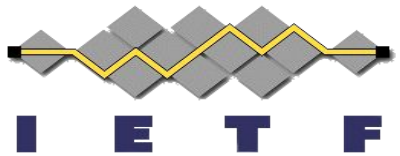
IETF 118
Secure Patterns for Internet CrEdentials (SPICE) BOF

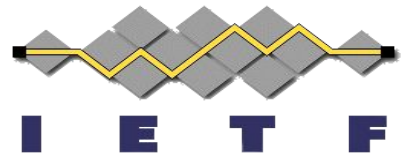


Pamela Dingle, Hannes Tschofenig

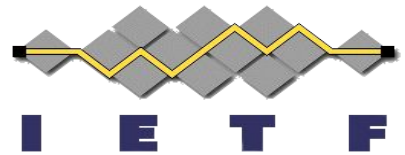
November 7th, 2023

Welcome and Introduction

Chairs (10 min)



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.

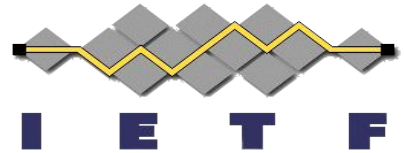
As a reminder:

- 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



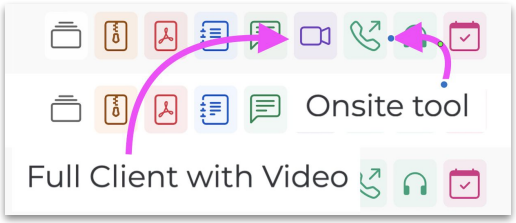
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, 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 118 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

Resources for IETF 118 Prague

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

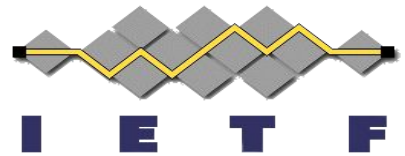
Agenda

- Welcome and Introduction (10 min): Chairs
- Problem Statement
  - Market Driver (10 min): Leif
  - Technology Driver (10 min): Orie
- Selection of proposed work items
  - "Identity" / Key Discovery document (5 min): Kristina
  - SD-CWT (5 min): Orie
- Privacy: Selective Disclosure and Unlinkability (10 min): Mike Jones
- Clarifying Questions (10 min): all
- Charter & Milestones (10 min): Henk
- Discussion (20 min): all
- BoF Questions (20 min): Chairs / Area Director
- Wrap-up and Conclusion (10 min): Area Director

Problem Statement

Market Driver - Leif (10 min)

Technology Driver - Brent (10 min)



EUDI - IETF TL;DR

Legislative Process

- Negotiation of the proposal for the revision of the **eIDAS regulation** underpinning the EUDI Framework

Wallet Technical Standards

- Member States and the Commission are in the process of establishing a **common toolbox** consisting of an **architecture and reference framework,** common standards and specifications and guidelines and best practices for the EUDI Wallet

Large-scale Pilots

- **Grants** under the Digital Europe Programme for l**arge-scale pilots around use-cases** for the EUDI Wallet including mobile driver licences, ePayments, eHealth and educational/professional qualifications

Wallet Reference Application

- Procurement of a **reference application** of the EUDI Wallet based on the technical standards agreed by the toolbox.

EUDI - IETF TL;DR

- End-state for the EUDI wallet process is…
  - de-jure standards referenced from the implementation act(s)
  - actual technical and semantic interoperability among the member states
  - a few operationally viable use-cases (eg social security card, edu credentials, etc)
- Current status
  - Dialogue between COM and ETSI about what standards needs to be put in place
  - Lots of work and focus in & around the ARF on in-person flows
  - Lots of work and focus in the LSPs on web flows
  - The majority of use-cases are about web-flows.
- **Also: global interop wouldn't hurt**

EUDI IETF “ask”

- Need foundational standards for web flow credentials
- Ensure interop with oidc4vc and oidc4vp
- Focus on issues related to credentials security and privacy

Technology Driver

Some use cases:

- A worker provides an assertion from A1 Forklifts about their forklift certification to a Construction company.
- A steel distributor provides assertions from suppliers about steel origins to purchasers.
- A loan seeker provides an assertion from their employer about their employment status to a mortgage broker.

Technology Driver

- a HOLDER provides an assertion from an ISSUER about a SUBJECT to a VERIFIER.

- the assertion is issued in a CREDENTIAL.
- the assertion is provided as a PRESENTATION.

- CREDENTIALS and PRESENTATIONS are evaluated according to policies.

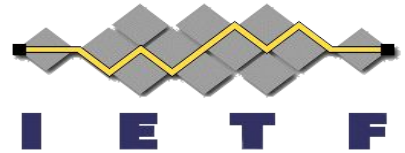
Technology Driver

Efficiency can be improved:

- decision making can be **automated**,
- processing time reduced,
- throughput increased

Without better technology (simpler, safer, faster, easier to use, etc.) we cannot automate safely.

Technology Driver



IETF (X.509)

Attribute Certs (2010)

IETF (OAUTH)

JSON Web Tokens (2015)

Demonstrating Proof of Possession (2023)

IETF (ACE)

CBOR Web Tokens (2018)

OSCORE (2022)

IETF (COSE)

COSE (2017)

COSE (2022)

W3C (VCWG)

Verifiable Credentials 1.0 (2019)

VC 1.1 (2022)

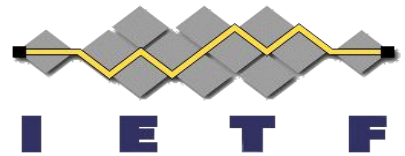
W3C (DIDWG)

Decentralized Identifiers 1.0 (2022)

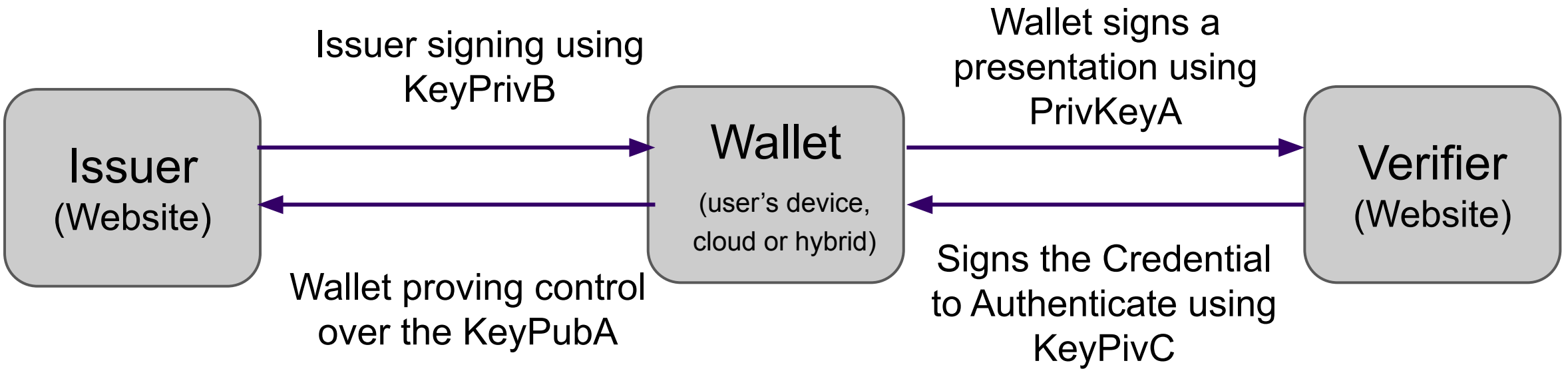
Some Proposed Work Items

Identifiers and Key Discovery - Kristina (5 min)

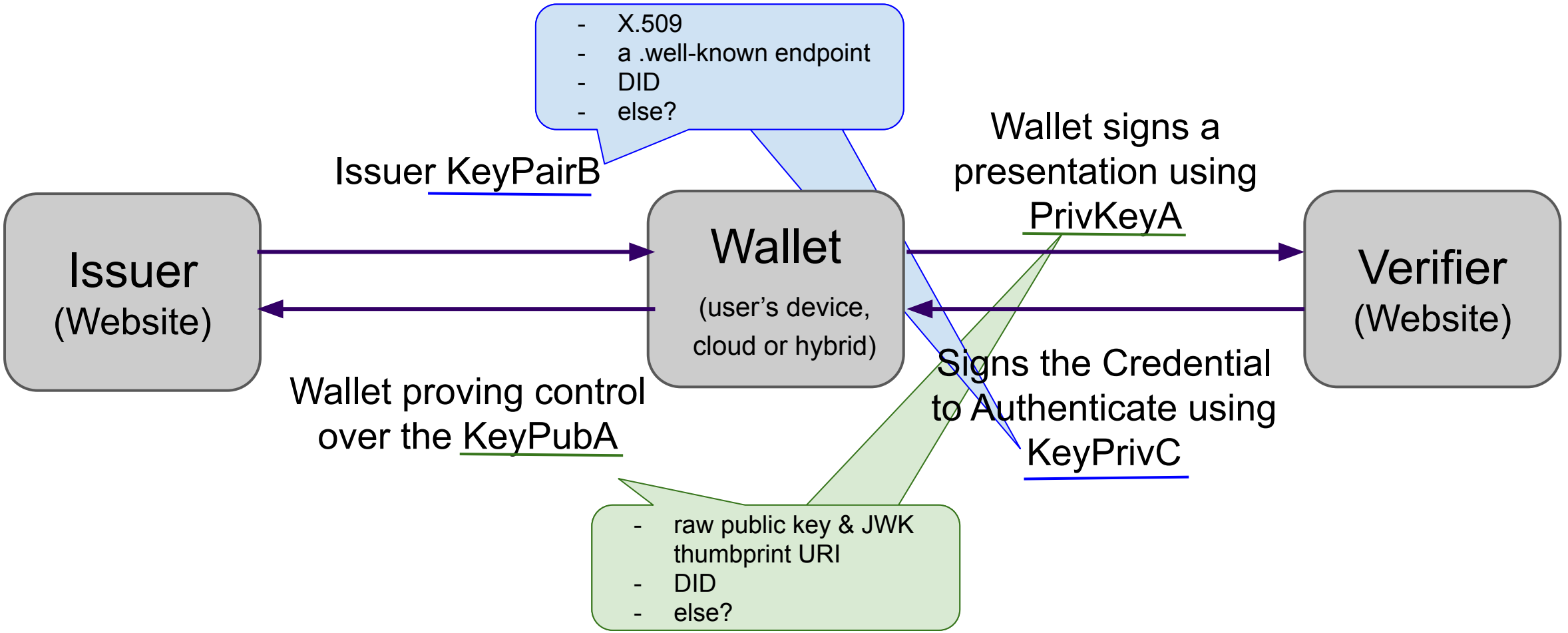
SD-CWT - Orie (5 min)



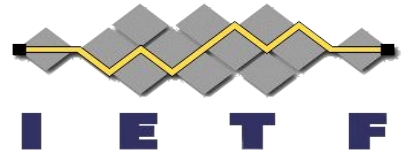
Identifiers and Key discovery in three party model



Options for these Identifiers and Key discovery

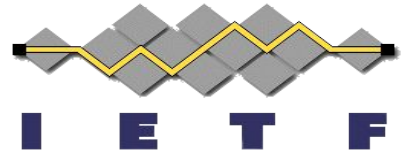


Pros and Cons of each approach



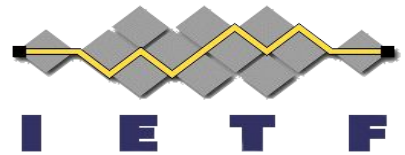
Option		Pros	Cons
X.509	⇒	- Well-established PKI	- SCITT (supply chain transparency and trust) needs a key history
.well-known endpoint	⇒	- Simpler than X.509 - Can be modular with per-purpose .well-known paths	- It actually does not exist for three party model… - First attempt in SD-JWT VC draft in the oauth wg
DIDs	⇒	- Indirection between the key document and the identifier - A document can contain endpoints in addition to keys	- JSON-LD/RDF - No off-the-shelf interop (i.e. too many possibilities) - Hesitation from the implementers (not the best public perception)

.well-known endpoint examples (1/2)



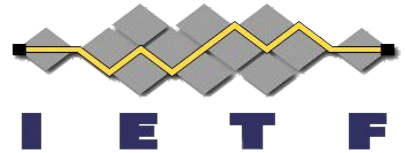

```
// COSE
{                                       / Protected                     /
  1: -35,                               / Algorithm                     /
  TBD: {                                / CWT Claims                    /
    1: https://issuer.example,          / Issuer                        /
    2: https://subject.example,         / Subject                       /
  }
}

// JOSE
{
  "alg": "ES384",
  "iss": "https://issuer.example",
  "sub": "https://subject.example",
}
```

.well-known endpoint examples (2/2)



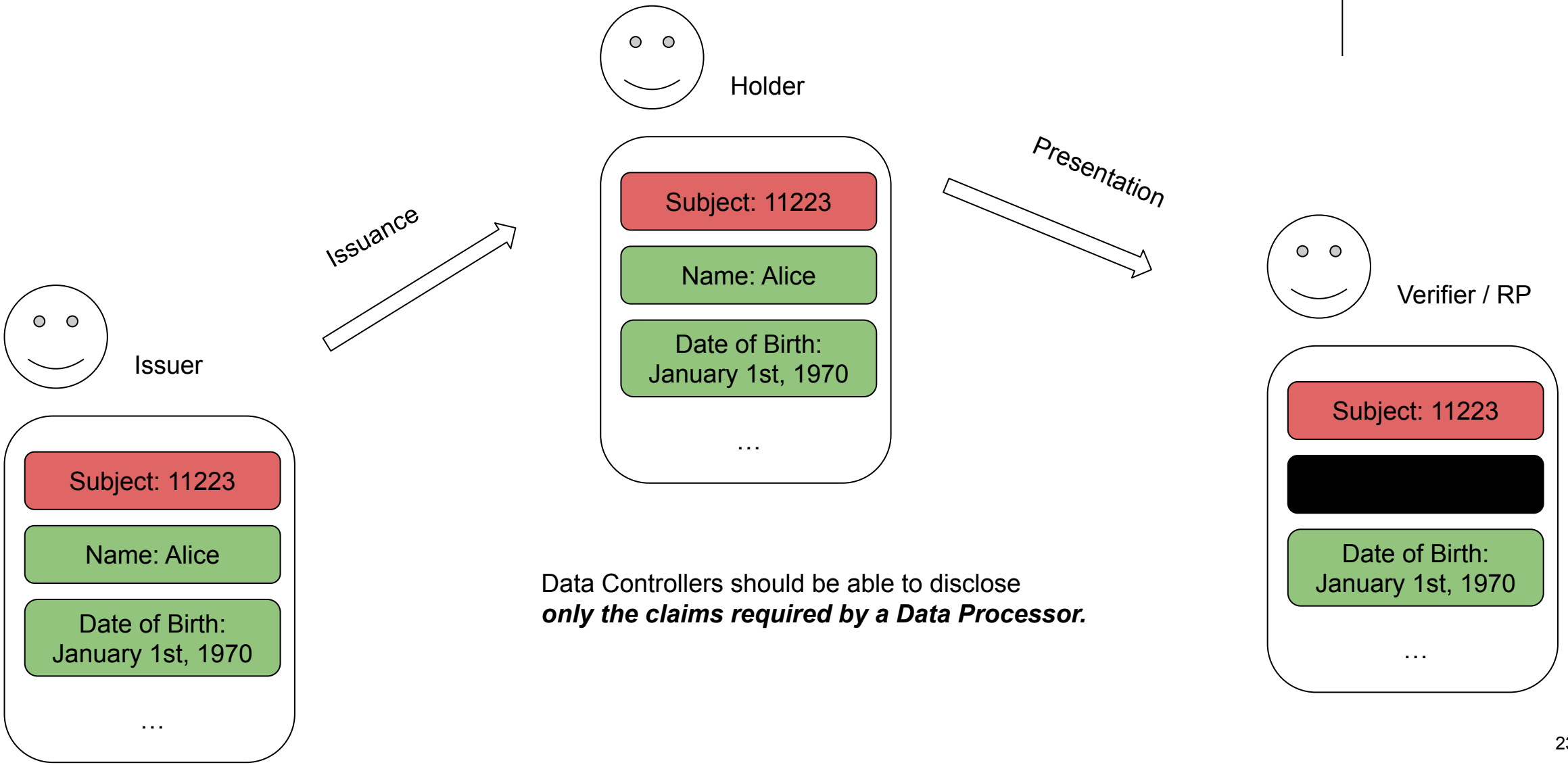

```
// https://issuer.example/.well-known/jwt-issuer

{
  "issuer": "https://issuer.example",
  "jwks_uri": "https://issuer.example/.well-known/jwks"
}

// https://issuer.example/.well-known/jwks

{
  "keys": [
    {
      "kid":
"urn:ietf:params:oauth:jwk-thumbprint:sha-256:NzbLsXh8uDCcd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xs",
      "kty": "EC",
      "crv": "P-384",
      "alg": "ES384",
      "x": "NbaI-0w2h8nUxN2mJnD_Ozq9q3E5KEuCg22p5WD0bW5g7u8izXOS0ANuQA7_xxG0",
      "y": "HmWJgIq4tfkVQkpMYRgp7yQyI20t9R6_wDI9CqYzF1Hy5AKIxRRXeWJN4ZNHa10P"
    }
  ]
}
```

Where to do this work?



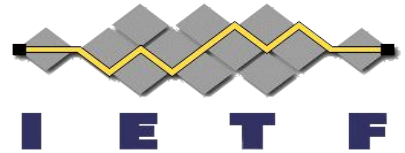
- the need to define an Identifier and Key discovery mechanism that meets the following requirements:
  - a document with the key pair information contains key rotation history
  - not JSON-LD/RDF
  - interoperable off-the-shelf (no concept similar to DID methods)
  - no hesitation from the implementers because no associated negative public perception associated with it
  - Could work with x.509s too

Selective Disclosure



Data Controllers should be able to disclose
only the claims required by a Data Processor.

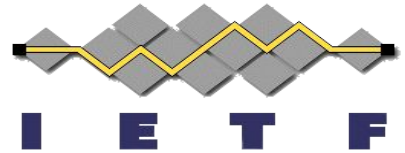
Selective Disclosure



Selective Disclosure is a building block for achieving ***data integrity with data minimization***.

Selective Disclosure can reduce the need to “over share”, which in turn can ***reduce the damage associated with compromise***.

Selective Disclosure in COSE



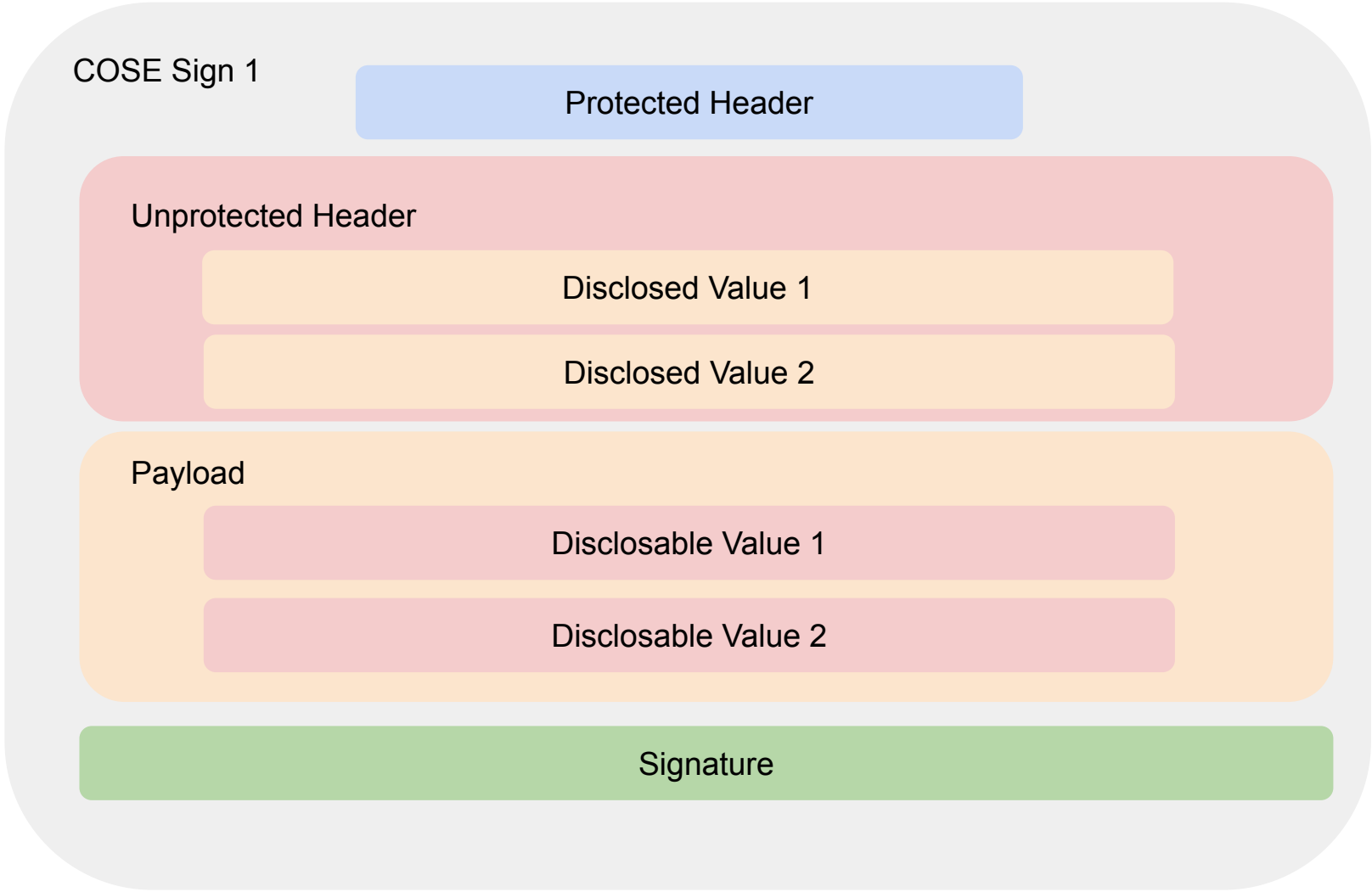
Benefits

- No double text encoding of binary (base64url bloat)
- Much smaller document sizes
- Familiar terminology and APIs for developers with JOSE experience

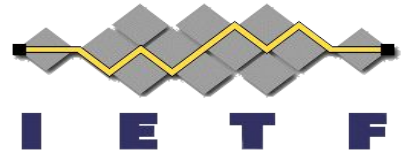
Challenges

- Tooling Maturity / Debug / Diagnostic time
- Strange deviations from JOSE experience
- Determinism / Language specific issues (Binary in JavaScript)

SD-CWT


COSE Sign 1
Protected Header
Unprotected Header
Disclosed Value 1
Disclosed Value 2
Payload
Disclosable Value 1
Disclosable Value 2
Signature

SD-CWT SBOM (use case)



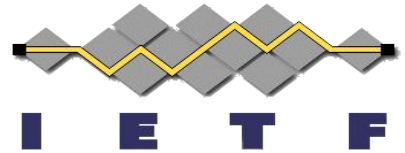
Envelope

```
{ / Protected Header /
  1: -35 / alg : ES384 /
}

18( / COSE Sign 1 /
  [
    h'A1013822', / Protected Header /
    { / Unprotected Header /
      333: [                    / Disclosures (2) /
        h'82502BD5...5254494F4E', / Disclosure 1 🔴 /
        h'825091B1...5254494F4E'  / Disclosure 2 🔵 /
      ]
    },
    h'AB6566696...61FF6765', / Payload /
    h'DCBCDD0C1...11DB6D16'  / Signature /
  ]
)
```

Payload

```
/ Payload /
…
"files": [
/ 🔴 Disclosable Value 1 /
{ 222: h'58F422BA59…A6D75858A68C' },
{
"fileName": "./README.md",
"SPDXID": "SPDXRef-File--README.md-534A3C13…D5E53B2B6023A",
…
"licenseConcluded": "NOASSERTION",
"licenseInfoInFiles": ["NOASSERTION"],
"copyrightText": "NOASSERTION"
},
/ 🔵 Disclosable Value 2 /
{ 222: h'7DE993F9918D0A14B0FC2…453C3A1C833B44' }
],
…
}
```

SD-CWT SBOM



Payload

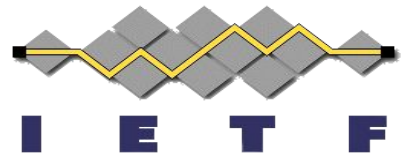
```
…
"files": [
/ 🔴 Disclosable Value 1 /
{ 222: h'58F422BA59…A6D75858A68C' },
{
"fileName": "./README.md",
"SPDXID": "SPDXRef-File--README.md-534A3C13…D5E53B2B6023A",
…
"licenseConcluded": "NOASSERTION",
"licenseInfoInFiles": ["NOASSERTION"],
"copyrightText": "NOASSERTION"
},
/ 🔵 Disclosable Value 2 /
{ 222: h'7DE993F9918D0A14B0FC2…453C3A1C833B44' }
],
…
}
```

Disclosures

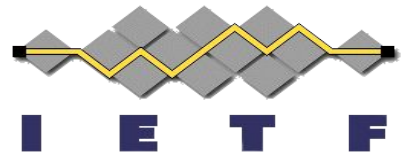
```
[
h'2BD5D126E016912A103D7B0B1B233AC6', / Salt /
{ / 🔴 Disclosed Value 1 /
"fileName": "./script.sh",
"SPDXID": "SPDXRef-File--script.sh-A5BE2A0E0FC9F8C2DA4F420B3046CD292AFB11C5",
"checksums": [
{
"algorithm": "SHA256",
"checksumValue": "e12fc416bf4aebf08117725577e05900aabf7ba7bda1c05e78cb519620c9a0b6"
},
…
]

[
h'91B103A152F115724C576344D268371B', / Salt /
{ / 🔵 Disclosed Value 2 /
"fileName": "./clean.sh",
"SPDXID": "SPDXRef-File--clean.sh-49B0B794639658A24ED0F30BCCC4124A886FA908",
"checksums": [
{
"algorithm": "SHA256",
"checksumValue": "a42c14e6502ccbc2a8abd051bd38fe1037f40e6084afb667a87bb59572c89657"
},
…
```

Privacy

Mike Jones (10 min)



Lots of possible privacy aspects when using digital identities



- I'll briefly touch on some of them
- Many aspects of privacy overlap and influence one another

- After my brief take, I'll leave time for you to
  - Tell me what I left out
  - Tell me how you see things differently

Minimal Disclosure

- Releasing only the information needed for an interaction
- Can be accomplished several ways
  - RP requests token with only needed claims and IdP issues it
  - Verifier asks Wallet for Presentation with only needed claims and Wallet issues it
  - Both of these are forms of Selective Disclosure
- Enabled by
  - OpenID Connect “claims” request parameter
  - SD-JWTs
  - ISO mDLs

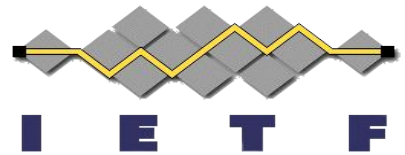
Not “Calling Home”

- You can use a physical driving license without consulting the Department of Motor Vehicles
  - The Washington DMV doesn’t know when I board a plane or purchase alcohol
- OpenID Connect and SAML “call home” to the Issuer
  - They issue tokens audienced to the RP/SP
- VCs using the 3-party model don’t “call home”
  - Some credentials held by the Wallet can be reused indefinitely
  - Some are single-use, which can be mitigated by batch issuance
- Wallet can see where you use VCs but not the Issuer

Non-Correlation among Verifiers

- Prevents Verifiers of your credentials from being able to determine that you used the same credential at both of them
- Requires the information in each Presentation to be different
- Of course, if you include constant claims such as e-mail address or name, all bets are off
- Enabled by
  - BBS signatures on Presentations
  - Single-use credentials

Non-Correlation for Issuers and Verifiers



- Some would also like prevent Issuer and Verifier from correlating your activities
  - Would prevent Issuer from being able to tell whether a Presentation was derived from a Credential it used
  -
- Not clear whether this is needed
- Not clear whether this is feasible

Tracking

- The ability for a party to observe and record your actions
  - OpenID Connect OPs can track the RPs you use
  - SAML can too (while calling them IdPs and SPs)
- Wallets can track which Issuers and Verifiers you use
- Browsers can track which Web Sites you use
- Some of this may be inevitable
- What they **do** with this information affects your privacy

Releasing Proofs Rather than Claims

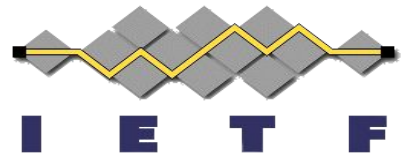
- In JWTs, CWTs, SD-JWTs, SAML Tokens, etc. typically release birthdate claim
  - Example: "1994-04-12"
- Or only release a proof of a property of the claim
  - Example: age ≥ 18 years
- Enabled by zero-knowledge proofs
  - In scope for JWP work in JOSE

What else to say about privacy?

- Join the microphone queue to add your thoughts
  - (Time permitting)

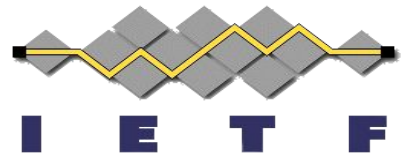
Clarifying Questions

(10 min)



Charter and Milestones

Henk (10 min)



https://github.com/transmute-industries/ietf-spice-charter/blob/main/charter.md

What to say about the charter?

TL;DR (by Identity Woman)

We are creating a venue for individuals who really want to work on verifiable credential stuff at IETF.

What else to say about the charter?

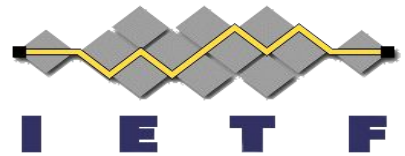
- Using IETF technologies for Verifiable Credentials, Selective Disclosure, and Unlinkablilty
- Using Issuer, Holder, Verifier model as a basis
- Alignment of JWT and CWT Claims Registration
- A more applicable open-world extensibility model based on industry-adoption
- Protocols are out-of-scope

Milestones – The Starter Set

- An informational **architecture** document
- Proposed standard documents covering **selective disclosure with CWT**
- Proposed standard documents covering **unlinkability with CWT**
- Proposed standard documents covering **identity documents with CWT**

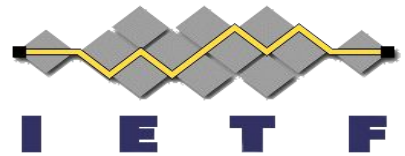
Discussion

(20 min)

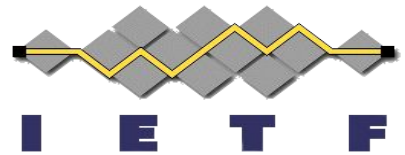


BoF Questions

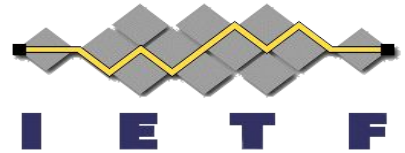
Chairs (20 min)



BoF Questions



- There is a problem that needs solving, and the **IETF is the right group** to attempt solving it.
- There is a **critical mass** of participants willing to work on the problem (e.g., write drafts, review drafts, etc.).
- The **scope** of the problem is **well defined** and understood, that is, people generally understand what the WG will work on (and what it won't) and what its actual deliverables will be.
- There is agreement that the specific **deliverables** (i.e., proposed documents) are the right set.
- It is believed that the WG has a **reasonable probability of having success** (i.e., in completing the deliverables in its charter in a timely fashion).


I E T F

Wrap-up and Conclusion

Area Director (10 min)