# 2021-10-18 TSWG Meeting Notes

## Meeting Date

- 18 Oct 2021

## Zoom Meeting Link / Recording

- https://zoom.us/j/98733571820?pwd=Z09yRWVCRUtNU0JVc0tvYkNhWk42UT09
  (This link will be replaced with a link to the recording of the meeting as soon as it is available)

## Attendees

- Darrell O'Donnell
- Drummond Reed
- Antti Kettunen
- Daniel Bachenheimer
- Steve McCown

## Main Goal of this Meeting

Start planning for developing and publishing the ToIP Technology Architecture Specification as a Core Four deliverable.

## Agenda Items and Notes (including all relevant links)

| Time | Agenda Item | Lead | Notes |
|---|---|---|---|
| 5 min | • Start recording<br>• Welcome & antitrust notice<br>• Introduction of new members<br>• 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.*<br>• New Members: None |
| 15 mins | Task Force Reports | TF Leads | Trust Registry TF — Darrell O'Donnell<br>• The ToIP Trust Registry Protocol Specification is ready to be circulated.<br>• GCCN has reviewed it and Vitor Pamplona has done a simple implementation.<br>• We discussed getting reviews from folks in the EU SSI communities.<br>• ACTION: Antti Kettunen will share the link to the Google doc version of the ToIP Trust Registry Protocol Specification with others in the Findy community.<br>• ACTION: Daniel Bachenheimer will share the link to the Google doc version of the ToIP Trust Registry Protocol Specification with ESSIF, EBSI, and INATBA<br>• ACTION: Darrell O'Donnell will send email sharing the Google doc version of the ToIP Trust Registry Protocol Specification wi th the Aries Interop communities.<br><br>ACDC TF — Drummond Reed<br>• Drummond Reed reported that ACDC TF members including Samuel Smith Phil Feairheller and Kevin Griffin gave several presentations on ACDC at Internet Identity Workshop.<br>• Attendees recognized that ACDC is a "fourth credential flavor" in addition to the three flavors supported in the W3C Verifiable Credentials Data Model 1.0 specification (the ISO mDL spec is a fifth).<br><br>Design Principles TF — Drummond Reed<br>• Progress was somewhat delayed by Internet Identity Workshop last week, but the first draft of the Design Principles for the ToIP Stack should be completed this week.<br>• Work is starting on revised graphics throughout—see the agenda items below.<br>• Antti Kettunen has made a comment on the second principle and will write it up. He is excited about building the "API of Me".<br><br>Technology Architecture TF — Drummond Reed<br>• This TF is now going to start moving full speed — see agenda item below. |
| 1 min | Approve Design Principles for the ToIP Stack as Draft Deliverable | Chairs | Call for consensus:<br>• **DECISION: Design Principles for the ToIP Stack is approved as a Draft Deliverable of the TSWG.** |

| | | | |
|---|---|---|---|
| 15 mins | Internet Identity Workshop Tech Highlights | All IIW Attendees | • Premature Standardization & Premature Interoperability (Darrell)<br>  ◦ We still have a long ways to go forward on standards.<br>  ◦ We have not done anything dead wrong, but we don't have real interoperability yet.<br>  ◦ Six or seven governments are operating Hyperledger Indy and Hyperledger Aries code bases but are not yet actually fully portable.<br>  ◦ Steve McCown pointed out that we have a limited set of companies and developers building out ToIP and they seem to be compartmentalized by platform.<br>  ◦ Darrell agreed with Steve, but pointed out the Aries Interop Test Suite. He hopes that it will enable the different platform implementations to actually interop.<br>  ◦ Darrell shared a story about the interop challenges in the geospatial mapping standards arena. All of the web mapping servers achieved interop at a specific version of the spec that proved to be sufficient for the market needs.<br>  ◦ Steve agreed that the different platform implementations are all similar. His company has been using a Mozilla toolkit called Uniffi that can lets you use the same toolkit in multiple places. It provides something more stable across the multiple toolkits — it is the easiest way to take a common library and implement it everywhere.<br>  ▪ Here are some tutorials Steve created as an intro to making portable libraries.<br>  ◦ Darrell would like Steve to share that with the Aries Interop effort.<br>  ◦ Antti observed that the EU Digital Identity Wallet initiative is amplifying efforts around feature comparisons vs. ISO mDL standards. If we look too far down the road, we're going to lose the battle to ISO mDL.<br>• mDL sessions — Drummond Reed reported that there were several sessions on mDL moderated by Andrew Hughes, who is now Director of Standards at Ping Identity.<br>  ◦ the mDL family of specs (not all of which are finalized yet) will tackle everything needed to establish real market interop, including the protocols.<br>  ◦ There was consensus that this was the level of interop that the Aries stack needs to reach — and the ToIP stack as quickly as we can define a V1.<br>• DIDComm — Drummond Reed<br>  ◦ Daniel Hardman gave a fantastic deck called Myth-conceptions that summarized the design goals for DIDComm V2.<br>  ◦ In particular it contains a great feature comparison chart with other protocols including the IETF MLS (Messaging Layer Security) specification. See screenshot below.<br>• BBS+ with LD Signatures — Drummond Reed<br>  ◦ Drummond did not attend this session but reported that Brent Zundel did and he said that the two Japanese cryptographers that gave this session showed a very compelling demonstration of how they solved the privacy leakage problems in the MATTR implementation. |
| 10 mins | Revised ToIP stack graphic | Drummond Reed | • We are producing a new version of the static ToIP stack diagram to use with our Core Four deliverables.<br>• We reviewed the proposed changes in this Google doc.<br>• They generated a lot of discussion, starting with "Agent / Wallet Governance Frameworks" at Layer 2.<br>• We ran out of time so we agreed to the following action item:<br>• ACTION: ALL TSWG members to review and comment on the proposed changes to the static ToIP stack diagram in this Google doc. |
| 10 mins | ToIP Technology Architecture Specification | Drummond Reed | • This is the final deliverable in the Core Four.<br>• One key task we can begin working on now is **a technical diagram of the ToIP Technology Stack as a protocol stack**—we need this for the Design Principles for the ToIP Stack paper.<br>• Should we begin having **weekly meetings of this TF** in order to finish this deliverable in November? The answer was yes.<br>• ACTION: Darrell O'Donnell and Drummond Reed to schedule a weekly ToIP Technology Stack TF meeting in the 7AM PT / 10AM ET time slot.<br>• Should we establish a **ToIP Architects Council** consisting of ToIP members who are recognized architects for decentralized digital trust infrastructure who we want closely reviewing this specification?<br>• We will take up this question in the new ToIP Technology Stack TF meeting. |
| 5 mins | • Review decisions /action items<br>• Planning for next meeting | Chairs | |

# Screenshots/Diagrams

| | | | DIDComm | HTTP + TLS | Signal, Matrix... | OIDC / OAuth2 | MLS (IETF) |
|---|---|---|---|---|---|---|---|
| security and privacy | confidentiality | Prevents eavesdropping. | y | y | y | y | y |
| | integrity | Impossible to tamper or forge. | y | y | y | y | y |
| | repudiability | Supports a mode where parties can speak off the record. | y | theoretical but not practical | y | n | y |
| | non-repudiability | Supports a mode where parties can speak on the record (provable to third parties). | y | built on top | built on top | built on top | y |
| | forward secrecy | Compromising long-term keys does not compromise old communication. | depends on rotation | y | y | partial | y |
| | privacy | Observers learn very little about the parties who are communicating. | y | correlated to login | y | maybe | y |
| | anonymous mode | Can send without identification/registration. | y | self-signed certs deprecated | n | n | y |
| | DIDs as foundation | Decentralized properties of DIDs are the basis for the mechanism. | y | Meh. practical fail | n | SIOP adapter | n |
| architecture | offline | Works without the internet. | y | n | n | n | undefined |
| | foundation for protocols | Defines how higher-order protocols can be composed atop. | y | client-server | n | n | undefined |
| | transport-agnostic | Usable with many different comm technologies. | y | n | partial | n | undefined |
| | 1 route, many transports | Mixed comm tech can deliver a single message. | y | n | n | n | undefined |
| | breaks silos | Security, authN, history can be used outside original context. | y | n | n | n | y |
| | peer to peer | Don't need a server. | y | n | partial | n | y |
| | usable on simplex | Useful with one-way transports. | y | n | n | n | y |
| | async | Send without other party listening. Receive without waiting. | y | modest | partial | n | y |
| authentication | 1 → org | Authenticates a single person or IoT device to an institution. | y | y | y | y | y |
| | org → 1 | Authenticates an institution to a single person or IoT device. | y | weak | n | n | y |
| | 1 → 1 | Authenticates a single person or IoT device to another single person or IoT device. | y | n | n | SIOP | y |
| | n-wise | Authenticate in a small, ad-hoc group. | y | n | n | n | y |
| latency | seconds | Comfortable to interact on a timescale of a few seconds. | y | y | y | y | y |
| | hours | Comfortable to interact on a timescale of a few hours. | y | maybe | y | maybe | y |
| | weeks | Comfortable to interact on a timescale of weeks or months. | y | n | y | maybe | y |

# Decisions

- [ ] **DECISION: Design Principles for the ToIP Stack is approved as a Draft Deliverable of the TSWG.**

# Action Items

- [ ] ACTION: Darrell O'Donnell to circulate the Google doc version of the ToIP Trust Registry Protocol Specification (and the Swagger) out to the TSWG community plus a few others (GCCN, EFWG, EU via Andre Kudra).
- [ ] ACTION: Antti Kettunen will share the link to the Google doc version of the ToIP Trust Registry Protocol Specification with others in the Findy community.
- [ ] ACTION: Daniel Bachenheimer will share the link to the Google doc version of the ToIP Trust Registry Protocol Specification with ESSIF, EBSI, and INATBA
- [ ] ACTION: ALL TSWG members to review and comment on the proposed changes to the static ToIP stack diagram in this Google doc.
- [ ] ACTION: Darrell O'Donnell and Drummond Reed to schedule a weekly ToIP Technology Stack TF meeting in the 7AM PT / 10AM ET time slot.