2022-01-20 TATF Meeting Notes

Meeting Date & Time

- 20 Jan 2022
  - **NA/EU 07:00-8:00 PT / 15:00-16:00 UTC**
  - **APAC 1:00-2:00PM PT / 21:00-22:00 UTC**

Zoom Meeting Links / Recordings

- NA/EU Meeting: https://zoom.us/rec/share/E8MH6GF3FZ5uWw0cohM6IgtPZYjjx4CxtSwTTlwR7RKWXjQpD8d4--_YF5ulv2S5.-PYdFxwjn8SmwKhI?startTime=1642691006000
- APAC Meeting: https://zoom.us/rec/share/C8GFmR-rUGF5tbeu_CWAQOoBe-1ADvKgIUxl7arV5RaX694aad3aFdsROVOIQFJd.OY7BL6EbRU6PD9Y1?startTime=1642712490000

Attendees

NA/EU

- Drummond Reed
- Darrell O'Donnell
- sankarshan
- Charles Lanahan
- Bart Suichies
- Henk van Cann
- Samuel Smith
- Adrian Gropper
- Isaac Henderson
- Jan Lindquist
- Phil Feairheller
- Kevin Griffin
- Steve McCown
- Vikas Malhotra
- Judith Fleenor
- Daniel Hardman
- Daniel Bachenheimer
- Wenjing Chu

APAC

- Drummond Reed
- Darrell O'Donnell
- Michael Nettles
- Wenjing Chu
- Judith Fleenor
- Jo Spencer

Main Goal of this Meeting

To have a deep-dive discussion with KERI architect Samuel Smith and DIDComm architect Daniel Hardman about the relationship of KERI and DIDComm and the implications for the design of the ToIP stack.

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes

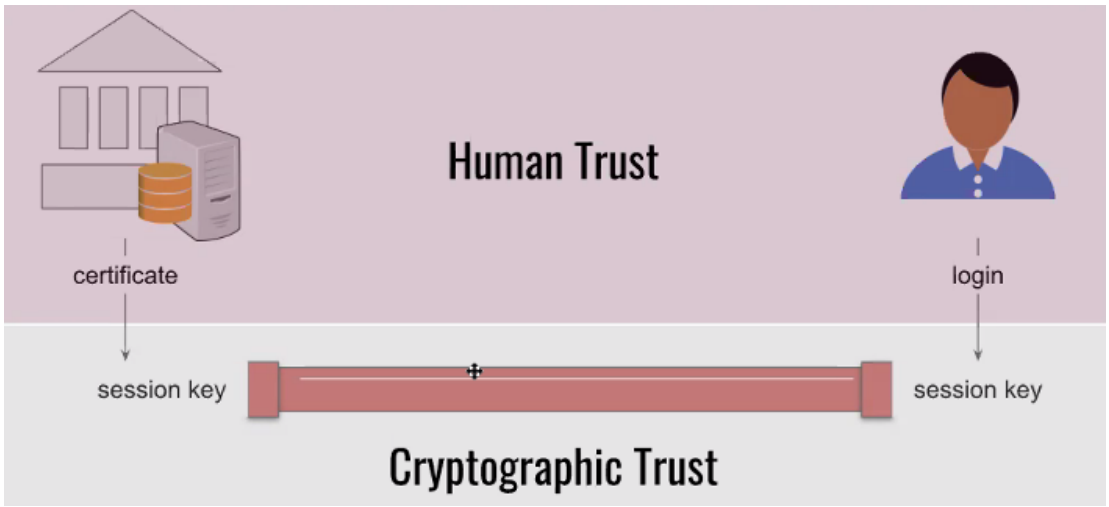
5 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • New Members: ◦ Charles Lanahan, Trust Science
5 min	Review of previous action items	Chairs	☑ ACTION: ALL TATF members to notify Vikas Malhotra if they want to participate in the planned IEEE workgroup on Cyber Security for Next Generation Systems
5 min	Announcements	All	Any announcements to share with the group.

40 mins	Special topic #1		Last week Drummond Reedgave this presentation on 3 key takeaways from the "Utah Protocol Stack Summit" that he was able to have over the holidays with Daniel Hardman and Samuel Smith on how KERI and DIDComm fit together. Today's meeting is a deep-dive discussion with Daniel and Sam to explore these takeaways and get their insights about what this means for the design of the ToIP stack.
			
			• Daniel Hardman offered that a fourth key takeaway from the "summit" was that he feels we should define a profile of KERI that can be mapped onto peer DIDs—that gives you a subset of the features of KERI that fulfills the requirements of the peer DID specification.
			  ◦ Samuel Smith agreed that it would make sense.
			  ◦ Daniel explained that the peer DID spec is currently maintained by the DIF ID & Discovery WG, but that since Daniel learned about KERI, he felt it was a subset of KERI, and that it could be superceded by a KERI-based spec.
			  ◦ Sam agreed because the functionality of peer DIDs is a "careful subset" of KERI.
			• Sam shared that the main problem that KERI solves is parties being able to trust other party's key state.
			  ◦ Each party does an "appraisal" of the key state of the other party before continuing.
			  ◦ KERI does cryptographic attribution to a cryptographically-generated identifier. Any other trust in a party is a higher-layer function.
			  ◦ Whether that identifier and its public key is shared publicly on only privately is use-case specific.
			  ◦ The question of how to **link** an identifier with an entity controlling a private key that has control over an identifier at an endpoint is a different question that requires identity binding.
			• Daniel shared one of his learnings from the "summit": for a long time he's believed that repudiability was an important
			  ◦ Sam advocated to have all messages signed.
			  ◦ DIDComm V1 and V2 put a lot of work into supporting authenticated encryption. But it was based on authenticated messages.
			  ◦ But Sam proposed that all messages be signed, and those that you want to have the capability of repudiation are accomplished by having repudiation of the identifier.
			  ◦ Tim shared an example of a Canadian government tip line, where the identity of the person never needed to be revealed.
			  ◦ Tim felt that KERI allows the separation of the question of repudiation from encryption.
			  ◦ Kevin shared that there are two types of pseudonymity. There is the example of a pseudonymity for a tip line that wants to be able to claim a reward. The other kind is a source talking to a reporter who needs to be able to prove that he has received information from the source but not reveal the source.
			  ◦ Tim likes the idea of profiles of KERI that can be specified for particular use cases.
			  ◦ Sam said that by separating repudiability by identifiers. It allows delayed accountability or latent accountability. It would allow a secure conversation to be pseudonymous for as long as needed, but then to be made accountable at a layer date if needed.
			  ◦ Big +1 from Daniel to Sam's observation about latent accountability
			• Bart asked the question: "Can we (or have we already) visualize the 'where KERI fits' in terms of jobs-to-be-done across an identity journey? Ie - most of the conversations to date are very technical, and less focused on arguments as to why people should get behind this."
			  ◦ Daniel said that in an "identity journey", KERI is the road building. At the very beginning of the journey, you need to plan your route to make sure there is a road that connects your destinations. KERI gives you that road. If it is a very short road, then you setup is relatively easy. But if it is a long road, such as an extensive dialog between a tipster and a reporter, KERI can be used to enable key rotation to keep the journey on the road safe. Other DID methods may not offer those functions to "keep the road safe".
			  ◦ Daniel said that if you need a high level of assurance in a DID method, KERI provides it.
			  ▪ Blockchain or verifiable data registry independence
			  ▪ VDR portability
			  ▪ Deep security guarantees
			  ◦ Sam said that if you put authenticity first, it makes the rest of the security challenges much easier
			  ▪ He used an example of a spam filter.
			• Daniel shared screenshot #1 (below) to show how separation of layers works.
			  ◦ KERI gives you the bottom layer of cryptographic trust. Anytime the cryptographic trust needs to be established, terminated, or changed, KERI is involved.
			  ◦ Sam pointed out that it does not require any human trust, it's done all technically.
			  ◦ Tim called it the separation between "institutional trust" and "technical trust".
			• Antti brought up the question of what the cryptographic binding should be to: a device or an identifier. The EU is saying that by binding to a wallet is binding to all the credentials in that wallet, but that is too blunt of an instrument. It should be to an identifier.
			  ◦ Daniel Bachenheimer explained that INATBA is the wallet binding is because it becomes the proxy for a national ID.
			  ◦ We agreed that the national ID should be used only in interactions that need it.
			  ◦ Drummond Reed suggested that the ToIP stack should support (and recommend) separation of identifiers used at the human trust layer from identifiers used at the cryptographic layer.
			  ◦ Darrell pointed out that a dependency on a specific device is a serious problem and KERI can solve it.
			  ◦ Sam agreed that KERI solves it by separating the primary and secondary root of trust. It also provides the multi-sig capability to have a highly-survivable infrastructure.
			  ◦ Tim said that the biggest trip-up for policymakers to be too prescriptive in legislation. Such as prescribing identifiers.
			  ▪ He's worried that the EU is headed down the centralization path.
			• We discussed the layering of the ToIP stack at length. We ran out of time but agreed that we now need to dive into the specifics of the layering in order to get the order correct. See diagram #3.
			
			Further discussion at the APAC Meeting:
			
			• Understanding KERI: once again we strongly recommend this podcast with Tim Bouma interviewing Samuel Smith
			• We loved the idea of testing our description of the stack using "Thing Explainer" : https://xkcd.com/thing-explainer/
			• Different trust issues are addressed/solved at different layers.
			• Wenjing Chu said that the best way to understand KERI is to compare it to the story "Tinker, Tailor, Soldier, Spy". It makes a very complicated set of small commitments to unearth who is the spy. But KERI makes a very simple commitment to a cryptographic secret and builds everything up from there.
			• Answering a question from Judith about performance, Darrell O'Donnell explained the difference between caches that must constantly poll the source vs. caches that are subscribed to the source and then be pushed to the cache.
			  ◦ DECISION: The design of the ToIP stack should accommodate both online and offline usage of the stack.
			  ◦ Jo Spencer explained that the same thing applied to mobile payments using tokens. Every transaction had to be stored as a unique token in the wallet so that it could be used offline. But if you use it completely offline for too long, the device will run out of stored tokens and you will have to refresh it.
			  ◦ So offline usage is almost always time-boxed.
			• Jo Spencer shared a project that is starting to use DIDs to identify components within an energy system: https://www.energyweb.org/aemo/

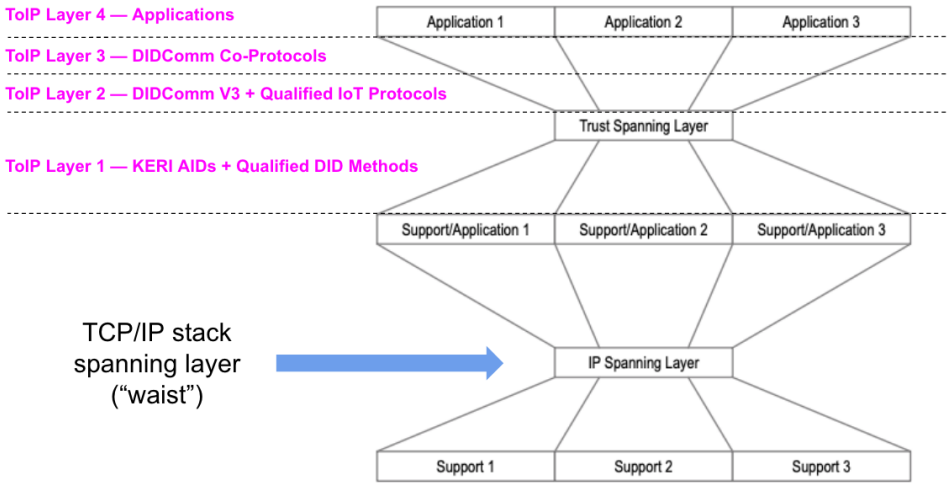
	• Review decisions/action items • Planning for next meeting	Chairs	ACTION: Chairs to develop a "plan of attack" for starting to refine the protocol stack diagram suggestions and begin drafting the ToIP Technology Architecture Specification.

Screenshots/Diagrams (numbered for reference in notes above)

#1

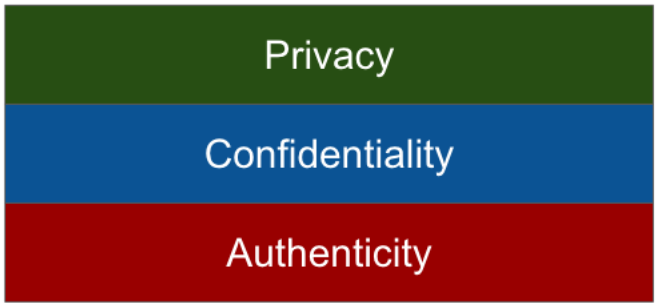


#2



#3

Sam and Daniel agree the order of the challenges addressed by the layers must look like this:



Decisions

- DECISION: The design of the ToIP stack should accommodate both online and offline usage of the stack.

Action Items

- [ ] ACTION: Chairs to develop a "plan of attack" for starting to refine the protocol stack diagram suggestions and begin drafting the ToIP Technology Architecture Specification.