2024-05-15 TSPTF Meeting Notes

Meeting Date & Time

15 May 2024 This Task Force meets every other Wednesday. The first meeting (for the NA/EU time zones) is dedicated to the TSPTF. The second meeting, for the APAC time zones, is the joint weekly APAC meeting of all Task Forces in the ToIP Technology Stack Working Group.

- NA/EU meeting: 08:00-09:00 PT / 15:00-16:00 UTC
- APAC meeting: 18:00-19:00 PT / 01:00-02:00 UTC

See the Calendar of ToIP Meetings for exact meeting dates, times and Zoom links.

Zoom Meeting Links / Recordings

- NA/EU Meeting: https://zoom.us/j/97402960831?pwd=dVdYRWNOOE3a3ZpQXVLM1h5VFpUQT09

Attendees

NA/EU:

- Drummond Reed (Host, me)
- Wenjing Chu
- Charles Lanahan
- Daniel Bachenheimer
- Darrel
- David Poltonak
- Eric Drury
- Jesse Carter
- Judith Fleenor (Trust Over IP)
- Keerthi Thomas
- Mark Scott
- Neil Thomson
- Rob Aaron
- Samuel Smith

Agenda Items and Notes (including all relevant links)
<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Chairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 m in</td>
<td>- Start recording&lt;br&gt;- Welcome &amp; antitrust notice&lt;br&gt;- New member introductions&lt;br&gt;- Agenda review</td>
<td><em>Antitrust Policy Notice</em>: 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.&lt;br&gt;- New Members:&lt;br&gt;  - David Poltorak, formerly with the Prism project</td>
</tr>
<tr>
<td>2 m in</td>
<td>Review of previous action items</td>
<td>ACTION: Wenjing Chu to post more information in our Slack channel about proposing an open source implementation of the Trust Spanning Protocol as a new project at the OpenWallet Foundation.&lt;br&gt; ACTION: Drummond Reed to start Github discussion on the following topics: 1) OID4VC family, 2) DIDComm, 3) Other secure Messaging protocol(s), 4) ACDC protocols (all of which leverage the key state mechanisms based on KERI and bind the messages in transaction set to a seal for security).&lt;br&gt; ACTION ITEM: Drummond Reed to have Michelle update the schedule for TSPTF meetings to every other week.&lt;br&gt; ACTION: Drummond Reed to share via Slack and the ToIP mailing list that the May 22 TSPTF meeting will be devoted to finishing the second public review draft of the ToIP Technology Architecture Specification and updating the ToIP website pages covering these artifacts.</td>
</tr>
</tbody>
</table>
| 20 ms | Review of the OpenWallet Foundation TSP Project Proposal | Wenjing will share more about the proposal to the OWF Technical Advisory Council (TAC). [Here is a link to the proposal](#). See screenshot #1 below.<br> Wenjing gave us a review of the proposal, which was approved unanimously by the OWF TAC. It will now be moved into an OWF repo. Accenture and Gen were also sponsors along with Futurewei.<br> The major questions about the proposal were about higher-level language bindings, because that's what's needed to make the TSP broadly useful. Wenjing explained that Rust was chosen to have a very secure base language, and then language wrappers can be written so the libraries can be used with the language of choice.<br> Wenjing just extended the invitation to any TSPTF members who are interested to join the 3 developers on his team who are currently working on the project.<br> **Eric Drury** asked how the TSP will work with identities/parties that currently use OpenID. Wenjing said that this is one of the open questions about interoperability.<br> David Poltorak expressed an interest in getting involved with the project. Wenjing will follow up offline.<br> See screenshot #1 for more info.<br> Drummond emphasized that anyone can join this OWF project and also participate in the Discord channel.<br> ACTION: Any TSPTF member interested in participating in the OWF TSP project, please contact [Wenjing Chu](mailto:Wenjing.Chu@Accenture.com).
We will discuss how the TSP can integrate KERI AIDs, did:webs AIDs, did:tdw DIDs, and X.509-backed DIDs—plus any other VID types that TF members plan to need.

Samuel Smith suggested that self-issued certs could be modified to incorporate a VID. Current X.509 infrastructure involves two key states: the registrant's key state and the CA's key state. So it would be possible to use X.509 certs as a serialization format in a fully decentralized, single key-state manner.

Wenjing Chu said that CAs could also give the full chain. Charles Lanahan said that the Microsoft X.509 DID method required signing the full X.509 cert chain.

The other topic is how KERI AIDs and non-KERI VIDs can interoperate. With did:webs, a KERI AID is appended to a Web URL.

Sam explained that with the TSP, a message is always directional and involves two key states: the sender's key state for signing the message, and the recipient's key state for encrypting the message. So even one-way communication requires that both sides support both VID types in order to have both the signing and the encryption keys. This also means that both parties must be confident in the VIDs that other party is using.

If there are more than two parties, all parties must support the VID types of all other parties.

Darrell:
  - Appraisability test - will I accept your VID?
  - Implementation - do I support your VID?

Drummond then asked about interactions with OpenID-based systems, which are fundamentally federated systems. Wenjing asked if this task force wanted to look into how that can work. Judith Fleenor asked if we wanted her to make an outreach to the OpenID Foundation. Darrell O'Donnell pointed out there are many questions involved in those questions. Wenjing's primary interest is in interoperability with the EU digital identity wallet infrastructure.

Darrell said there are 3 key questions in this area:
1. Do we support OIDC, i.e., interfacing with an OpenID Federation?
2. What is the specific VID that we would be interacting with?
3. How would we tackle the difference in interaction models, i.e., message-driven vs. API-driven.

Judith suggested that, after conference season, we might ask to be guest speakers at an OpenID meeting to discuss the TSP and how it might be of interest.

Neil Thomson: As Darrell pointed out - OIDC that spins up a compatible VID to use TSP and APIs wrapper the TSP for use by OIDC. Sounds like a joint discussion.

Sam pointed out that there are fundamentally different underlying models for how key state is managed. It will most likely require that integrators support both. Those integrators who need both will make the effort to do that.

Darrell O'Donnell summarized the discussion and conclusions with screenshot #2 below.

Drummond suggested that we socialize this discussion during the conferences.

Wenjing asked a question: when we are doing nested mode, there are private VIDs that are effectively using DID peer, which has been supplanted by KERI direct mode, which is for private use. KERI direct mode is specified in the KERI spec. Sam explained that it is very simple: once you do an OObI, you share your KEL with the other party, and any time there is a change to the key state, you send it as a signed message to the other party. KERI direct mode uses CESR primitives.

For ephemeral VIDs, a KERI AID works just like a did:key.

---

Screenshots/Diagrams (numbered for reference in notes above)

#1
Decisions

- None.

Action Items

- ACTION: Drummond Reed to start Github discussion on the following topics: 1) OID4VC family, 2) DIDComm, 3) other secure Messaging protocol (s), 4) ACDC protocols (all of which leverage the key state mechanisms based on KERI and bind the messages in transaction set to a seal for security).

- ACTION: Drummond Reed to share via Slack and the ToIP mailing list that the May 22 TSPTF meeting will be devoted to finishing the second public review draft of the ToIP Technology Architecture Specification and updating the ToIP website pages covering these artifacts.

- ACTION: Any TSPTF member interested in participating in the OWF TSP project, please contact Wenjing Chu.