SD-JWT-based Verifiable Credentials (SD-JWT VC)

draft-terbu-oauth-sd-jwt-vc-00

- Oliver Terbu (SprucelD)
- Daniel Fett (Authlete)
Recap SD-JWT

- Adopted by the OAuth WG
- Enables selective disclosure (SD) of individual claims included in a JWT
- No assumption about the included JWT claims
- Not a Verifiable Credential format
Recap SD-JWT

1. Issuer gives Holder:
   SD-JWT + all Disclosures

2. Holder gives
   Verifier: SD-JWT + selected Disclosures

3. Verifier checks:
   signature of SD-JWT + Disclosures are included in SD-JWT

*Claim given_name:*

- SHA-256 Hash: jsu9yVulwQQhFm_M3JlzMa5FzglhQG0DpfayQwLUK4
- Disclosure: WyIyR0xDNDJzS1FZUNmR2ZyeU5STjL3IiwgImdpmVu3X5hbbWUuLCAlCA1Sm90bl3d
- Contents: ["2GLC42sQveCfafryNR93W", "given_name", "John"]
Verifiable Credential

- An Issuer-signed assertion with claims about a Subject.
SD-JWT Verifiable Credentials (SD-JWT VC)

- Defines a profile of SD-JWT for Verifiable Credentials, similar to an ID Token is a specific profile of JWT
- Defines data formats and media types for Verifiable Credentials based on SD-JWTs with JSON payloads
- Defines validation and processing rules for verifiers and holders of Verifiable Credentials based on SD-JWTs
- Includes support for plain JWTs (non-SD)
Issuer-Holder-Verifier Model

draft-looker-oauth-jwt-cwt-status-list-01
Use Cases

- Issuing and presenting digital identity documents
- Supply chain integrity and transparency (SCITT) and content authenticity
- Client attestations
- Covers Issuer-Verifier-Holder Model cases with high security requirements...
  - Enables cloning/forgery/MITM protection
  - Can use hardware cryptography
    - (Cloud) HSMs
    - Hardware-backed keystores on mobile devices
  - Can be combined with FIPS-compliant or PQC algorithms
Why not other Technologies?

- “Simple” is a feature
  - Uses a JSON-based data model and JWT Claim Sets
  - Builds on well-understood technologies
  - Other technologies are
    - more complex
    - rely on less proven building blocks
    - less composable
    - Have licensing issues
    - Do not support hardware-backed cryptography

- SD-JWT and JWTs?
  - Good basis, but do not define specific requirements for Verifiable Credentials
SD-JWT VC

- Work started in April 2023
- Referenced by OIDF OID4VC High Assurance Profile
- Interested: eIDAS 2.0 ARF
- Current Github activity
  - 28 open issues
  - 12 contributors
Why OAuth WG?

- SD-JWT VC is based on specifications from OAuth WG
  - Data model uses JWT Claims and is JSON only
  - Uses existing (SD-)JWT security
  - Not based on W3C Verifiable Credential Data Model (VCDM)
- Community
  - Existing contributors are members of OAuth WG
  - OAuth members are the right experts for SD-JWT VC with focus on ...
    - Security & privacy
    - Online and remote flows
Next Steps

- Reviews from OAuth WG
- Work on open issues
- Call for adoption?
Deep Dive
Data Format

- Based on SD-JWT and contains
  - Issuer-signed JWT
  - Disclosures
  - Optional key binding JWT for presentations
- Has new media type: `application/vc+sd-jwt`
  - IANA consideration → media type registry
  - Serialized SD-JWT with specific JWT Claim Sets
  - Indicates JWT claim sets with plain JSON data
    - Registered IANA JWT claims; existing and new ones
    - Public and private claims
Data Format

- Required issuer-signed JWT Headers:
  - "typ": "vc+sd-jwt"
Data Format

- JWT Claim Sets in issuer-signed JWT
  - iss (required)
    VC issuer
  - iat (required)
    Issuance date of the VC proof
  - nbf (optional)
    Valid from date of the VC proof
  - exp (optional)
    Valid until date of the VC proof
  - cnf (optional)
    Cryptographic key binding method for cloning protection
New JWT Claim Sets in issuer-signed JWT (IANA considerations)

- type (required)
  VC type (IANA considerations)

- status (optional)
  Information how to read VC status

As defined in
https://datatracker.ietf.org/doc/draft-looker-oauth-jwt-cwt-status-list/
Data Format

- **type**
  - IANA consideration \(\rightarrow\) JWT claim registry
  - Defines required and optional claims in Issuer-signed JWT and SD-JWT Disclosures
    - SD and non-SD JWT claims
Data Format

- JWT Claim Set in key binding JWT
  - Now, as defined in latest SD-JWT spec
  - Note, prior version of SD-JWT did not specify claims
Verification and Processing

- Defines verification and processing rules for SD-JWT VCs
  - Requires SD-JWT verification and processing
  - And additional rules ...  
    - Optional validation of the VC status based on the `status` claim
    - Optional mechanism to retrieve the public key of the issuer based on JWT Issuer Metadata
JWT Issuer Metadata

- JWT Issuer Metadata
  - Based on issuer identifier → iss claim
- JWT Issuer Metadata Request
  - Based on .well-known URL
    - ./well-known/jwt-issuer
- JWT Issuer Metadata Response Parameters
  - issuer
  - jwks_uri
  - jwks
JWT Issuer Metadata

```
{
  "issuer":"https://example.com",
  "jwks":{
    "keys": [ 
      {
        "kid":"doc-signer-05-25-2022",
        "e":"AQAB",
        "n":"nj3YJwsLU ... OwMuzifQrMI9bQ",
        "kty":"RSA"
      }
    ]
  }
}

{
  "issuer":"https://example.com",
  "jwks_uri":"https://jwt-issuer.example.org/my_public_keys.jwks"
}
```
Verification and Processing

- Defines verification and processing rules for presentations of SD-JWT VCs
  - Requires SD-JWT verification and processing
  - And additional rules ...
    - Optional key binding JWT has to be verified by `cnf` claim
Example: Input JWT Claim Set for SD-JWT

{
    "iss": "https://pid-provider.memberstate.example.eu",
    "iat": 1541493724,
    "type": "PersonIdentificationData",
    "first_name": "Erika",
    "family_name": "Mustermann",
    "nationalities": [
        "DE"
    ],
    "birth_family_name": "Schmidt",
    "birthdate": "1973-01-01",
    "address": {
        "postal_code": "12345",
        "locality": "Irgendwo",
        "street_address": "Sonnenstrasse 23",
        "country_code": "DE"
    },
    "is_over_18": true,
    "is_over_21": true,
    "is_over_65": false
}
Example: `cnf` results in the following SD-JWT VC

```
eyJhbGciOiAiRVMyNTYiOjEyJfSc2QiOiAiBhJjA5VGJTdT8xMmkxyQ3FaYmczMUFG22JHeV9vbkJJEW1lB01qC0VMcHVrcWiCiaGM4xeXpGUld2819CVUhpYULoLTEyZzhyQ3RFYYh8yR0c2XY1rYWlAteVWXNCISiCI0Vms9BMExVz71QGkzhXSW4zzEG9zUWyyZ29EFz91Ltz7JFVNF1siZQiw1gjVBoDhBwBF1QWFLVVFbTmFtOVDDVVrVVBVOGk1xd2B2xshWcRAOJoJd2MjLCAiOTEwN1y1MVWUnFS1FvUhpCcy2CnMG0tZUl1ncFpBaEXOKOln40tm9H1yUy1sICJC0a16qMM2t11F1w1313d1uk1p1kT1V1cGfC1T1WnpvRMnRmkiakWvIgIwkgW1gj1j1rVFRDdMnWx1515MvqeVBzcO0RFR2FXTmVBgo1e19h0q22z1dCAi1kWID1NYVBhBr1dU1vzu1xZwF110UhmYx2u59WFc0CNW9C4nr4oX0qKVUXVZi2T0NCIS1CJ2MXVYY0pW6iy1JQdkuU2Ys5dE2P3d319NN6JQ1i2ld0V6iz1n01aR611sGtvAChs1S0teDdCv1dJVMviri111MVW1xWExNOG1lWihEMOyylrP1ZM3iy1LCAiVTcBEzc0T2jeFFFFHRNPblxAhJxQmrNvGRGTPTV91Zk2sV5W5ER1hPrM1vdv0TRSi1ISiC6JTQL1mMrrzxR2SF5q4WnvIZhXLe1NDWUXuUT0WEy0TFnxw8EZU1hOFBrI1sICJpc3Mi31011AaHR0cDHP6y9z70yQVJtdmKi1VL1wUVTvM1yvYm5C3rdGUx2xhbbXZs251dSiSC1JiQYXQi11axNTQWDXkzNz10LCAiXh1v1jogMTg4MzAwMDAwMCw15G1iO11aUIVGyc29uSWR1bnRp2m1jYXRpb25EYXRhWi1g9z199fghbic01iczh1LT1nIviSIQjJmyi1b71mp3ay1i6h1sa3R5ioglKVD1iwi1mNyd1i6iCQLT1I1ISiC4IjOj9LDVVQU5MT1d1uZ0thN1GGOv0rZ221NWb0hJUDFJTGlLsRGxXN3Z2DU1biW1MCIAeiS161CJaeGppVid1wK1R0hW0vC0UTWY201NjxAjXzVm121WNDRu2v0OUPYySFpRi1e19FQ.K5011gOQyT3FGBoj8yMpm11a5eSt0QhExAEO4-6l3Bc3q_aq2AQySVRnHzhQPyju4CngCJ1kreyHLO2i1LMdw1e0W-Wy1yr0DNzJX4ZUmmR2y2eUSSTj1131iwqmpcn0UX5hbW1CaIARKjpe2E1XQ-WyL1hiNWUNuMn2dHTTkj1OEOVze4w6tXVjmc11vEiu9Y1W1l1w1gk11c3R1cm1hmb41XQ-WyI2SWo3eUTYTPv1BHVWv9TUNrd21Iiw1gk1F10Q-Wy1j17Tha205W5LUBOUGV025129h1wmg1hQvmF1Pr2XMQLCBveyil4i0i1sAIvNVMZrNER6aXps1wq0xq12m1hbanAclg1Zt221wq12kKwprdpzqBy1j9XV0-WyJR1z19jN5l6cUF4F23QXmXmexMhdpbmc918tj1mpc3nr0X22bhwl1se9vUWY1l1wi1g1n1jg1p2H1Q1XQ-WyJBSngtDk1v1BycFRO7jRTT9Ux9hb1Im1iw1qmpcnr02GOFZOISiCIOTcZ1MtLAXLTA110-WyItNmhD2ZJFV3JljWg1VTVR1iwmgkF1Kj1c3MILCj71r1sC16Fi5s0h4e1j1V0WP1GdGI50wq2Wdpd0ZB3rco3yFXs6LYGc10nUT1T19xvBXVUSi1CJDeHEx0OycvVWYbdMVUUXzTsOGzd12a311NkFKZ1BaTh3kDvMF7M11gwImjxMk8wreER4xW1dL2M4cjJERKc3eWfSusXUZxhXOE1313Z6W6BBRIJpNGM1XSxIiqw1nb3rckv3Fb91jRIoj1EiyMzQ1l1wi1mMyx1Y2saXRI5jog1kLy2V2uHdv1iw1niNomC1dF9hZGYRZxbrj1jog1N1vbn5i1n0CC2F2G12Umg1mLcAI1Y291bnRyeV9j2bR1j1oqIKRFln1d-WyJzYnxpVXj1la12zyuF0d2hJe04401u0oMri1zZx292ZJFmpLiCBOc0nV1XQ-WyJXevFUB0k1xOGxxR1YREEtQk0Rkh1iwigIm1zX292ZXJF
fNjU1LC8y1WzxZw0-```
Example: Decoded Issuer-signed JWT Payload

```
{
  "sd": [
    "09TbSuol2i2Cq2bg31AFgbGy_UnMIXIHoMjsELpukqg",
    "0nyzFSWvK_BUH1aMhm12ghrCtVahrGJ6_-k2P-ySqa",
    "4VoA3a1VpmxMD8WIn3pOqQf3gfoVOvDYsN5E5R5Kd0",
    "5A88AmauAao-QANao95CYUKUPNTi_d_gAR8ayt29R2w",
    "910byr3UVRqRzQoPx8a2c0m-eMgp2AhLN6xNoGF5mc",
    "Ch-DBcL3kb4VbHIwtknn2dNUHthEq9M3joPdg6idih0",
    "I00fcdU0oDc5ucp5yy2ujqPssDVGaWNiUliNZ_awD0gc",
    "X9MaPaFwM4PfFEdytRdacinYoErz8EztBEGQaW0e44",
    "YlurWJy_-HBGns9f9tFOwv4cICRBCiKwEHfXFSfjpo",
    "rNhKoraag--x7BWIVhbbGXu1XXXLM8i2X3m2FZMgs",
    "xpsq6cqXQp2N0ZWhrqBckTkOM_efElUnDFXOFmowLSE",
    "zU4521kGbEKh82uH_8Kx3CUnvn1F4y1g2lq1DTgLx_8Pk"
  ],
  "iss": "https://pid-provider.memberstate.example.eu",
  "iat": 1541493724,
  "exp": 1883000000,
  "type": "PersonIdentificationData",
  "sd_alg": "sha-256",
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "X": "TCAER19Zvu3OHF4j4W4vfSV0HIP1IL11D1s7vCeGemc",
      "Y": "ZxjIWB2MQGHVWKVQ4hhSIirsVfuecCE6t4jT9F2HZQ"
    }
  }
}
```
SD-JWT-based Verifiable Credentials with Signed-JWT payloads (SD-JWT VC)
draft-terbu-sd-jwt-vc-

<table>
<thead>
<tr>
<th>Status</th>
<th>Email expansions</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Versions:**

<table>
<thead>
<tr>
<th></th>
<th>00</th>
<th>01</th>
<th>02</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-terbu-sd-jwt-vc</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Document**

<table>
<thead>
<tr>
<th>Type</th>
<th>Authors</th>
<th>Last updated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Current IETF Data Tracker

SD-JWT-based Verifiable Credentials (SD-JWT VC)
draft-terbu-oauth-sd-jwt-vc-00

<table>
<thead>
<tr>
<th>Status</th>
<th>Email expansions</th>
<th>History</th>
</tr>
</thead>
</table>

**Versions:**

00

draft-terbu-oauth-sd-jwt-vc 00

**Document** | **Type** | **Authors** | **Last updated**
---|---|---|---
| | Active Internet-Draft (individual) | Oliver Terbu, Daniel Fett |
| | | |

2023-07-10


Open Q&A
Thank you