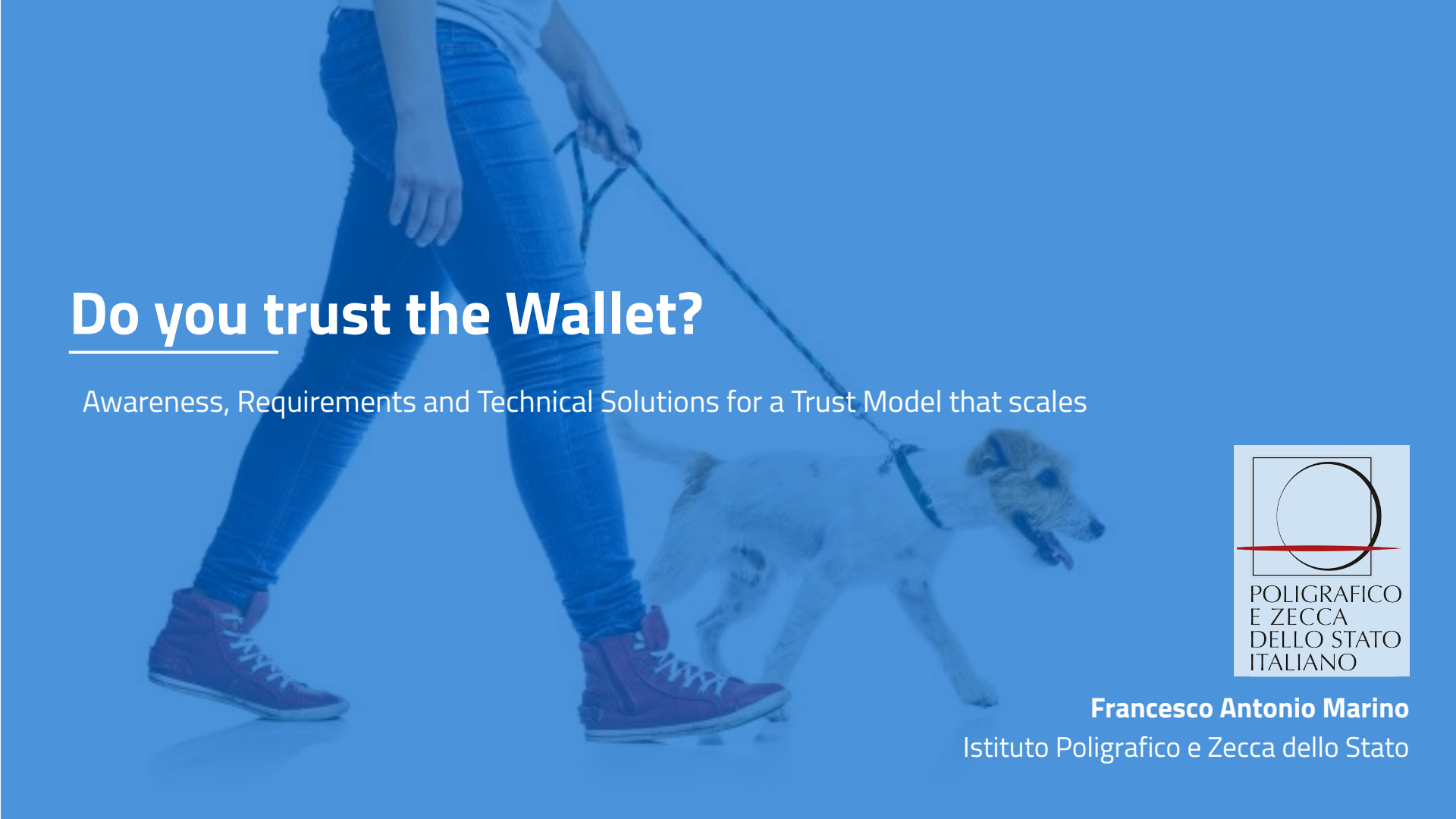


Do you trust the Wallet?

Awareness, Requirements and Technical Solutions for a Trust Model that scales

POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO

Francesco Antonio Marino
Istituto Poligrafico e Zecca dello Stato

Today we talk about

- What's **Trust** and why we're looking to a **Trust Model**:
  - Distributed, scalable, decentralized.
- **Digital Relationships** in the EUDI Wallet ecosystem.
- Awareness, assumptions, **Requirements** and **Solutions**.

FIRST OF ALL

What is Trust?

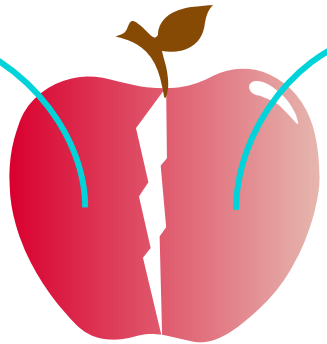
Trust is a strategy that reduces the complexity of reality and avoids the unwanted actions that in the real world may happen.

Trust Evaluation produces a positive proof of compliance to shared rules.

TRUST

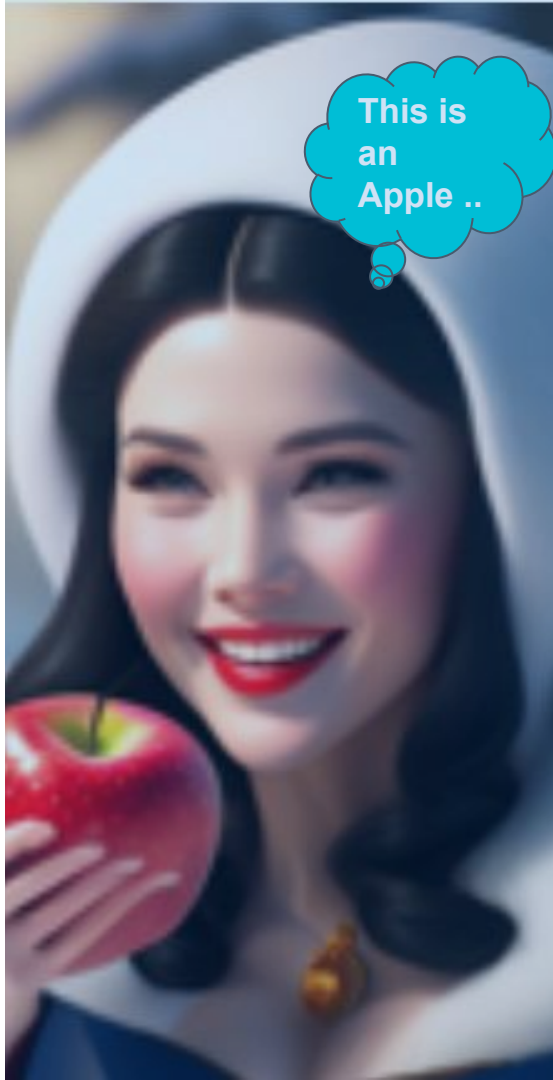
Identity

It's important to know who the party is that you're interacting with



Compliance

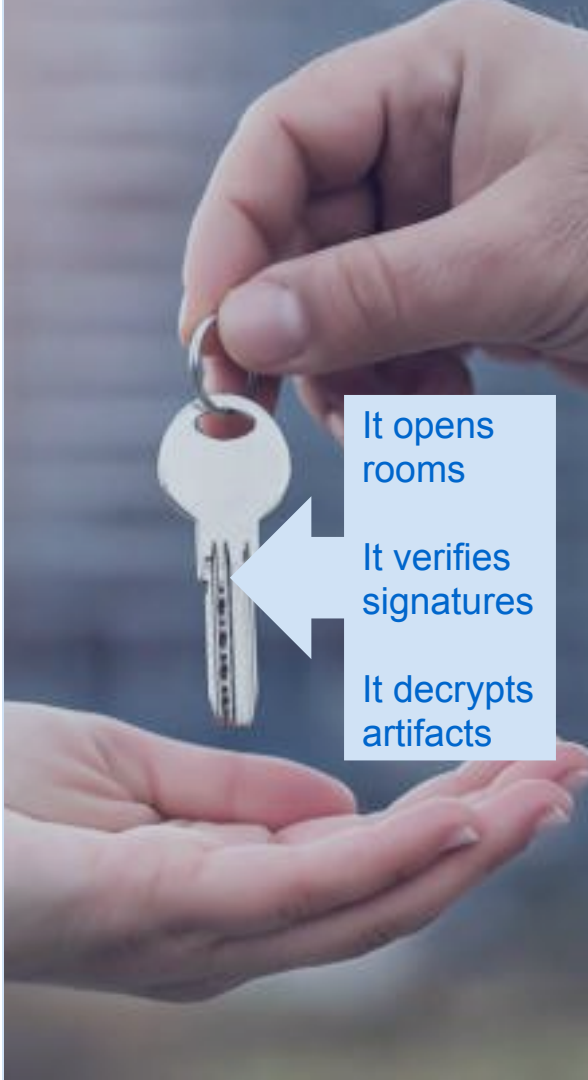
whether that party complies with terms and conditions shared by both parties



Key Attestation is just a part of the Trust

- Many of us today have a key of a hotel room in our pocket … isn't so?

- Obtaining the key **is the last thing after** the following actions has done:
  a. Issuer **discovery** -> Hotel research
  b. Issuer **evaluation** -> stars, ranking, reputation, compliance.
  c. Establishment of a **relationship** (contract) that cannot be repudiated over time (verifiable).



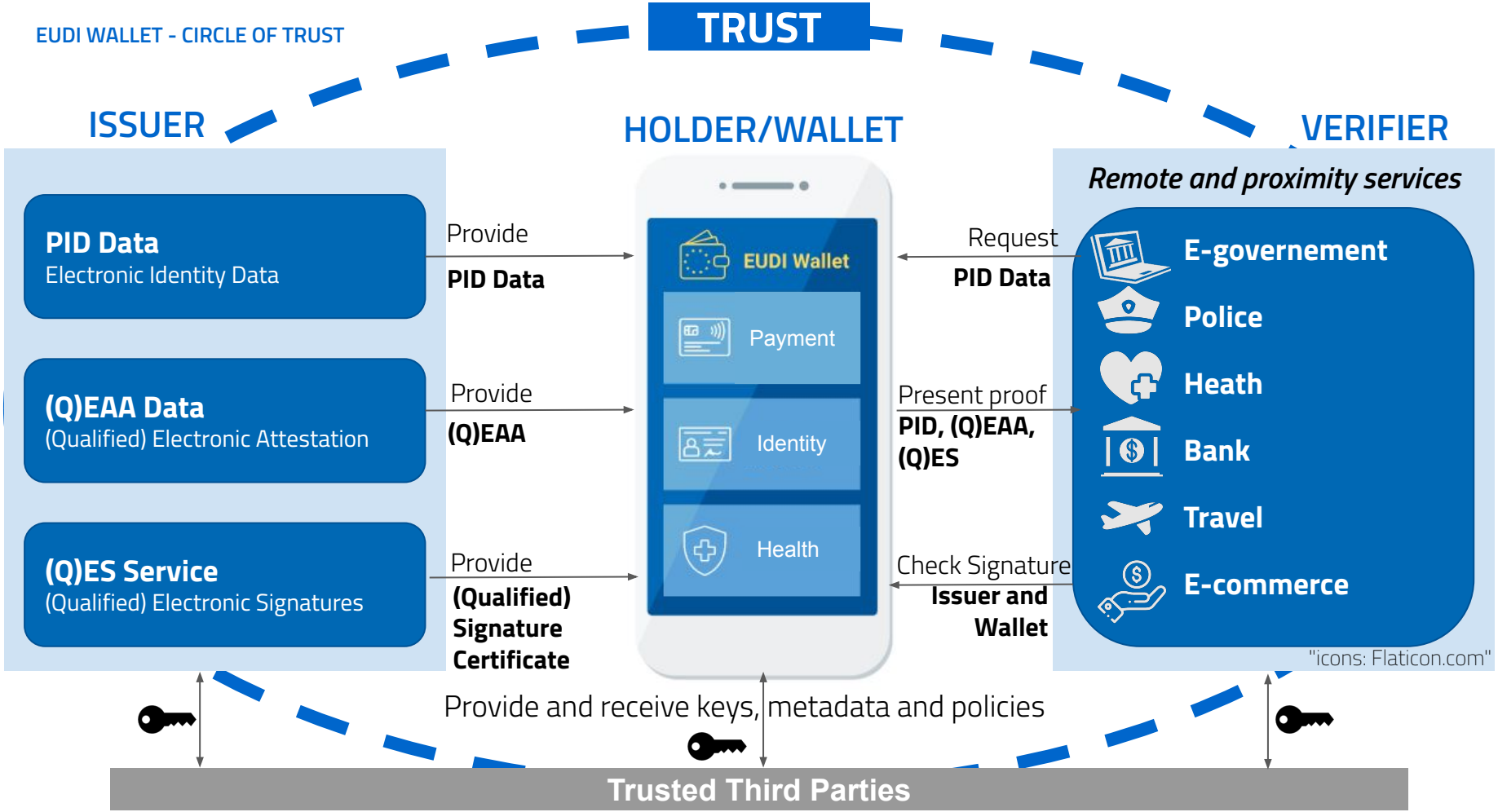
CRYPTOGRAPHIC KEYS ALONE ARE NOT ENOUGH TO CONSIDER A PARTY TRUSTWORTHY

EVERYDAY WE USE IDENTIFICATION OF FQDN AND KEY ATTESTIONS OVER THE WEB

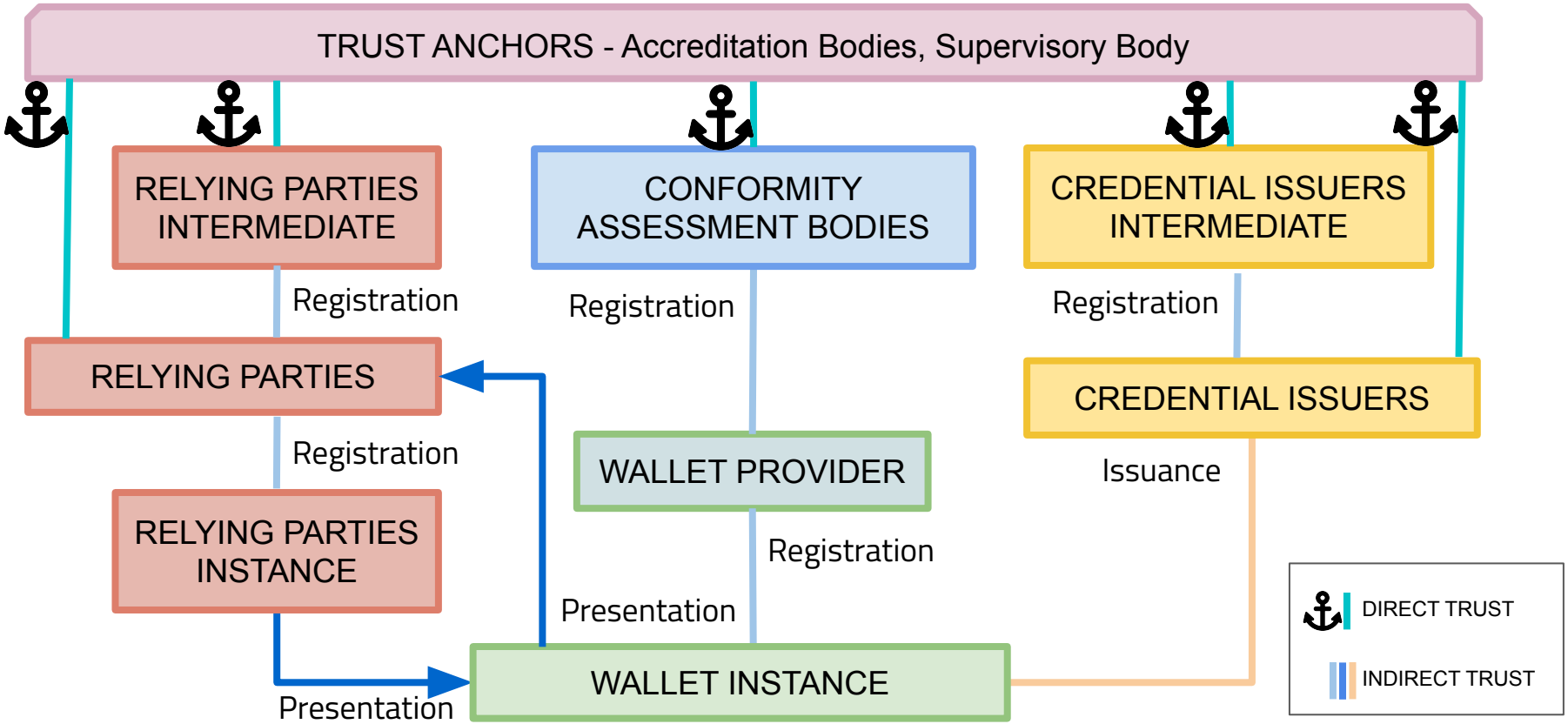
TLS offers us confidentiality and integrity over the transport by proving who we are talking to.

TLS alone doesn't tell us if it is compliant to the rules and if it will respect them.

“ TLS IS NOT ENOUGH FOR TRUST RELATIONSHIPS”


EUDI WALLET - CIRCLE OF TRUST
TRUST
ISSUER
HOLDER/WALLET
VERIFIER
PID Data
Electronic Identity Data
(Q)EAA Data
(Qualified) Electronic Attestation
(Q)ES Service
(Qualified) Electronic Signatures
Provide
PID Data
Provide
(Q)EAA
Provide
(Qualified) Signature Certificate
EUDI Wallet
Payment
Identity
Health
Request
PID Data
Present proof
PID, (Q)EAA, (Q)ES
Check Signature
Issuer and Wallet
Remote and proximity services
E-governement
Police
Heath
Bank
Travel
E-commerce
"icons: Flaticon.com"
Provide and receive keys, metadata and policies
Trusted Third Parties

EUDI WALLET - DIGITAL RELATIONSHIPS



THE USERS NEEDS THAT THEIR WALLET INSTANCES, THE ISSUERS AND THE RELYING PARTIES HAVE THE FOLLOWINGS

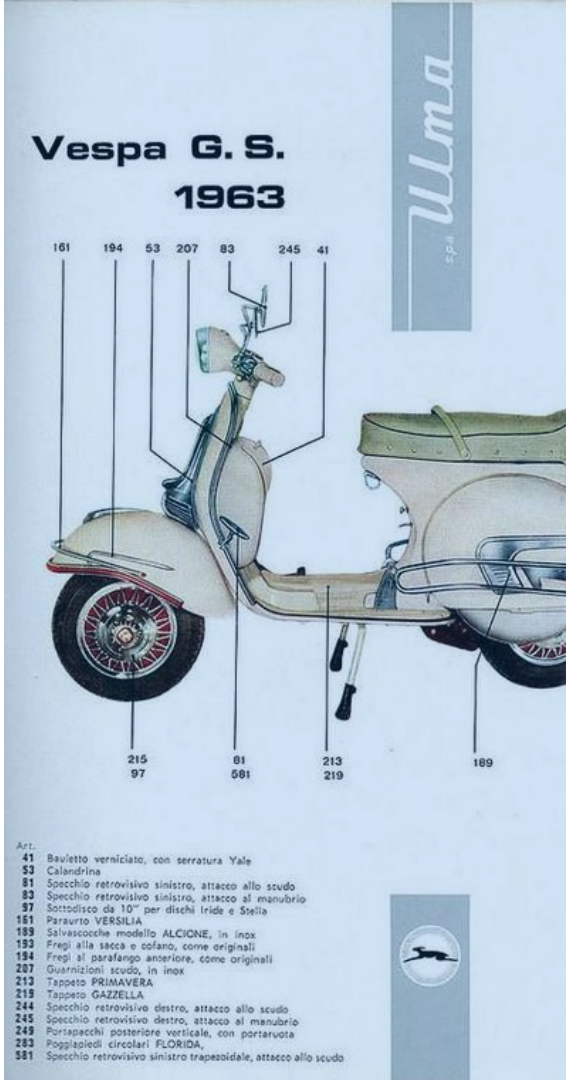
General TRUST REQUIREMENTS

1. Are they **who they say they are**? IDENTIFICATION
2. Are they compliant with the **security and privacy requirements** mandated by the **trust framework**? COMPLIANCE
3. **Verifiability**:
   a. cryptographic keys KEY ATTESTATION
   b. in both **remote** and **proximity** flows. USE CASE driven
   c. **over time.** NON-REPUDIATION

THE USERS NEEDS THAT THEIR WALLET INSTANCES HAVE THE FOLLOWINGS

REQUIREMENTS for Wallet Instance

1. It must prove that it is a valid instance of a trusted Wallet Solution, compliant with security and privacy requirements
    a. **secure storage** that prevents the steal/export of the private keys
    b. **proof of possession**, during presentations
    c. It must ensure user control
2. **Wallet Provider** can be banned and **needs periodical trust renewals**.



THE USERS NEEDS THAT RELYING PARTIES THEY INTERACT WITH HAVE THE FOLLOWING

REQUIREMENTS for Relying Party

1. It must be eIDAS compliant.
2. It verifies trust with Credential Issuers when validates credentials.
3. It verify trust with the Wallet Provider and compliance of Wallet Instances.
4. It cannot deny to have requested some credential or attributes to a Wallet Instance (**non repudiation** of the requests).

Photo by bearphotos from freepik

THE USERS NEEDS THAT CREDENTIAL ISSUERS THEY INTERACT WITH HAVE THE FOLLOWING

REQUIREMENTS for Credential Issuer

1. It must check the Wallet Instance authenticity and integrity and its compliance with the policies.
2. It must establish trust with the Wallet Provider.
3. It must provide a **non repudiation** mechanism so that it cannot deny to have issued some credential or attributes to a Wallet Instance.

ONCE WE HAVE DEFINED ASSUMPTIONS AND REQUIREMENTS ...

... IT'S TIME FOR SOLUTIONS

X509 PKI OR OpenID Federation 1.0

{
"**x5c**": […]
}
	{
	"**trust_chain**": […]
	}

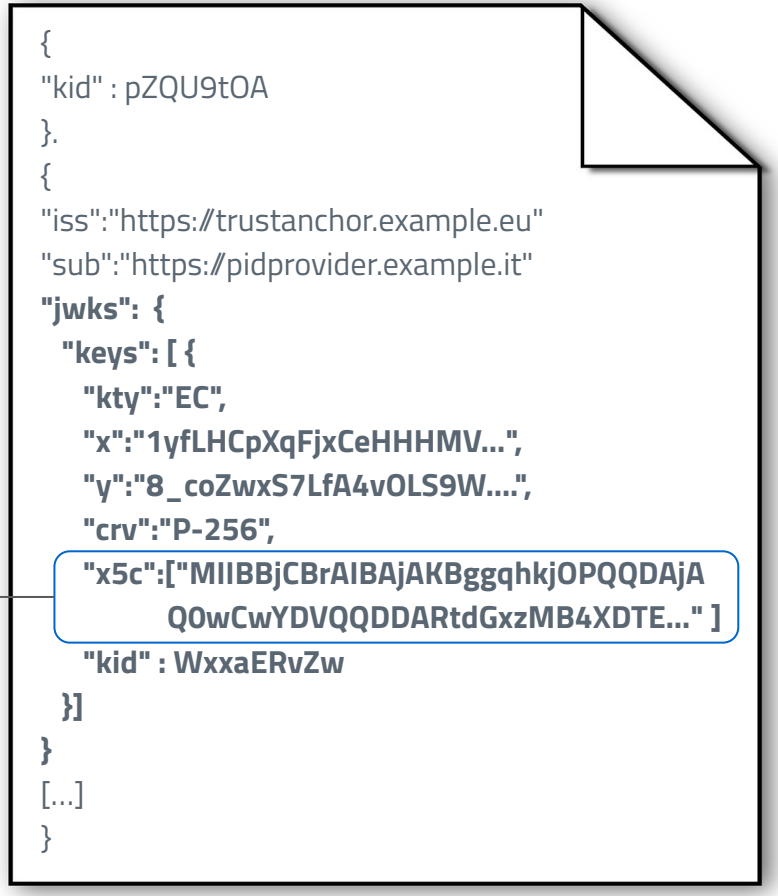
Chain of x509 Certificates	Chain of JWS
Verifiable with Root CA Certificate (Trust Anchor)	Verifiable with Trust Anchor public key
Revocation mechanisms are handled by CRL/OCSP	Revocation mechanisms are built in, as **also Trust Marks, Metadata Policies, Constraints, REST API**
It's x509!	JWT costs less and it's developer friendly … It can publish even x509!

X509 PKI AND **OIDC Federation 1.0**

Entity Statement

1. publishes the descendant's certificate.
2. X.509 Certificates Chain is carried within the Trust Chain.

-----BEGIN CERTIFICATE-----
MIIBBjCBrAIBAjAKBggqhkjOPQQDAjAPMQ0wCwYDVQQDDARtdGx
zMB4XDTE4MTAxDEyMzcwOVoXDTIyMDUwMjEyMzcwOVowDzE
NMAsGA1UEAwwEbXRsczBZMBMGByqGSM49AgEGCCqGSM49A
wEHA0IABNcnyxwqV6hY8QnhxxzFQ03C7HKW9OylMbnQZjjJ/Au08
/coZwxS7LfA4vO[...]
-----END CERTIFICATE-----



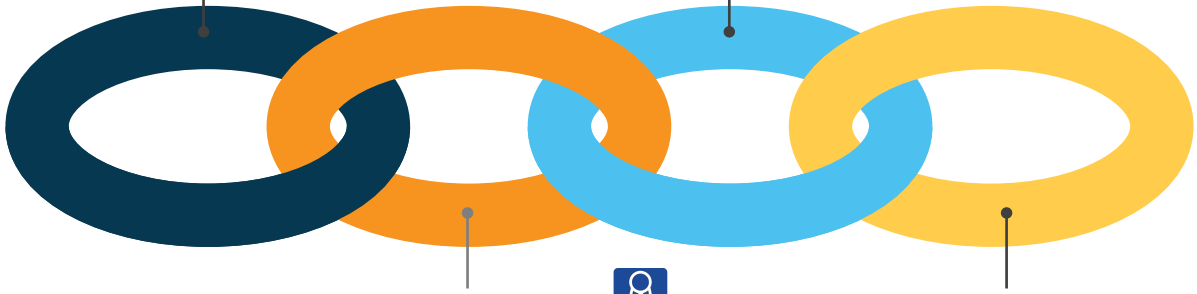
TRUST CHAIN for a WALLET PROVIDER that issues a WALLET INSTANCE ATTESTATION

1. Trust Anchor

Entity Configuration (JWS) with the **public key** or the **root x509 certificate** for chain validation.
Statement (JWS) related to the CAB with the **public key or the X509 certificate of the CAB**.

3. Wallet Provider

Wallet Instance Attestation (JWS) issued to the Wallet Instance, containing the **public key or the x509 certificate of the Wallet Instance.**
Entire verifiable trust chain of the Waller Provider in the header of JWS.



2. Conformity Assessment Body

Statement (JWS) related to the Wallet Provider with the **public key or the X509 certificate of the Wallet Provider**.

4. Wallet Instance

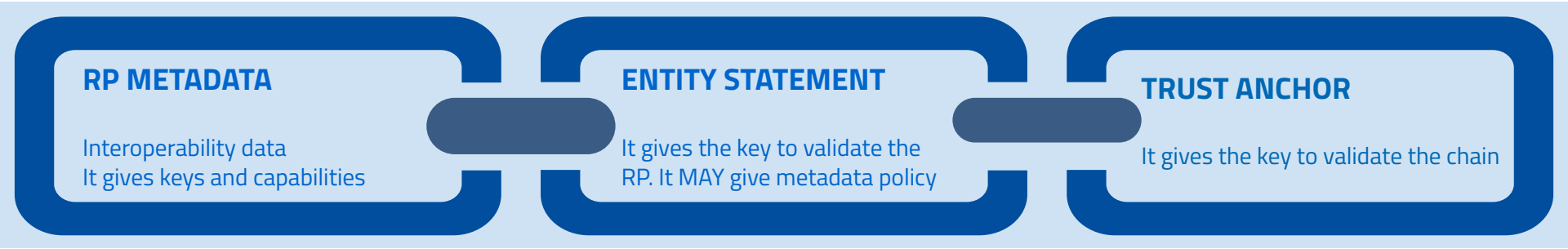
It generates a key pair whose **public key is contained in the Wallet Attestation** and **signed by the Wallet Provider**.

```
{
  "alg": "ES256",
  "kid": "$va-issuer-kid",
  "typ": "va+jwt",
  "trust_chain": [WalletProvider Trust Chain]
}
.
{
  "iss": "https://wp.example.org",
  "sub": "https://wp.example.org/$jwk-thumbp",
  "iat": 1665137911,
  "exp": 1665138911,
  "type": "WalletInstanceAttestation",
  "supported_loa": "high",
  "policy_uri": "https://.../policy",
  "tos_uri": "https://.../tos",
  "logo_uri": "https://.../logo.svg",
  "status": "https://.../status",
  "cnf": {
    "jwk": {
        "kty": "EC",
        "kid": "$wallet-jwk-thumbprint",
        "crv": "P-256",
        "x": "a1MdTboSUbq ...",
        "y": "f8n1IgpfYOBFZM0KxkTd0N5 ..."
    }
  }
}
```

COULD A RELYING PARTY ASK FOR USER ATTRIBUTES BESIDES THE PURPOSES OF ITS SERVICE? ONLY IF ALLOWED!

RP METADATA AND METADATA POLICY

TRUST CHAIN




```
{
  …
  "scope":
eu.europa.ec.eudiw.pid.1
eu.europa.ec.eudiw.pid.it.1

  “claims_required”:
given_name
email …
```

```
{
  …
  "metadata_policy":
    "claims_required":
      "subset_of”:
        [
          eu.europa.ec.eudiw.pid.1#given_name,
          eu.europa.ec.eudiw.pid.it.1#email
        ] … }
```

SD-JWT with Issuer Trust Chain in ...

The header

```
{
  "typ":"vc+sd-jwt",
  "alg":"RS512",
  "kid":"dB67gL7ck3TFiIAf7N6",
  "trust_chain" : [
    "NEhRdERpYnlHY3 ...",
    "eyJhbGciOiJSUzI1  ...",
    "lkJYdmZybG5oQU  ..."
   ]
}
```

The payload

```
{
  "iss": "https://pidprovider.example.it",
  "jti": "nw4J0zMwRk4kRbQ53G7z",
  "iat": "1541493724",
  "exp": "1541493724",
  "status": "https://pidprovider.example.it/status",
  "cnf": {
     "jwk": {   [...]  }
  },
  "type": "eu.europa.ec.eudiw.pid.it.1",
  "verified_claims": {
   "verification": {
    "_sd": [ "i6Zl0JOAHvDAoZKr_fYro1oIwX…" ],
    "trust_framework": "eidas",
    "assurance_level": "high"
   },
   "claims": {
    "_sd": [
     "8JjozBfovMNvQ3HflmPWy4O19Gpx…",
     "CFLGzentGNRFngnLVVQVcoAFi05r…",
     "JU_sTaHCngS32X-0ajHrd1-HCLCkp…",
     …
    ]
   }
  },
  "_sd_alg": "sha-256"
}
```

ISO 18013-5
Mobile Security Object

We can have OIDC Federation Trust Chain in *COSE Sign1* objects.

A binary json (BSON) can contain an entire Trust Chain.

CBOR Tag 262 enables embedded JSON Object but … a specialized COSE Header Parameters would be the way to go (27)

```
{
        "version": "1.0",
        "documents": [
        {
        "docType": "org.iso.18013.5.1.mDL",
        "issuerSigned": {
        "nameSpaces": {
                "org.iso.18013.5.1": [ ... ],
        },
        "issuerAuth": [
                h'a10126',
                {
                27: [EC, ES, ES, EC],
                },
                h'd81859039da66776657273696f6e6 ...',
                h'cff12c17d4739aba806035a9cb2b3 ...',
        ],
        ...
```

Federation Historical Keys endpoint...

... solves the problem of verifying historical Trust Chains when the Trust Anchors public keys are changed, due to expiry or revocation.


```
{
   "iss": "https://trust-anchor.federation.example.com",
   "iat": 123972394272,
   "keys":
      [
         {
            "kty":"RSA",
            "n":"5s4qi …",
            "e":"AQAB",
            "kid":"2HnoFS3YnC9tjiCaivhWLVUJ3Ax",
            "iat": 123972394872,
            "exp": 123974395972
         },
         {
            "kty":"RSA",
            "n":"ng5jr …",
            "e":"AQAB",
            "kid":"8KnoFS3YnC9tjiCaivhWLVUJ3Axw",
            "iat": 123972394872,
            "exp": 123974394972
            "revoked": {
              "revoked_at": 123972495172,
              "reason": "keyCompromise",
              "reason_code": 1
            }
         }
      ]
}
```

Conclusions

All the TRUST REQUIREMENTS are satisfied by:

- **OIDC Federation 1.0 capabilities** (Statements, Trust Chain, Policy, etc.), including the **ability to convey X.509 Certificate within Statements**.
- **Wallet Attestation** for the trust verification of the Wallet Instance.
- **Trust Chain** of the issuer **as JWS header parameter** and in the **Mobile Security Object**

Francesco Antonio Marino <**fa.marino at ipzs.it**>

Image by Zigmars Berzins from Pixabay