

IETF 119, Vancouver
OAuth WG
July 2024



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

Oliver Terbu (MATTR), Daniel Fett (Authlete), Brian Campbell (Ping Identity)

Rough Agenda:

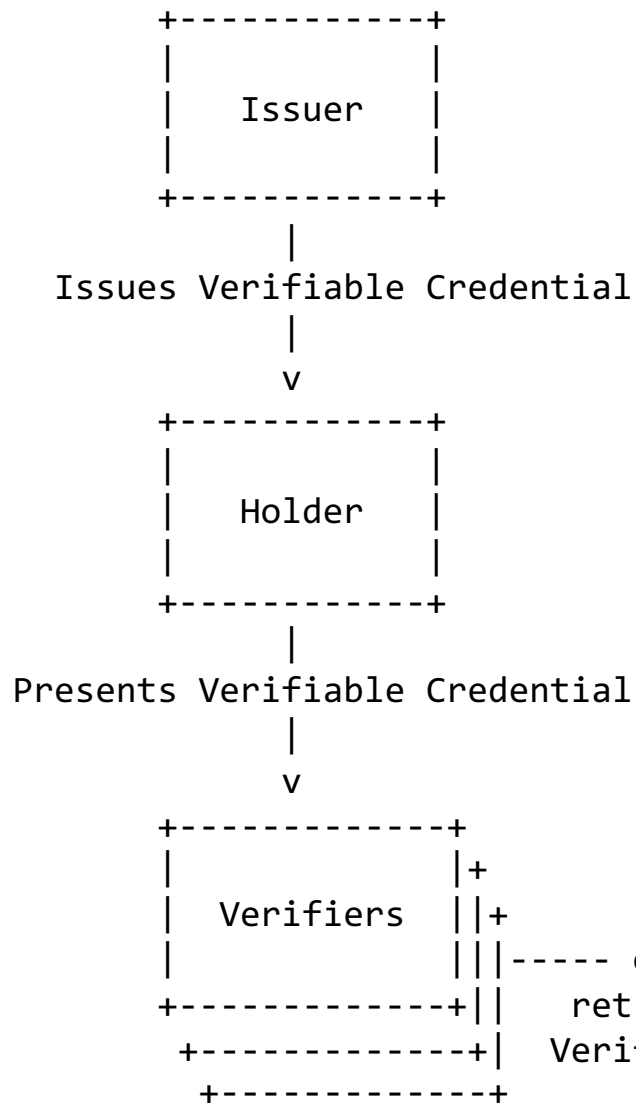
- Overview / refresher
- Changes since last time
- Open issues/questions
 - Next steps!



<https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/>

SD-JWT VC

Abstracting the Abstract



- Describes data formats as well as validation and processing rules to express Verifiable Credentials with JSON payloads with and without selective disclosure based on the SD-JWT format
- Uses SD-JWT and the well-established JWT content rules and extensibility model as basis for representing VCs
- Does **not** utilize the W3C's Verifiable Credentials Data Model v1.0, v1.1, or v2.0

Examples is as Examples does

Example shows how this stuff could be used to represent the concept of Person Identification Data (PID) using the data of a German citizen.

Input claims:

```
{
  "vct": "https://bmi.bund.example/credential/pid/1.0",
  "given_name": "Erika",
  "family_name": "Mustermann",
  "birthdate": "1963-08-12",
  "source_document_type": "id_card",
  "address": {
    "street_address": "Heidestraße 17",
    "locality": "Köln",
    "postal_code": "51147",
    "country": "DE"
  },
  "nationalities": ["DE"],
  "gender": "female",
  "birth_family_name": "Gabler",
  "place_of_birth": {"locality": "Berlin", "country": "DE"},
  "also_known_as": "Schwester Agnes",
  "age_equal_or_over": {"12": true, "14": true, "16": true, "18": true, "21": true, "65": false}
}
```

Examples is as Examples does

Example shows how this stuff could be used to represent the concept of Person Identification Data (PID) using the data of a German citizen.

Issued SD-JWT:

eyJhbGciOiAiRmYNTYiLCJAidHlwIjogInR5c2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6T6kxqMnZoOW80U0VYT2ZNaVlEdXZUeWtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDMm9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNMbHhLdUVBT0dHQNlQ3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0IiwiaXNjgZMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY3JlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6T6kxqMnZoOW80U0VYT2ZNaVlEdXZUeWtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDMm9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNMbHhLdUVBT0dHQNlQ3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0IiwiaXNjgZMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY3JlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6T6kxqMnZoOW80U0VYT2ZNaVlEdXZUeWtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDMm9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNMbHhLdUVBT0dHQNlQ3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0IiwiaXNjgZMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY3JlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6T6kxqMnZoOW80U0VYT2ZNaVlEdXZUeWtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDMm9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNMbHhLdUVBT0dHQNlQ3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0IiwiaXNjgZMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY3JlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6T6kxqMnZoOW80U0VYT2ZNaVlEdXZUeWtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDMm9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNMbHhLdUVBT0dHQNlQ3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0IiwiaXNjgZMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY3JlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6T6kxqMnZoOW80U0VYT2ZNaVlEdXZUeWtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDMm9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNMbHhLdUVBT0dHQNlQ3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0IiwiaXNjgZMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY3JlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2Q0IiwiaWw1U0lQeJmZn2tTV2U3QzM0bC0tODhnekppLWVCsjJwcl9ISndBVGciLCIAiOvpicGdN1RkRVc3cWfsNkJCwmXNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJJMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdEMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4eWtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGfPnklVNmQ3R1FhZ1hSN0F2R1RyblhU2xkM3o4RUlnXZ2ZM2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EYt3RqdUxBY3dBtXBEc2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVF

Examples is as Examples does

Example shows how this stuff could be used to represent the concept of Person Identification Data (PID) using the data of a German citizen.

SD-JWT payload:

```
{
  "_sd": [
    "0HZmnSIPz337kSWe7C34l--88gzJi-eBJ2Vz_HJwATg",
    "9Zbp1C7TdEW7qa16BBZ1MtqJdmeEOiXevdJ1oXVJdRQ",
    "I00fcFUoDXCucp5yy2ujqPssDVGaWNiUlinz_awD0gc",
    "IEBYSJGNhXIlrQo58ykXm2Zx3y119Z1TtToPo17QQiY",
    "Lai6IU6d7GQagXR7AvGTrnXgSld3z8EIg_fv3fOZ1Wg",
    "hvDXhwmGcJQsBCA20tjuLAcwAMpDsaU0nkovcK0qWNE",
    "ikuur8Q4k8q3VcyA7dC-mNjZBkReDTU-CG4niTE70TU",
    "qvzNLj2vh9o4SEXOfMiYDuvTykdsWCNg0wTdlr0AEIM",
    "wzW15bhCkvksxVvuJ8RF3xi8i64ln1jo_76BC2oa1ug",
    "z0eBXh xvIS4ZzmQcLlxKuEAOGGByj0qa1z2IoVx_YDQ"
  ],
  "iss": "https://example.com/issuer",
  "iat": 1683000000,
  "exp": 1883000000,
  "vct": "https://bmi.bund.example/credential/pid/1.0",
  "age_equal_or_over": {
    "_sd": [
      "Fc8I_07L0cgPwrDJKQyIG097wVsOp1MLjHvRC4R4-Wg",
      "XLtLjadUWc9zN_9hMJRoqy46UsCKb1IshZuuqUFKSCA",
      "aoCCzsC7p4qhZIAh_idRCSCa641uycnc8zPfNWz8nx0",
      "f1-P0A2dKWavv1uFnMX2A7-EXxvhoxv5aHhuEIN-W64",
      "k5hy2r018vrsJjo-Vjd6g6yt7AaonKonniuJ9ze13jo",
      "qp7Z_Ky1Yip0sYgD03zVug2MFuPNjHxksBDnJZ4aI-c"
    ]
  },
  "_sd_alg": "sha-256",
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu30HF4j4W4vfSVoHIP1ILilDls7vCeGemc",
      "y": "ZxjiWWbZMQGHVWKVQ4hbSIirsVfuecCE6t4jT9F2HZQ"
    }
  }
}
```

Examples is as Examples does

Example shows how this stuff could be used to represent the concept of Person Identification Data (PID) using the data of a German citizen.

Some Disclosures:

Claim given_name:

- SHA-256 Hash: 0HZmnSIPz337kSWe7C34l--88gzJi-eBJ2Vz_HJwATg
- Disclosure:
WyIyR0xDNDJzS1F2ZUNmR2ZyeU5STj13IiwgImdpdmVuX25hbWUiLCAiRXJp
a2EiXQ
- Contents: ["2GLC42sKQveCfGfryNRN9w", "given_name", "Erika"]

Claim family_name:

- SHA-256 Hash: I00fcFUoDXCucp5yy2ujqPssDVGaWNiUlinz_awD0gc
- Disclosure:
WyJlbHVWNU9nM2dTTk1J0EVZbnN4QV9BIiwgImZhbWlseV9uYW11IiwgIk11
c3Rlcm1hbm4iXQ
- Contents: ["e1uV50g3gSNII8EYnsxA_A", "family_name", "Mustermann"]

Claim birthdate:

- SHA-256 Hash: Lai6IU6d7GQagXR7AvGTrnXgSld3z8EIg_fv3f0Z1Wg
- Disclosure:
WyI2SWo3dE0tYTVpVlBHYm9TNXRtdlZBIiwgImJpcnRoZGF0ZSIsICIxOTYz
LTA4LTEyIl0
- Contents: ["6Ij7tM-a5iVPGboS5tmvVA", "birthdate", "1963-08-12"]

Claim source_document_type:

- SHA-256 Hash: qvzNLj2vh9o4SEX0fMiYDuvTykdsWCNg0wTd1r0AEIM
- Disclosure:
WyJlSThaV205UW5LUHB0UGVOZW5IZGhRIiwgInNvdXJjZV9kb2N1bWVudF90
eXB1IiwgImlkX2NhcmQiXQ
- Contents: ["eI8ZWm9QnKPPnPeNenHdhQ", "source_document_type",
"id_card"]

Claim street_address:

- SHA-256 Hash: bd1EVzgNopUk4EW3_eQ2n3_NU4iuX0Hv9XbGHN3g1TE
- Disclosure:
WyJRZ19PNjR6cUF4ZTQxMmExMDhpcm9BIiwgInN0cmVldF9hZGRyZXNzIiwg
IkhlaWRlc3RyYVx1MDBkZmUgMTciXQ
- Contents: ["Qg_064zqAxe412a108iroA", "street_address",
"Heidestra\u00dfe 17"]

Claim locality:

- SHA-256 Hash: f_FQYgvQWvyVqNnIXsARlNye7YGp8E77gRAjaq-wvnw
- Disclosure:
WyJBSngtMDk1VlBvcFR0TjRRTU9xUk9BIiwgImxvY2FsaXR5IiwgIktcdTAw
ZjZsbiJd
- Contents: ["AJx-095VPrpTtN4QM0qROA", "locality", "K\u00f6ln"]

Examples is as Examples does

Example shows how this stuff could be used to represent the concept of Person Identification Data (PID) using the data of a German citizen.

~~SD-JWT with a KB-JWT~~ SD-JWT+KB disclosing only nationality and that the person is over 18 years old:

eyJhbGciOiAiRVMyNTYiLCJAidHlwIjogInZjK3NkLWp3dCJ9.eyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6TktXqMnZoOW80U0VYT2ZNaVlEdXZUewtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDmM9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNmbHhLdUVBT0dHqn1qT3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0iAxNjgzMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY29tL2lzc3VlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6TktXqMnZoOW80U0VYT2ZNaVlEdXZUewtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDmM9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNmbHhLdUVBT0dHqn1qT3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0iAxNjgzMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY29tL2lzc3VlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6TktXqMnZoOW80U0VYT2ZNaVlEdXZUewtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDmM9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNmbHhLdUVBT0dHqn1qT3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0iAxNjgzMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY29tL2lzc3VlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6TktXqMnZoOW80U0VYT2ZNaVlEdXZUewtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDmM9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNmbHhLdUVBT0dHqn1qT3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0iAxNjgzMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY29tL2lzc3VlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6TktXqMnZoOW80U0VYT2ZNaVlEdXZUewtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDmM9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNmbHhLdUVBT0dHqn1qT3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0iAxNjgzMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY29tL2lzc3VlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS09xV05FIiwgIm1rdXVyOFE0azhxM1ZjeUE3ZEMtbU5qWkjrUmVEVFUQtQ0c0bmlURTdPVFUiLCAicXZ6TktXqMnZoOW80U0VYT2ZNaVlEdXZUewtkc1dDTmcwd1RkbHIwQUVJTSIsICJ3elcxNWJoQ2t2a3N4VnZ1SjhSRjN4aThpNjRsbjFqb183NkJDmM9hMXVnIiwgInpPZUJYaHh2SVM0WnptUWNmbHhLdUVBT0dHqn1qT3FhMXoySW9WeF9ZRFEiXSwgIm1zcyI6ICJodHRwcZovL2V4YW1wbGUuY29tL2lzc3VlciIsICJpYXQ0iAxNjgzMDAwMDAwLCAiZXhwIjogMTg4MzAwMDAwMCwgInZjdCI6ICJodHRwcZovL2JtaS5idW5kLmV4YW1wbGUuY29tL2lzc3VlZGVudGlhbC9waWQvMS4wIiwgImFnZV9lcXVhbF9vc19vdmVyIjogeyJfc2QiOiBbIjBIWm1uU0lQejMzN2tTV2U3QzM0bC0tODhnekppLWVCSjJwJ19ISndBVGciLCIAiOVpicGdN1RkrVc3cWFSNkJCWmxNdHFKZG1lRU9pWGV2ZEpsb1hWSmRSUSIsICJjMDBmY0ZVb0RYQ3VjcDV5eTJ1anFQc3NEVkdhV05pVWxpTnpfYXdeMGdjIiwgIk1FQl1TSkdOaFhJbHJRbzU4ewtYbTJaedN5bGw5WmxUdFRvUG8xN1FRaVkiLCAiTGFPnk1VNmQ3R1FhZ1hSN0F2R1RyblhnU2xkM3o4RUlnX2Z2M2ZPWjFXZyIsICJodkRYaHdtR2NKUXNcQ0EyT3RqdUxBY3dBtXBEC2FVMG5rb3ZjS0

Payload of the corresponding Key Binding JWT:

```
{
  "nonce": "1234567890",
  "aud": "https://example.com/verifier",
  "iat": 1720454295,
  "sd_hash": "VEz3t1Kj9V4S57M6hEhoV4Hs_RvjWeh3Tsu91Cn1neI"
}
```

Examples is as Examples does

Example shows how this stuff could be used to represent the concept of Person Identification Data (PID) using the data of a German citizen.

After validation, the Verifier will have this data for further processing:

```
{
  "iss": "https://example.com/issuer",
  "iat": 1683000000,
  "exp": 1883000000,
  "vct": "https://bmi.bund.example/credential/pid/1.0",
  "age_equal_or_over": {
    "18": true
  },
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu3OHF4j4W4vfSVoHIP1ILi1D1s7vCeGemc",
      "y": "ZxjiWWbZMQGHVWQVQ4hbSIirsVfuecCE6t4jT9F2HZQ"
    }
  },
  "nationalities": [
    "DE"
  ]
}
```

Since IETF 119 Brisbane...



What's new in -04?

- update reference to IETF Status List
- **Include Type Metadata**
- Include schema Type Metadata
- Editorial changes
- Updated terminology to clarify digital signatures are one way to secure VCs and presentations
- Rework key resolution/validation for x5c

Open Issues

☐	21 Open ✓ 106 Closed	Author ▾	Label ▾	Projects ▾	Milestones ▾	Assignee ▾	Sort ▾
☐	clarify example(s) #246 opened 1 hour ago by bc-pi						
☐	Ambiguity what should happen when no kid parameter is present in header when DID is used as iss value #245 opened 7 hours ago by TimoGlastra						
☐	use SD-JWT+KB in place of SD-JWT with a Key Binding JWT #243 opened last week by bc-pi						1
☐	Add 'vct' in well-known registry #242 opened last week by jtalir						
☐	Claim 'vct' is missing in Type Metadata Format #241 opened last week by jtalir						
☐	Add language on x5c protection #240 opened 2 weeks ago by awoie						1
☐	Is it required to validate the whole chain of schemas? #238 opened 3 weeks ago by awoie						
☐	Distinguish between issuance and presentation schemas discuss #237 opened 3 weeks ago by awoie						
☐	Fix resolving type metadata from URL and limit to HTTPS URLs #233 opened on May 17 by awoie						
☐	Consider recommending a way to encode other data types. #225 opened on Apr 2 by danielifett						1
☐	Add type metadata for basic display/rendering information metadata wg-05 #224 opened on Apr 2 by bc-pi						3
☐	I18N for Metadata discuss metadata PRIO wg-05 #223 opened on Apr 2 by awoie						1
☐	Add JWS JSON serialization example NEEDS PR wg-05 #222 opened on Mar 26 by awoie						2
☐	Security considerations on integrity of Type Metadata metadata NEEDS PR PRIO wg-05 #221 opened on Mar 26 by danielifett						2
☐	the wallet finding the user claims in the credential discuss #215 opened on Feb 27 by Sakurann						5
☐	Embedded Issuer Policies discuss #212 opened on Feb 16 by paulbastian						3
☐	defining how DID can be used as user's identifier discuss #205 opened on Feb 5 by Sakurann						29
☐	Add output example wg-05 #194 opened on Dec 5, 2023 by tlodderstedt						2
☐	How to choose type values for your credential format? #171 opened on Oct 4, 2023 by danielifett						10
☐	how cnf claim can be used with any other types of "binding" discuss #145 opened on Jun 28, 2023 by Sakurann						15
☐	Need a way to define confidence or assurance levels discuss #116 opened on Jun 7, 2023 by awoie						5

Current Work in Progress

Add display and claim metadata #236

[New issue](#)[Open](#) danielzett wants to merge 6 commits into [main](#) from [danielzett/fix-224-add-display-metadata](#)

Conversation 13 Commits 6 Checks 2 Files changed 1

Changes from all commits File filter Conversations Jump to

215	draft-ietf-oauth-sd-jwt-vc.md
546	546 * 'extends'
547	547 * OPTIONAL. A URI of another type that this type extends, as described in
548	548 (#extending-type-metadata).
549	549 + * 'display': An object containing display information for the type, as described
550	550 + in (#display-metadata). This property is OPTIONAL.
551	551 + * 'claims': An object containing claim information for the type, as described in
552	552 + (#claim-metadata). This property is OPTIONAL.
bc-pi marked this conversation as resolved. Show resolved	
549	553
550	554 ## Extending Type Metadata (#extending-type-metadata)
551	555
625	629 @@ -625,11 +629,221 @@ document MAY be accompanied by a respective claim suffixed with '#integrity', in
626	630 * 'vct' as defined in (#claims),
627	631 * 'extends' as defined in (#extending-type-metadata)
632	632 + * 'uri' as used in two places in (#rendering-metadata)
628	633
629	634 The value MUST be an "integrity metadata" string as defined in Section 3 of
630	635 [!W3C.SRI]. A Consumer of the respective documents MUST verify the
631	636 integrity of the retrieved document as defined in Section 3.3.5 of [!W3C.SRI].
632	637
638	638 +
639	639 +
640	640 + # Display Metadata (#display-metadata)
641	641 +
642	642 + The 'display' property is an object containing display information for the type.
643	643 + The object MUST contain a property for each language that is supported by the
644	644 + type. The property name MUST be a language tag as defined in Section 2 of

- bc-pi on Jun 10 · edited · Collaborator ...
- I don't love the property name as a language tag value approach. And I know it's been discussed in other forums too. We can discuss during a call a day later than usual and maybe an hour or two earlier but I'm wondering about an array of objects with the language tag as a property of each alongside name, description, etc.
- bc-pi on Jun 10 · Collaborator ...
- same thought for #claim-display-metadata
- bc-pi last week · Collaborator ...
- which is also fwiw more similar to how oid4vi approached it https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-13.html#name-credential-issuer-metadata-6

645 + [!RFC5646]. The property value MUST be an object containing the following

646 + properties:

```
{
  "vct": "https://betelgeuse.example.com/education_credential",
  ...
  "display": [ { "en-US": { "..."} }, { "de-DE": { "..."} } ],
  "claims": [ { "path": [ "name" ],
    "display": {
      "de-DE": { "label": "Vor- und Nachname",
        "description": "Der Name des Studenten" },
      "en-US": { "label": "Name", "description": "The name of the student" }
    },
    "verification": "verified", "sd": "allowed"
  }, { "path": [ "address" ],
    "display": {
      "de-DE": { "label": "Adresse",
        "description": "Adresse zum Zeitpunkt des Abschlusses" },
      "en-US": { "label": "Address",
        "description": "Address at the time of graduation" }
    },
    "verification": "self-attested", "sd": "always"
  }, { "path": [ "address", "street_address" ],
    "display": {
      "de-DE": { "label": "Straße",
        "en-US": { "label": "Street Address" }
    },
    "verification": "self-attested",
    "sd": "always"
  }, ...
}
```

More Fewer Media Type Suffixes, More Problems



How it started:
application/vc+ld+json
application/vp+ld+json
application/vc+ld+json+jwt
application/vp+ld+json+jwt
application/vc+ld+json+sd-jwt
application/vp+ld+json+sd-jwt
application/vc+ld+json+cose
application/vp+ld+json+cose
+ld+json+jwt
+json+jwt
+ld+json+sd-jwt
+json+sd-jwt
+ld+json+cose
+json+cose



How it's going:

application/vc
application/vp
application/vc+jwt
application/v+jwt

application/vc+sd-jwt

application/vp+sd-jwt
application/vc+cose
application/vp+cose

Next Steps ...



Keep Griding towards IETF 121 Dublin and 122 Bangkok