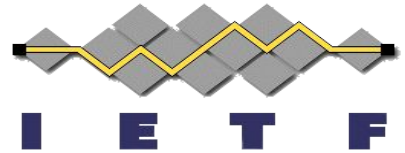
SPICE

`draft-prorock-spice-cose-sd-cwt`

*(*or: *first is not always better)*

IETF 120, Vancouver

July, 2024



an SD-CWT is a CWT with claims that require **confirmation** and support **selective disclosure**

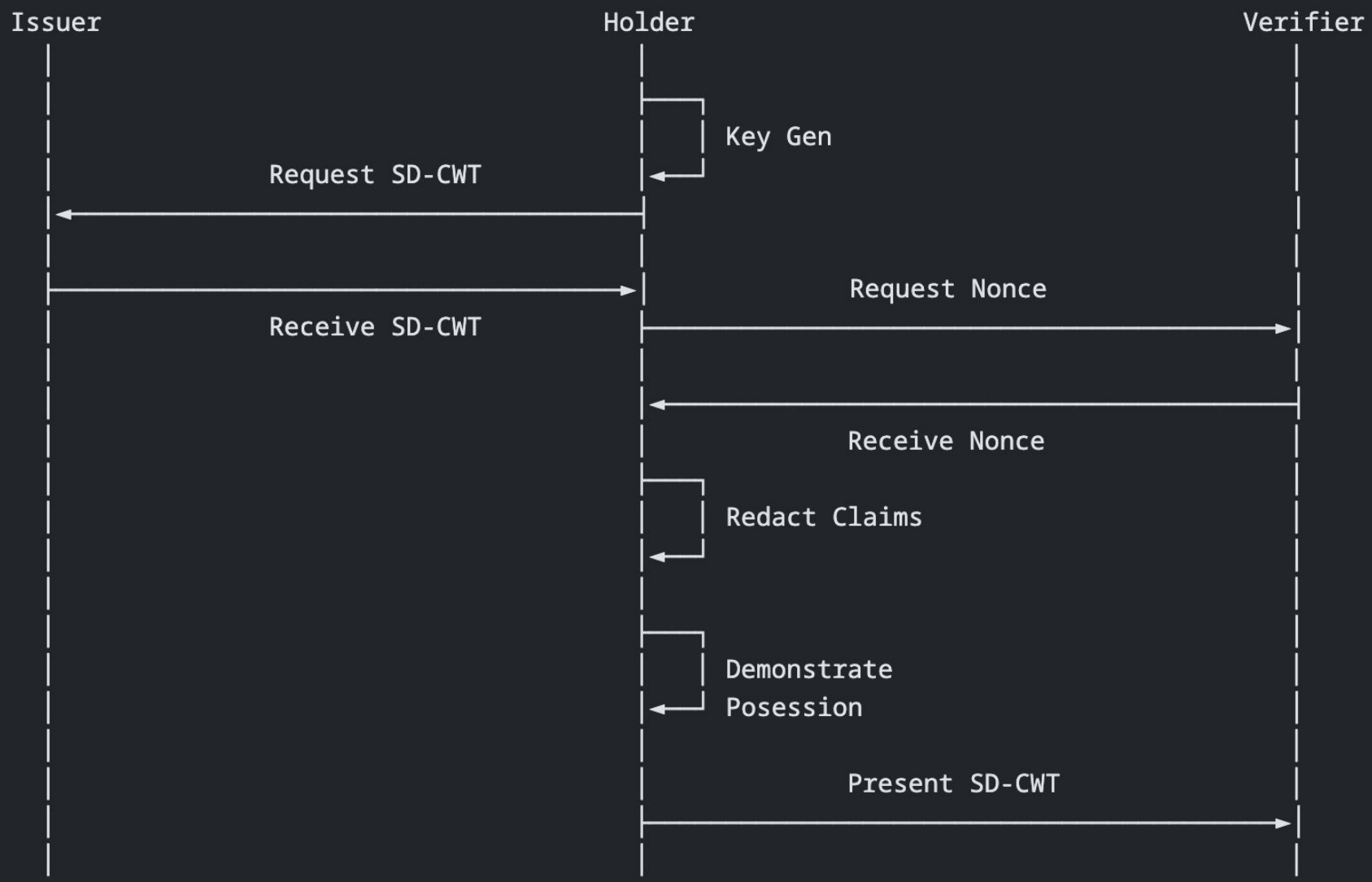
Selective disclosure enables **data minimization**

- The mechanism through which map keys and array elements are disclosed is different
- CWT Claims which are not explicitly marked redactable by the Issuer are mandatory to disclose by the Holder

SD-CWT draft-prorock-spice-cose-sd-cwt-01

3.1. Overview

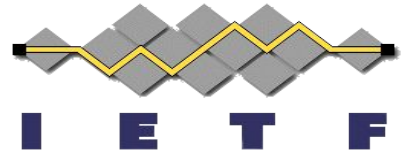
Figure 1: High level SD-CWT Issuance and Presentation Flow



Important concepts:

Issuer
Verifier
Holder

Redaction



SD-CWT Issuance

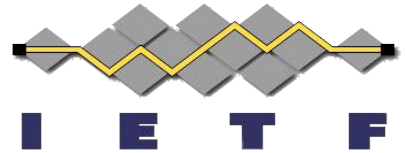
An SD-CWT is a CWT containing … (Digested) Salted Disclosed Claim(s). The salt acts as a blinding factor, preventing a Verifier of an SD-CWT from learning claims that were not intentionally disclosed by a Holder.

A confirmation claim `cnf (8)` **MUST** be present in the CWT Claimset.

The `sd_kbt` **MUST NOT** be set by the Issuer, and **MUST** be set by the Holder

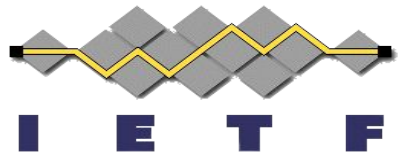
1. The issuer SHOULD confirm the holder controls all confirmation material before issuing credentials using the cnf claim.

2. To protect against replay attacks, the verifier SHOULD provide a nonce, and reject requests that do not include an acceptable an nonce (cnonce). This guidance can be ignored in cases where replay attacks are mitigated at another layer.



SD-CWT Validation

First the Verifier must validate the SD-CWT as described in {{Section 7.2 of RFC 8392}}.



… extract and decode the disclosed claims from the `sd_claims` in the unprotected header.

The decoded `sd_claims` are converted to an intermediate data structure called a Digest To Disclosed Claim Map which is used to transform the Presented Disclosed Claimset, into a Validated Disclosed Claimset.

The Verifier **MUST** compute the hash of each salted-disclosed-claim, in order to match each disclosed value to each entry of the Presented Disclosed Claimset.

SD-CWT draft-prorock-spice-cose-sd-cwt-01

Example

```
/ cose-sign1 / 18([
    / protected / << {
      / alg / 1  : -35 / ES384 /
      / typ / 16 : "application/sd+cwt"
      / kid /    : "https://issuer.example/cwt-key3"
    } >>,
    / unprotected / {
      / disclosed claims /
      / sd_claims / TBD1 : <<[
          [
            / salt /   h'c93c7ff5...72c71e26',
            / claim /  "age_over_18",
            / value /  true
          ],
          [
            / salt /   h'399c641e...2aa18c1e',
            / claim /  "region",
            / value /  "ca" / California /
          ],
          [
            / salt /   h'82501bb4...6c655f32',
            / value /  "4.1.7"
          ]
      ]
      / sd_kbt    / TBD2 : << [
        / protected / …,
        / signature / h'1237af2e...6789456'
      ] >>
    },
    / payload / << …
    >>,
    / signature / h'3337af2e...66959614'
  ])
```

```
/ protected / << {
            / alg / 1 : -35 / ES384 /
            / typ / 16 : "application/kb+cwt"
          } >>,
          / unprotected / {},
          / payload / <<
            / cnonce / 39    : h'e0a156bb3f',
            / aud     / 3    : "https://verifier.example",
            / iat     / 6    : 1783000000,
            / sd_alg  / TBD4 : -16  /SHA-256/
            / sd_hash / TBD3 : h'c341bb...4a5f3f',  / hash of sd_claims  /
                                                    / using sd_alg       /
          >>,
          / signature / h'1237af2e...6789456'
        ] >>
```

```
/ payload / <<
        / iss / 1   : "https://issuer.example",
        / sub / 2   : "https://device.example",
        / exp / 2   : 1883000000,
        / iat / 2   : 1683000000,
        / cnf / 8   : {
          / cose key / 1 : {
            / alg: ES256 /  3: 35,
            / kty: EC2   /  1: 2,
            / crv: P-256 / -1: 1,
            / x / -2: h'768ed8...8626e',
            / y / -3: h'6a48cc...fd5d5'
          }
        },
        / sd_alg / TBD4        : -16, / SHA-256 /
        / redacted_keys / TBD5 : [
            h'abbd...efef',  / redacted age_over_18 /
            h'132d...75e7',  / redacted age_over_21 /
        ],
        / example array as map value / -65537 : [
          123,
          { TBD6 : h'45dd...87af'  / redacted_element / },
          789,
  { TBD6 : h'45dd...87af'  / redacted_element / },
        ],
        "address": {
            "country" : "us",            / United States /
            / redacted_keys / TBD5 : [
                h'adb70604...03da225b',  / redacted region /
                h'e04bdfc4...4d3d40bc'   / redacted post_code /
            ]
        }
```

COSE vs JOSE Differences

- CBOR Tags
  - We can use them instead of the custom “_sd” and “...” that SD-JWT uses.

- Extended Diagnostic Notation
  - We an use it to convey which issuer claims should be made disclosable (instead of the !sd, approach used in SD-JWT YAML test cases).

- Unprotected headers
  - We can use them instead of “~”.

Questions for the group

Any questions for me (or other authors/contributors)?

Adoption?