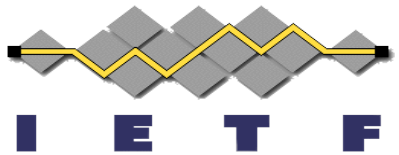
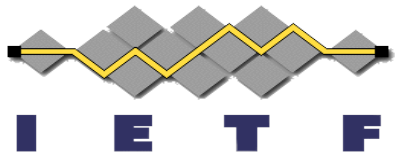
SPICE



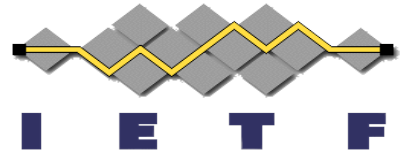
BOF Chair: Hannes Tschofenig

IETF 119, Brisbane
March 19, 2024

Welcome and Introduction



Note Well



This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

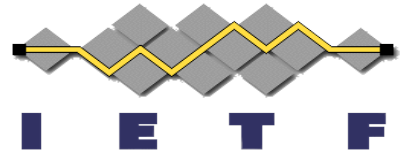
As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Note Really Well



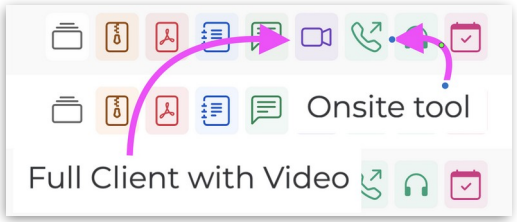
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

This session is being recorded

IETF 119 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Status

- Successful BOF at the IETF#118
  - Asked important BOF questions and there was strong support for the work.
  - Charter text was, however, not ready

- Focus on charter discussions after IETF#118
  - Scheduled regular conference calls
  - Discussions on the list with refinements of milestones and scope
  - Comments from experts on ISO mDoc, OAuth, JWT, CWT,...
  - Published several drafts along the way

Charter text is here: https://datatracker.ietf.org/doc/charter-ietf-spice/

Agenda

Summary of the proposed work items

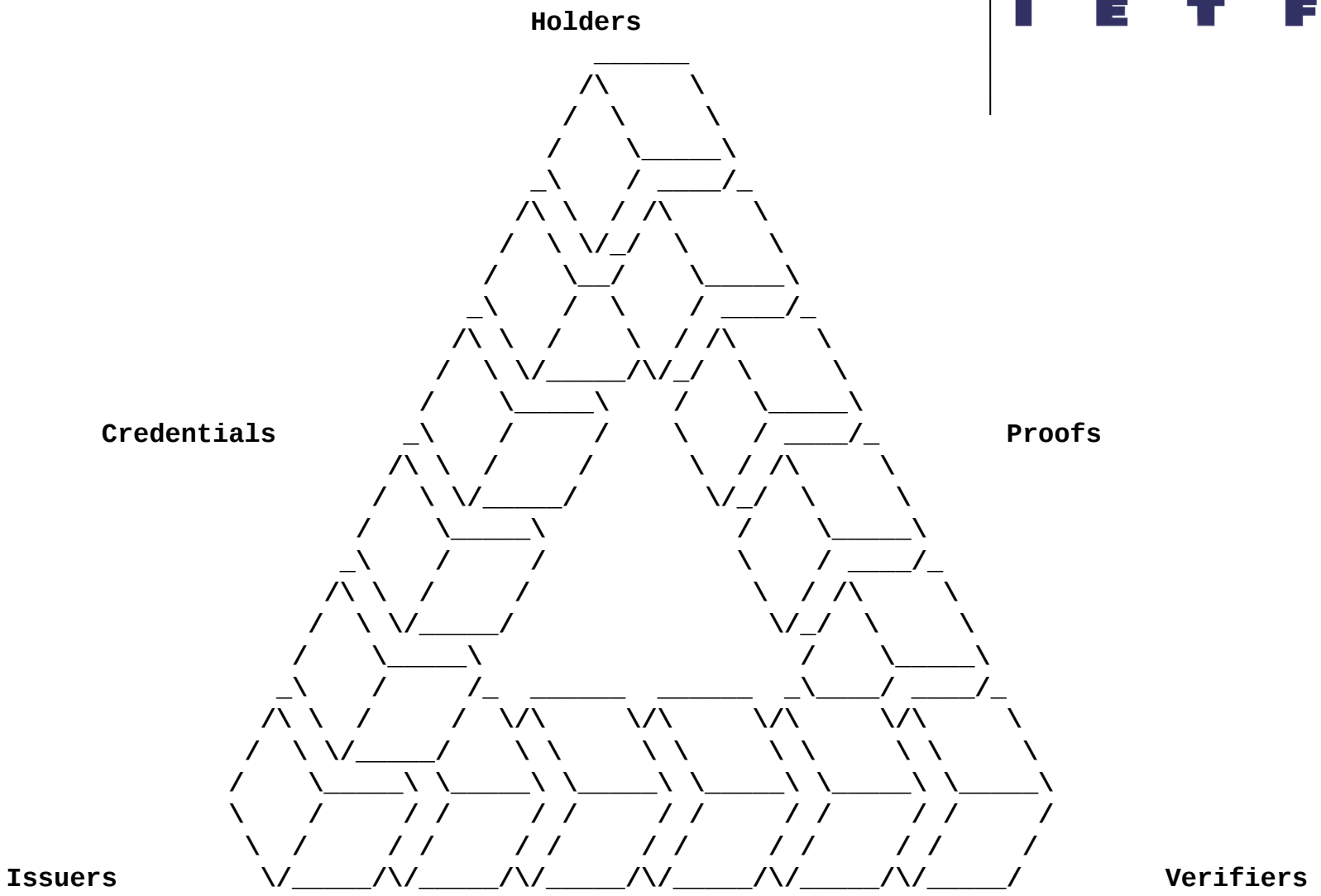
- Architecture
- Use Cases
- SD-CWT
- Meta-data/Capability Discovery

Charter Text Discussion

Architecture

Input documents:

- Transparency Tokens (by Orie)
- A reference architecture for direct presentation credential flows (by Leif)



Use Cases

-01 published before the cut off!

5.2. Physical Supply Chain Credentials

Physical supply chain credentials create several unique scenarios and requirements for technical implementers. There is a strong movement towards digitization of physical supply chain data which is often exchanged in **paper or scanned pdf** form today using **legacy approaches**.

…

Common use cases for physical supply chains include:

* **Regulatory data capture** and exchange with governmental bodies
* Requirements around capturing specific types of data including:
  - **Inspection information**
  - **Permits**
  - **Compliance certification** (both regulatory and private)
  - Traceability information, **including change of control and geospatial coordinates**

…

* Passing of data between multiple intermediaries, before being sent along to customs agencies or consignees.
* **Moving large amounts of signed data asynchronously**, and bi-directionally over a network channel

architecture is how we exchange this data

sd-cwt and related is the credential format

transparency tokens help

Use Cases

-01 published before the cut off!

5.2. Physical Supply Chain Credentials

* Providing the ability for **3rd parties** to "certify" information about another actor in the supply chain. e.g. Vendor A is an approved supplier for Company X

* **Identifying actors in a supply chain and linking them with legal entity information**

sd-cwt is a way of 3rd parties to make claims regarding the identity of an actor in the architecture

These items should likely be their own section, and also cover identity requirements for physical supply chain

Use Cases

-01 published before the cut off!

5.3. Credentials related to **Authenticity** and **Provenance**

Due to a proliferation of AI generated or modified content, there has been an increased need to provide the ability to establish the provenance of digital material. Questions of authenticity and the means of creation (human created, machine assisted, machine created) also abound, and in cases where AI generated content, providing the model information related to the generation of that content is becoming increasingly important.

Common use cases include:

* Understanding if a received piece of media is human created, and that the content is authorized for certain uses.
* Providing the ability to trace training materials for LLMs and similar models to output
* Understanding if media was created by an authoritative or trustworthy source

SCITT lets us "witness" the receipt of data

COSE w/ detached sigs let us sign that data

Strong Linkage to Physical Supply Chain credentials, *we should restate/clarify this section of the doc*:

What, when, how was data collected in relation to a regulatory item

Provides a link between legacy and modern data in the supply chain

SD-CWT

-02 published before the cut off!

```
Credential = #6.18(SD-CWT)

SD-CWT = [
  protected,
  unprotected: {
    ? disclosures: [* claim-pair] / nil
  },
  payload : bstr / nil,
  signature : bstr,
]

claim-pair = {
  1 => uint .size 4,  ; 32-bit salt
  2 => bstr           ; disclosed value
}
```

```
; Counter signatures on CBOR credential with selective disclosure:

SD-CWT = [
  protected,
  unprotected: {
  ? disclosures: [* claim-pair] / nil
    COSE_Countersignature0: bstr
  },
  payload : bstr / nil,
  signature : bstr,
]

; SCITT Receipt for CBOR credential with selective disclosure:

SD-CWT = [
  protected,
  unprotected: {
  ? disclosures: [* claim-pair] / nil
    Receipt: [ +bstr]
  },
  payload : bstr / nil,
  signature : bstr,
]
```

Early Implementation of SD-CWT
- https://github.com/transmute-industries/sd-cwt

Metadata (Capability) Discovery

-01 published January 1st

OAuth SD-JWT-based Verifiable Credentials
…for Inspiration: draft-ietf-oauth-sd-jwt-vc

iss: https://example.com/tenant/1234

```
GET /.well-known/jwt-vc-issuer/tenant/1234 HTTP/1.1
Host: example.com

{
   "issuer":"https://example.com",
   "jwks":{
      "keys":[
         {
           "kid": "urn:...lj1rXPagRo",
           "alg": "ES256",
           "use": "sig",
           "kty": "EC",
           "crv": "P-256",
           "x": "p-kZ4u…RjZaOS9w",
           "y": "ymXE…NVfdg0"
         }
      ]
   }
}
```

Discovering Issuer / Holder / Verifier Keys

iss: did:example:123

```
GET /identifiers/did:example:123 HTTP/1.1
Host: resolver.example
Accept: application/did+json
…
HTTP/1.1 200 Ok
Content-Type: application/json
{
  "id": "did:example:123"
}
```

SCITT API Definitions
…for Inspiration: draft-ietf-scitt-scrapi

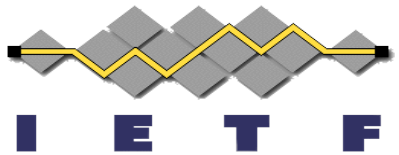
iss: https://transparency.example

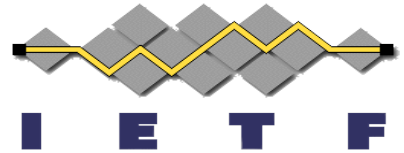
```
GET /.well-known/transparency-configuration HTTP/1.1
Host: transparency.example
Accept: application/json

{
     "issuer": "https://transparency.example",
     "registration_endpoint": "https://transparency.example/entries",
     "nonce_endpoint": "https://transparency.example/nonce",
     …
     "supported_signature_algorithms": ["ES256"],
     "jwks": {
       "keys": [
         {
           "kid": "urn:ietf:params:oauth:...1rXPagRo",
           "alg": "ES256",
           "use": "sig",
           "kty": "EC",
           "crv": "P-256",
           "x": "p-kZ4uOASt9IjQRTrWikGnlbGb-z3LU1ltwRjZaOS9w",
           "y": "ymXE1yltJPXgjQSRe9NweN3TLlSUALYZTzy83NVfdg0"
         },
         {
           "kid": "urn:ietf:params:oauth:...AFM8jyXKW0ClE",
           "alg": "HPKE-Base-P256-SHA256-AES128GCM",
           "use": "enc",
           "kty": "EC",
           "crv": "P-256",
           "x": "Vreuil95vzR6ixutgBBf2ota-rj97MvKfuJWB4qqp5w",
           "y": "NkUTeaoNlLRRsVRxHGDA-RsA0ex2tSpcd3G-4SmKXbs"
         }
       ]
     }
   }
```

Early Implementation of Metadata Discovery
- https://github.com/transmute-industries/dune

Charter Discussion





Introduction

A digital credential expresses claims, assertions, or attributes about a subject, such as their name or age, and their cryptographic keys. Some sets of claim names have already been defined by the IETF and other standards development groups (e.g., OpenID Foundation).

Digital credentials typically involve at least three entities. An issuer constructs and secures a digital credential for a holder. Holders may be willing either to partially disclose some values of their attributes or to demonstrate some properties about their attributes without disclosing their values. Holders disclose credentials, attributes, or proofs regarding attributes in what is called a "digital presentation" to a verifier.

Some holders may wish to carry more than one digital credential. These credentials, together with associated key material, can be stored in an identity digital wallet.

Goal

The SPICE WG will profile existing IETF technologies and address residual gaps that would enable their use in digital credentials and presentations.

- The JOSE WG is already standardizing a token format for unlinkability & selective disclosure in the form of JWP/CWP (draft-ietf-jose-json-web-proof). The SPICE WG will profile these token formats for use with digital credentials.

- The OAUTH WG is already standardizing a token format for unlinkability & selective disclosure in the form of SD-JWT/SD-JWT-VC (draft-ietf-oauth-selective-disclosure-jwt and draft-ietf-oauth-sd-jwt-vc). The SPICE WG will define SD-CWT/SD-CWT-VC, analogs for these JWT-based tokens but based on CWT.

The SPICE WG coordinates with RATS, OAuth, JOSE, COSE, and SCITT working groups that develop documents related to the identity and credential space. The SPICE WG builds on existing cryptographic primitives and does not define novel cryptographic schemes.

Goal, cont.

The SPICE WG develops digital credential profiles which can support a number of use cases. To help guide engineering decisions, requirements for proposed standards in the program of work will be created in coordination with the working groups listed above. The profiles developed by the SPICE WG will enable digital credentials to leverage existing IETF technologies.

Privacy by design, confidentiality, and consent will be considered, and implementation guidance will be given for each proposed standard in the program of work.

The privacy and security considerations related to the impact of confidential computing, remote attestation, trusted execution environments (TEE), and hardware security modules (HSM) on digital credentials will be developed in coordination with relevant IETF WGs (e.g., TEEP) and feedback from experts on the mailing list.

Privacy and security considerations regarding redaction, linkability and selective disclosure will be developed for proposed standards in the program of work.

Out of Scope

- General Key discovery is out of scope for this WG. There are several mechanisms for distributing or discovering key material (e.g., https://openid.net/specs/openid-connect-discovery-1_0.html).

Program of Work

- An informational **Architecture** that defines the terminology (e.g., Issuer, Holder, Verifier, Claims, Credentials, Presentations) and the essential communication patterns between roles, such as credential issuance, where an issuer delivers a credential to a holder, and presentation, where a holder delivers a presentation to a verifier.

- Proposed standard documents for **digital credential profiles covering JWP and CWP** (from JOSE) that enable digital credentials with unlinkability and selective disclosure. This work will include registering claims that are in the JWT and CWT registries to enable digital credentials to transition from one security format to another (i.e., JSON/CBOR).

Program of Work, cont.

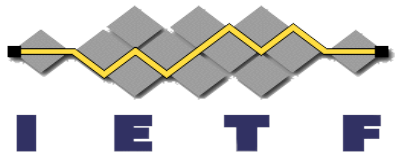
- Proposed standard document defining **SD-CWT**, a profile of CWT inspired by SD-JWT (from OAuth) that enables digital credentials with unlinkability and selective disclosure.

- A proposed standard **Metadata & Capability Discovery** protocol for JWT, CWT, SD-JWT, SD-CWT, CWP and JWP using HTTPS/CoAP for CBOR-based digital credentials to enable the 3 roles (issuers, holders and verifiers) to discover supported capabilities, protocols and formats for keys, claims, credential types and proofs. The design will be inspired by the OAuth "vc-jwt-issuer" metadata work (draft-ietf-oauth-sd-jwt-vc) which supports ecosystems using JSON serialization.

Milestones

- 04/2025 - Submit an informational Architecture document to the IESG for publication
- 10/2025 - Submit a proposed standard document covering a JWP/CWP profile for digital credentials to the IESG for publication
- 10/2025 - Submit a proposed standard document defining SD-CWT to the IESG for publication
- 03/2026 - Submit a document as a proposed standard covering Metadata & Capability Discovery protocol to the IESG for publication

Backup



Community Updates

Open ID Foundation has been developing several interesting protocols regarding digital credential presentations, includings ones that interact with web platform and mobile/os platforms:

- https://openid.net/wg/digital-credentials-protocols/

EBSI has published information regarding Conformant Wallets for Digital Credentials:

- https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Conformant+wallets

W3C Verifiable Credentials 2.0 has entered first candidate review.

- https://www.w3.org/TR/2024/CRD-vc-data-model-2.0-20240303/

W3C WICG has been incubating web platform and mobile/os platform APIs to digital credentials including considering support for ISO mDoc, OAuth SD-JWT, and CWT

- https://github.com/WICG/digital-identities

W3C CCG has been incubating B2B credential and presentation use cases for securing global supply chains, and recently focused on JWT based digital credentials

- https://w3c-ccg.github.io/traceability-vocab/

Miscellaneous Drafts Submitted to SPICE

Guidance for Government and Industry Adopters of Digital Credential Profiles
- https://datatracker.ietf.org/doc/draft-steele-spice-profiles-bcp/

Presentations of Digital Credentials through animated QR Codes
- https://datatracker.ietf.org/doc/draft-steele-spice-cryptovolense/

Contact Management Systems and Digital Credential Presentations
- https://datatracker.ietf.org/doc/draft-steele-spice-vcard-credentials/

Privacy Preserving Credential Status Lists
- https://datatracker.ietf.org/doc/draft-steele-spice-oblivious-credential-state/