2022-02-24 TATF Meeting Notes

Meeting Date & Time

- 24 Feb 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/OnU9QB8k3lSBC4l7YDNB-rS8dDw5oebWHSGp2yq7IJW5wVsu9OQeoCmhqcxnOueF.mCPU6ZDTbW5aPHb
- APAC Meeting: https://zoom.us/rec/share/_l-oE0G2KDsOtxU2d1hoglgPpYXb-i6oSIGxldMccNYWEz5PmID9qcEm9a-SVg_1.-VDJ9wrHq_S3l3sv
(This links will be replaced with links to the recordings of the meetings as soon as they are available)

Attendees

NA/EU

- Drummond Reed
- Wenjing Chu
- Antti Kettunen
- Bart Suichies
- Daniel Bachenheimer
- Isaac Henderson
- Judith Fleenor
- Kevin Griffin
- Lance Byrd
- Nuttawut Kongsuwan
- Phil Feairheller
- sankarshan
- Tim Bouma
- Vladimir Vujovic
- Vlad Zubenko
- Xavier Vila

APAC

- Drummond Reed
- Darrell O'Donnell
- Judith Fleenor
- Wenjing Chu
- Jo Spencer
- Lance Byrd
- Andre Kudra
- Daniel Bachenheimer

Main Goals of this Meeting

1) Discuss new European digital identity architecture and reference framework from the eIDAS Expert Group, 2) Wenjing Chu to present a reference view of the ToIP stack, 3) Bart Suichies to present his view of the stack, 4) Drummond Reed to review proposed Layer 1 requirements in the storyline slide deck (Google Slides).

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes

3 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: ◦ Vlad from SICPA - Product Manager
5 min	Announcements	All	Updates of general interest to TATF members. • Drummond Reed shared • Tim Bouma said that the CIO Council of Canada is working on a draft of a management regime for the issuance of credentials.
2 min	Review of previous action items	Chairs	☑ ACTION: Wenjing Chu to prepare a "reference view" diagram of the ToIP stack to present next week ☑ ACTION: Bart Suichies to prepare presentation detailing some of his perspective on the protocol stack ☑ ACTION: Drummond Reed will add the point about "accommodating legacy approaches" into the narrative of the storyline deck. ☑ ACTION: Drummond Reed — and any other TATF members — to fill in more sections of the storyline deck for next week's call.

10 min	New EU eIDAS 2.0 reference framework	Bart Suichies	Discuss new European digital identity architecture and reference framework from the eIDAS Expert Group. Bart shared his key insights:
			
			• The document does put digital wallets very much in the forefront.
			• His impression is that "it focuses on the car, not the roads", i.e., it focuses on the wallet vs. the agent.
			• The document talks about "issuing the wallet" and having the wallets being certified by assessment bodies. Bart is doubtful that will work for 450M+ endpoints.
			• Wallets need to be privacy-preserving but also revocable.
			• They introduce new stakeholders into the mix — the device manufacturers.
			• The wallet is a new electronic identification means, capable of multi-factor authentication.
			• The principle is that the wallet is the default means of e-identification, which implies a few key credentials, instead of lots of micro-credentials.
			• Not sure about the "verifying the verifier" principle we have discussed here.
			• It talks about trust registries as "schema catalogs" and verification requirements.
			• Neither recovery or delegation are covered.
			• It MUST support combining credential claims. There are two ways of doing that:
			  ◦ Individual signed claims.
			  ◦ ZKP-based claims.
			• Users must be notified about breaches of control when sharing data. Bart is unsure how that would be implemented.
			• A lot of it is about implementation details.
			• The document is published to gather feedback. **This is the time for ToIP to provide feedback.**
			• Bart recommends that we should author a series of posts about key topics, e.g., storage, recovery, certified wallets, etc.
			• Bart's view is that, "in part, the ship has sailed", but we still need to provide as much feedback as possible.
			• Antti Kettunen pointed out that the authors were careful to point out the need for common protocols and standards. Antti felt that it was an implicit endorsement of the protocols already being used, yet keep the door open to SSI and ToIP.
			• Antti said there was some very interesting features not mentioned before. One example is a "constrained code" — an alternate password that would automatically signal the wallet was being used under duress. Could be very useful for voting.
			• There is a lot of comparison against the Qualified Trust Service Provider (QTSP) model.
			• We should raise up in feedback the ability to be able to use the ToIP stack and other types of providers.
			• Bart highlighted the recently formed Harms Task Force at ToIP.
			• He said much of the document reads like "a technical solution to a social problem".
			• He felt the document is a call to the community for feedback.
			• Bart felt if that there is not a mature protocol available within the few months, eIDAS will use the existing ones.
			• Bart said that Fraunhofer has a nice framework for connecting to multiple frameworks. He did at SICPA https://github.com/sicpa-dlab/essif-bridge links SSI to different trust frameworks.
			• Daniel Bachenheimer said he has glanced through the doc looking for biometric authentication info. There is only one reference to it. He believed that it was going to be a requirement for the user to do biometric authentication to the wallet before release of the credentials.
			  ◦ Bart said that his understanding is that such authentication would be desireable, and it could be based on a biometric.
			  ◦ Dan said that two factors are needed including proof of knowledge, proof of presence, and proof of _____.
			  ◦ Bart said that the EU is assuming there will be a separate ID credential as part of the mix.
			  ◦ Bart said that the personal data required for provisioning must be kept separate from any other data in the wallet.
			  ◦ Dan wondered how the EU digital identity wallet was then supposed to be used for online identification if another EU identity card was required.
			  ◦ Bart explained that the document-centric thinking "has not left the building yet". There is an assumption about having a passport, for example, that is an original, where there is no such thing digitally. The fact that the EU is conceiving of "issuing wallets" is problematic. He believes the EU is trying to expand from COVID-19 credentials to a generalized solution is a challenge.
			• Tim Bouma's take was that this approach was likely to fail because the EU is focused on the wallet vs. the credential. He felt that it was prosecuting a political agenda about the current dominant vendors.
			• Isaac Henderson is from the Fraunhofer team and shared that the requirement for discovery like TRAIN is also part of the initiative. He offered to share more about TRAIN.
			• Vlad said that they are NOT defining the EU wallet as a single application, rather a set of capabilities. He believes because this is to leverage the existing COVID-19 credential infrastructure. They don't talk about "verifiable credentials", but they do talk about both QTSPs and "non-qualified" TSPs, which could open the market. But the "attestations" are essentially verifiable credentials.
			  ◦ Vlad agrees with Bart that "issuance" of digital wallets to citizens is going to be a challenge.
			  ◦ But they are saying that there must be some way for the citizen for the wallet to "load" the data from existing ID credentials such as an identity card or passport.
			• Additional comments in chat:
			  ◦ Bart Suichies: Another 'cautious' ambition: "EUDI Wallet Issuers are Member States or organisations either mandated or recognized by Member States making the EUDI Wallet available for end users. The terms and conditions of the mandate or recognition
			  would be for each Member State to determine."
			
			APAC MEETING
			
			• We continued the discuss and agreed that eIDAS 2.0 is a critical subject for ToIP.
			• ACTION: Judith Fleenor to create a Slack channel and a Google doc to start gathering suggested topics for a series of blog posts on eIDAS 2.0.

15 mins	Reference view of the ToIP stack	Wenjing Chu	From the first action item above. Notes:
			
			• Wenjing's slides are shown in screenshots #1 through #9 below.
			• The main argument is that by combining a reference view with a protocol stack view can provide much greater understanding.
			• Slide #8 in particular shows that the "true Layer 1" is not really a lower-level protocol stack, but a peer protocol stack.
			• Bart Suichies totally agreed about the need for a reference view. By decomposing them into two pictures — reference view and protocol stack view — it makes it much more tractable.
			• Judith Fleenor reflected that this could be communicated as an interactive view where you could move from the "horizontal view" to the "vertical view" and vice versa.
			• Wenjing Chu said that it should make it easier for different audiences to focus on what they need.
			• Tim Bouma used the analogy of the stack as "a front elevation view of the house" when in fact a full set of plans requires many other views.
			• Drummond Reed strongly agreed and thanked Wenjing for his advocacy of this view. He proposed and Wenjing agreed to this action item:
			• ACTION: Wenjing Chu to collaborate with Drummond Reed on deciding how incorporating the reference view of the stack should be reflected in the structure of the ToIP Technology Architecture Specification.
			
			APAC Session:
			
			• Wenjing Chu went over his presentation again, more slowly than in the NA/EU session, and thus in more detail. In particular he explained diagram #8 in the screenshots below.
			• Drummond Reed had the revelation that Wenjing's diagram shows for the first time how the ToIP stack can operate against a local secure enclave or a TPM as its Layer 1 "VDR" OR use a DID resolution or KERI tunnel protocol to access a remote VDR.
			• ACTION: Drummond Reedto send Daniel Hardman a link to Wenjing's presentation and reference diagram for his feedback.
			• We also discussed the relationship of Layer 2 as the common trust spanning layer and Layer 3 consists of. Jo Spencer suggested:
			  ◦ Protocols for higher-level protocol interactions (e.g., credential issuance, credential presentation, payments, auctions, rich messaging, etc.)
			  ◦ Data formats (such as verifiable credentials, invoices, and other payloads)
			  ◦ Signature formats
			• Jo Spencer said that we need to establish common requirements for endpoint identification and description.
			• ACTION: Drummond Reed to add to the storyline a requirement that Layer 2 must enable discovery, description, and basic negotiation of endpoints such that the endpoints can elevate to a Layer 3 protocol.
			• ACTION: Drummond Reed to add to the storyline that we want to include examples of the use of the interfaces at each layer to help them understand them.
			• Judith Fleenor I loved the analogy that was used in the morning meeting of Blue Print. And that with blue prints there are different views. Structural view, Electrical view, etc. —The nice thing about the horizontal view is that is can have a deep technical view… but also serves better for a human experience view.
			• Wenjing said that each layer must have an interface, but there was a long discussion about how much detail is needed at Layer 1 vs. the essential requirements of Layer 2. Wenjing and Jo had different views about the Layer 1 interface.
			• ACTION: Wenjing Chu to prepare for next week's call separate diagrams of the reference architecture view, where one is the stack implemented entirely on a local device such as a mobile phone (and thus the VDR is a local secure enclave or TPM

15 mins	Another view of the ToIP stack	Bart Suichies	From the second action item above. We ran out of time for this agenda item. • ACTION: Drummond Reed to move the agenda item for Bart Suichies to present his view of the stack in next week's NA/EU meeting.
5 mins	Review of proposed Layer 1 requirements	Drummond Reed	See the new slides in the **Layer 1 Requirements** section of the storyline slide deck (Google Slides). We ran out of time for this agenda item. • ACTION: ALL to continue work on the storyline slide deck (Google Slides) to see if we can complete the storyline narrative for the entire document within the next two weeks.
5 mins	• Review decisions/action items • Planning for next meeting	Chairs	

Screenshots/Diagrams (numbered for reference in notes above)

This is the complete set of slides from Wenjing Chu's presentation about a reference architecture view of the ToIP stack.

#1

Designing a complex system requires decomposition of its components and ways they interact with each other.

#2

A *Stack* view is to view the decomposition vertically in functionality, where each higher layer incrementally adds functionality above the layer(s) below it.

#3

A *reference* view is a horizontal (or landscape) view of how components (parties) interact with each other to complete the overall functionality. The interaction points are defined by protocols.

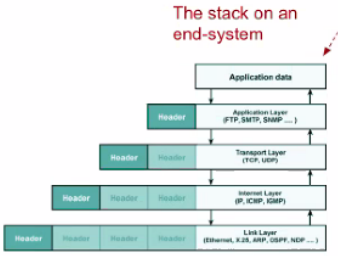
#4

Putting the 2 views together in 3D: each party in the *reference framework* has its own *stack of protocols*.

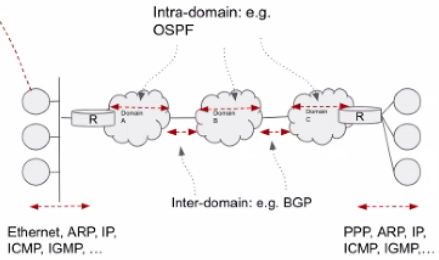
#5

For example: Internet architecture in 2 views

The familiar Internet stack view is usually focused on end systems



The Internet reference architecture



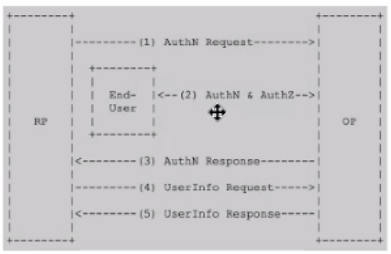
#6

Another example: OIDC in the reference view

The OpenID Connect protocol, in abstract, follows the following steps.

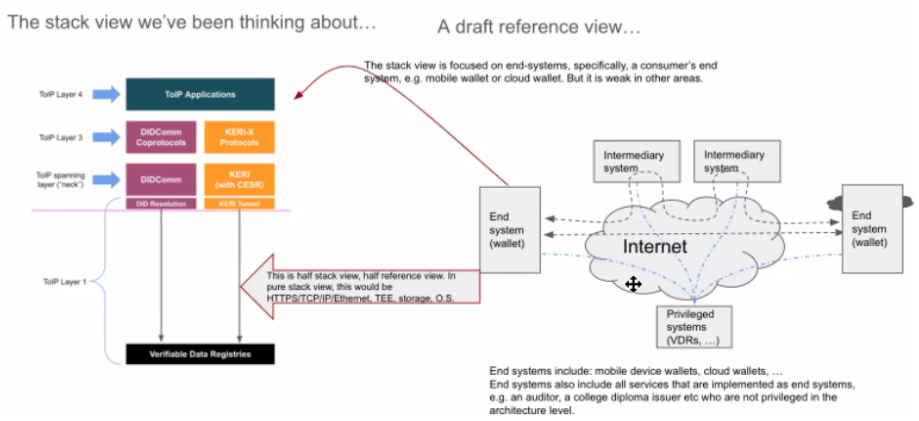
1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.

These steps are illustrated in the following diagram:



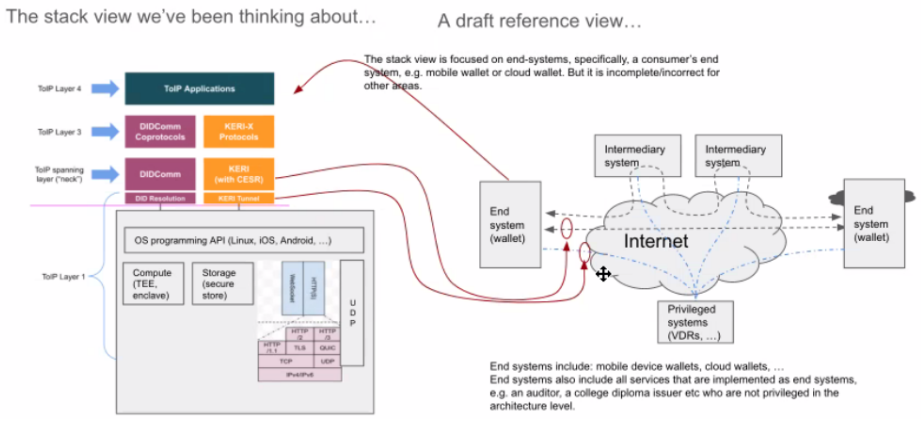
#7

Get to a ToIP Reference Framework



#8

Get to a ToIP Reference Framework



#9

To fully specify the ToIP stack, we need to (1) define the reference framework and supporting use cases (2) define each protocol stack required in the reference framework and use cases.

So the reference framework is a critical part of our overall architecture.

Decisions

- None

Action Items

- [ ] ACTION: Judith Fleenor to create a Slack channel and a Google doc to start gathering suggested topics for a series of blog posts on eIDAS 2.0.
- [ ] ACTION: Drummond Reed to move the agenda item for Bart Suichies to present his view of the stack in next week's NA/EU meeting.
- [ ] ACTION: Wenjing Chu to prepare for next week's call separate diagrams of the reference architecture view, where one is the stack implemented entirely on a local device such as a mobile phone (and thus the VDR is a local secure enclave or TPM
- [ ] ACTION: Wenjing Chu to collaborate with Drummond Reed on deciding how incorporating the reference view of the stack should be reflected in the structure of the ToIP Technology Architecture Specification.
- [ ] ACTION: Drummond Reedto send Daniel Hardman a link to Wenjing's presentation and reference diagram for his feedback.
- [ ] ACTION: Drummond Reed to add to the storyline a requirement that Layer 2 must enable discovery, description, and basic negotiation of endpoints such that the endpoints can elevate to a Layer 3 protocol.
- [ ] ACTION: Drummond Reed to add to the storyline that we want to include examples of the use of the interfaces at each layer to help them understand them.
- [ ] ACTION: ALL to continue work on the storyline slide deck (Google Slides) to see if we can complete the storyline narrative for the entire document within the next two weeks.