SD-JWT VC

Daniel Fett, Oliver Terbu, Brian Campbell

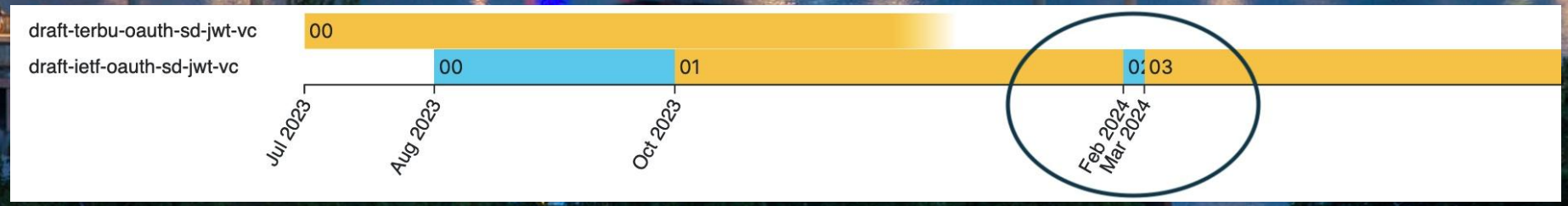
IETF 119 Brisbane

March 2024

Agenda

- Changes since -01
- SD-JWT VC DM
  - Problem statement
  - Current thinking
  - Changes for SD-JWT VC

Since IETF 118 Prague…



What’s New in -02/-03

-02

- Made specific rules for public verification key validation conditional
- Fine-tuned rules for obtaining public verification key
- Editorial changes
- Renamed JWT Issuer Metadata to JWT VC Issuer Metadata
- 'iat' is now optional and allowed to be selectively disclosable
- Fix inconsistency in the .well-known path construction
- Added registration request to IANA for the well-known URI
- Fix some formatting and text in the media type and JWT claim registration requests
- Clarify the optionality of the cnf claim
- Added relationships to other documents
- Added PID example

-03

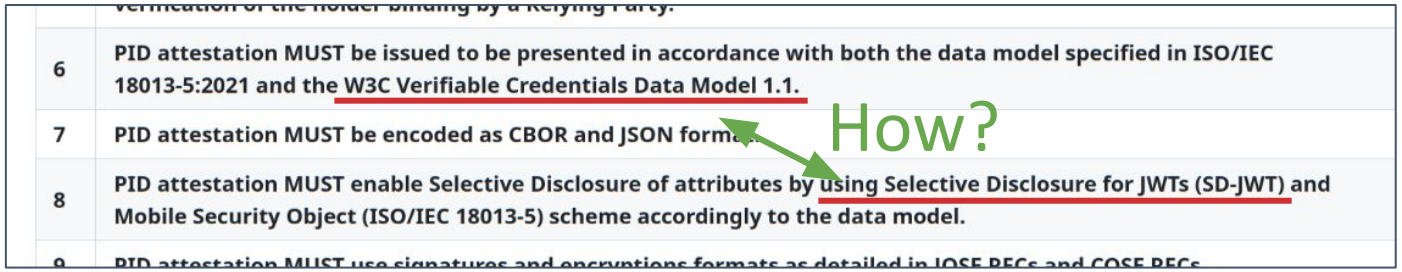
- Include disclosure of age_equal_or_over/18 in the PID example

What’s Next?

What’s happening in Europe?

EU Digital Identity Wallet

Architecture and Reference Framework:



6	PID attestation MUST be issued to be presented in accordance with both the data model specified in ISO/IEC 18013-5:2021 and the W3C Verifiable Credentials Data Model 1.1.
7	PID attestation MUST be encoded as CBOR and JSON forma…
8	PID attestation MUST enable Selective Disclosure of attributes by using Selective Disclosure for JWTs (SD-JWT) and Mobile Security Object (ISO/IEC 18013-5) scheme accordingly to the data model.

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

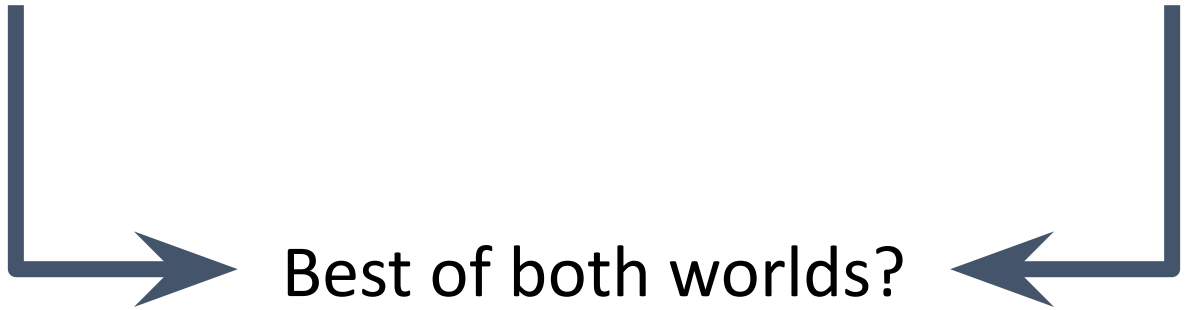
Both are not ideal

W3C VCDM drawbacks:

- Lacks selective disclosure
- JSON/JSON-LD processing ambiguity
- Complexity for simple credentials
- Not immediately AdES compatible

SD-JWT VC drawbacks:

- No schemas or vocabularies
- Not immediately AdES compatible



SD-JWT VC DM Proposal

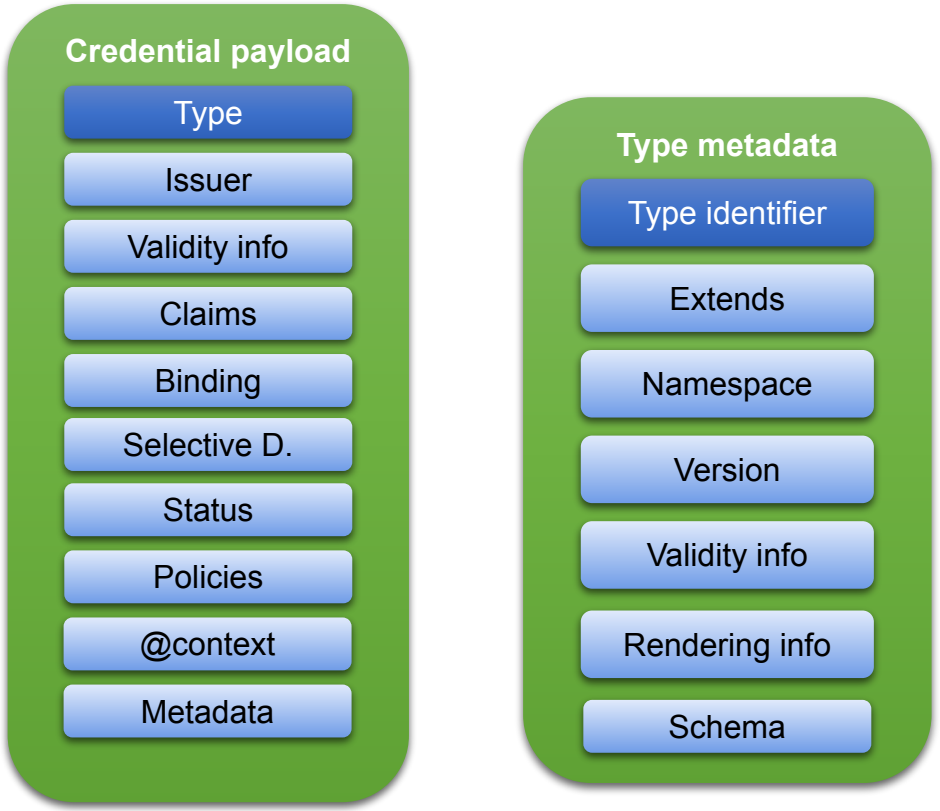
A format suitable for creating and securing JSON-based PIDs and (Q)EAAs based on Verifiable Credentials taking into consideration the existing data models, formats, and securing mechanisms.

The proposal covers

- Data model
- Data format
- Securing mechanisms
- Signature format

Data model and format - best of both worlds!

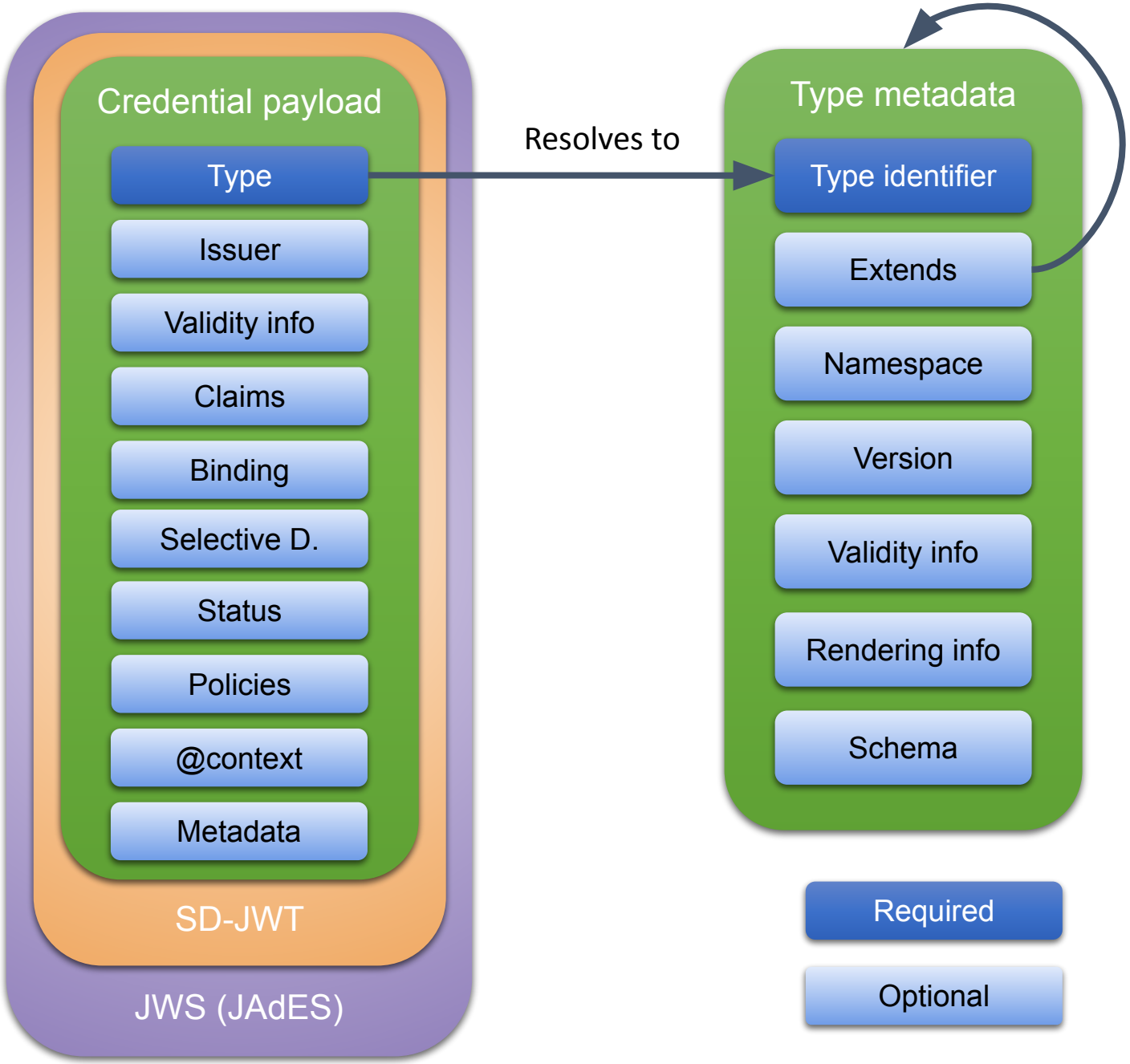
- SD-JWT VC[(1)] with Type Metadata
- Supports open-world data modelling
- Compatible to W3C VCDM v2
- JSON-LD supported, but not required



(1) With minor updates

Overview

- The **core data model** consists of a set of required and optional claims
- The **type identifier** resolves to **type metadata** that contains additional information about the credential
- The data model allows to express simple and complex information sets



Feature	SD-JWT VC	W3C VCDM	SD-JWT VC DM
(Q)EAAs with nested data structures and arrays	🟩	🟩	🟩
Simple credentials	🟩	❌	🟩
Schemas and Vocabularies	❌	🟩	🟩
Selective Disclosure	🟩	❌	🟩
Signing Algorithms (ETSI/SOG-IS)	🟩	🟩	🟩
Key Binding Approaches (cryptographic, non-cryptographic)	🟩	🟩	🟩
Short, Medium, and Long-Lived Credentials	🟩	🟩	🟩
Different Identifiers (x509-based, cnf, DIDs)	🟩	🟩	🟩
Online and Offline Exchange of Credentials	🟩	🟩	🟩
Revocation/Suspension	🟩	🟩	🟩
Policies	🟩	🟩	🟩

Example: Simplified PID

The data model represents a simplified PID without selective disclosure

Exact claim names, definitions and the PID signature profile are out of scope.

(All examples shortened for presentation.)


```
{
 "vct": "eudi:example:pid",

 "given_name": "Jack",
 "family_name": "Dougherty",
 "birthdate": "1980-05-23",

 "cnf": {
   "jwk": {
     "kty": "EC",
     "crv": "P-256",
     "x": "52aDI_ur05n1f_p3jiYGUU82oKZr3m4LsAErM536crQ",
     "y": "ckhZ-KQ5aXNL91R8Eufg1aOf8Z5pZJnIvuCzNGfdnzo"
   }
 }
}
```

Example: Simplified PID

Same as before, with selective disclosure.

After processing, data structure as shown on previous slide is restored.

(All examples shortened for presentation.)

Example: PDA-1

Simplified Portable Document A1.


```
{
 "vct": "empl:pda1",

 "valid_from": "2022-11-10T19:19:47.287Z",
 "valid_until": "2022-11-10T19:19:47.287Z",

 "id": "635ba519cd19764e84ea67dd",
 "legal_entity_verifiable_id": {
   "legal_name": "Ministry of Wonderland"
 },
 "claims": {
   "personal_information": {
     "personal_identification_number": "1",
     "sex": "01",
     "surname": "Dalton",
     "forenames": "Joe Jack William Averell",
     "date_birth": "1985-08-15",
     "nationalities": [
       "BE"
     ],
     "state_of_residence_address": {
       "street_no": "sss, nnn ",
       "post_code": "ppp",
       "town": "ccc",
       "country_code": "BE"
     }
   }
 },

 "cnf": {
   "jwk": { … }
 }
}
```


(All examples shortened for presentation.)

Example: PDA-1 Metadata

As resolved from `"vct": "empl:pda1"` type identifier

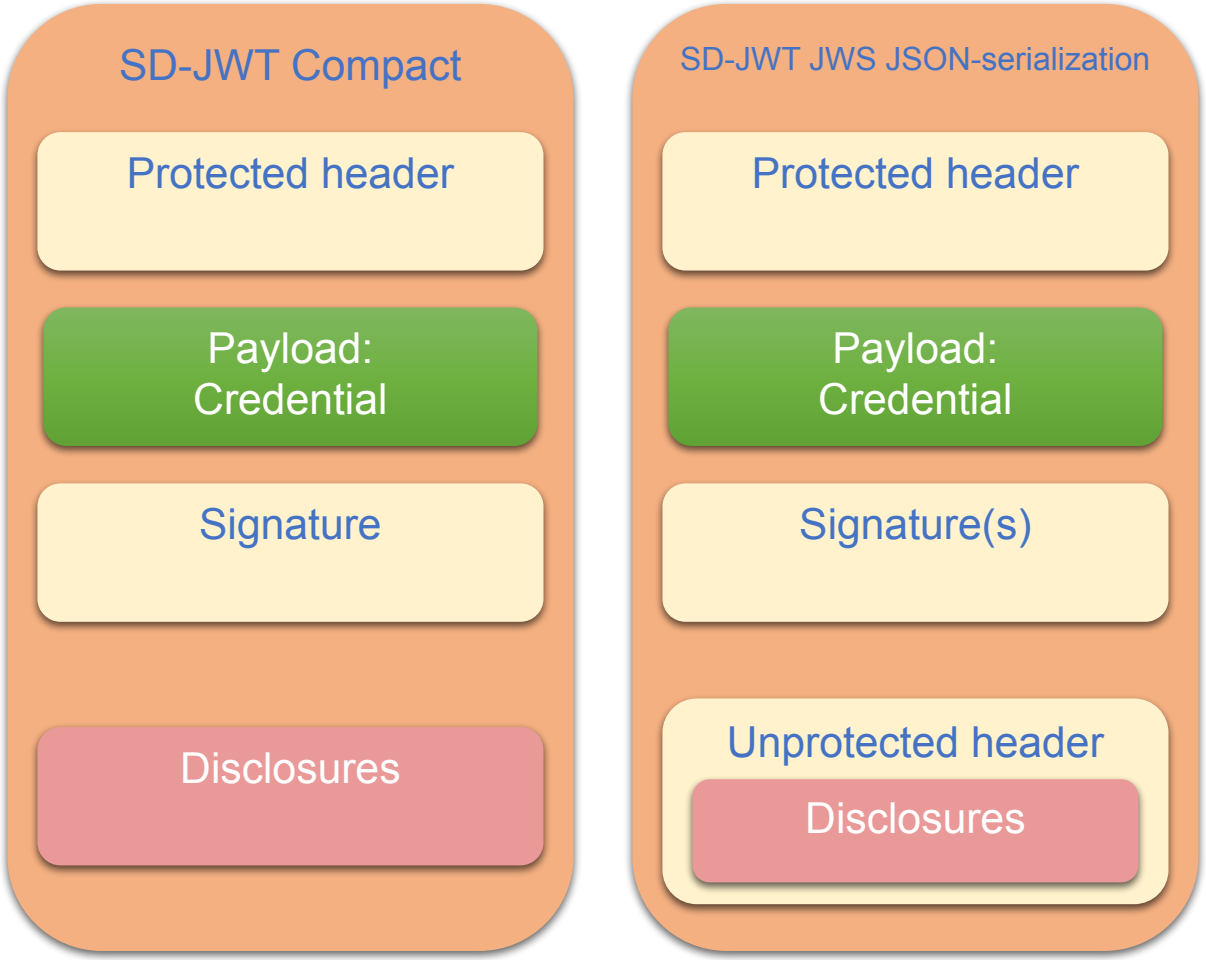
(All examples shortened for presentation.)


```
{
 "language": "en-gb",
 "namespace": "empl",

 "vct": "empl:pda1",
 "extends": "iana:sd-jwt-vc",
 "extends#integrity": "sha256-786b8dfc26a9b...1854dd2",

 "version": "1.0",
 "name": "Portable Document A1",
 "description": "Example metadata for PDA1",

 "schema": {
   "json_schema": {
     "uri": "https://empl.eu/credential-schema-1.0",
     "uri#integrity": "sha256-742289d058bc...5aef1620ac02",
   }
 },
 "display": [
   {
     "en-GB": {
       "name": "Portable Document A1",
       "rendering": {
         "simple": {
           "logo": {
             "uri": "https://empl.eu/pda1/logo.png",
             "uri#integrity": "sha256-e737d7...da26762acb",
             "alt_text": "a square logo of a university"
           },
           "background_color": "#12107c",
           "text_color": "#FFFFFF"
         }
       }
     }
   }
 ]
}
```

Signature Format

- **Compact SD-JWT signature format** for simple credentials
- **JSON-serialized signature format** for rich signatures (self-contained credentials*, multiple signatures, re-signing)
- Supports all ETSI/SOG-IS signing algorithms

* incl. Type metadata



How to get there?

Roadmap

- IETF SD-JWT VC
  - Define type metadata (proposal exists)
  - Define extension points, e.g., status/policies/… (details to be discussed)
- IETF SD-JWT
  - Minor updates for JAdES alignment (in progress)
- ETSI JAdES
  - Update JAdES profiles (starting)

Thank you!

(gratuitous photo of Vancouver in anticipation of IETF 120)