EFWG 2024-04-25 Meeting - IIW Recap

Meeting Schedule

- Bi-Weekly at 8:00-9:00 am PDT / 11:00-12:00 am EDT / 15:00 – 16:00 UTC / 17:00 - 16:00 CEST

Attendees

- Eric Drury
- Carly Huitema
- Feng Hou
- Charles Lanahan
- Drummond Reed
- Neil Thomson
- Scott Whitmire
- Jordan Evans
- Darrell O'Donnell
- Steve Magennis
- Judith Fleenor
- Stephen Curran

Main Goal of this Meeting

We're using this week's EFWG meeting to give the floor to anyone who'd like to give an update on IIW.

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • New Member Introductions:
1 min	Announcements	TF Leads	News or events of interest to EFWG members:
5 min	Review of action items from the previous meeting	Chairs	Bhutan NDI Case Study update
40 min	IIW Recap	All	Sessions or content that we'd be interested in hearing about: Trust Registry Face-Off Apple / Google POC DID:webs DID:tdw Connecting X.509 and DIDs and VIDs Personal Data Stores or anything else you found interesting or insightful ...
5 min	• Review decisions /action items • Planning for the next meeting	Chairs	

Recording

Notes

AI notes - coming

TDW - Trust DID Web is a new DID method but doesn't get DID doc from HTTP location but instead you get a log of all the entries of the changes of the DID doc. Every line is tied to the previous via a hash of the entry. The controller determined according to DID spec who much sign every transition. Very similar to DID: webs, but the difference is the transition state is the DID doc. Can you pre-rotation of keys. Next step, take the spec to a task force to evolve the specification. This DID has portability that lets you move the location of the DID, this changes the DID but the SCID (self certifying identifier) plus the history stays the same. Combine with high assurance DNS as with DID:webs will work the same. Long term storage - 30yr+, what kind of archival storage for this information?

DID:web is becoming well used but it really lasts history verifiability and this specification (TDW) adds ledger based features without a ledger but still fits very well with DID:web.

Comparison to DID:webs - DID:webs is KERI focused with a side of DID. But DID:tdw is DID focused and has less complexity compared to KERI and DID: webs.

DID:webs - uses KERI to take you state to state (using KERI and then producing a DID document out of that), you have to go further to generate a DID doc, requires more complexity to fit within the DID standard specification. The implication is that DID:tdw is easier from an adoption standpoint.

did:tdw Specification (rendered): https://bcgov.github.io/trustdidweb/
did:tdw Specification (repository): https://github.com/bcgov/trustdidweb
Presentation at IIW -- the details start at slide 11: https://docs.google.com/presentation/d/1PHo16asyceRiNKN7UkV8BSmtWtN6Wp3A6_9MV0IQ2jg/edit?usp=sharing
Typescript Implementation: https://github.com/bcgov/trustdidweb-ts
Python Implementation: https://github.com/bcgov/trustdidweb-py

Compared to DID:webs there are some risks compared to KERI but it is more secure than DID:web.

Is there a migration path from DID:tdw to DID:webs - they are totally different and it would have challenges.

Witness, watcher features of KERI could be added to DID:tdw but it doesn't belong in the specification but may appear in the implementation guide.

Apple session - prof of concept across android and IOS. Asked to provide a credential on a website but your credential is stored on your mobile device and they create a tunnel to establish a connection between the browser and the mobile device. The mobile OS can then ask different wallets for the needed credential which can be passed back to the browser where it can be shared. Interoperability across the two, use of protocols (uses the method that passkeys uses to communicate, it doesn't use passkeys: https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html). They make no standardization calls or opinions on standards. Multiple wallets on a device - Apple may allow that on their devices.

Trust registries - about 7 trust registry initiatives that are being worked on, they were outlined and how they operate. Checq, ToIP, OID federation, trust establishment with DIF)
EBSI Trust Chains: This standard tracks “Verifiable Accreditations” and is also used by cheqd. It involves a governing authority for the ecosystem with a DI D on a blockchain, tracking DIDs authorized for specific actions.
Trust over IP Trust Registry Protocol v2: Version 2 is under implementor’s review as of April 2024. See this ToIP blog post for a full description. It offers a R ESTful API with a query API standardizing how to query which entities are authorized to do what in which context.
OpenID Federation: This standard, particularly OpenID Federation 1.0, is already used in systems worldwide, including university networks and Brazil’ s open banking. It allows each entity to provide trust lists, including common trust anchors with other lists.

Credential Trust Establishment 1.0: This standard, part of the DIF Trust Establishment specification, is a data model rather than a protocol or interaction model. It involves creating a document and hosting it behind a URI, with no centralization. It allows roles for each participant and is complementary to VC-based decentralized trust.

There was also brief discussion of two others: TRAIN, from the Fraunhofer Institute, and the W3C Verified Issuer/Verified Verifier model.

An elegant solution to work X.509 into DIDs - use alternative names field of the X.509 certificate to include the DID reference. No need to create a separate DID method to work with X.509.

Eric Scouten at Adobe also co-chairs the X.509 VID Task Force at ToIP (meets every other week, Thursdays 8:30AM PT—
I attend most meetings). The goal is to build a bridge between X.509 certs and decentralized identifiers (DIDs
/VIDs) so that an ecosystem or an issuer does not have to choose one or the other. After researching all the options, it has become clear the best one is al so the easiest: just publish a DID/VID in the Subject Alternative Name field of the X.509 cert. That makes it easy to go from the cert to the DID
/VID. (To go in the other direction—from the DID document to the X.509 cert—
there are several options, including putting a specific service endpoint type in the DID document.)

To do a sanity check with the IIW community on this design and on the value of an X.509-to-DID
/VID bridge, on Thursday Eric and I called a session together with WebTrust auditor **Scott Perry** and BC Gov architecture **Stephen Curran** (who had alrea dy given his **Last Great DID Method** session). We had a number of X.509 savvy architects and developers attend, plus a woman from Digicert who used to work on X.509 at Adobe.

AI notes from meeting transcript:

The document is a detailed transcript of a meeting discussing advancements and concerns related to digital identity standards, particularly decentralized identifiers (DIDs) and their interaction with various protocols and specifications. Key highlights include:

Architecture Comparison: Drummond Reed clarified that TDW uses a simpler version of the architecture used by did:webs, focusing on a self-certifying identifier (SCID) to address security and portability challenges.

Implementation and Compatibility: Stephen Currran shared links to the TDW specification and its implementations in Typescript and Python. Discussions also covered compatibility with the Trust over IP (ToIP) Trust Spanning Layer and various identifier systems like VID.

Standards and Specifications Discussion: Drummond Reed overviewed several trust and identity standards, including EBSI Trust Chains, ToIP Trust Registry Protocol, OpenID Federation, and Credential Trust Establishment. Each has unique attributes suited to different needs in the identity verification ecosystem.

Future Considerations: Neil Thomson highlighted the need for interoperable and secure data storage solutions for credentials to avoid management issues across different platforms.

Action Items:

Review and Feedback: Participants are encouraged to review the linked TDW specifications and provide feedback, particularly regarding their implementation and compatibility with other systems like VID and TSP.

Community Engagement: Drummond Reed and Eric Scouten plan to engage the IIW community to evaluate the proposed X.509-to-DID/VID bridge design for viability and value.

Further Research and Development: There's a call for continued exploration of how various trust and identity standards can coexist and support each other, ensuring seamless interoperability and security across platforms.

These action items aim to drive the next steps in the development and integration of these digital identity standards and to ensure broad acceptance and compatibility within the community.

Decisions

Action Items

Coming up