2022-01-27 TATF Meeting Notes

Meeting Date & Time

- 27 Jan 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/Io2Jg6mNPz_5Q8QsSaZ0TZRiMDd6RkFiHIGxZkLbwmqrn-YTKCM9tOZ_BzxP_cU8.dGggV8Ok9vePyiPb?startTime=1643295764000
- APAC Meeting: https://zoom.us/rec/share/hpxkqP034wr9mznYgHuRgUBIzKjmxj3_aF_Wfyq6R0VtDUXD9YxTLK_tXCekx-ss.0m70FIMZbtF7JU8G?startTime=1643317093000

Attendees

NA/EU

- Drummond Reed
- Darrell O'Donnell
- Neil Thomson
- Wenjing Chu
- Daniel Bachenheimer
- Michael Nettles
- Vikas Malhotra
- Antti Kettunen
- Bart Suichies
- Burak Serdar
- Isaac Henderson
- Jan Lindquist
- Neil Thomson
- Phil Feairheller
- sankarshan
- Tim Bouma
- Wenjing Chu

APAC

- Darrell O'Donnell
- Drummond Reed
- Judith Fleenor
- Andre Kudra
- Judith Fleenor
- Neil Thomson
- Wenjing Chu
- Daniel Bachenheimer
- Michael Nettles
- Vikas Malhotra
- Darrell O'Donnell

Main Goal of this Meeting

Jan Lindquist and Paul Knowles will discuss the role of intermediaries in the ToIP stack; discuss a "plan of attack" for developing a consensus picture of ToIP protocol stack layering.

Agenda Items and Notes (including all relevant links)

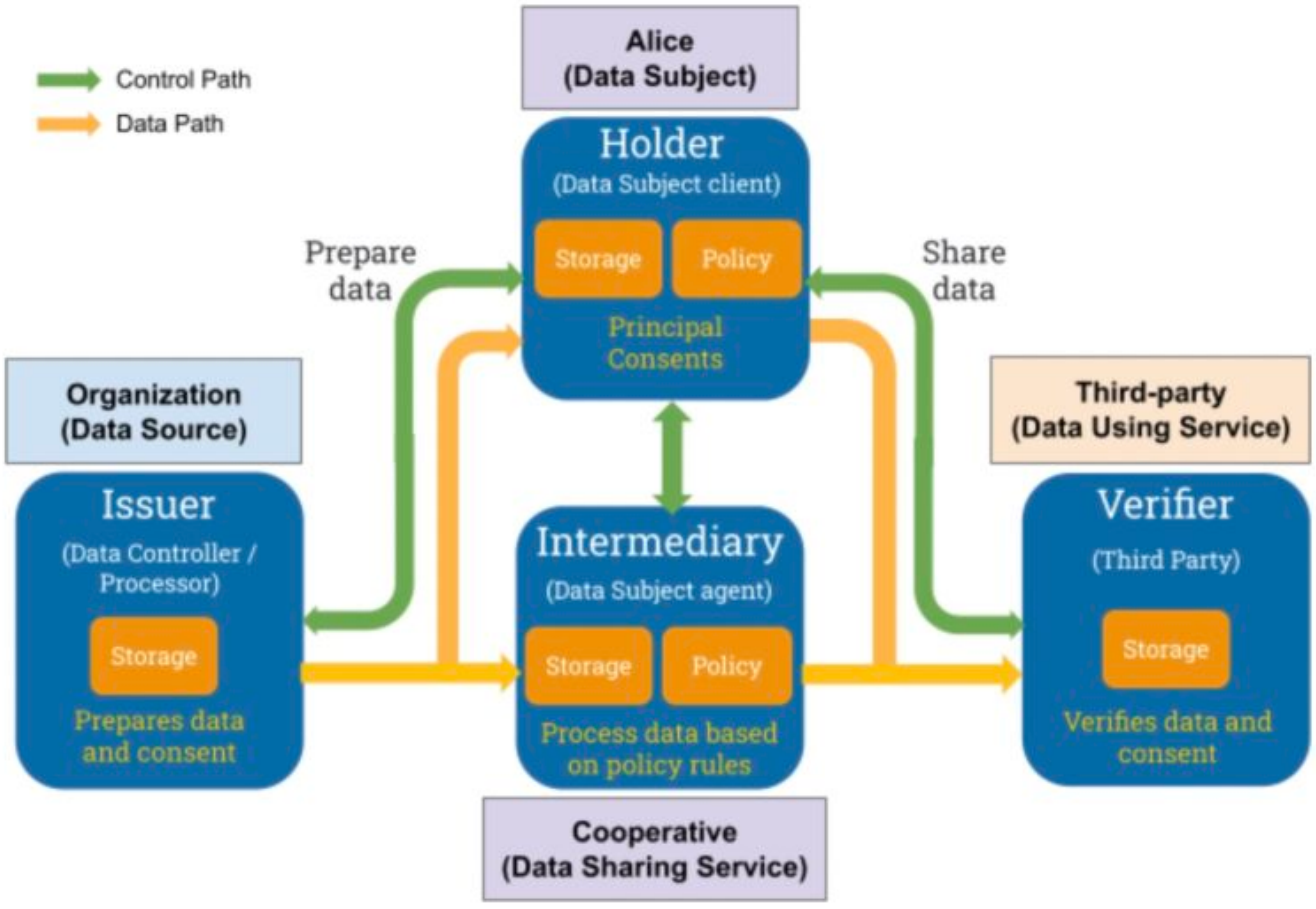
Time	Agenda Item	Lead	Notes
5 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • New Members:

5 min	Review of previous action items	Chairs	☑ ACTION: Chairs to develop a "plan of attack" for starting to refine the protocol stack diagram suggestions and begin drafting the ToIP Technology Architecture Specification. ◦ This PoA was agreed to in this meeting.
30 mins	The potential role of intermediaries in the ToIP stack	Jan Lindquist Paul Knowles	Jan and Paul will take us deep into the question of the role of intermediaries in the ToIP stack. See this January 13th ToIP blog post — and especially diagram #1 below (taken from that post). • The blog post was inspired by the adoption of the **Data Governance Act** (DGA) in the EU. ◦ It was written by members of the Inputs and Semantics WG. • The Data Governance Act builds on EU GDPR (General Data Protection Regulation). ◦ See diagram #2 below for an overview of how the GDPR roles (data subject, data controller, data processor) map into the DGA architecture. ◦ A very important aspect of the DGA is that all the intermediaries must be registered with the government. • To map the DGA architecture into the ToIP model, Jan and his co-authors created diagram #1 below. ◦ The key new role in that diagram is the **Intermediary**. This is essentially a specialized form of **agent**. ◦ The intermediary serves a number of key functions in this enhanced model. ◦ One of the them is adding/enhancing the data semantics per the ISWG model. • Daniel Bachenheimer pointed out that one of the main points of the ToIP model is to "disintermediate" current intermediaries. ◦ An example he used is the IATA Travel Pass architecture (and the Good Health Pass architecture) where the intermediary became another **secondary issuer**. ◦ Jan was interested in how the intermediary could share the data in other forms besides verifiable credentials. ◦ This role can take advantage of a semantic container as defined by the ISWG. • Darrell O'Donnell did not feel that this model needs to break anything in the ToIP model. ◦ The intermediary model can fit within the ToIP model by becoming a credential. ◦ He shared diagram #3 below. ◦ His point was the key privacy issues are: ▪ Awareness of connections. ▪ Content of data communicated within for connections. ▪ If both of these can be controlled by the subject/holder, then it can all fit the ToIP model. • Antti Kettunen explained that there are a whole bunch of ToIP Layer 4 uses cases that can take great advantage of intermediaries. ◦ This is the key role highlighted in the MyData operator role. • Daniel Bachenheimer asked the question about how one cryptographically verifies the provenance of the data passing through the intermediary. • Tim Bouma compared this to the Canadian concept of "civic data trusts", which are very useful. ◦ But Canadian privacy legislation does need to catch up. • Bart Suichies asked the question about the "semantic data container" part. ◦ He pointed out the Web3 meme that "no one wants to run their own server". ◦ But this raises the question of where the data is hosted/processed. ◦ Jan suggested that this is a core focus of the Data Storage and Portability Task Force meetings hosted by the Inputs and Semantics WG. ◦ Bart suggested that it's basically a service using protocols, rather than a protocol itself (it might require some additional protocols, to sort out the secure storage for instance) • Daniel Bachenheimer brought up the challenges of ICAO and their ePassport standards. ◦ They currently don't allow any form of selective disclosure. ◦ ICAO also does not allow any form of intermediation of the passport object. The big question will be whether the government will allow the ICAO data to be intermediated. ◦ Darrell O'Donnell suggested that will eventually change, but it's not a battle to fight now. • Antti Kettunen said that an intermediary as a role in ToIP scenarios and potentially directly in the stack architecture. ◦ Darrell O'Donnell said that role can fit into many co-protocol patterns. ◦ Wenjing Chu said that this pattern can be generalized at Layer 3, but it may also be carried out at other layers. ◦ Jan said that we should look at the functions necessary to support an intermediary. ◦ Wenjing pointed out that is can be a question of the legal parties in a flow. ◦ Drummond pointed out that intermediaries play a very critical role in the payment protocol proposed by TBDex: https://tbdex.io/whitepaper.pdf • Neil Thomson suggested that the role of an intermediary may be part of a complete separate stack. ◦ It does not always have to be credential exchange. • The two ISWG task forces that alternate weekly are Mondays at 6PM CET: ◦ Storage and Portability ◦ Privacy and Risk APAC Discussion: • Neil said that the topic of intermediaries also intersects with the work of the ACDC Task Force on chained credentials. • Darrell spoke to diagram #3 below about what privacy/confidentiality needs to apply to the ToIP stack. The different types of confidentiality are what we need to support in the design of the stack. As a result, Darrell believes that our design is capable of supporting all those requirements. • DanB and Drummond both agreed that it is a very important to separate confidentially of the **existence** of a connection vs. the **contents** of a communication within the connection. • Judith asked about legal regulation. Wenjing pointed out that the distinction about awareness by a third party does not apply in the U.S. to telecos because under law they are not considered a third-party. This is also true for ISPs and HTTP. • Drummond pointed out that this may vary with legal jurisdictions. Wenjing pointed out that the actual physics of what information is available where is the same for all TCP/IP and HTTP. • We agreed that when we are defining the ToIP stack, this consideration of what metadata is "out of the party's control" is a critical design consideration.

15 mins	Plan-of-attack on preparing a more detailed ToIP protocol stack diagram i.e. is it time for a Drummond-style story deck?	Drummond Reed	Update on a conversation Drummond had with Samuel Smith about how we could start to "decompose" the components of KERI and DIDComm to assemble a unified stack. • Darrell O'Donnell suggested that we need to move into "writing mode" and follow the "storyline" format that Drummond has used. • Tim Bouma said he is a big fan of Dan Roam's approach https://www.amazon.com/Pop-up-Pitch-Two-Hour-Persuasive-Presentation/dp/1541774515 • Samuel Smith talked about the overall approach to "decomposing" the layers involved with KERI and DIDComm. ◦ This involves covering how connections are formed securely - using out-of-band interactions (OOBI) and and out-of-band authentication (OOBA) APAC • We agreed to start a "storyline" format deck to tackle the written description and diagramming of the stack. • ACTION: Drummond Reed to prepare a starting storyline deck and share via Slack before next week's meeting. • Drummond also explained that Samuel Smith is working out the layering approach he recommends "from the bottom up" (i.e., starting with KERI AIDs and how connections are formed and authenticated). • ACTION: Drummond Reed to interview Sam to start to document Sam's approach to "filling in the details" of the four layers.
5 mins	• Review decisions /action items • Planning for next meeting	Chairs	• Next meeting will focus on development of the storyline deck.

Screenshots/Diagrams (numbered for reference in notes above)

#1



#2

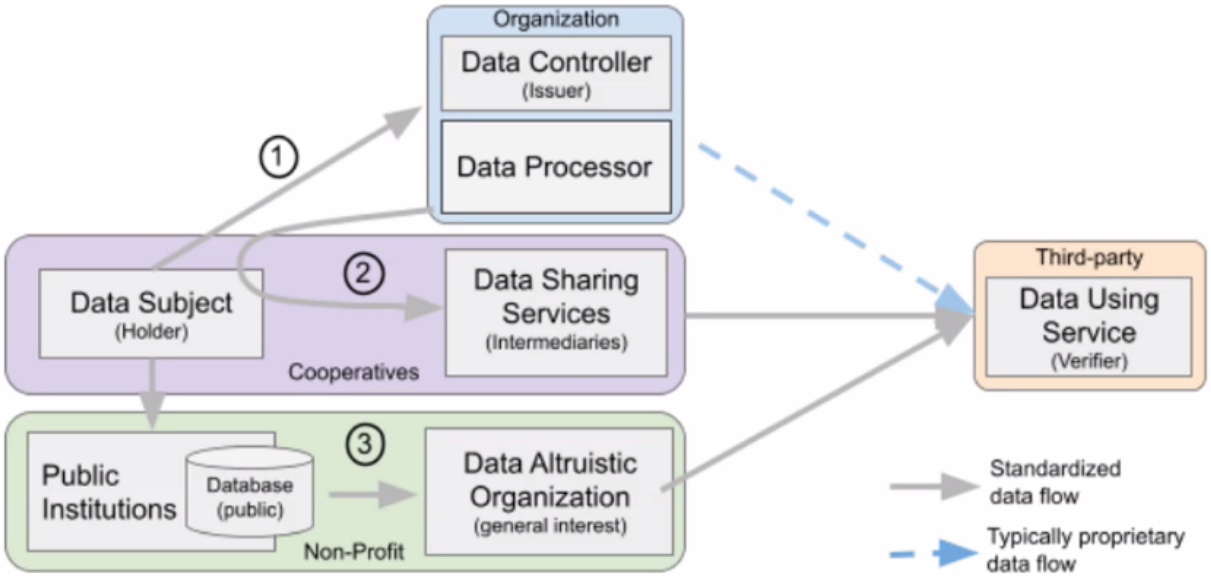
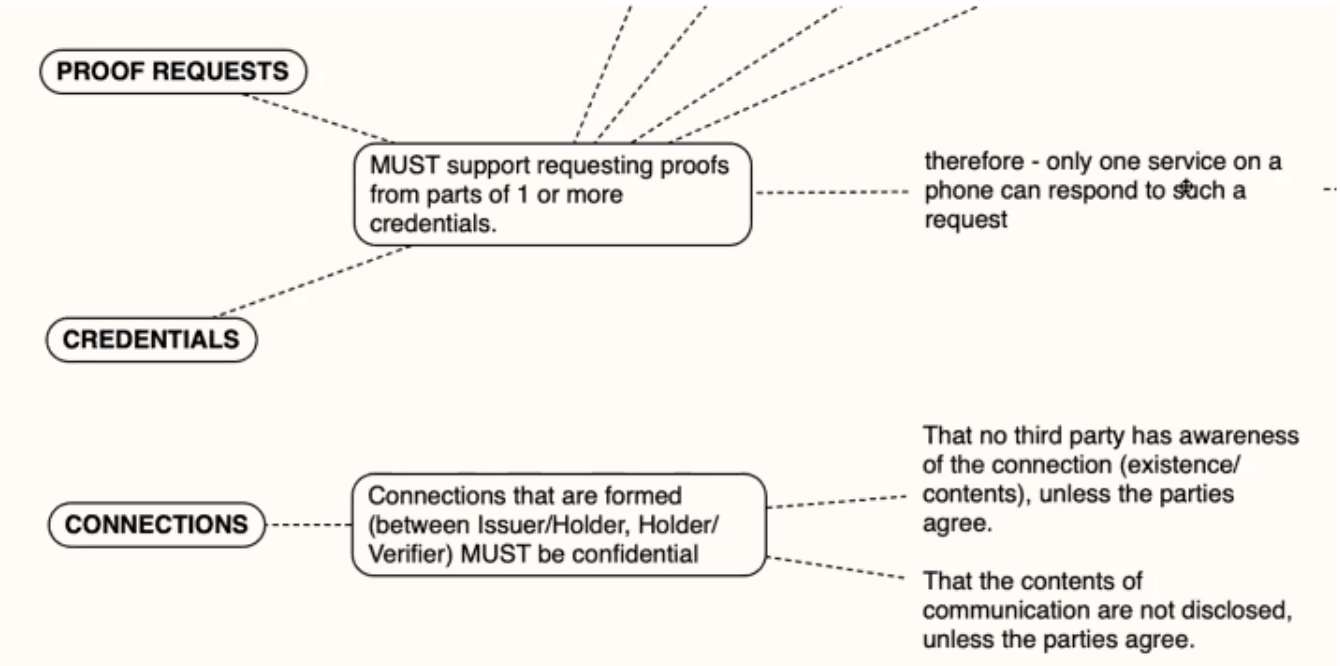
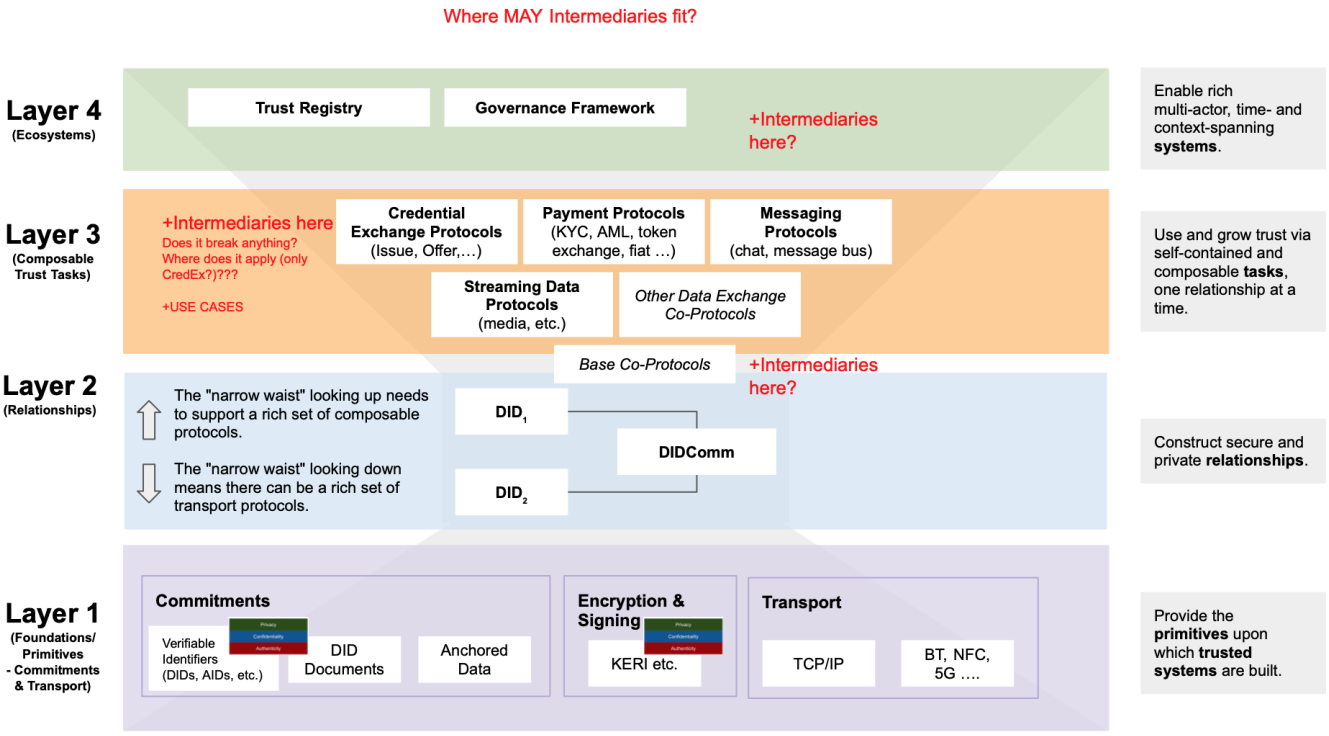


Figure 1: Data Governance Act Architecture Overview

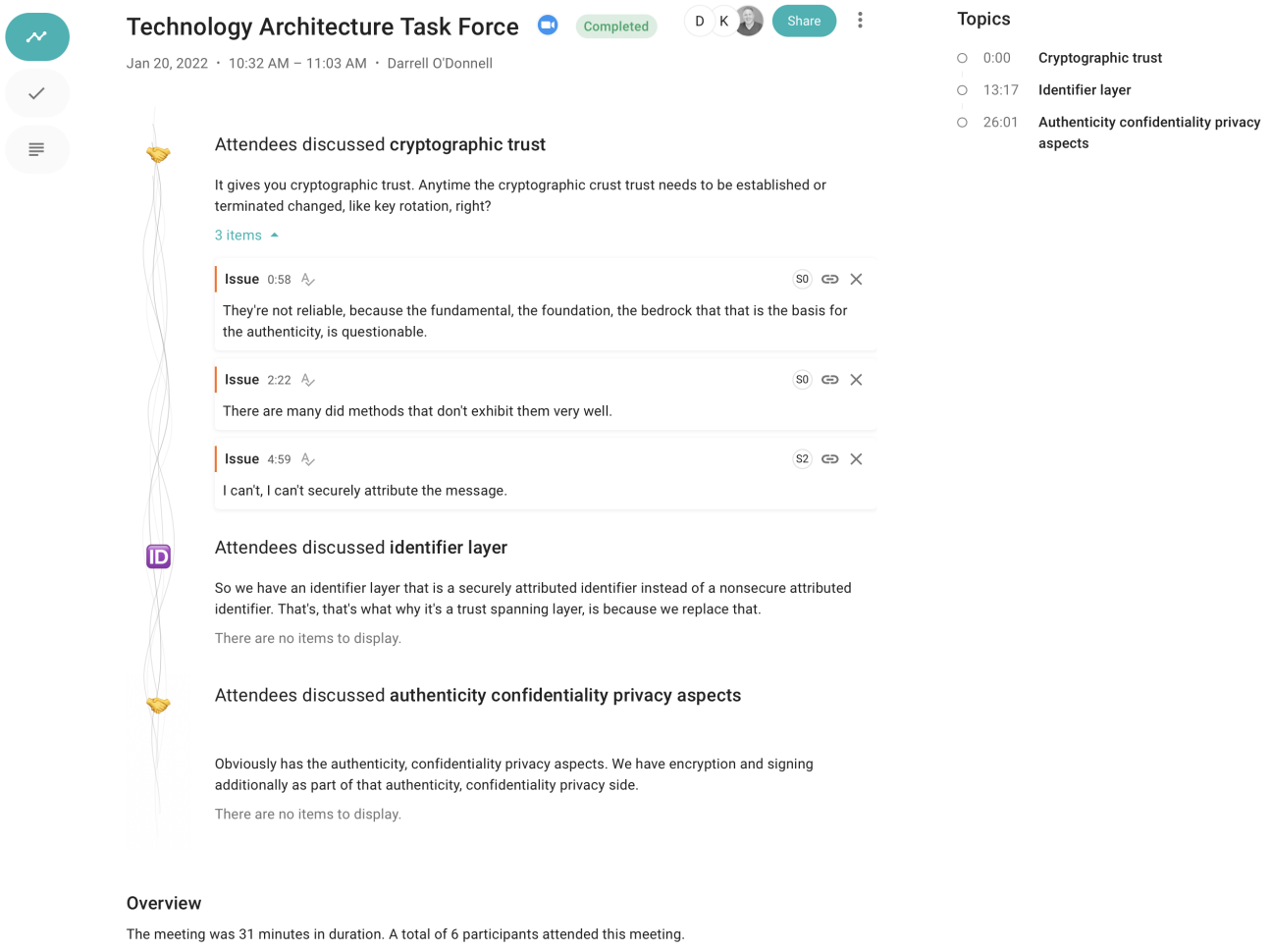
#3



#4



Sembly sample from last halfhour of last week AM meeting:



Decisions

- DECISION: Our next steps in drafting the spec will be to prepare a narrative-form "storyline" slide deck (see first action item below).

Action Items

- [ ] ACTION: Drummond Reed to prepare a starting storyline deck and share via Slack before next week's meeting.
- [ ] ACTION: Drummond Reed to interview Sam to start to document Sam's approach to "filling in the details" of the four layers.