2023-04-06 TSPTF Special Workshop Meeting Notes

Meeting Date & Time

06 Apr 2023 This was a special 2-hour meeting of the ToIP Trust Spanning Protocol Task Force in order to have a deep-dive workshop to begin the consolidation stage of our work on the trust spanning protocol (TSP).

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

Zoom Meeting Recording

This recording covers the entire 2 hour workshop meeting:

- https://zoom.us/rec/share/k8SbTOiSn3FNEAW2F62Ec3Z3r29gB6h3vZCXk1mMyfLIiId8qOsdBpySOn43ThAy.Zc7_WF_x74P1cMf4

Attendees

- Drummond Reed
- Daniel Hardman
- Wenjing Chu
- Samuel Smith
- Darrell O'Donnell
- Abbie Barbir
- Anita Rao
- Antti Kettunen
- Christine Martin
- Daniel Bachenheimer
- Dima Postnikov
- Jo Spencer
- Judith Fleenor
- Markus Sabadello
- Mathieu Glaude
- Neil Thomson
- Oskar van Deventer
- Phil Feairheller
- Subhasis Ojha
- Willem de Kok

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
3 min	• Start recording • Welcome & antitrust notice • New member introductions • Agenda review	Leads	• **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:
30 mins	Review of the ToIP Technology Architecture Specification V1.0	Wenjing Chu	Wenjing reviewed the key points of the TAS as they bear on the design of the TSP, including screenshots #1, #2, and #3 below. He clarified that the TSP is the protocol that connects any two ToIP Endpoints, and explained the special roles of Intermediate Systems and Supporting Systems.
90 mins	Open Discussion	All	Daniel Hardman The opening topic he proposed, using screenshot #4 to highlight the specific TAS requirement (L2.9), to what extent do we want the TSP to be **descriptive** or **prescriptive**. • Descriptive would allow the parties using the TSP to describe their trust basis such that they can decide whether to trust each other. • Prescriptive would specify that certain types of trust guarantees are required. Wenjing Chu proposed that the TSP protocol itself should be descriptive, but that the ToIP stack as a whole can be prescriptive. Oskar van Deventer asked for more clarification of what the question means. Daniel Hardman gave the example of whether the TSP should require VIDs (most descriptive), DIDs (more prescriptive), or AIDs (most prescriptive). Oskar van Deventer wanted to be sure that implementations are interoperable.

Samuel Smith primary concern is that the security of the higher layers depends on the security of the lower layers, so if the lower layer is weak, you can't fix it at a higher layer.

Oskar van Deventer "Where in the ToIP layer is "message routing"? Is it part of Layer 2, "Trust Spanning"?"

Daniel Hardman replied: "There is a section of the TAS about message routing. I proposed that we move it to layer 3. I think several others feel like routing beongs in 3, also. But right now it is in 2."

Jo Spencer replied: "As covered in Sam's proposal, Routing can be at the Layer 1, 2 or 3 level depending on what is resolves."

Judith Fleenor "@Oskar, If you haven't yet, would recommend you read the Reference Arch document… it was developed after the conceptual diagram. Many discussion are going on right now to determine where specific compensates fit into the conceptual diagram where, based on the Ref Arch and work being done in on Trust Registries etc."

Oskar van Deventer "Good to see different answers to my question. Apparently, it is not just my confusion :-). I like the new stack with "Trust Support", including internet transport."

Drummond Reed "Yes, me too, it helps answer other questions that the first and second generation diagrams didn't."

Darrell O'Donnell "@Oskar - agreed. Comms (addressing and transport) are crucial (and very aimed at the Layer 2 TSP). These diagrams are missing the OTHER trust support systems - ledgers, resolvers, etc."

Jo Spencer "@Darrell - I think Wenjing covered this point... "OTHER trust support systems" are themselves endpoints (supporting, intermediaries or other endpoints) that support trust tasks at the Layer 3 as described in the Tech Architecture. Resolvers or routers that are local to the endpoint can be at layer 1."

Drummond Reed asked the question: can the strength of the security at the ToIP layer be selected by the ToIP endpoints involved as part of their governance frameworks or security policies?

Wenjing Chu believes the benefits of providing a wider set of connectivity options.

Willem de Kok said that the lower level of trust you put in the system, that is likely to become the lowest common denominator that the system normalizes on. "As I interpret it: More descriptive = More inclusive/interoperable More prescriptive = More trust guarantees. Is it really one or the other? Or is the question: To what extent should the TSP be descriptive/prescriptive?"

Darrell O'Donnell "I believe Sam and Daniel both state (please correct me gents) is that a higher-level protocol cannot repair the damage done below where Authenticity is degraded. Am I correct on that?"

Daniel Hardman "@darrell: yes, that is approximately what we have argued — You can't layer trust on top (that's the claim)."

Jo Spencer "We have to decide what we need to be prescriptive about and what we can be more "flexible" based on a descriptive definitions. Levels of interoperability depends on levels of prescription. E.g. We can't do "rip and replace" if we're not prescriptive and both options adhere."

Oskar van Deventer "This discussion seems to relate to a worry that European banks have: they may feel forced to accept the EUDI wallet as identification means, but what are the guarantees that these are secure, and what happens if a bank makes an incorrect decision, based on incorrect security assumptions about the EUDI wallet?"

Willem de Kok "By doing so, we also choose where the trust weaknesses are. I think it is good to be, as much as possible, in control of where the risks/weaknesses of the TSP are."

Neil Thomson "It someone has poor key management, then the decision is - don't trust them. That is the principle of the stack, that the stack provides the means to collection information on trust-ability, it is up to the parties to determine Trust Y/N."

Oskar van Deventer "I deal with websites on a daily basis, including governmental ones, that leak my details to criminals. I don't trust those websites, but I am coerced to use them ..."

Neil Thomson "Question. does prescriptive impact: - adoption - potential fragility - if the prescription is upgraded then does everyone have to upgrade immediately?"

Oskar van Deventer "This exactly the reason why DRM is not standardised. Hollywood only buys DRM solutions from parties that can control both end."

Darrell O'Donnell "I summarize Oskar & Willem as "you're coerced to the the lowest-common denominator…"

Willem de Kok "To me it feels like ToIP can choose what the lowest-common denominator of their system is."

Jo Spencer "In establishing a trusted link, the protocol has to allow the connection to be established with an agreed level of authenticity, integrity and security. If either of these endpoints don't believe that the other end is doing the right thing, they shouldn't establish the connection."

Antti Kettunen "IMO, the various layers need address the question of 'who can / should define the layer-specific requirements'. E.g. on Layer 3, IMO the trust task contents should be likely defined by business architects, who understand what value should the process handle. This is very important, that we don't mix the responsibilities of each layer, when looking at who should be defining their requirements."

Darrell O'Donnell "this is Oskar's coercion point - I need to step down to the level because I need to connect with them more than the other party."

Bree-Ana Blazicevic: the TSP is the most vital for establishing the "gold standard", and ToIP should be the gold standard.

Samuel Smith To support multiple levels of trust, it must be appraisable by the user, and the user must be able to have control of those. As long as they have an appraisable trust basis that can be communicated to an end-user.

Jo Spencer "Sam's nailed it! You have to make it visible..."

Darrell O'Donnell "Developers don't wake up wanting to make deep Authenticity decisions (at least this recovering developer never did)."

Daniel Hardman understands what Wenjing said that higher-level layers can help with trust, but Sam's concern is that the trust basis must be established at a lower layer. However it is important that individual persons must have the ability to decide about the trust level they are willing to accept — but users are not equipped to make those decisions.

Wenjing Chu The key is verifiability. If the TSP layer guarantees authenticity — and we do that by defining how verifiability is achieved — we can be in the same camp. Two other quick points:

- There is no "gold standard" of trust. Security is not a one-dimensional thing. It is n-dimensional. You can be very strong in one sense and very weak in another. There also can be tradeoffs between security and privacy (though that is not always true). So we want to be sure that users who want strong security guarantees of different types have a way to achieve this.
- Wenjing feels that you almost all trust tasks will use another layer over the TSP protocol.

Daniel Hardman "@wenjing: you are saying "as long as we guarantee authenticity" as if this guarantee is binary. But it is not binary; it is guaranteed with a level of assurance."

Neil Thomson is this a problem that ToIP needs to solve? He used an example of data privacy. If the leap is too high, adoption won't happen. But if we have a "ladder", folks can slowly climb it.

Judith Fleenor "@Neil, shouldn't we learn from consent that it didn't work to leave choice up to the developers and people. Therefore, don't you need prescriptive to make sure that it is built in…. because it would take forever for legislation to become real. But I get your point abut adoption, but it's tricky."

Neil Thomson "My response is that there are organizations that are doing high quality consent (privacy by design). One thing ToIP can do is to provide reference technology (as open source) that makes the easy path to follow which provides the high trust/security. But leave the options as to whether to use the highest level of trust/security or not."

Judith Fleenor "So then the TSP would include a way for the relying party can apprise the method fo authenticity. Is that what I'm hearing?"

Neil Thomson "Yes, propose trust questions ask a do you support <this trust aspect> for evidence and proof, where there are different levels of evidence and different types of proofs (including level of governance). I would suggest this is a way to support "appraisability"."

Darrell O'Donnell "@Judith - I think it would be more of an opening gambit - we won't connect unless we meet each other's threshold. I need at least X, can you meet that bar?"

Willem de Kok "Could somebody add the term 'appraisability' for the Terminology Design Training Session and his/her idea of the meaning here: https://github.com/trustoverip/trust-spanning-protocol/discussions/41"

Daniel Bachenheimer "Right 'I need at least X from entity A' and I can verify that entity A is legit provider at that level."

Samuel Smith If we define "verifiability" to include "appraisability of the trust basis", then he is in agreement with Wenjing.

Drummond Reed said that "appraisability" may in fact be a new requirement that we didn't capture in the TAS yet. He'd prefer that vs. trying to "stuff it" into "verifiability".

Daniel Bachenheimer used the FIDO protocol as an example of how, by deciding on how to describe the assurance factors, the verifier can apply their own policy against that info.

Drummond Reed agreed and said that he's working on similar descriptive claims for identity assurance.

Wenjing Chu said that he supports "appraisability" as a factor that could be incorporated into the TSP.

Daniel Hardman shared that "appraisability" could be a solution here but his biggest concern is how we can precisely define that.

Subhasis Ojha: "Can appraisability ensure identity frauds can be detected?"

Darrell O'Donnell "SSL Certs have lost part of their meaning - it now means "this is encrypted". An SSL certificate used to also mean "this is really Company/Entity X"."

Jo Spencer was also in favor of this solution, and said that each party to a communication should be able to decide about the levels of trust needed for different communications and trust tasks. He also said that there will likely be standard profiles created that enable such.

Drummond Reed mentioned that providing more descriptive information about the policies and procedures implemented by any actor in a ToIP trust community was in many ways exactly why the ToIP stack has two sides. In other words, it is what unites the Technology Stack (implementation) with the Governance Stack (policy).

Samuel Smith explained the different types of trust basis and said that we could make it very simple or very complex. We need to be careful about how complex we make it. When asked for an example of how appraisability works in practice, he gave the example of the Trusted Computing Group DICE (Device Identifier Composition Engine) Attestation Architecture specification.

Samuel Smith also gave these definitions in chat (the references are to the spec linked above):

- Appraisal: The action of assessing the trustworthiness of an Attester based on the attestation Claims it provides.
- Appraisal Policy for Evidence: A set of rules that direct how a Verifier evaluates the validity of information about an Attester. Typically, a policy is authorized by the Verifier Owner. Compare "security policy" in [2].
- Appraisal Policy for Attestation Results: A set of rules that direct how a Relying Party evaluates the validity of information about an Attester. Typically, a policy is authorized by the Relying Party Owner. Compare "security policy" in [2].

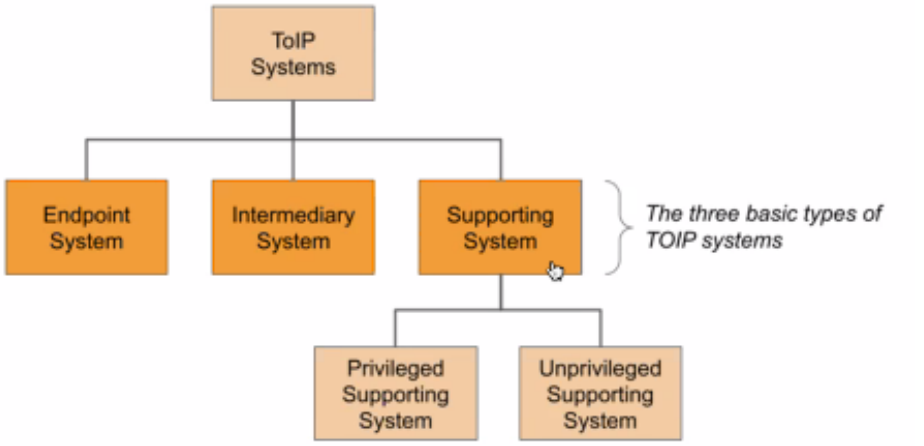
Drummond Reed Used the example of the step-up from HTTP to HTTPS as the only consumer-level signals providing "appraisability". Initially, only a small subset of websites added support for HTTPS. But as security issues on the Web got worse, the whole Web upgraded — to the point where Google will not serve up a website that does not use HTTPS. That changed the whole security landscape.

Drummond Reed thanked everyone for an most excellent and intense two-hour discussion.

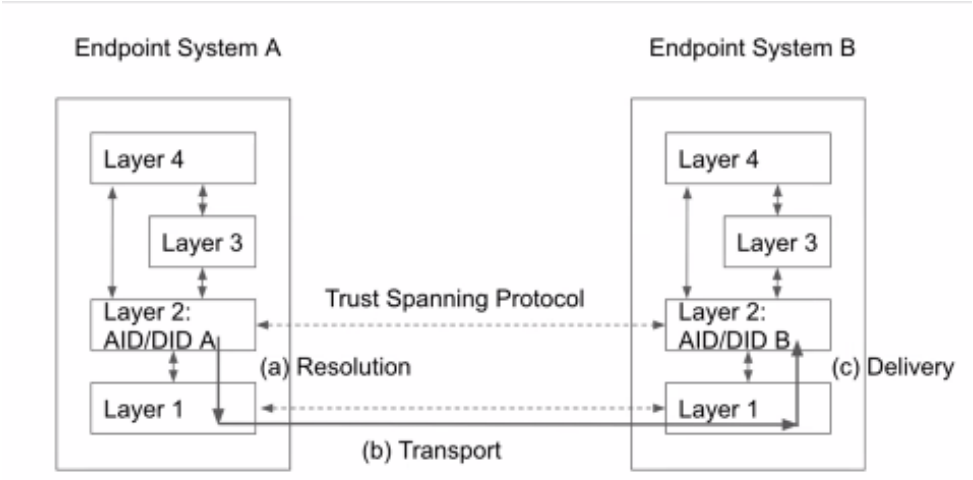
5 mins	• Review decisions /action items • Planning for next TSP Workshop	Leads	Drummond Reed announced that, in addition to next Wednesday's standard TSPTF meetings, there would be a second TSP Workshop at the same time next week, i.e., **Thursday 13 April 2023 at 1:00-3:00PM PDT / 20:00-22:00 UTC / 22:00-24:00 CEST / 06:00-08:00 AEST.**

Screenshots/Diagrams (numbered for reference in notes above)

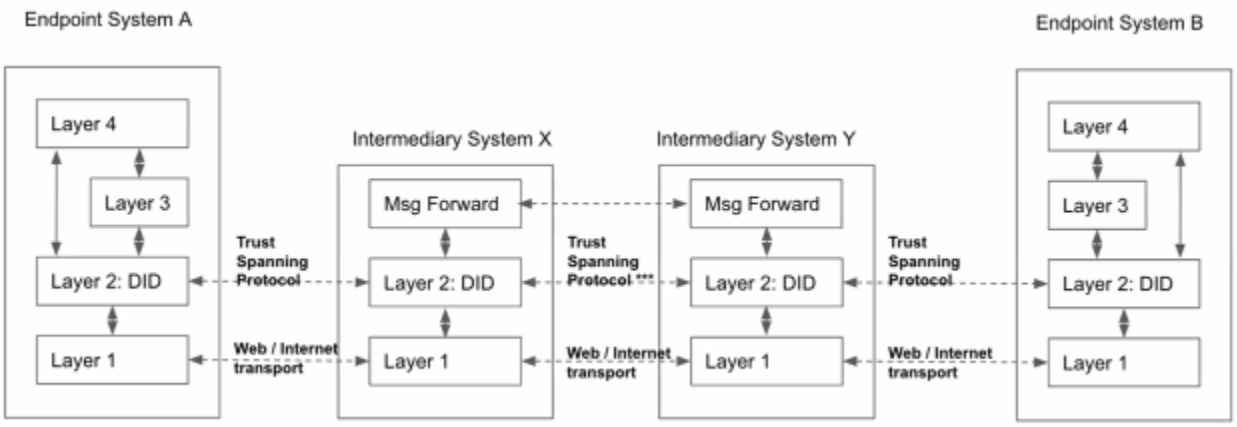
#1



#2



#3



#4

L2.9	The ToIP Trust Spanning Protocol specification MUST define how to construct and format messages that are cryptographically verifiable to have the following four properties: (1) Authenticity: the message was sent from a sender who has control over the ToIP identifier. (2) Integrity: the contents of the message transmitted by the sender are received by the recipient without modification. (3) Confidentiality: the contents of the message are only accessible by authorized parties. (4) Privacy: the contents of the message are bound to conditions of usage agreed to by the parties

Decisions

- Sample Decision Item

Action Items

- [ ] Sample Action Item