How do you know who to trust?

Trust establishment at scale with OpenID Connect Federation 1.0

Dr. Michael B. Jones
OpenID Foundation

Giuseppe De Marco
Department for Digital Transformation of the Presidency of the Council of the Minister, Italian Government

THE KEY QUESTION

How do you know who to trust?

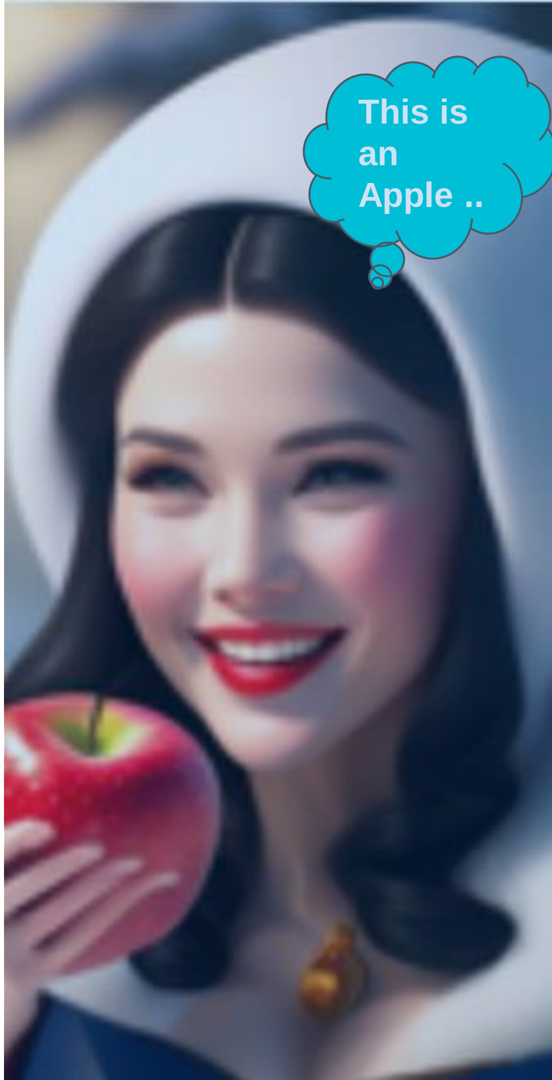
It's important to know who the party is that you're interacting with

IDENTITY

AND

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

COMPLIANCE



WE ESTABLISH THE TRUST WITH SIMPLE RULES

Equation for a relationship

PROOF of **IDENTITY**

+

PROOF of **COMPLIANCE** to requirements

=

TRUST

It is periodically renewed,
just like human relationships!

Picture by best5.it

KNOWING WHO IT IS DOESN'T MEAN YOU CAN TRUST THEM

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

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

“ TLS IS NOT ENOUGH FOR TRUST RELATIONSHIPS”

DETAILS MATTERS, ESPECIALLY WHEN THEY ARE MORE THAN DETAILS

OpenID Connect 1.0

Enables identities of participants to be securely established

Doesn’t answer the question of whether a participant is trusted to access a resource, such as your personal data

A complementary mechanism is needed for Trust establishment

Photo by Trae Nguyen from Burst

REQUIREMENTS FOR LARGE SCALE AND DYNAMIC DEPLOYMENTS

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**

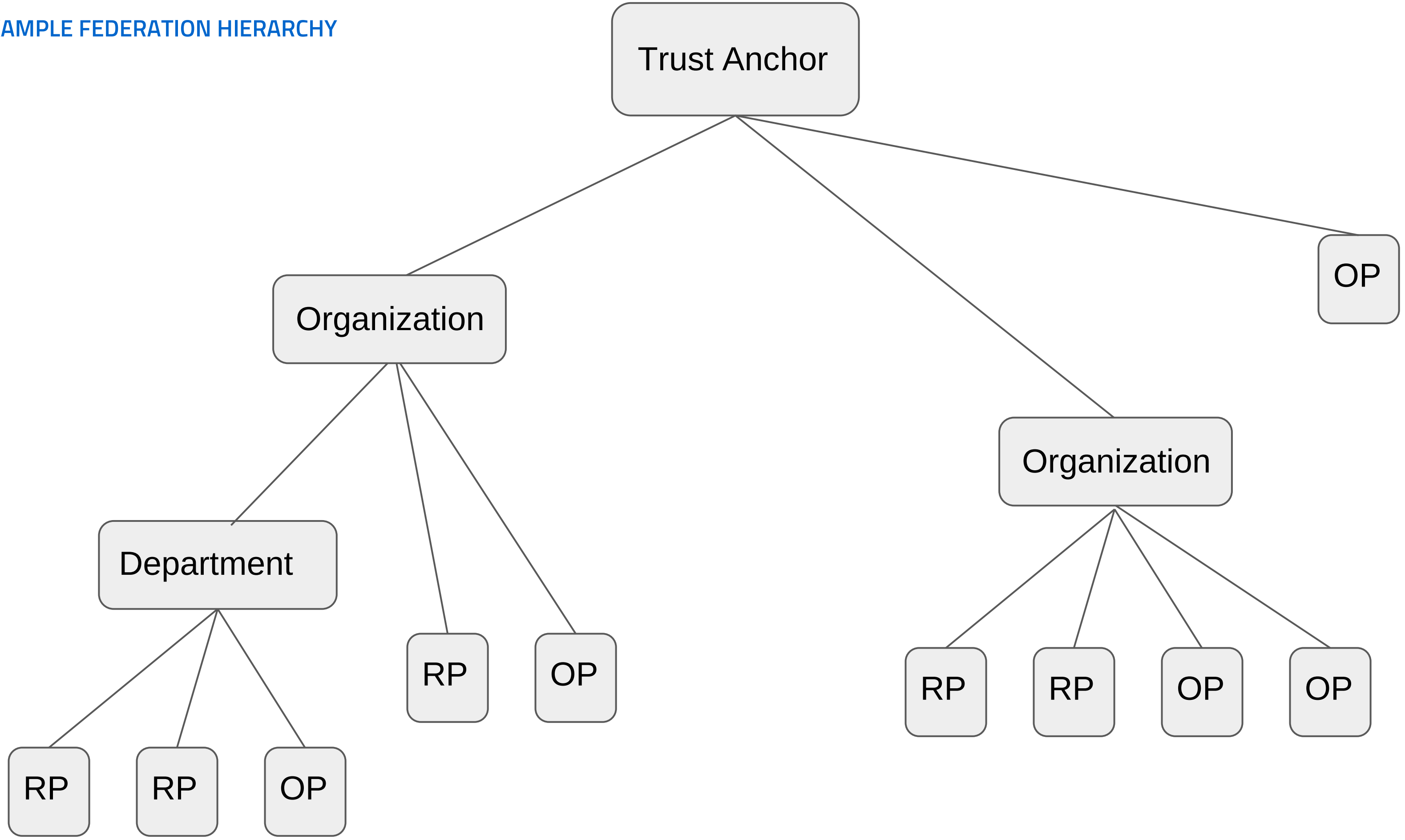
Public domain picture: Dreamstime.cor

TODAY WE TALK ABOUT

OpenID Connect Federation 1.0

- Enables scalable multilateral trust establishment
  - Determining that parties are both in a federation
  - Meaning that they both agree to the federation's legal agreements
- Enables policies to be applied
  - For instance, constraining participants to a particular set of signing algorithms
- Enables parties to be in multiple federations

EXAMPLE FEDERATION HIERARCHY



Trust Anchor

Organization

Organization

OP

Department

RP

OP

RP

RP

OP

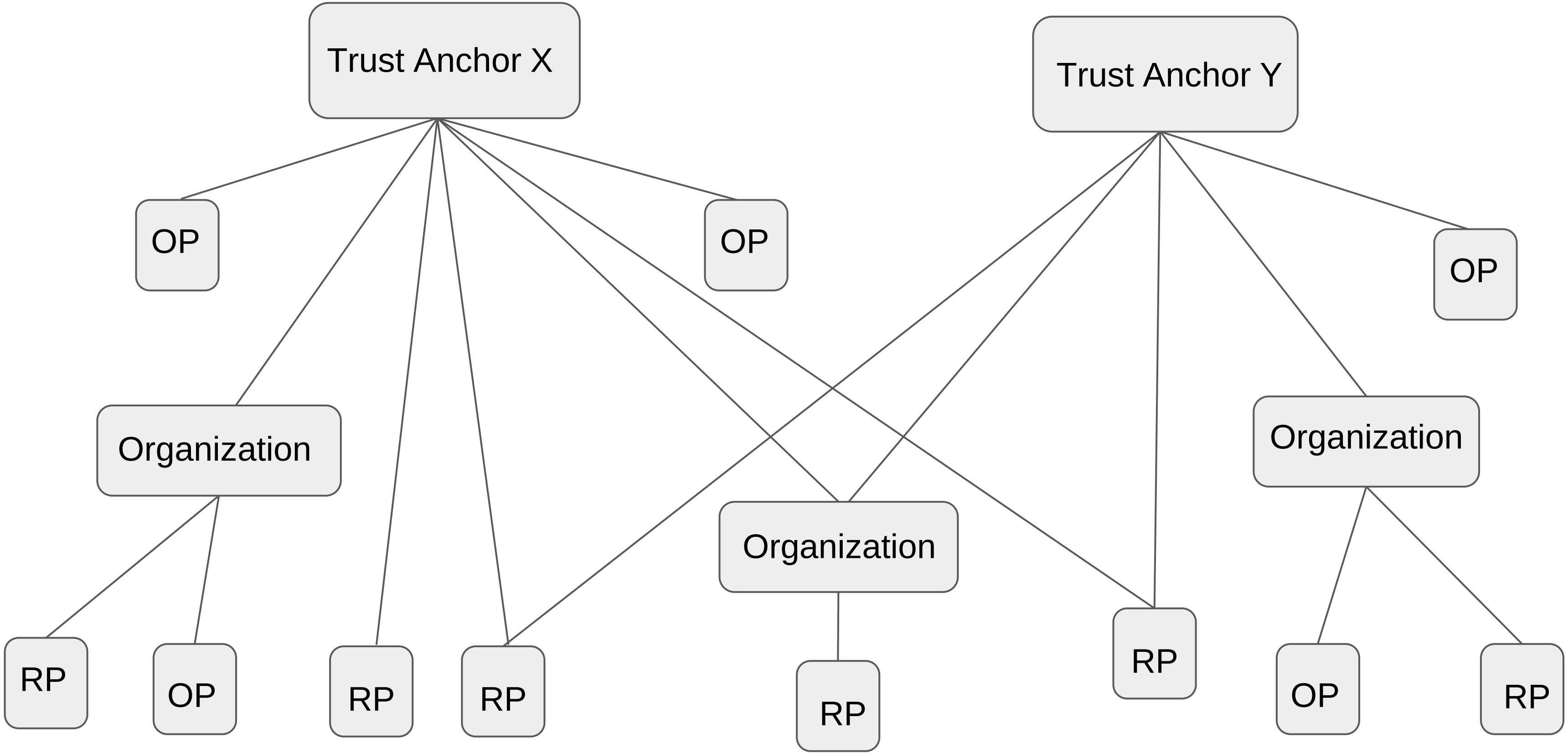
OP

RP

RP

OP

PORTRAIT OF MULTIPLE PARTICIPANTS OVER MULTIPLE FEDERATIONS OR TRUST SCOPES

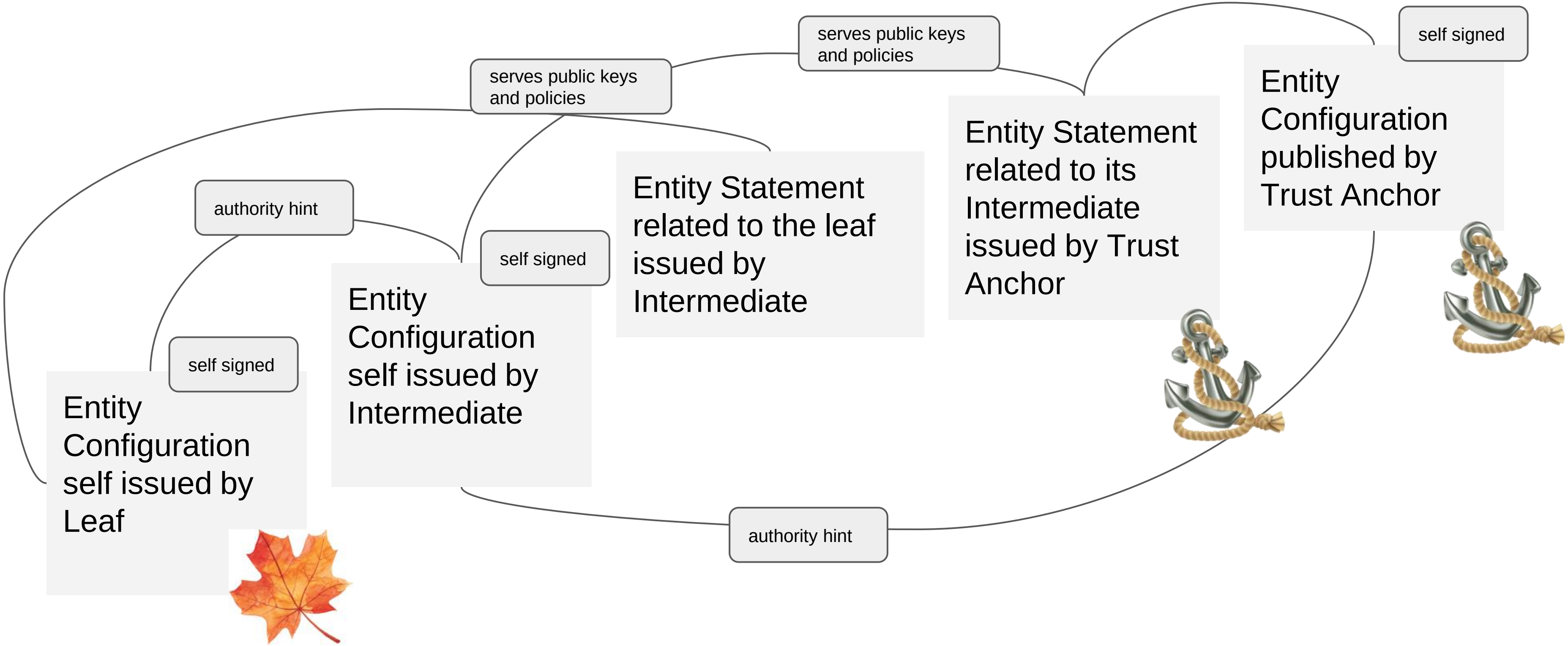


FEDERATION SPECIFICATION FEATURE

Trust Establishment

- Enables scalable multilateral trust establishment
- Trust established by demonstrating that participants share a trust anchor
- Participants host public statements about themselves
- Chain of signed statements about participants used to demonstrate trust anchor in common
- Chains part of a hierarchy of signed statements

THE PATH OF THE TRUST ESTABLISHMENT



Entity Configuration self issued by Leaf

self signed

authority hint

serves public keys and policies

Entity Configuration self issued by Intermediate

self signed

authority hint

Entity Statement related to the leaf issued by Intermediate

serves public keys and policies

Entity Statement related to its Intermediate issued by Trust Anchor

Entity Configuration published by Trust Anchor

self signed

THE TRUST CHAIN

- It expires; it must be renewed periodically
- It carries the policies used to produce the final metadata for the participant
- All you need is the public keys of the Trust Anchor to verify it at any time, even in the future
- What it attests is not repudiated over time, even if the keys change
- The compromise of a single node in the chain (Statement Issuer) invalidates the entire Chain

CRYPTOGRAPHICALLY VERIFIABLE ATTESTATIONS OF TRUST

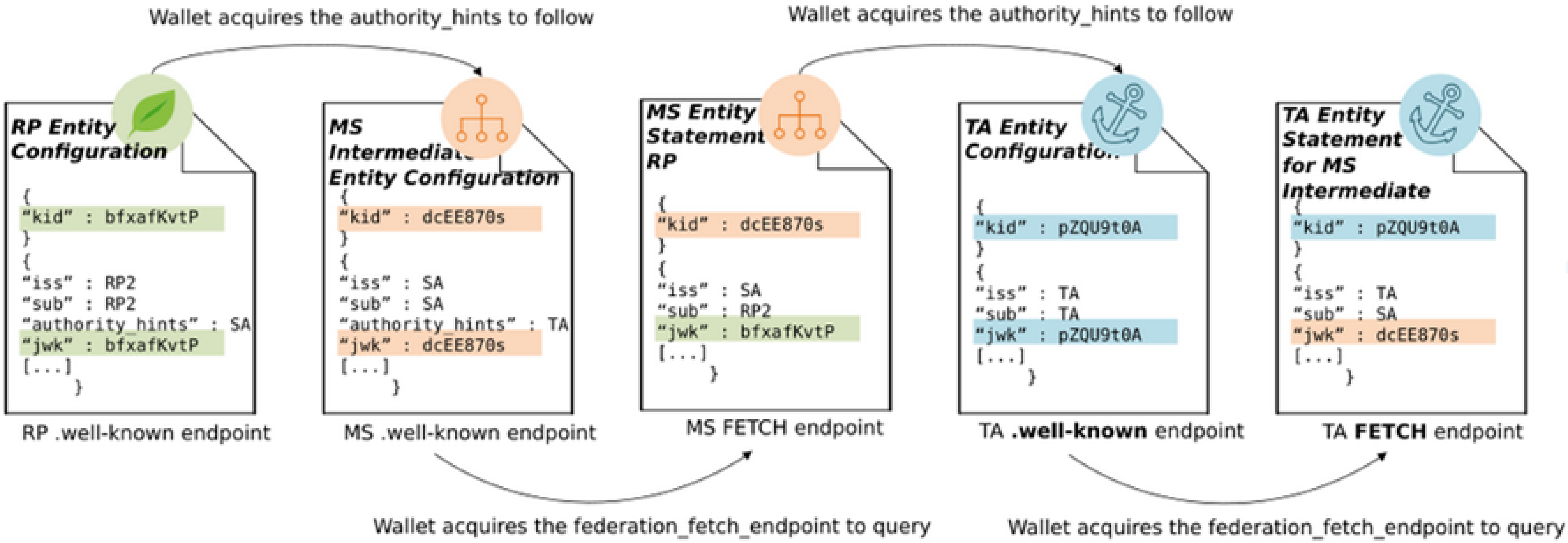
TRUST CHAIN

- A sequence of signed JWTs concatenated together
- The first element is self-signed by a subject (Leaf)
- From the second onwards, each JWT contains the JWK needed to verify the signature of the previous
- Issuer, subject, signature and public key bindings

```
trust_chain = [
   $EntityConfiguration-as-SignedJWT-selfissued-byLeaf,
   $EntityStatement-as-SignedJWT-issued-byTrustAnchor,
   $EntityConfiguration-as-SignedJWT-issued-byTrustAncor
]
```

BUILDING A TRUST CHAIN

Colored elements show the cryptographic bindings



Wallet acquires the authority_hints to follow

Wallet acquires the authority_hints to follow

RP Entity Configuration

```
{
"kid" : bfxafKvtP
}
{
"iss" : RP2
"sub" : RP2
"authority_hints" : SA
"jwk" : bfxafKvtP
[...]
    }
```

RP .well-known endpoint

MS Intermediate Entity Configuration

```
{
"kid" : dcEE870s
}
{
"iss" : SA
"sub" : SA
"authority_hints" : TA
"jwk" : dcEE870s
[...]
    }
```

MS .well-known endpoint

MS Entity Statement RP

```
{
"kid" : dcEE870s
}
{
"iss" : SA
"sub" : RP2
"jwk" : bfxafKvtP
[...]
    }
```

MS FETCH endpoint

TA Entity Configuration

```
{
"kid" : pZQU9t0A
}
{
"iss" : TA
"sub" : TA
"jwk" : pZQU9t0A
[...]
    }
```

TA **.well-known** endpoint

TA Entity Statement for MS Intermediate

```
{
"kid" : pZQU9t0A
}
{
"iss" : TA
"sub" : SA
"jwk" : dcEE870s
[...]
    }
```

TA **FETCH** endpoint

Wallet acquires the federation_fetch_endpoint to query

Wallet acquires the federation_fetch_endpoint to query

* NOTE: only the Key ID of the JWK is shown

FEDERATION SPECIFICATION FEATURE

Applying Policies

- Superior entities can apply policies to superiors
  - Trust roots can apply policies to all federation members
  - Organizations can apply policies to members

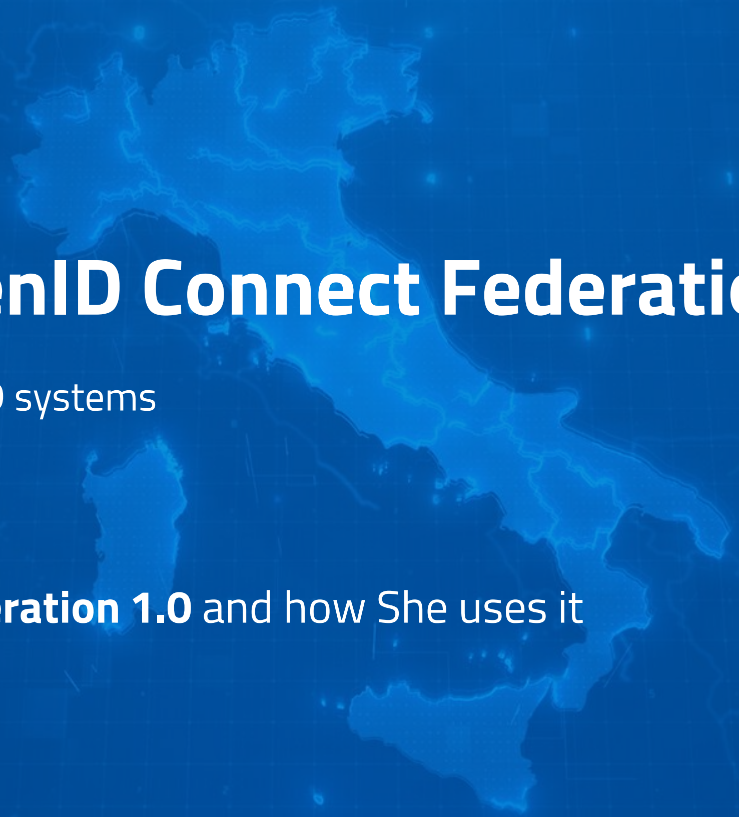
- Policies can be applied to any metadata values
  - For instance, algorithms used

FEDERATION SPECIFICATION FEATURE

Optimizations and Persistence

- REST API to evaluate entity relationships in real time
    - Rather than having to dynamically retrieve entity statements to make every trust decision

- Historical keys can be retained
    - Enables non-repudiation of long-lived assertions



The Italian OpenID Connect Federation

SPID and CIE id, the Italian eID systems

Why Italy uses OIDC Federation 1.0 and how She uses it

NATIONAL DIGITAL IDENTITY SCHEMES THAT LOOK TO THE FUTURE OF the EUROPEAN electronic IDentification, Authentication and trust Services

SPID

- **P**ublic **D**igital **I**dentity **S**ystem
- Over **34.9 millions of identity** provided to citizens
- Over **72 million accesses per month**
- 11 Private Service Identity Providers
- More than 14600 Service Providers

CIE id

- **E**lectronic **I**dentity **C**ard
- Over **35 millions of identity** provided to citizens
- Over **2 million accesses per month**
- 1 Public Service Identity Provider
- More than 7000 Service Providers

Born in 2014 and made operational in 2016 with SAML 2

OpenID Connect iGov implementation profile preview published in 2019

Implementation profile adopted in 2022 with OpenID Connect Federation 1.0

STARTING FROM THE REQUIREMENTS RATHER THAN FROM THE TECHNOLOGICAL EQUIPMENT

What were we looking for

- → **A way for all participants to publish their metadata online**
  ... not only for Identity Providers
- → **An accreditation mechanism across different organizations**
  ... to scale the accreditation bodies
- → **Safe and certifiable flows and attestations over time**
  ... no one can repudiate a request or data, for years

Photo by Matthew Henry from Burst

A STORY OF NON-REPUDIABILITY

The fate of long-lived attestations

Let’s imagine a request signed and issued by a RP to an OP and an ID Token issued and signed by an OP

After years, neither party can deny having asked for or received the data

The Trust Chain carries proof of metadata and keys

The Trust Anchor publishes the history of its revoked and expired keys, historical Trust Chain are always verifiable

AN OPEN SPECIFICATION, IN AN OPEN STANDARDIZATION PROCESS

What did we find

- **.well-known/openid-federation** endpoint
  … signed multiple metadata for multiple roles

- **Intermediates**
  … a standard way of delegating accreditation functions across multiple organizations… delegation of trust!

- **Trust Marks**
  … Custom definitions of compliance profiles according to our trust framework, without touching protocols metadata

Photo by Farah from Burst

WHAT DID WE FIND

… And more …

- **Metadata Policy**
  allow us to apply security countermeasures on a large scale, automatically and with certainty of adoption within a configurable period of time

- **Freedom** for the participants
  … to **change their protocols metadata** without having to re-submit anything to the accreditation authorities. A dynamic infrastructure which reconfigures itself automatically, periodically

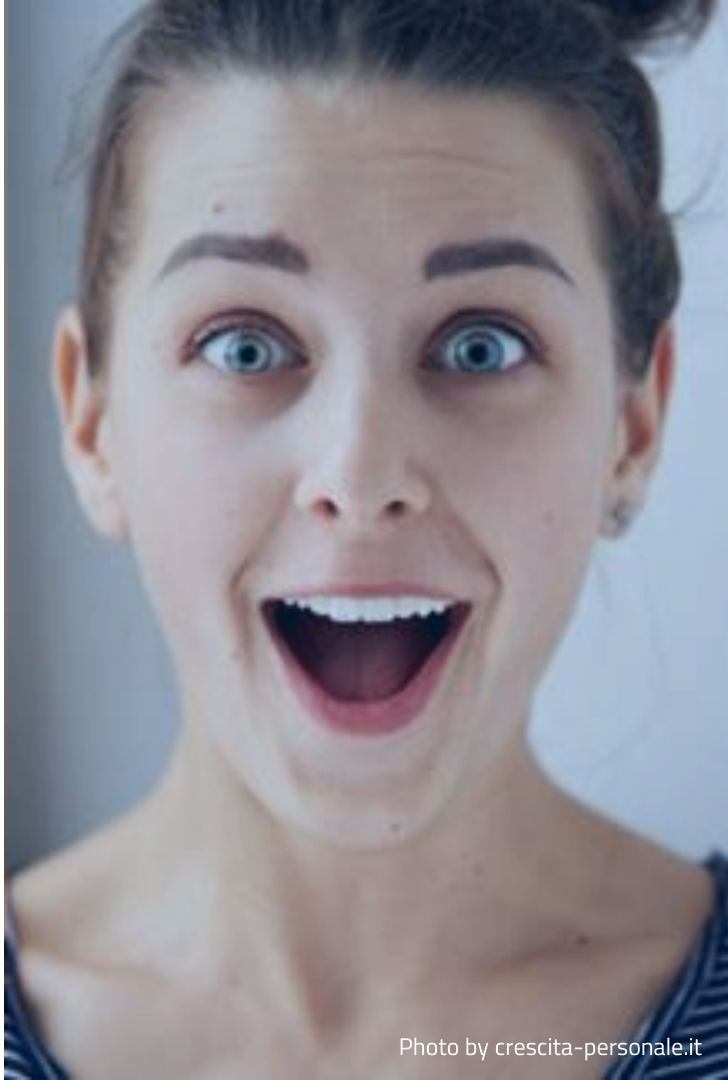


Photo by crescita-personale.it

IS OPENID FEDERATION A PKI? NOT ONLY, BUT YES.

x509 and OpenID Federation 1.0

{
“**x5c**”: […]
}
	{
	“**trust_chain**”: […]
	}

Sequence of x509 Certificates	Sequence of signed JWTs
Verifiable with the sole Trust Anchor public key	Verifiable with the sole Trust Anchor public key
Extended with CRL and 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!

WHAT ARE WE WORKING ON

It’s Time To Go … eIDAS 2.0

- ➔ Revision of the regulation has started by European Parliament
- ➔ Technological, market and legal developments in relation to the paradigms of Decentralised Identity and Self-Sovereign Identity
- ➔ Ongoing work for the development of the European digital identity Wallet, the EUDI Wallet
- ➔ **The user-centered paradigm exposes this to great dangers, trust mechanisms require automatic checks**. We really can’t leave the users alone is establish the trust with third parties.

Photo by Farah from Burst

Thank you

If you have any question please ask …

Mike Jones <**michael_b_jones at hotmail.com**>
Giuseppe De Marco <**demarcog83 at gmail.com**>

… Who you know you can trust !

Image by Zigmars Berzins from Pixabay