

2022-04-07 TATF Meeting Notes

Meeting Date & Time

- 07 Apr 2022
 - NA/EU 07:00-8:00 PT / 14:00-15:00 UTC
 - APAC 1:00-2:00PM PT / 20:00-21:00 UTC

Zoom Meeting Recordings

- NA/EU Meeting:
 - Part One: https://zoom.us/rec/share/m24XNjHacUAie15pYmi0dK3MoMgK2JEhNvnZ8FWg-ilX9S-DNVHVvsaHd4mekZjc.Jxl6mrBn_ld2a13J
 - Part Two: https://zoom.us/rec/share/tovnBPlj5msAj70A_WdL-HFs-8bSkUkhnzpzct7LXDolGOCqIrt6vZfVWUUU-ftE.BypO-twOzzwmelfN
- APAC Meeting: https://zoom.us/rec/share/GGA53gAXTXL-a5cCfv2JB0HabtViJJ0uA8MFqxtb_etirCNgZtfEiGbHo86Zy-Uc.3YlQrhFG1nim3qH4

Attendees

NA/EU

- [Drummond Reed](#)
- [Darrell O'Donnell](#)
- [Phil Wolff](#)
- [Neil Thomson](#)
- [Tim Bouma](#)
- [Wenjing Chu](#)
- [Daniel Bachenheimer](#)
- [Antti Kettunen](#)
- [Isaac Henderson](#)
- [Kevin Dean](#)
- [Lance Byrd](#)
- [Vikas Malhotra](#)
- [Goutam Sinha](#)
- [Samuel Smith](#)

APAC

- [Darrell O'Donnell](#)
- [Drummond Reed](#)
- [Judith Fleenor](#)
- [John Jordan](#)
- [Samuel Smith](#)
- [Vikas Malhotra](#)
- [Wenjing Chu](#)
- [Daniel Bachenheimer](#)
- [Allan Thomson](#)

Main Goal of this Meeting

NA/EU MEETING: 1) Canonical use cases and scope limitations for the V1 ToIP stack, 2) review new **Working Draft 01** of ToIP Technology Architecture Specification, 3) Recap the trust spanning layer discussion from last week; **APAC MEETING ONLY:** [Samuel Smith](#) will present about **chain-link confidentiality**.

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: <i>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.</i> • New Members — APAC call: ◦ Allan Thomson introduced himself as Chief Architect Threat Defense Technology at Avast. He's also been a co-chair of several OASIS Technical Committees, including STIX/TAXII 2.x Interoperability. It turns out that he and Wenjing Chu also worked together at a company called Airspace. Allan explained that Airspace was a big proponent of standardization, particularly around 802.11.

5 min	Announcements	All	Updates of general interest to TATF members. • Tim Bouma said that the Canadian federal government budget will come out later today and he will report how much they will be spending on digital identity. ◦ We had a short discussion about the relative investment levels in the EU, Canada, and the USA. ◦ Daniel Bachenheimer shared that governments should invest in just enough digital identity infrastructure to support self-sovereign identity for citizens. ◦ Tim Bouma shared the view that government should provide foundational identity and then let the market provide the rest. ◦ Neil Thomson felt that government should not be the only issuer of foundational identity—and should not require the use of such foundational identities. And that the government could also certify other legal entities to be issuers of foundational identity. ◦ Daniel Bachenheimer said that foundational identities do one thing very useful: establish uniqueness within a population. Government-issued foundational identities also confer legal rights within a country. ◦ Tim Bouma pointed out that the issue is that there is no legal definition of foundational identity, which creates an issue for policy development. ◦ Vikas Malhotra added that there was a discussion at UNDP about that definition of legal identity and the role of SSI.
5 min	Review of previous action items	Chairs	✓ ACTION: Drummond Reed to start a discussion on our Slack channel about the canonical use cases and scope limitations for the V1 ToIP stack in preparation for next week's meeting. ✓ ACTION: Drummond Reed to make the first agenda item for next week's meeting a discussion of the canonical use cases and scope limitations for the V1 ToIP stack. ✓ ACTION: Drummond Reed to add chained root of trust topic to the agenda for next week's calls. ✓ ACTION: Drummond Reed to add spanning layer discussion to the agenda for next week's calls. ✓ ACTION: Drummond Reed to prepare a revised outline of the Google doc version of the ToIP Technology Architecture Specification for review at next week's meeting.
15 mins	Canonical use cases and scope limitations for the V1 ToIP stack	All	Per the second action item above, we want to gather inputs about scope limitations for the first version of the ToIP stack. • Wenjing Chu encouraged everyone on the Task Force to contribute their thoughts about canonical use cases. • ACTION: Drummond Reed to add a section to the ToIP Technology Architecture Specification on Canonical Use Cases and Scope Limitation. We then had quite a wide discussion about the Architectural Layering of the ToIP Stack section of the document. • Samuel Smith pointed out that self-certifying identifiers and data structures are what enable the ability to cross trust domains. Everything needed to prove a trustworthy identifier needs to be “in the belly” because then everything necessary for secure attribution to an identifier is present. ◦ There is a key difference between control of an identifier and control of a credential. By going down to self-certifying identifiers, we establish the atomic building blocks of transitive trust. ◦ PGP failed because it relied just on public/private key pairs, which don't inherently support persistence. ◦ Persistent identifiers can then develop reputation that can be carried across trust domains. • Wenjing Chu commented on the confusion between identifiers and VCs. “You can always trust a liar but you can never trust an incompetent person.” What he means that in Layer 2, one is not establishing human trust, just cryptographic trust. L2 gives you what is necessary to establish this autonomous control of an identifier (and thus the basis for detecting duplicity). • Vikas Malhotra summarized that first someone sets up an autonomous system, THEN they can issue or receive VCs. • Darrell pointed out that L2 must support the ability to make conclusions at the higher layers. • Wenjing gave the example of two spies who can trust each other without either of them knowing the true identity of the other. • Sam called such identifiers “cryptographic pseudonyms” or “cryptonyms”. You may know who (or what) is behind a cryptonym, but you can prove that you said them. ◦ IP addresses do not have the properties necessary to establish a trust spanning layer. What we need is the right kind of identifier: a cryptography verifiable identifier that can be proved. ◦ Use of a ledger can be both below and above L2 because it is two different uses. Sam distinguishes between putting identifier or key rotation history on ledger is support for L1 vs. the use of a public utility as a trust registry is support for L3. • Wenjing pointed that the reference architecture needs to go early in the flow. • Layer 2 needs to include the addressing layer because that is common to all above that. • Tim: the IP layer enabled the spanning of network domains (LANs), where as the trust spanning layer enables the spanning trust domains. Enables a “zero-to-one” transformation. Enables a “trust network of trust networks” that anyone can plug into because the identifiers. The border gateway protocol refers to “autonomous systems” that are all self-governing. • The idea came up that this new “layer” needs a name. Suggestions discussed included: Web of trust, Trustnet, trust fabric. Others?
20 mins	New Working Draft 01 of ToIP Technology Architecture Specification	Drummond Reed	Per the last action item above, Drummond has prepared a new version of the Google doc that is now a full Working Draft and started filling in content that needs review and feedback. • ACTION: Drummond Reed to finish conversion of the storyline slide deck text into the ToIP Technology Architecture Specification and then post to the TATF Slack channel that it is ready for review of those portions of content.

10 mins	Spanning layer discussion	Wenjing Chu Drummond Reed Samuel Smith	This is to recap a discussion between Wenjing Chu and Samuel Smith from last week—which Drummond listened to on the recording and has already reflected in the Working Draft 01 outline. - Wenjing summarized the NA/EU discussion that the core requirement of the trust spanning layer is similar to the goal of the TCP/IP spanning layer (the IP layer). That means we want the ToIP trust spanning layer to be "as simple as possible but no simpler". - By those two notions, the only thing that the trust spanning layer needs to be able to do is provide autonomous, cryptographic verifiable identifiers that can support non-repudiable communications. - Anything that is needed to support Layer 2 is in Layer 1. Anything that is a higher layer protocol is L3 or L4. John Jordan asked if L1 was always needed. There was a consensus that it is not except for IP connectivity. Darrell O'Donnell explained that we have recast the public utilities at L1 because they can support different functions needed at all higher. Drummond Reed added that this means L1 public utilities can support all the higher layers in different ways. Judith Fleenor said that we might want to look depicting public utilities in different ways in the ToIP stack. Wenjing Chu suggested that we may want to actually choose a better name for it, such as "supporting infrastructure". - Judith suggests that the TSWG needs to do a "road show" with this spec and the layer definitions in order to get consensus all the way around.
APAC CALL ONLY	Chain-link confidentiality	Samuel Smith	APAC CALL ONLY—Sam would like to explain the ACDC concept of chain-link confidentiality and how it provides a different type of privacy protection/preservation that selective disclosure and zero-knowledge proofs. Here is a link to the slides Sam presented (PDF). - Sam started with the PAC theorem—slide #1 below. - He then gave the definitions he's working with—#2 below. - Sam contended that strong privacy is essentially impossible if the primary party is going to share authentic content with other parties. - So the only way that the goal of real privacy can be realized by incorporating an exchange of value. - A solution to the kinds of exploitation in slide #5 below is chain-link confidentiality. ACTION: Samuel Smith to post to the Meeting Notes and TATF Slack channel a link to his paper and/or slides on chain-link confidentiality.
5 mins	- Review decisions /action items - Planning for next meeting	Chairs	THERE ARE ONLY TWO MORE MEETINGS BEFORE Internet Identity Workshop (April 26-28). So the next two meetings will focus heavily on finishing a complete Working Draft of the ToIP Technology Architecture Specification so we can be ready to present it at IIW.

Screenshots/Diagrams (numbered for reference in notes above)

#1

PAC Theorem

A conversation may be two of the three, *private*, *authentic*, and *confidential* to the same degree, but not all three at the same degree.



#2

Definitions

Private:

The parties to a conversation are only known by the parties to that conversation.

Authentic:

The origin and content of any statement by a party to a conversation is provable to any other party.

Confidential:

All statements in a conversation are only known by the parties to that conversation.

Privacy:

about control over the disclosure of who participated in the conversation (non-content meta-data)

Authenticity:

about proving who said what in the conversation (secure attribution)

Confidentiality:

about control over the disclosure of what was said in the conversation (content data)

Relatively weak legal protection for non-content (supoena)

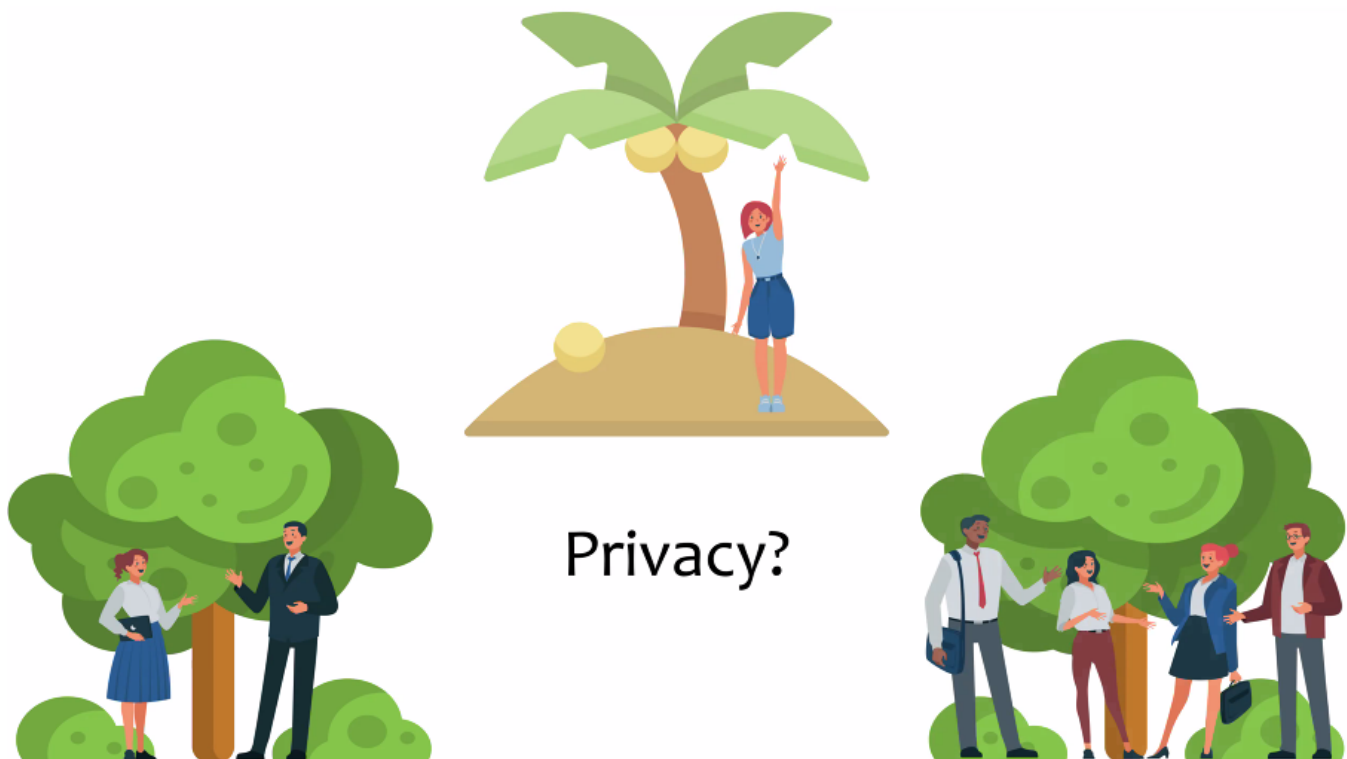
Relatively strong legal protection for content (search warrant)

<https://www.lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line>

<https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/>



#3



#4

Operating Regimes

Political	Legitimate	Hide or Bribe	Regulation and/or Legally Enforced Contracts
	Illegitimate	Hide and Bribe	Criminally Enforced Contracts ?
		Illegitimate	Legitimate
		Economic	

#5

Three Party Exploitation Model

First-Party = Discloser of data.

Second-Party = Disclosee of data received from First Party (Discloser).

Third-Party = Observer of data disclosed by First Party (Discloser) to Second Party (Disclosee).

Second-Party (Disclosee) Exploitation

implicit permissioned correlation.

no contractual restrictions on the use of disclosed data.

explicit permissioned correlation.

use as permitted by contract

explicit unpermissioned correlation with other second parties or third parties.

malicious use in violation of contract

Third-Party (Observer) Exploitation

implicit permissioned correlation.

no contractual restrictions on use of observed data.

explicit unpermissioned correlation via collusion with second parties.

malicious use in violation of second party contract

Decisions

- None

Action Items



- ☐ ACTION: [Drummond Reed](#) to add a section to the [ToIP Technology Architecture Specification](#) on Canonical Use Cases and Scope Limitation.
- ☐ ACTION: [Drummond Reed](#) to finish conversion of the storyline slide deck text into the [ToIP Technology Architecture Specification](#) and then post to the TATF Slack channel that it is ready for review of those portions of content.
- ☐ ACTION: [Samuel Smith](#) to post to the Meeting Notes and TATF Slack channel a link to his paper and/or slides on chain-link confidentiality.