2022-04-21 TATF Meeting Notes

Meeting Date & Time

- 21 Apr 2022
  - **NA/EU 07:00-8:00 PT / 14:00-15:00 UTC**
  - **APAC 1:00-2:00PM PT / 20:00-21:00 UTC**

Zoom Meeting Links / Recordings

- NA/EU Meeting: https://zoom.us/j/99376159509?pwd=UlNyZWFNbDBnanFPeVBablNzdXpBZz09
- APAC Meeting: https://zoom.us/j/99851532700?pwd=b0dvM0QxdXlCUHBwd21najlNSUN6UT09
  (This links will be replaced with links to the recordings of the meetings as soon as they are available)

Attendees

NA/EU

- Drummond Reed
- Darrell O'Donnell - London
- Wenjing Chu
- Scott Perry
- Kevin Dean
- Antti Kettunen
- Judith Fleenor
- Isaac Henderson
- Michael Nettles
- Vlad Zubenko
- Rodolfo Miranda
- Allan Thomson
- Troy Ronda
- Neil Thomson
- Goutam Sinha
- Vikas Malhotra

APAC

- Daniel Bachenheimer
- Wenjing Chu
- Neil Thomson
- Vlad Zubenko
- Drummond Reed
- Samuel Smith
- John Jordan

Main Goals of this Meeting

1) Review Working Draft 01 of the ToIP Technology Architecture Specification now that it is close to content-complete, 2) review Wenjing Chu's proposal for the Reference Architecture section, 3) Discuss final preparations for a session on the spec at Internet Identity Workshop #34 next week.

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:

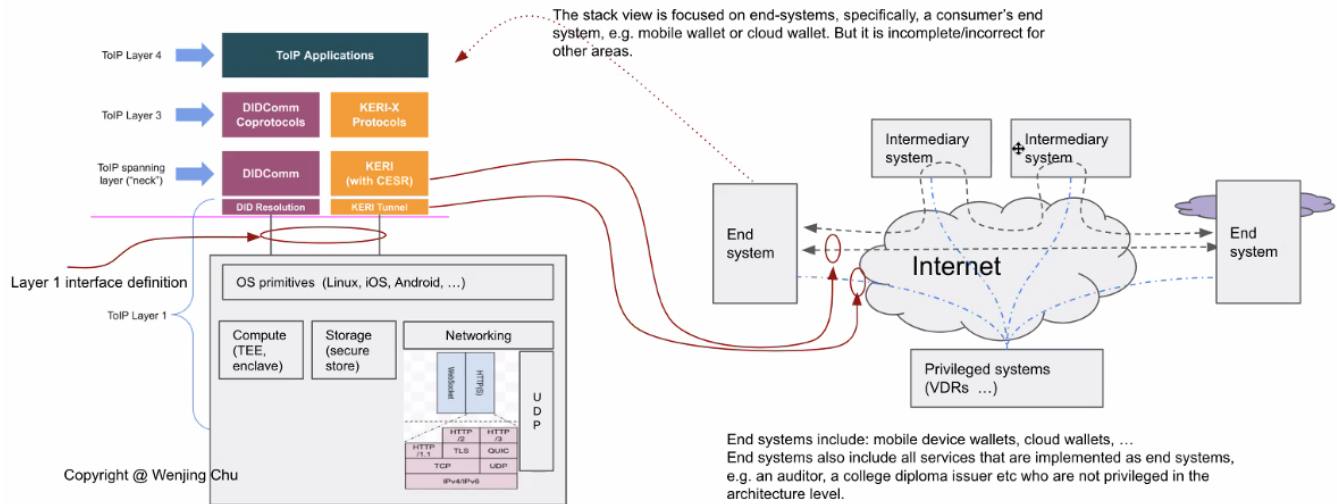| 5 min	Announcements	All	Updates of general interest to TATF members. • Scott Perry announced the Governance Stack WG meeting later today — 11AM PT — will be addressing layer-specific task force. • Drummond Reed on eIDAS 2.0 _____ • Isaac Henderson shared that the eSSIF-Lab TRAIN project had a successful pilot and they have some interest from the GAIN community in the trust registry and framework. GAIN (Global Assured Identity Network).
5 min	Review of previous action items	Chairs	☑ ACTION: Wenjing Chu to: a) draft the content for section 5: Reference Architecture, and b) edit/revise/shorten the content in section 7: Architectural Layering of the ToIP Stack. ☑ ACTION: Drummond Reed to a) add initial content to sections 7.4 through 7.7, and b) convert the rest of the content from the storyline slide deck into sections 9, 10, and 11.
10 mins	Overview of updates to Working Draft 01	Drummond Reed	Per the second action item above, in the ToIP Technology Architecture Specification Google doc, Drummond has completed content for section 7 and finished moving content from the storyline slide deck into sections 8, 9, 10, and 11. **Note the complete list of requirements in sections 8 thru 11.** Please review carefully.
5 mins	Merging sections 3 & 4?	Wenjing Chu	Wenjing suggested we consider merging section 3: Motivations and section 4: Canonical Uses Cases & Scope Limitations. We did not have time to discuss this in the NA/EU meeting. In the APAC meeting we had consensus on the following action: • ACTION: Drummond Reed to merge sections 3: Motivations and section 4: Canonical Uses Cases & Scope Limitations.
20 mins	Proposal for section 6 content	Wenjing Chu	Wenjing presented a proposal for the Reference Architecture section. See screenshots #1 through ___ below. **For the full narration of his slide deck from Wenjing, listen to the recording of the APAC meeting** (because Wenjing covered his entire slide deck in that meeting vs. only part of it in the NA/EU meeting).
5 mins	Final preparations for Internet Identity Workshop	Drummond Reed	We will discuss the proposed format for a session on the spec at IIW.
5 mins	• Review decisions /action items • Planning for next meeting	Chairs	NOTE: NO MEETING NEXT WEEK due to Internet Identity Workshop #34

Screenshots/Diagrams (numbered for reference in notes above)

#1

Getting to a ToIP Reference Framework

The stack view we've been thinking about…

A draft reference view…

The stack view is focused on end-systems, specifically, a consumer's end system, e.g. mobile wallet or cloud wallet. But it is incomplete/incorrect for other areas.

ToIP Layer 4 → **ToIP Applications**

ToIP Layer 3 → **DIDComm Coprotocols** | **KERI-X Protocols**

ToIP spanning layer ("neck") → **DIDComm** | **KERI (with CESR)**

DID Resolution | **KERI Tunnel**

Layer 1 interface definition

ToIP Layer 1

OS primitives (Linux, iOS, Android, …)

Compute (TEE, enclave) | Storage (secure store) | Networking

WebSocket | HTTP(S)

HTTP /2 | HTTP /3

HTTP /1.1 | TLS | QUIC

TCP | UDP

IPv4/IPv6

U D P

Copyright @ Wenjing Chu

Intermediary system

Intermediary system

End system

Internet

End system

Privileged systems (VDRs …)

End systems include: mobile device wallets, cloud wallets, …
End systems also include all services that are implemented as end systems, e.g. an auditor, a college diploma issuer etc who are not privileged in the architecture level.
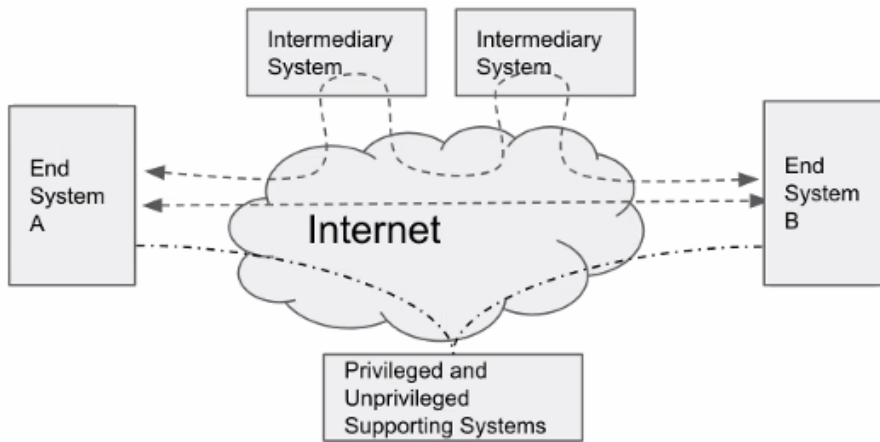
#2

A Reference Architecture of a complex system is an abstract framework consisting of a list of component subsystems and interactions with each other and with external systems.

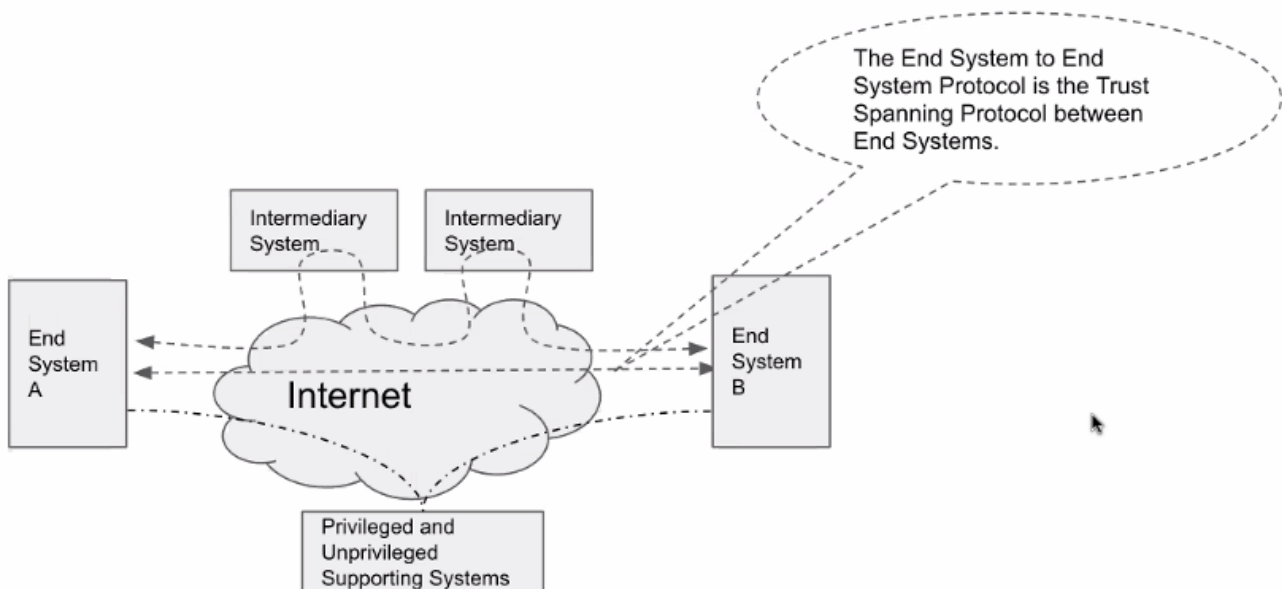It is a generalization of various viable solutions.

It helps crystalize the most important architecture considerations while leave some details for substantiation.
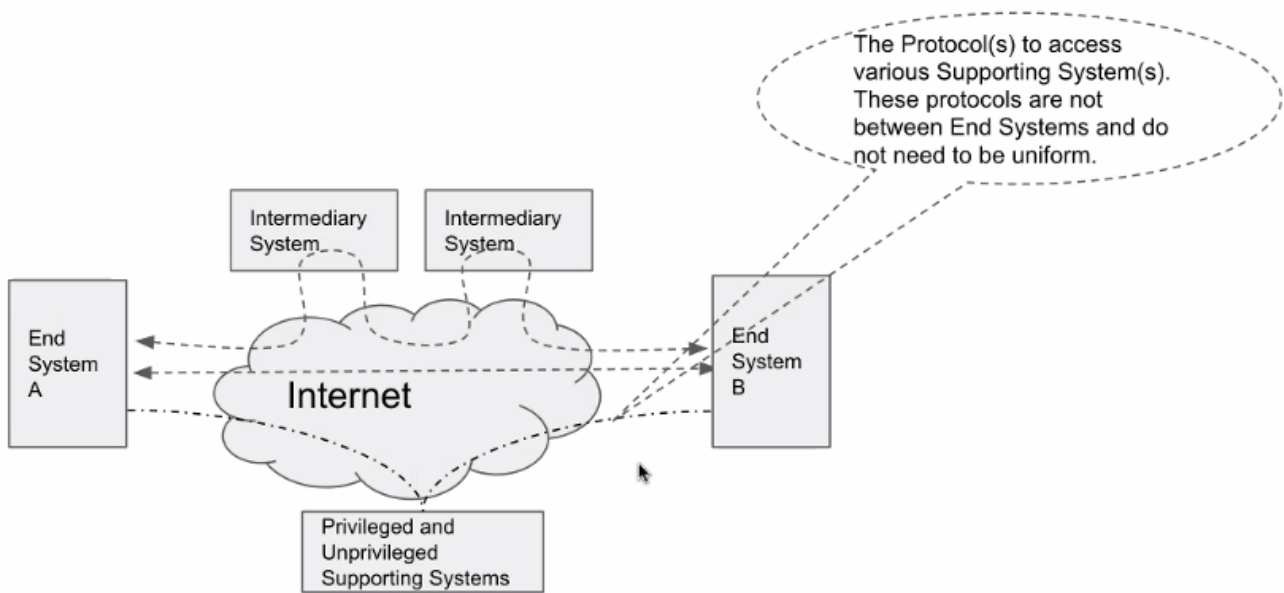
#3

- Subsystems are delineated by locus of control
- They interact through a set of protocols, not just one.
- Each **type** of subsystems has a shared stack*, but that is not true across different types**.

#4
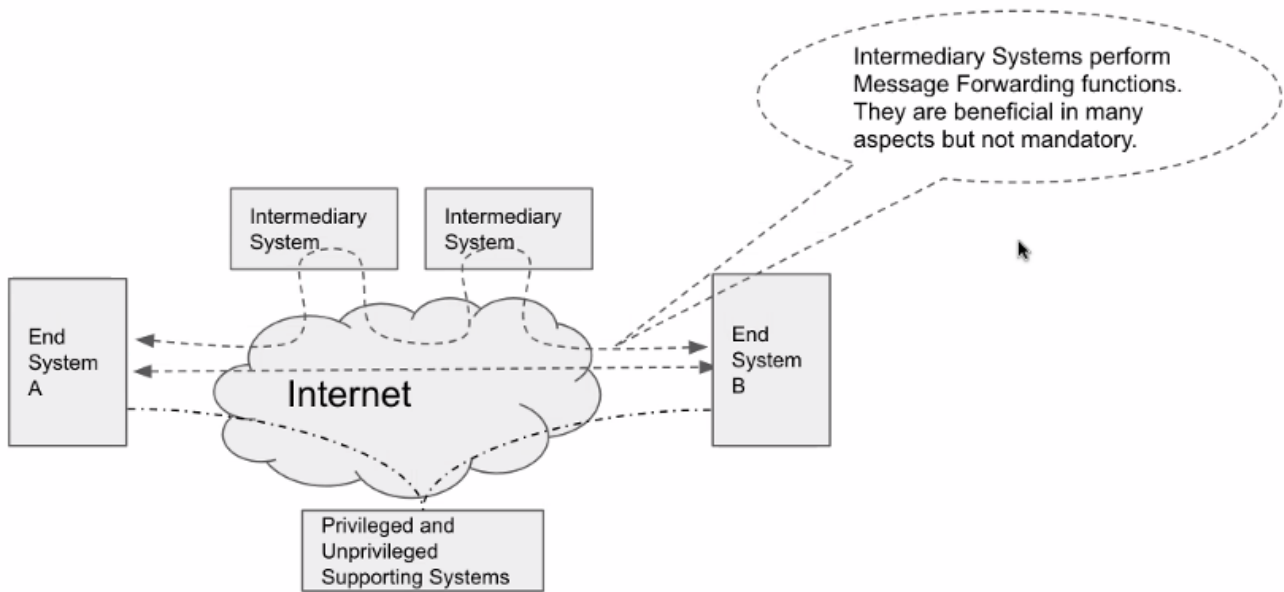

The End System to End System Protocol is the Trust Spanning Protocol between End Systems.

#5

The Protocol(s) to access various Supporting System(s). These protocols are not between End Systems and do not need to be uniform.

Intermediary System

Intermediary System

End System A

Internet

End System B

Privileged and Unprivileged Supporting Systems

#6

Intermediary Systems perform Message Forwarding functions. They are beneficial in many aspects but not mandatory.

Intermediary System

Intermediary System

End System A

Internet

End System B

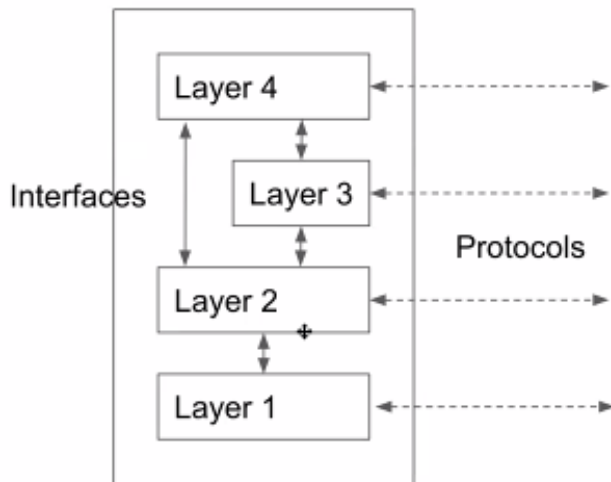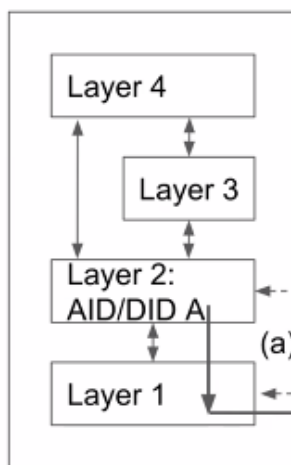Privileged and Unprivileged Supporting Systems
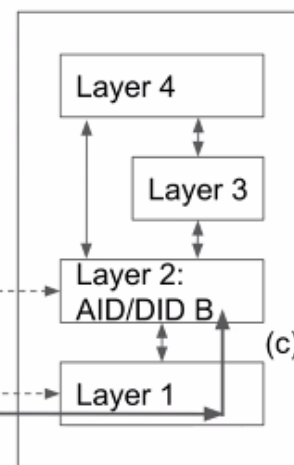
#7

An End System

Interfaces

Protocols

Locus of control

#8

End System A

End System B

End System to End System Protocol

(a) Resolution

(b) Transport

(c) Delivery

What Layer 2 needs and *only* needs: (1) AID/DID; (2) An end-to-end verifiable messaging protocol***. Of course, **with proper properties for each**: (i) authenticity (ii) optional confidentiality (iii) optional privacy

Note that the dotted arrows represent different protocols but not the actual flow of messages — that is represented by the solid arrows.

The "verifiability" in slide #8 refers to secure attribution to the source. This is the core problem we are solving in a universal way.

#9

An End System

*These are tightly bounded in the Indy-Aries design. What is shown here is how I would separate ID from Credentials.
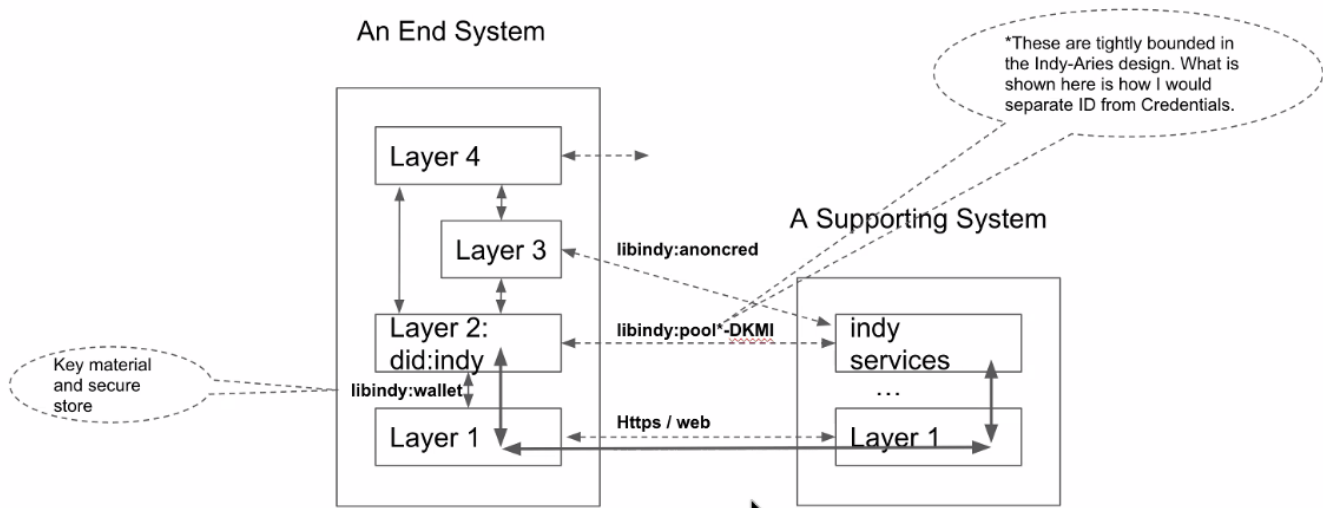
Indy-Aries example

There was discussion about the separation of the "tight binding" described in this diagram. Troy Ronda shared the observation that the tight binding shown in this diagram from Wenjing Chu does not reflect how the Aries Framework Go implementation works, because it does not make the same tight binding.
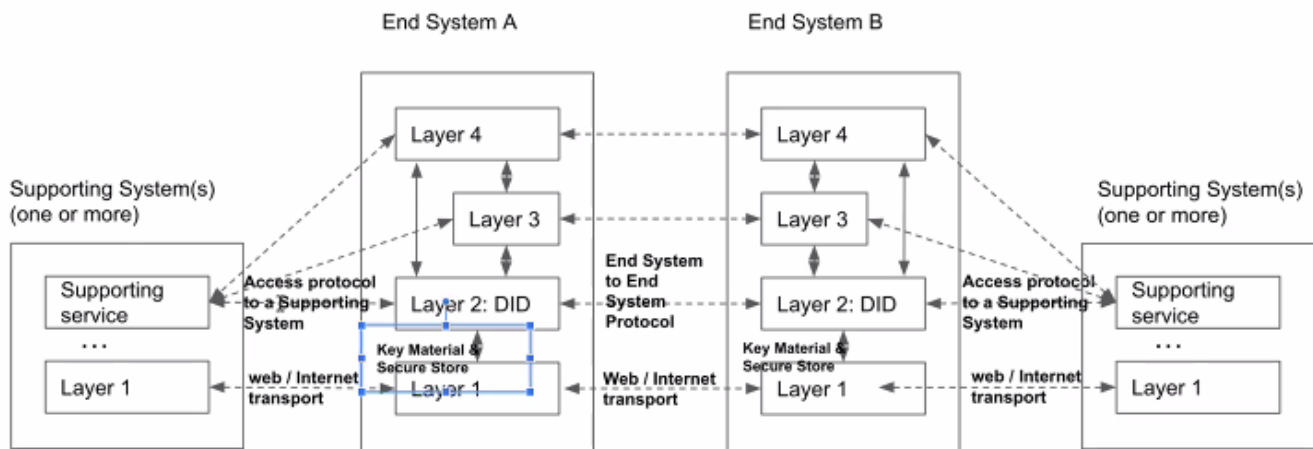
Wenjing welcomed other examples.

#10

An End System
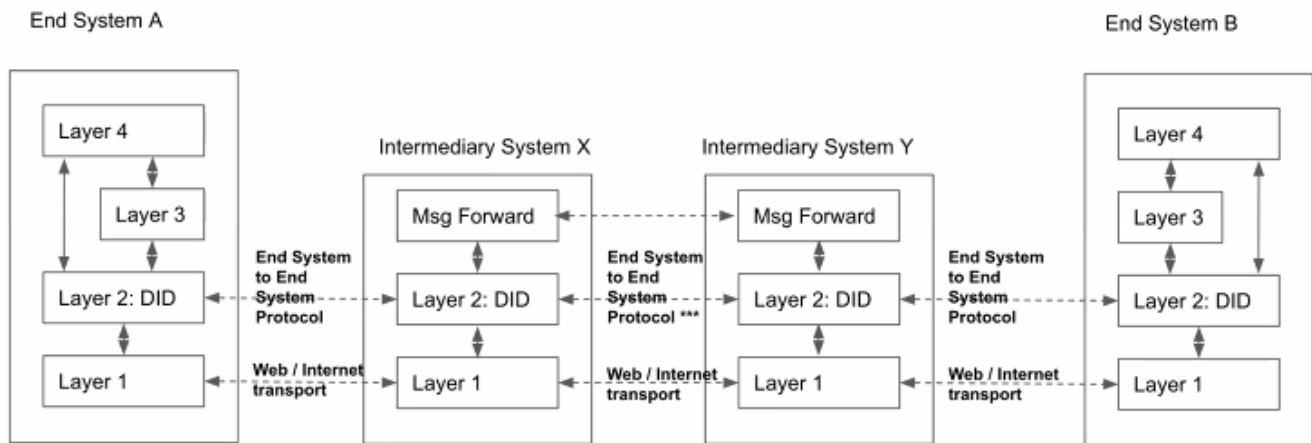
John: Askar?

A Supporting System
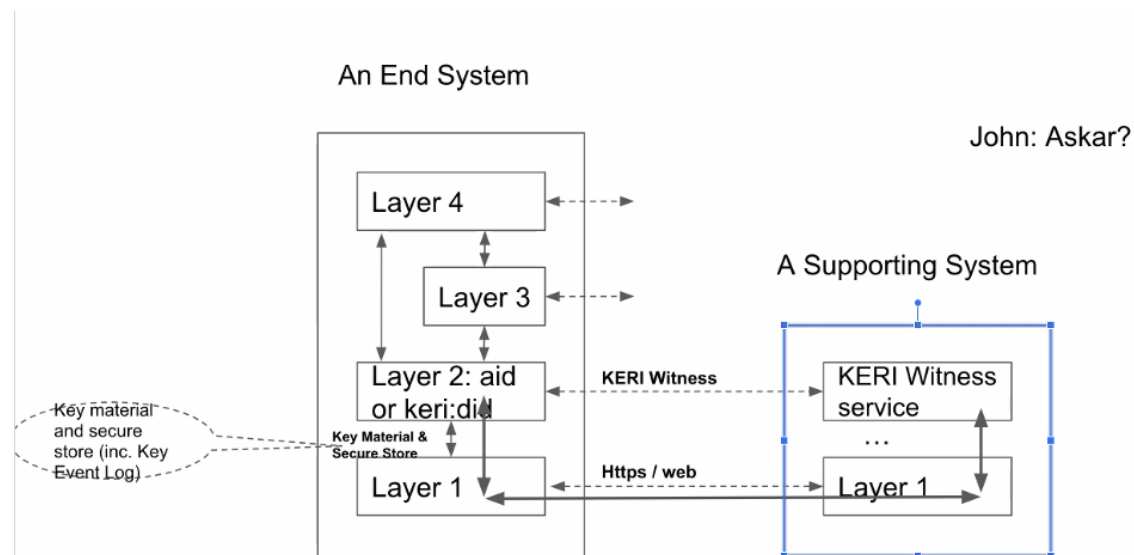
- KERI example: Witnesses with Key Event Logs.
- KERI uses other supporting systems (eg Watcher for confirmation) in addition to Witness pool.
- As long as such services are required for the functioning of AID and E2E communication, they belong to Layer 2 and the pattern shown here should still

#11

A Generalized Reference Architecture

Supporting System(s) (one or more)

End System A

End System B

Supporting System(s) (one or more)

Layer 4

Layer 3

Layer 2: DID

Key Material & Secure Store

Layer 1

Supporting service

...

Layer 1

Access protocol to a Supporting System

web / Internet transport

End System to End System Protocol

Web / Internet transport

Key Material & Secure Store

Access protocol to a Supporting System

web / Internet transport

Supporting service

...

Layer 1

#12

Intermediary Systems

End System A

Intermediary System X

Intermediary System Y

End System B

Layer 4

Layer 3

Layer 2: DID

Layer 1

Msg Forward

Layer 2: DID

Layer 1

Msg Forward

Layer 2: DID

Layer 1

Layer 4

Layer 3

Layer 2: DID

Layer 1

End System to End System Protocol

Web / Internet transport

End System to End System Protocol ***

Web / Internet transport

End System to End System Protocol

Web / Internet transport

#13

An End System's Protocol Stack

Layer 4

Layer 3

Zero, One or More Access
Protocol(s) to Supporting
System(s)

Layer 2

A Common Trust
Spanning End System to
End System Protocol

Interfaces to Layer 1
- Key material and storage***
- Transport over Internet

Layer 1

Transport over Internet

#14

An End System's Protocol Stack

Layer 4

Layer 3

Zero, One or More Access
Protocol(s) to Supporting
System(s)

Layer 2

A Common Trust
Spanning End System to
End System Protocol

Key material and storage***
Provided by a Supporting
System

"Cloud wallet"
service

…

Layer 1

Interfaces to Layer 1
- Key material and storage***
- Transport over Internet

Wallet Service Protocol

Layer 1

Transport over Internet

17

#15

With this Reference Architecture, the details of each layer, interface, protocol can be specified one by one which, taken as a whole, completes the architecture specification.

Decisions

- None

Action Items

- [ ] ACTION: Drummond Reed to merge sections 3: Motivations and section 4: Canonical Uses Cases & Scope Limitations.
- [ ] ACTION: Wenjing Chu to prepare slide deck for Internet Identity Workshop presentation on the ToIP Technology Stack.