

# **COSE Header Parameter for Carrying OpenID Connect Federation Trust Chains**

---

draft-demarco-cose-header-federation-trust-chain

**Giuseppe De Marco**

## **cose-header-federation-trust-chain**

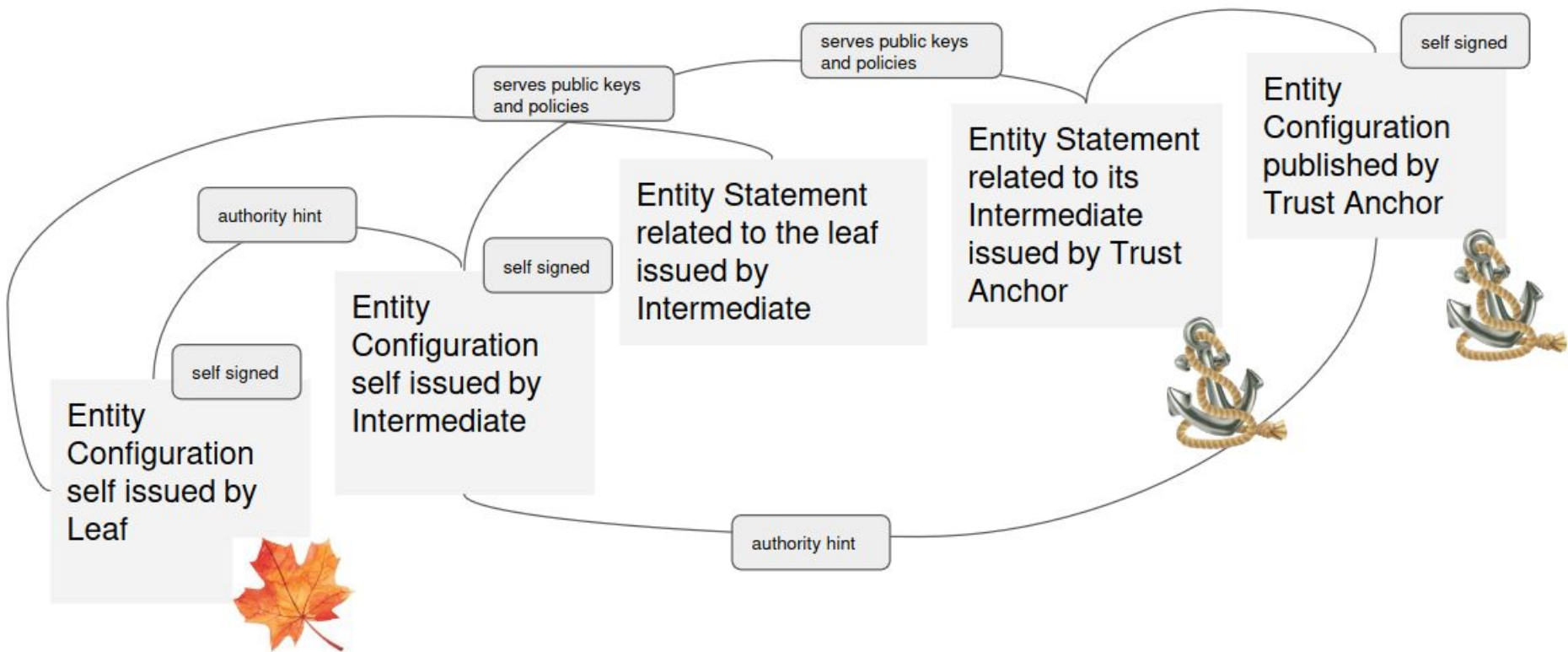
Proposes the use of the Trust Chains defined in OpenID Connect Federation 1.0 within the protected and the unprotected COSE Sign document headers.

# OpenID Connect Federation 1.0

## Trust Chain

A sequence of Entity Statements that represents a chain starting at a Leaf Entity and ending in a Trust Anchor.

## THE PATH OF THE TRUST ESTABLISHMENT



IS OPENID FEDERATION A PKI? NOT ONLY, BUT YES, IT'S SIMILAR BUT WITH SOME MORE POWERS

## X509 PKI and OpenID Federation 1.0

<pre>{   "x5c": [ ... ] }</pre>	<pre>{   "trust_chain": [ ... ] }</pre>
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 <b>also Trust Marks, Metadata Policies, Constraints, REST API</b>
It's x509!	Its API can even publish x509!



# FEDERATION TRUST CHAIN

## RP ENTITY CONFIGURATION

Interoperability data  
It gives keys and capabilities

```
{  
  ...  
  "claims_required":  
    eu.europa.ec.eudiw.pid.1  
}
```

## ENTITY STATEMENT

It gives the key to validate the  
RP. It MAY give metadata policy

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

## TRUST ANCHOR

It gives the key to validate the chain

## 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
      }
    }
  ]
}
```

# ISO 18013-5 Mobile Security Object

MSO it's a COSE Sign1 Document.

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

The Label 27 contains an entire Trust Chain.

```
{  
  "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 ...!  
        ],  
        ...  
      }  
    }  
  ]  
}
```

## Resources

the first implementation of this draft will be in this library:

- <https://github.com/IdentityPython/pyMDOC-CBOR>

That is born in support of the trust model for the Italian digital identity wallet, that looks forward to eIDAS 2.0 (EUDI Wallet) and has started its PoC using OpenID Connect Federation for building the trust infrastructure.

Here its draft:

- <https://italia.github.io/eudi-wallet-it-docs/versione-corrente/en/>

# Thank you

Giuseppe De Marco <demarcog83@gmail.com>



Image by Zigmars Berzins from Pixabay