Multi-Proof VCs

DIF Interop Call US/EU 3 Feb 2020

DIF

markus@danubetech.com

Linked Data Proofs 1.0

https://w3c-ccg.github.io/ld-proofs/

Proof Sets
Proof Chains

EXAMPLE 3: A proof set in a Linked Data document

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "title": "Hello World!",
  "proof": [{
    "type": "Ed25519Signature2018",
    "proofPurpose": "assertionMethod",
    "created": "2019-08-23T20:21:34Z",
    "verificationMethod": "did:example:123456#key1",
    "challenge": "2bbgh3dgjg2302d-d2b3gi423d42",
    "domain": "example.org",
    "jws": "eyJ0eXAiOiJK...gFWFOEjXk"
  },
  {
    "type": "RsaSignature2018",
    "proofPurpose": "assertionMethod",
    "created": "2017-09-23T20:21:34Z",
    "verificationMethod": "https://example.com/i/pat/keys/5",
    "challenge": "2bbgh3dgjg2302d-d2b3gi423d42",
    "domain": "example.org",
    "jws": "eyJ0eXAiOiJK...gFWFOEjXk"
  }]
}
```

```
{
  "@context": [
       "https://www.w3.org/2018/credentials/v1",
       "https://essif.europa.eu/schemas/vc/2019/v1",
       "https://essif.europa.eu/schemas/eidas/2019/v1"],
  "id": "did:ebsi-eth:00000001/credentials/1872",
  "type": ["VerifiableCredential", "EssifVerifiableID"],
  "issuer": "did:ebsi-eth:00000001",
  "issuanceDate": "2019-06-22T14:11:44Z",
  "credentialSubject": {
       "id": "did:ebsi-eth:00000002",
       "currentFamilyName": "Franz",
       "currentGivenName": "Hinterberger",
       "dateOfBirth": "1999-03-22T00:00:00Z",
       "placeOfBirth": "Salzburg, Austria"
  },
  "proof": [ {
       "type": "EcdsaSecp256k1Signature2019",
       "created": "2019-06-22T14:11:44Z",
       "proofPurpose": "assertionMethod",
       "verificationMethod": "did:ebsi-eth:00000001#key-1",
       "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
       sITJX1CxPCT8yAV-TvkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-Wuc"
  }, {
       "type": "EidasSeal2019",
       "created": "2019-06-22T14:11:44Z",
       "proofPurpose": "assertionMethod",
       "verificationMethod": {
         "type": "EidasCertificate2019",
         "CertSerial": "1088321447"
        },
        "proofValue": "BD21J4fdlnBvBA+y6D...fnC8Y="
  } ]
}
```


ESSIF v1 Verifiable ID

Early draft from ESSIF v1 (outdated).

ESSIF v2 will provide updated specifications and examples.

Signatures and other Proofs

Proofs could be proof-of-work, or notarization on a blockchain, etc.


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/citizenship/v1"
  ],
  "type": ["VerifiableCredential","PermanentResidentCard"],
  "issuer": "did:sov:danube:YD1qi3CSxrHUs18Zu6dK8z",
  "issuanceDate": "2021-02-03T00:38:24Z",
  "identifier": "83627465",
  "name": "Permanent Resident Card",
  "description": "Government of Example Permanent Resident Card.",
  "credentialSubject": {
    "id": "did:gov:usa:dhs:uscis:d656a3c3-0f14-477c-9a9f-ae4c2524af32",
    "type": ["PermanentResident","Person"]
    "givenName": "JOHN",
    "familyName": "SMITH"
  },
  "proof": [ {
    "type": "Ed25519Signature2018",
    "created": "2021-02-03T00:38:24Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:sov:danube:YD1qi3CSxrHUs18Zu6dK8z#key-1",
    "jws":
"eyJjcml0IjpbImI2NCJdLCJiNjQiOmZhbHNlLCJhbGciOiJFZERTQSJ9..B_tDATN8_tdRpym6e5d7sNDVE4eUkv3qnBAKSK1PMF0PKRn2Cy2DLk
oLw-w4EMHA-cXX7fJ3J4xA9EcYBQtuBQ"
  }, {
    "type": "MerkleProof2019",
    "created": "2020-11-03T14:13:42.808099Z",
    "proofValue": "zMcm4LfQFUZk...",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:example:23adb1f712ebc6f1c276eba4dfa#key-1"
  }, {
    .. proof of blockchain notarization ..
  } ]
}
```