2023-02-15 TSPTF Meeting Notes

Meeting Date & Time

15 Feb 2023 This Task Force meets **three out of every four Wednesdays** (the fourth Wednesday is the Technology Stack WG plenary meeting). There are two meetings each Wednesday to serve different time zones:

- **NA/EU meeting: 08:00-09:00 PT / 16:00-17:00 UTC**
- **APAC meeting: 18:00-19:00 PT / 02:00-03:00 UTC**

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

Zoom Meeting Recordings

- NA/EU Meeting: https://zoom.us/rec/share/KAMhJvjZmEiCGTSFQ9060uCzgEWuI_3oKPFMIstl8un4JkjUUDE_iO9MNtCWeajI.wqxZH3QOw1Yw4eYf
- APAC Meeting: https://zoom.us/rec/share/_HyuvlplN9YsA47x7BlpNPR0-2Wwog8ED5sOzkEWs8HWbIcC9J11IdLZUzFtt1Ma.tIQ_22oKQNtJFEOK

NOTE: These Zoom meeting links will be replaced by links to recordings of the meetings once they are available.

Attendees

NA/EU:

- Drummond Reed
- Daniel Hardman
- Wenjing Chu
- Samuel Smith
- Oskar van Deventer
- Scott Whitmire
- Steve McCown
- Matteo Midena
- Partha Pal
- Alex Andrei
- Antti Kettunen
- Andor Kesselman
- Daniel Bachenheimer
- Jorge Flores
- Keerthi Thomas
- Lance Byrd
- Mathieu Glaude
- Michal Pietrus
- Raul Quino
- Sam Curren
- sankarshan
- Scott Perry
- Steve McCown
- Subhasis Ojha
- Viky Manaila
- Willem de Kok
- Rodolfo Miranda
- Michael Palage
- Abbie Barbir
- Sumabala Nair

APAC:

- Drummond Reed
- Andor Kesselman
- Daniel Bachenheimer
- Eric Drury
- Michael Herman
- Jo Spencer
- Dima Postnikov

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes

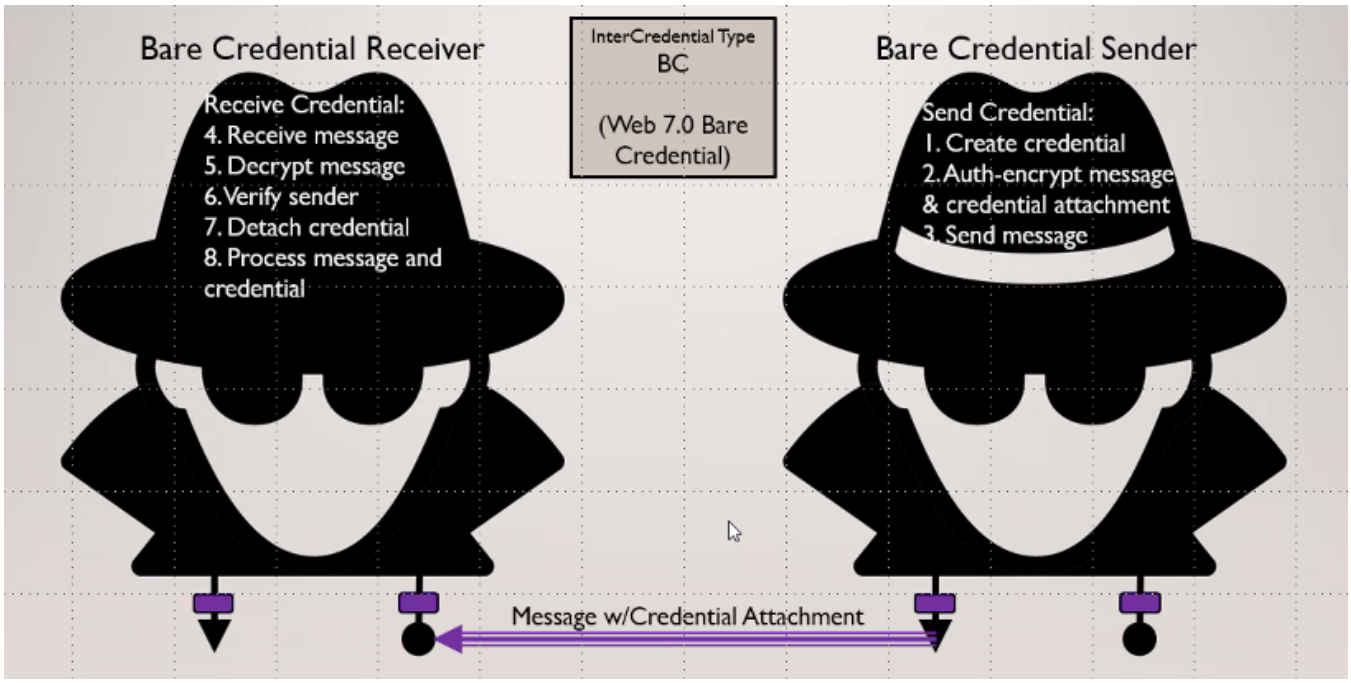
3 min	• Start recording • Welcome & antitrust notice • New member introductions • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • New Members:
2 min	Review of previous action items	Chairs	☑ ACTION: All TSPTF members who missed the meeting: review Sam's slides, watch at least the NA/EU recording (and ideally the APAC recording as well), and if possible, read and contributed to the Github Discussion threads.
40 mins	TSP Proposal #2: Daniel Hardman	Daniel Hardman	Daniel will present his proposal for design of the TSP based largely (but not completely) on his experience as an architect of DIDComm. • Here is the recording of Daniel's presentation in the NA/EU meeting. • Here are the slides Daniel used. • Here is the Github Discussion thread that Daniel has started for his proposal. Please use it this week for asynchronous discussion of his proposal.

15 mins	Chat & Q&A on Proposal #2		NA/EU:
			
			• Samuel Smith: " like the term protocol suite it better captures a set of thin layers." Drummond Reed, Antti Kettunen, and Oskar van Deventer all agreed.
			• Partha Pal: "Does 'contextual trust' include time bound?"
			  ◦ Drummond Reed: "Yes, time can be one factor in context."
			  ◦ Daniel Bachenheimer: "right - temporal certs are the medium of exchange in the FIDO protocol."
			• Scott Perry: "Trust in this context will always be broken into two separate components: 1) Do I trust whether the originator of the message actually sent the message and 2) Do I trust the message. My contention is that only "1" can be solved in this task force. "2" can only be assured through governance."
			  ◦ Scott Whitmire: "How can “2” be solved through governance? Trusting the message has a meaning, what meaning are you using?"
			• Samuel Smith: "There are several defintions of "authenticity" in the dictionary. One is expressed by what is called "authentication" as a process. Daniel is using other definitions of authenticity besides the narrow definition of authentication implied by authenticatable. So to the extent we desire to support other types of authenticity, then we need additional information."
			• Partha Pal: "Human <> Human trust , Human <> System trust , System <> System trust , need to be addressed separately ? Curious to know..."
			• Scott Perry: "In this delivery message, the payload is a blob. Anyone can say anything. How someone trusts the blob is based on the ToIP trust principles. Many factors go into that such as reputation of sender, a trust registry process, a trust assurance scheme, etc."
			  ◦ Drummond Reed: "Scott, that’s true, but there are many “trust task-specific” elements of making trust decisions. What I think Daniel is getting at is the “universal” elements of trust decisions that belong at the TSP layer, i.e., they are shared by many if not all trust tasks."
			  ◦ Scott Whitmire: "Anything related to the payload blob, as Scott put it, is the responsibility of higher layers. Thus, trusting the actual message, including context and purpose, are not the responsibility of the spanning layer."
			  ◦ Keerthi Thomas: "How the payload will be interpreted will depend on the application context."
			  ◦ Drummond Reed: "That’s the debate we’ll have: which elements are universal enough to be at the spanning layer."
			  ◦ Scott Perry: "Given Sam's minimization tenet, we cannot expect the trust spanning layer to do anything about the payload. Consistent with IP, the neck of the hourglass does nothing about the payload."
			• Samuel Smith: "Other elements in a protocol header like message type can make it unambigous what the intent of the speaker was without providing a destination identifier. I think it is misstating that my minimization is only the weakest bottom layer I have stated several times that we need to build a protocol stack of thin additive layers so we should consider whats in the payload at upper layers in a suite of layers."
			  ◦ Scott Whitmire: "I think we’re on the same page. In IP, the payload is just a package that needs to be delivered. The header contains only what is necessary to carry that out. If we follow that idea, any decision that depends on the content of a specific payload belongs in a higher layer."
			  ◦ Scott Perry: "@Sam, then the focus is on the attributes of the payload not the content of the payload."
			• Oskar van Deventer: "More weakness" == "Fewer features"?"
			  ◦ Drummond Reed: "Yes, but with the subtleties that Daniel is explaining."
			• Scott Whitmire: "So, what should go into the spanning layer? Basically, what is required to authenticate the source and provenance of the payload. Anything related to a specific payload goes elsewhere."
			• Andor Kesselman: "Great stuff. Has some big implications for the TRTF, so looking forward to learn more." Antti Kettunen agreed.
			• Andor Kesselman: "Thanks @Daniel. Great presentation. Loving these proposals." Multiple thumbs up.
			
			Samuel Smith also started this new Github Discussions thread.
			
			APAC (note that Daniel Hardman was not able to attend due to his time zone in Switzerland):
			
			• Michael Herman shared screenshot #1 below as a way of illustrating the credential sender-receiver model. A video of this Internet Credential (InterCredential) Architecture Reference Model 0.70 ft. 4-Corner Interop Model is available here.
			• Michael also shared screenshot #2 to discuss interfaces between senders and receivers in a series of protocol usages.
			• We had a good discussion about Daniel Hardman's proposed "destination" element and the challenge of multiple recipients and group messaging.
			  ◦ Drummond pointed out this was intentionally put out of scope for the DIDComm V2 Working Group, but that they are keen on tackling it in a subsequent version.
			  ◦ Andor Kesselman said he plans to raise this question in the Proposal #2 discussion thread.
			• At the end of the all, Drummond Reed pointed out one of the final slides in Daniel Hardman's deck (screenshot #3) that maps many of the features of the DIDComm V2 basic protocol (and other "DIDComm protocols" built on top of the basic protocol) to the ToIP stack, both at the TSP layer (Layer 2) and at the trust task layer (Layer 3). In his view, that slide could be worthy of an entire dedicated TSPTF meeting to discuss in depth — and certainly should be discussed in depth in Github Discussions.
			  ◦ Drummond noted that 6 attendees on the NA/EU call agreed it was a seminal slide.

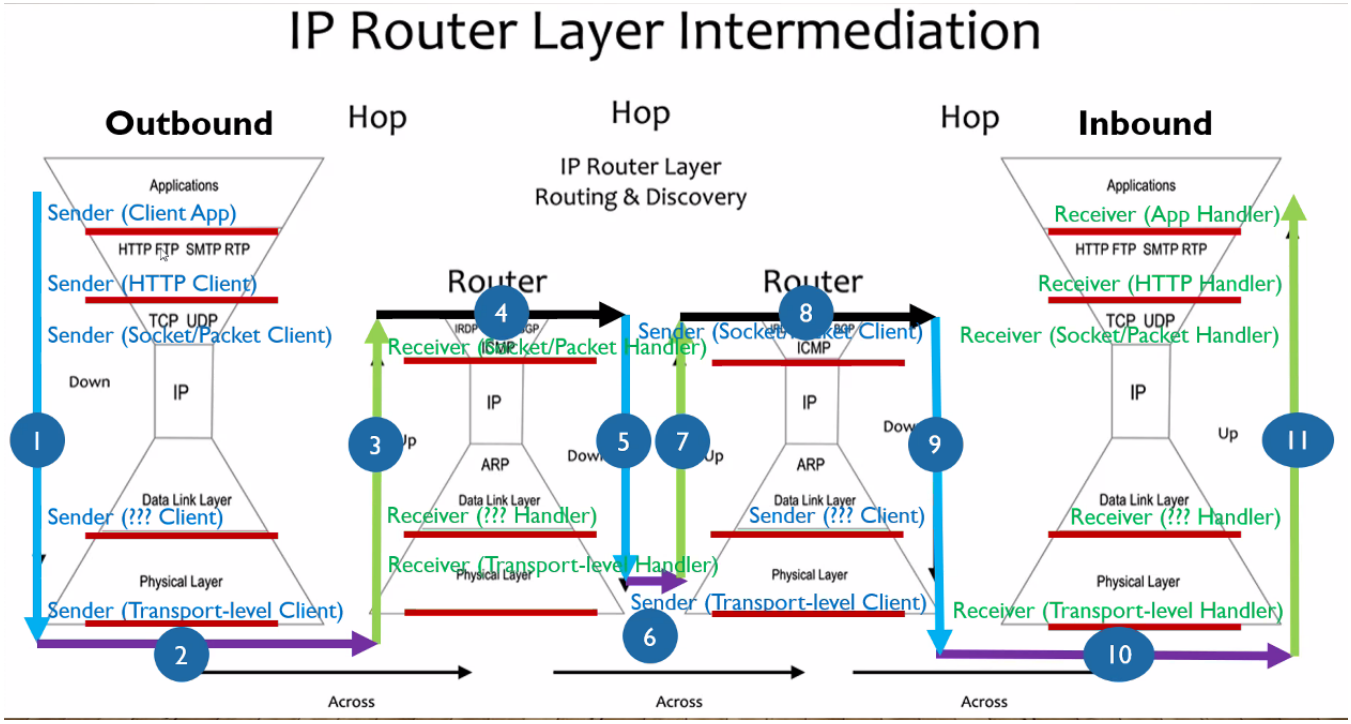
0 mins	• Review decisions/action items • Planning for next meeting	Chairs	Next week's meeting will be Proposal #3 from Wenjing Chu.

Screenshots/Diagrams (numbered for reference in notes above)

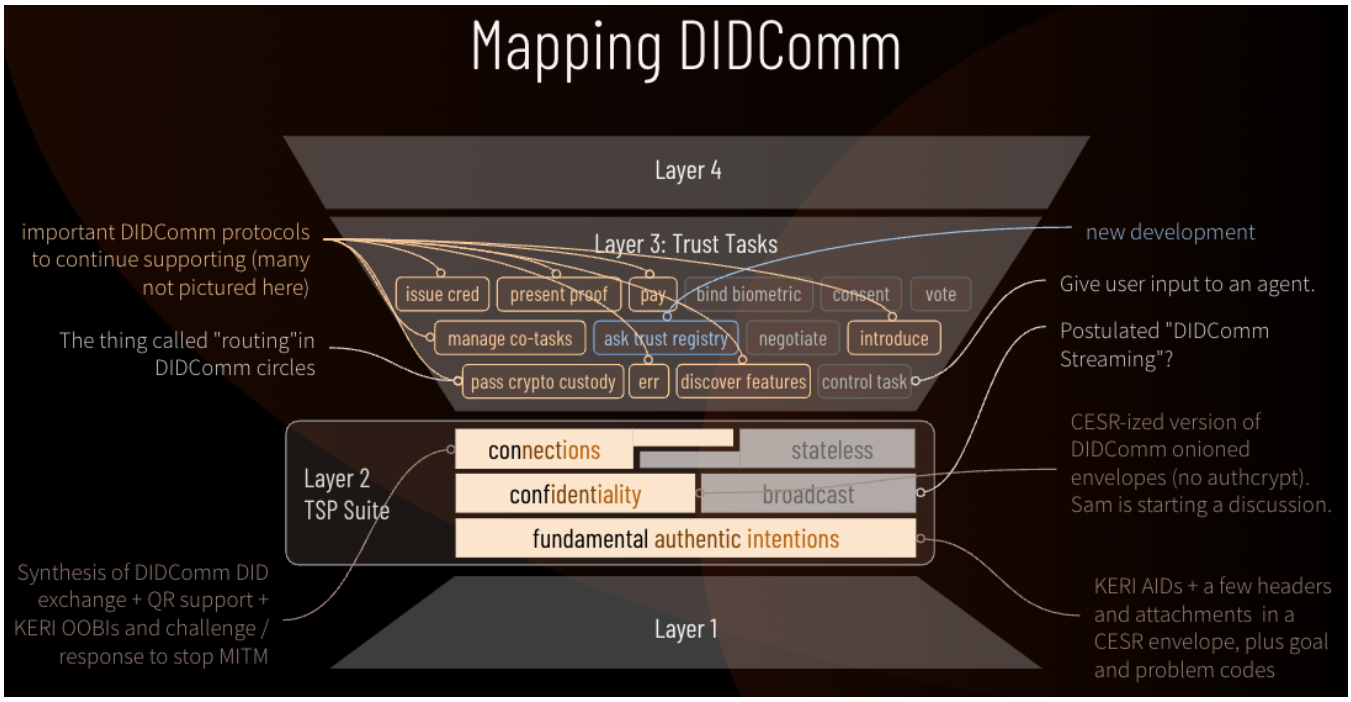
#1


Bare Credential Receiver
Receive Credential:
4. Receive message
5. Decrypt message
6. Verify sender
7. Detach credential
8. Process message and credential
InterCredential Type
BC
(Web 7.0 Bare Credential)
Bare Credential Sender
Send Credential:
1. Create credential
2. Auth-encrypt message & credential attachment
3. Send message
Message w/Credential Attachment

#2


IP Router Layer Intermediation
Outbound
Hop
Hop
Hop
Inbound
IP Router Layer
Routing & Discovery
Applications
Sender (Client App)
HTTP FTP SMTP RTP
Sender (HTTP Client)
TCP UDP
Sender (Socket/Packet Client)
Down
IP
Data Link Layer
Sender (??? Client)
Physical Layer
Sender (Transport-level Client)
Router
Receiver (Socket/Packet Handler)
ICMP
IP
ARP
Up
Down
Data Link Layer
Receiver (??? Handler)
Physical Layer
Receiver (Transport-level Handler)
Router
Sender (Socket/Packet Client)
ICMP
IP
ARP
Down
Up
Data Link Layer
Sender (??? Client)
Physical Layer
Sender (Transport-level Client)
Applications
Receiver (App Handler)
HTTP FTP SMTP RTP
Receiver (HTTP Handler)
TCP UDP
Receiver (Socket/Packet Handler)
IP
Up
Data Link Layer
Receiver (??? Handler)
Physical Layer
Receiver (Transport-level Handler)
1
2
3
4
5
6
7
8
9
10
11
Across
Across
Across

#3



Decisions

- None.

Action Items

- [ ] ACTION: All TSPTF members who missed the meeting: review Daniel Hardman's slides, watch his presentation in the NA/EU recording, and if possible, read and contributed to the Github Discussion thread on his presentation along with the other related discussions.