2023-12-06 TSPTF Meeting Notes

Meeting Date & Time

06 Dec 2023 This Task Force meets **every Wednesday.** There are two meetings 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 Links / Recordings

- NA/EU Meeting: https://zoom.us/rec/share/FgL9IIiH2TwFEu6JhOadvzmo9ULwvyPiXyOJSmA_n-LyiTe7AjQSo-p_EHNPudOL.XVtkdnswmnRV7yhN
- APAC Meeting: https://zoom.us/j/96772881287?pwd=bzZUNXRhVUNzVjR2Z3B2cVVxc2ZUZz09

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

Attendees

NA/EU:

- Drummond Reed <== 30 minutes late due to OpenWallet Foundation board meeting
- Wenjing Chu <== 30 minutes late due to OpenWallet Foundation board meeting
- Samuel Smith
- Darrell O'Donnell
- Ed Eykholt
- Ajay Jadhav
- Bo Harald
- Charles Lanahan
- Daniel Bachenheimer
- Eric Scouten
- Jesse Carter
- Jonathan Rayback
- Judith Fleenor
- Tim Bouma
- Christine Martin
- Phil Feairheller
- Mark Scott
- Neil Thomson
- Steven Milstein
- Wendy Seltzer

APAC:

- Drummond Reed
- Darrell O'Donnell
- Jo Spencer
- sankarshan
- Daniel Bachenheimer

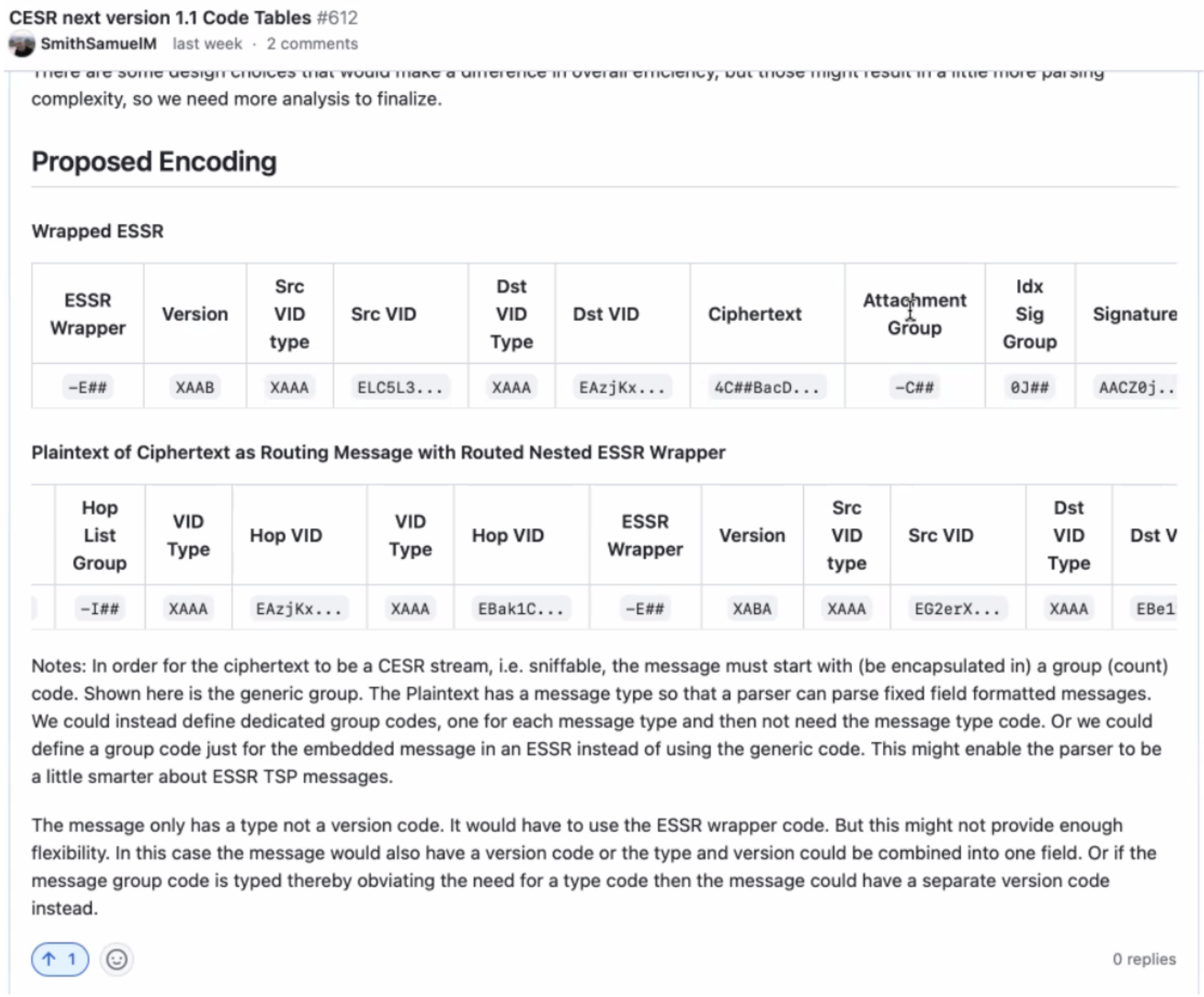
Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 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:
0 min	Review of previous action items	Leads	None

25 mins	CESR and CBOR Deterministic Encoding	Samuel Smith	Sam will give an update on the CESR (Composable Event Streaming Representation) specifications. Ideally he will also be able to contrast CESR with a new IETF specification called CBOR Common Deterministic Encoding (CDE) aka draft-ietf-cbor-cde-00. On the W3C Credentials Community Group mailing list, Anders Rundgren said CDE may be significant because: - JSON and XML require 33% more space than CBOR for dealing with binary data. - The availability of a textual counterpart (Diagnostic Notation) makes CBOR suited for configuration files. - Last but not least, deterministic encoding eliminates stuffing data-to-be signed in B64 or relying on complex canonicalization schemes. Although the standard is not yet finalized, outstanding issues only relate to edge-cases like NaN payloads. Anders also pointed to this testbed where you can try CDE. Sam explained that TSP routing is a unique combination of vector and table routing. He shared this discussion thread from the KERI work: https://github.com/WebOfTrust/keripy/discussions/612 See screenshot #1 below. Ed Eykholt asked if it is proposed that CESR is the only serialization format for the TSP. Sam explained that yes, because CESR can carry JSON, CBOR, and MsgPack.
25 mins	Working Draft Review	Wenjing Chu	Wenjing went over the latest additions to the spec as it nears content completion. See screenshots #2-#6 below that cover control messages and relationship formation. ACTION: Wenjing Chu and Samuel Smith to prepare a "spec reviewer's tour guide" to highlight particular sections and issues on which they as editors would like feedback as TSPTF members do a full-spec read-through over our 3 week holiday break.
NA	Cross-Group Collaboration	All	On the APAC call, sankarshan brought up the more general question of how different ToIP WGs are or are not coordinating their work. He noted that some groups are widely separated in terms of how closely they are aligning with others—in particular with the TSWG specs coming out in the first half of 2024.
5 mins	• Review decisions/action items • Planning for next meeting	Leads	We plan to have one more regular meeting this month (Wednesday 13 December) and then take off 3 weeks for the holidays, i.e., skip the Dec 20, 27, and Jan 3 meetings. So our first meeting in 2024 will be Wednesday Jan 10.

Screenshots/Diagrams (numbered for reference in notes above)

#1



CESR next version 1.1 Code Tables #612

SmithSamuelM last week · 2 comments

There are some design choices that would make a difference in overall efficiency, but those might result in a little more parsing complexity, so we need more analysis to finalize.

Proposed Encoding

Wrapped ESSR

ESSR Wrapper	Version	Src VID type	Src VID	Dst VID Type	Dst VID	Ciphertext	Attachment Group	Idx Sig Group	Signature
`-E##`	`XAAB`	`XAAA`	`ELC5L3...`	`XAAA`	`EAzjKx...`	`4C##BacD...`	`-C##`	`0J##`	`AACZ0j..`

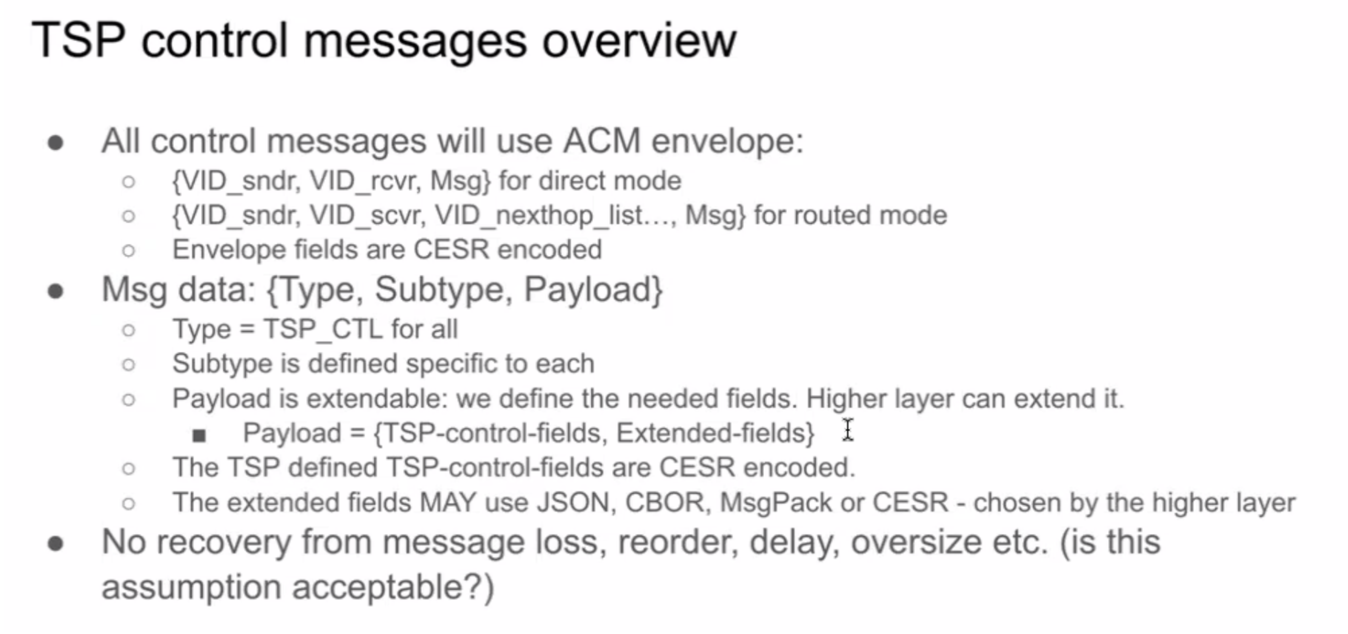
Plaintext of Ciphertext as Routing Message with Routed Nested ESSR Wrapper

Hop List Group	VID Type	Hop VID	VID Type	Hop VID	ESSR Wrapper	Version	Src VID type	Src VID	Dst VID Type	Dst V
`-I##`	`XAAA`	`EAzjKx...`	`XAAA`	`EBak1C...`	`-E##`	`XABA`	`XAAA`	`EG2erX...`	`XAAA`	`EBe1`

Notes: In order for the ciphertext to be a CESR stream, i.e. sniffable, the message must start with (be encapsulated in) a group (count) code. Shown here is the generic group. The Plaintext has a message type so that a parser can parse fixed field formatted messages. We could instead define dedicated group codes, one for each message type and then not need the message type code. Or we could define a group code just for the embedded message in an ESSR instead of using the generic code. This might enable the parser to be a little smarter about ESSR TSP messages.

The message only has a type not a version code. It would have to use the ESSR wrapper code. But this might not provide enough flexibility. In this case the message would also have a version code or the type and version could be combined into one field. Or if the message group code is typed thereby obviating the need for a type code then the message could have a separate version code instead.

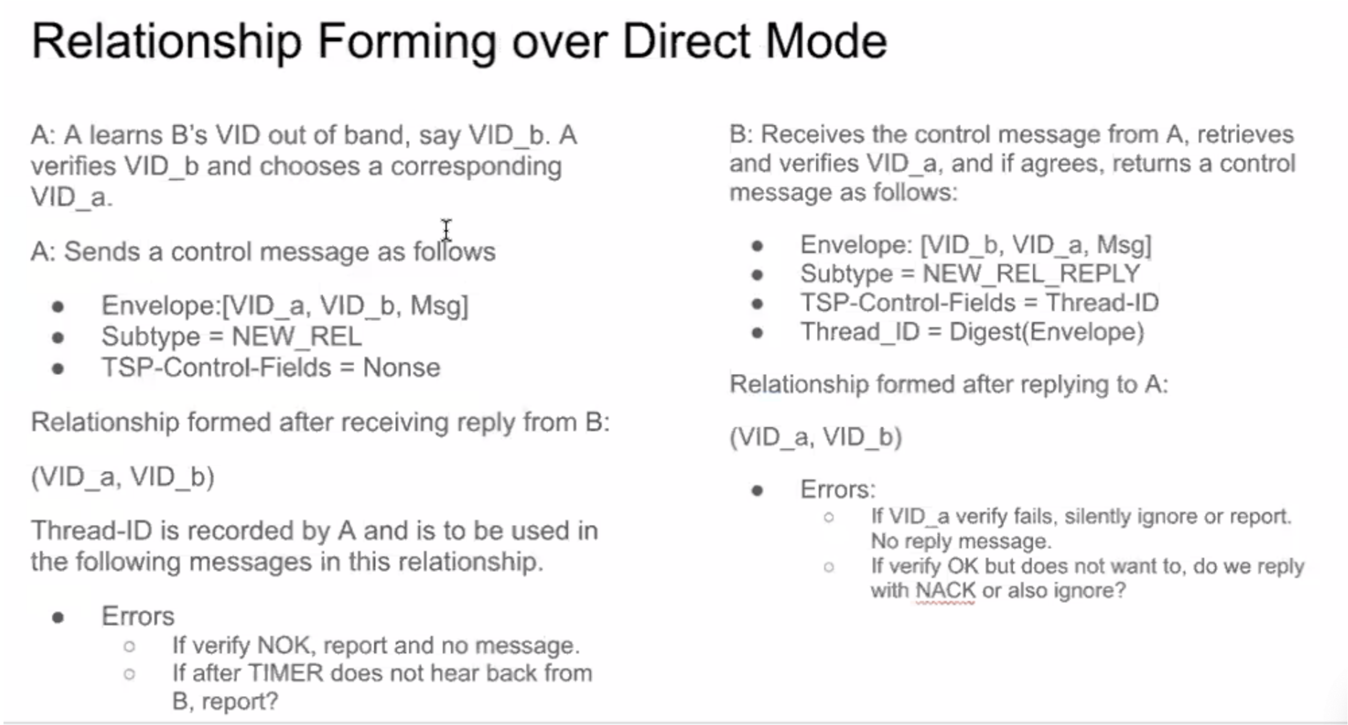
#2



TSP control messages overview

- All control messages will use ACM envelope:
  - {VID_sndr, VID_rcvr, Msg} for direct mode
  - {VID_sndr, VID_scvr, VID_nexthop_list…, Msg} for routed mode
  - Envelope fields are CESR encoded
- Msg data: {Type, Subtype, Payload}
  - Type = TSP_CTL for all
  - Subtype is defined specific to each
  - Payload is extendable: we define the needed fields. Higher layer can extend it.
    - Payload = {TSP-control-fields, Extended-fields}
  - The TSP defined TSP-control-fields are CESR encoded.
  - The extended fields MAY use JSON, CBOR, MsgPack or CESR - chosen by the higher layer
- No recovery from message loss, reorder, delay, oversize etc. (is this assumption acceptable?)

#3



Relationship Forming over Direct Mode

A: A learns B's VID out of band, say VID_b. A verifies VID_b and chooses a corresponding VID_a.

A: Sends a control message as follows

- Envelope:[VID_a, VID_b, Msg]
- Subtype = NEW_REL
- TSP-Control-Fields = Nonse

Relationship formed after receiving reply from B:

(VID_a, VID_b)

Thread-ID is recorded by A and is to be used in the following messages in this relationship.

- Errors
  - If verify NOK, report and no message.
  - If after TIMER does not hear back from B, report?

B: Receives the control message from A, retrieves and verifies VID_a, and if agrees, returns a control message as follows:

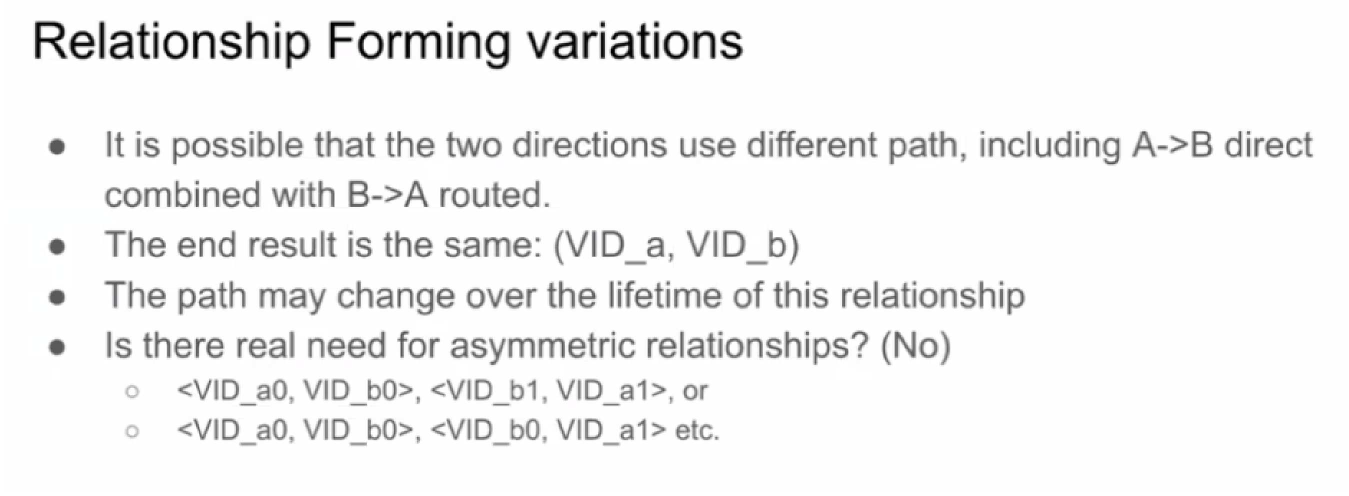
- Envelope: [VID_b, VID_a, Msg]
- Subtype = NEW_REL_REPLY
- TSP-Control-Fields = Thread-ID
- Thread_ID = Digest(Envelope)

Relationship formed after replying to A:

(VID_a, VID_b)

- Errors:
  - If VID_a verify fails, silently ignore or report. No reply message.
  - If verify OK but does not want to, do we reply with NACK or also ignore?

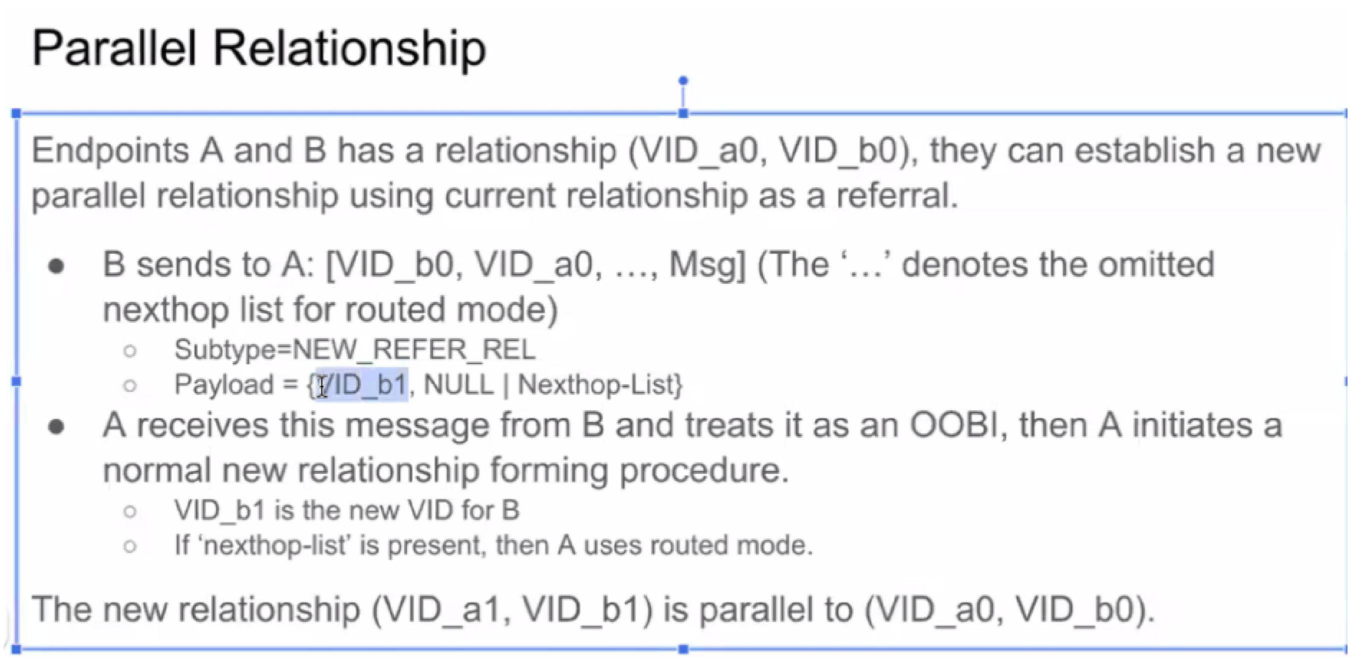
#4



Relationship Forming variations

- It is possible that the two directions use different path, including A->B direct combined with B->A routed.
- The end result is the same: (VID_a, VID_b)
- The path may change over the lifetime of this relationship
- Is there real need for asymmetric relationships? (No)
  - <VID_a0, VID_b0>, <VID_b1, VID_a1>, or
  - <VID_a0, VID_b0>, <VID_b0, VID_a1> etc.

#5



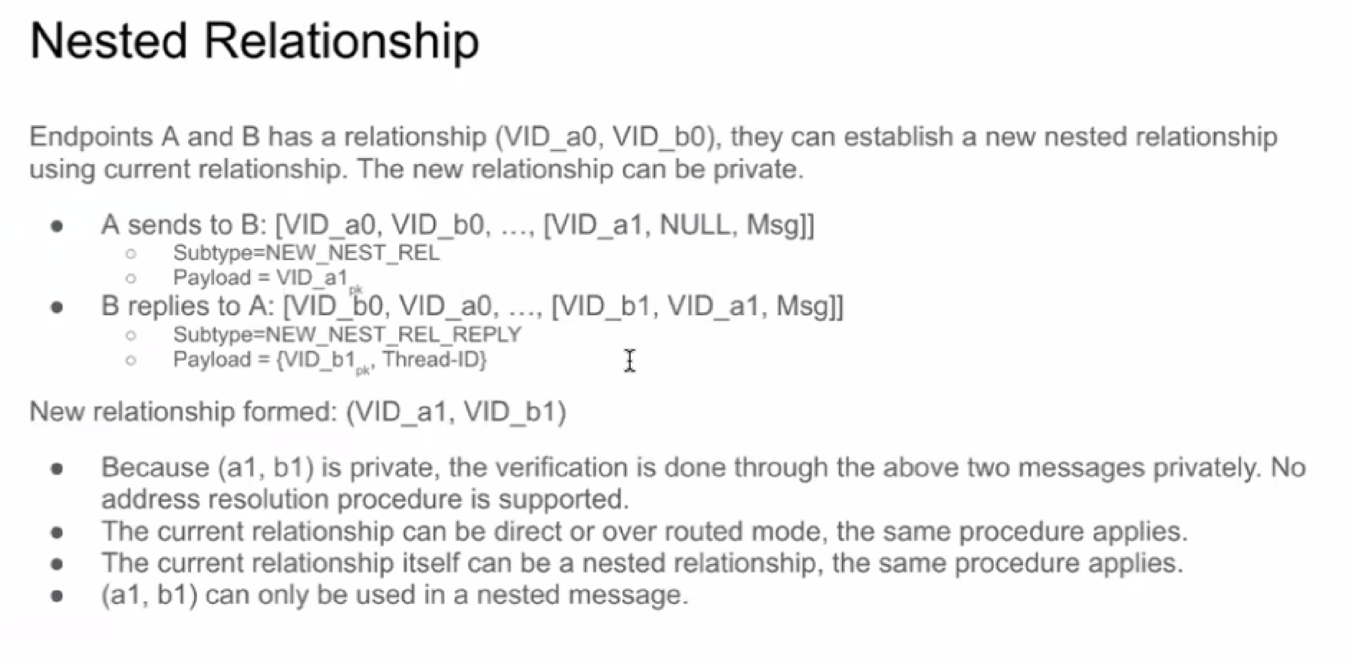
Parallel Relationship

Endpoints A and B has a relationship (VID_a0, VID_b0), they can establish a new parallel relationship using current relationship as a referral.

- B sends to A: [VID_b0, VID_a0, …, Msg] (The '…' denotes the omitted nexthop list for routed mode)
  - Subtype=NEW_REFER_REL
  - Payload = {VID_b1, NULL | Nexthop-List}
- A receives this message from B and treats it as an OOBI, then A initiates a normal new relationship forming procedure.
  - VID_b1 is the new VID for B
  - If 'nexthop-list' is present, then A uses routed mode.

The new relationship (VID_a1, VID_b1) is parallel to (VID_a0, VID_b0).

#6



Nested Relationship

Endpoints A and B has a relationship (VID_a0, VID_b0), they can establish a new nested relationship using current relationship. The new relationship can be private.

- A sends to B: [VID_a0, VID_b0, …, [VID_a1, NULL, Msg]]
  - Subtype=NEW_NEST_REL
  - Payload = VID_a1$_{pk}$
- B replies to A: [VID_b0, VID_a0, …, [VID_b1, VID_a1, Msg]]
  - Subtype=NEW_NEST_REL_REPLY
  - Payload = {VID_b1$_{pk}$, Thread-ID}

New relationship formed: (VID_a1, VID_b1)

- Because (a1, b1) is private, the verification is done through the above two messages privately. No address resolution procedure is supported.
- The current relationship can be direct or over routed mode, the same procedure applies.
- The current relationship itself can be a nested relationship, the same procedure applies.
- (a1, b1) can only be used in a nested message.

Decisions

- None

Action Items

□ ACTION: Wenjing Chu and Samuel Smith to prepare a "spec reviewer's tour guide" for next week's meetings to highlight particular sections and issues on which they as editors would like feedback as TSPTF members do a full-spec read-through over our 3 week holiday break.