OpenID Connect for W3C Verifiable Credential Objects

OIDF SIOP Special Topics Call, 14.4.2021

Kristina Yasuda, Oliver Terbu, Torsten Lodderstedt, Adam Lemmon, Tobias Looker

Objectives

- Support request and presentation of Verifiable Credentials in ID Tokens and Userinfo responses
- Usable with all OpenID Connect Flows (SIOP, code, CIBA, …)
- Leverage OpenID Connect as simple to use protocol for wallet integrations
- Leverage W3C verifiable credentials to existing OpenID Connect deployments

Ideas

- Requests via “claims” parameter
- Simply claims or credential type + claims (selective disclosure)
- Delivery under discussion
  - VP Token as separate artifact + ID Token as Verifiable Presentation (current revision)
    - https://github.com/awoie/vp-token-spec
  - vp_jwt/vp_ldp/vc_jwt/vc_ldp Claims (https://github.com/awoie/vp-token-spec/pull/20)
    - https://github.com/Sakurann/vp-token-spec
  - Aggregated & Distributed Claims (https://github.com/awoie/vp-token-spec/pull/23)
    - https://github.com/awoie/vp-token-spec/tree/adc

vp_jwt Claim

```
{
   "id_token":{
      "acr":null,
      "vp_jwt":{
         "credential_types":[
            "https://www.w3.org/2018/cre
         ]
      }
   }
}
```

```
{
  "kid": "did:ion:EiC6Y9_aDaCsITlY06HId4seJjJ...b1df31ec42d0",
  "typ": "JWT",
  "alg": "ES256K"
}.{
   "iss":"https://self-issued.me",
   "aud":"https://book.itsourweb.org:3000/client_api/authresp/uhn",
   "iat":1615910538,
   "exp":1615911138,
   "sub":"did:ion:EiC6Y9_aDaCsITlY06HId4seJjJ-9...mS3NBIn19",
   "auth_time":1615910535,
   "nonce":"960848874",
   "vp_jwt":[
            "ewogICAgImlzcyI6Imh0dHBzOi8vYm9vay5pdHNvdXJ3ZWIub...IH0="
   ],
   "sub_jwk":{
      "crv":"P-384",
      "kty":"EC",
      "kid": "c7298a61a6904426a580b1df31ec42d0",
      "x":"jf3a6dquclZ4PJ0JMU8RuucG9T1O3hpU_S_79sHQi7VZBD9e2VKXPts9lUjaytBm",
      "y":"38VlVE3kNiMEjklFe4Wo4DqdTKkFbK6QrmZf77lCMN2x9bENZoGF2EYFiBsOsnq0"
   }
}
```

vp_ldp Claim

```
{
    "id_token": {
      "vp_ldp": {
        "credential
         "claims":
        {
          "given_na
          "family_n
          "birthdat
        }
      }
    }
}
```

```
{
   "iss":"https://self-issued.me",
   "aud":"https://book.itsourweb.org:3000/client_api/authresp/uhn",
   "iat":1615910538,
   "exp":1615911138,
   "sub":"did:ion:EiC6Y9_aDaCsITlY06HId4seJjJ...b1df31ec42d0",
   "auth_time":1615910535,
   "vp_ldp":[
     {
      "@context":[
         "https://www.w3.org/2018/credentials/v1"
      ],
      "type":[
         "VerifiablePresentation"
      ],
      "verifiableCredential":[
         {
            "@context":[
               "https://www.w3.org/2018/credentials/v1",
               "https://www.w3.org/2018/credentials/examples/v1"
            ],
            "id":"https://example.com/credentials/1872",
            "type":[
               "VerifiableCredential",
               "IDCardCredential"
            ],
            "issuer":{
               "id":"did:example:issuer"
            },
            "issuanceDate":"2010-01-01T19:23:24Z",
            "credentialSubject":{
```

Aggregated Claims

```
{
   "id_token":{
      "acr":null,
      "verifiable_credenti
         "credential_types
            "https://www.w
         ]
      }
   }
}
```


```
{
   "iss":"https://book.itsourweb.org:3000/wallet/wallet.html",
   "aud":"https://book.itsourweb.org:3000/client_api/authresp/uhn",
   "iat":1615910538,
   "exp":1615911138,
   "sub":"urn:uuid:68f874e2-377c-437f-a447-b304967ca351",
   "auth_time":1615910535,
   "nonce":"960848874",
   "sub_jwk":{
      "crv":"P-384",
      "ext":true,
      "key_ops":[
         "verify"
      ],
      "kty":"EC",
      "x":"jf3a6dquclZ4PJ0JMU8RuucG9T1O3hpU_S_79sHQi7VZBD9e2VKXPts9lUjaytBm",
      "y":"38VlVE3kNiMEjklFe4Wo4DqdTKkFbK6QrmZf77lCMN2x9bENZoGF2EYFiBsOsnq0"
   },
   "_credential_types":{
      "https://www.w3.org/2018/credentials/examples/v1/IDCardCredential":[
         "src1"
      ]
   },
   "_claim_sources":{
      "src1":{
         "format":"vp_jwt",
         "value":"eyJraWQiOiJkaWQ6aW9uOkVpQzZZOV9hRGFDc0lUbFkwNkhJZDRzZUpq...5SRU16ZEdsUWR6SkdTbWNpZ
      }
   }
}
```

Distributed Claims

```
{
   "id_token":{
      "acr":null,
      "verifiable_credential":{
         "credential_types":[
            "https://www.w3.org/2018/cr
         ]
      }
   }
}
```

```
{
   "iss":"http://server.example.com",
   "sub":"248289761001",
   "aud":"s6BhdRkqt3",
   "iat":1615910538,
   "exp":1615911138,
   "auth_time":1615910535,
   "nonce":"960848874",
   "sub_jwk":{
      "crv":"P-384",
      "ext":true,
      "key_ops":[
         "verify"
      ],
      "kty":"EC",
      "x":"jf3a6dquclZ4PJ0JMU8RuucG9T1O3hpU_S_79sHQi7VZBD9e2VKXPts9lUjaytBm",
      "y":"38VlVE3kNiMEjklFe4Wo4DqdTKkFbK6QrmZf77lCMN2x9bENZoGF2EYFiBsOsnq0"
   },
   "_credential_types":{
      "https://www.w3.org/2018/credentials/examples/v1/IDCardCredential":[
         "src1"
      ]
   },
   "_claim_sources":{
     "src1":{
         "format":"vp_jwt",
         "endpoint":"https://op.example.com/presentations/1234564",
         "access_token":"ksj3n283dkeafb76cdef"
      }
   }
}
```

Distributed Claims

```
GET /presentations/1234564 HTTP/1.1
Host: op.example.com
Authorization: BEARER ksj3n283dkeafb76cdef

HTTP/1.1 200 OK
Content-Type: application/ld+json

{
   "format":"vp_ldp",
   "value":{
      "@context":[
         "https://www.w3.org/2018/credentials/v1"
      ],
      "type":[
         "VerifiablePresentation"
      ],
      "verifiableCredential":[
         {
            "@context":[
               "https://www.w3.org/2018/credentials/v1",
               "https://www.w3.org/2018/credentials/examples/v1"
            ],
            "id":"https://example.com/credentials/1872",
            "type":[
               "VerifiableCredential",
               "IDCardCredential"
            ],
            "issuer":{
               "id":"did:example:issuer"
            },
            "issuanceDate":"2010-01-01T19:23:24Z",
            "credentialSubject":{
               "given_name":"Fredrik",
               "family_name":"Strömberg",
```

Next Steps

- Discuss and decide delivery method
- Ask Connect WG for adoption
- Incorporate encryption (e.g. confidentiality protection in case where OP is just a cloud agent)