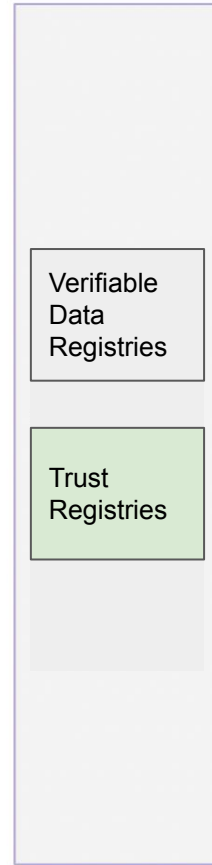
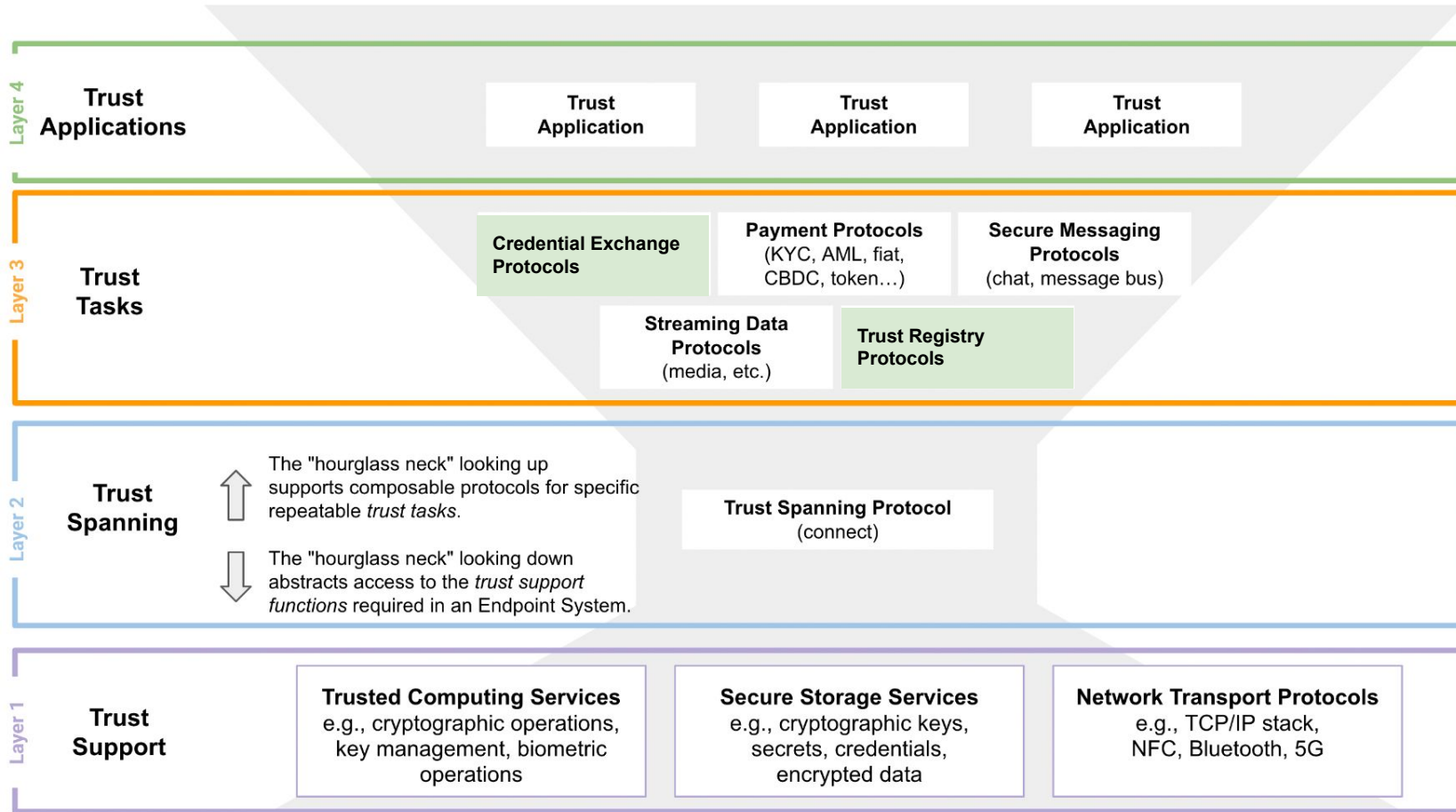


Trust Input Protocols

Mathieu Glaude

ToIP TRTF Proposal

June 29, 2023



When a party is presented with a *verifiable* claim, there are three things that they will want to ensure:

1. That a claim hasn't been altered/falsified at any point in time

(cryptographic verifiability, verifiable data registry)

= technical trust

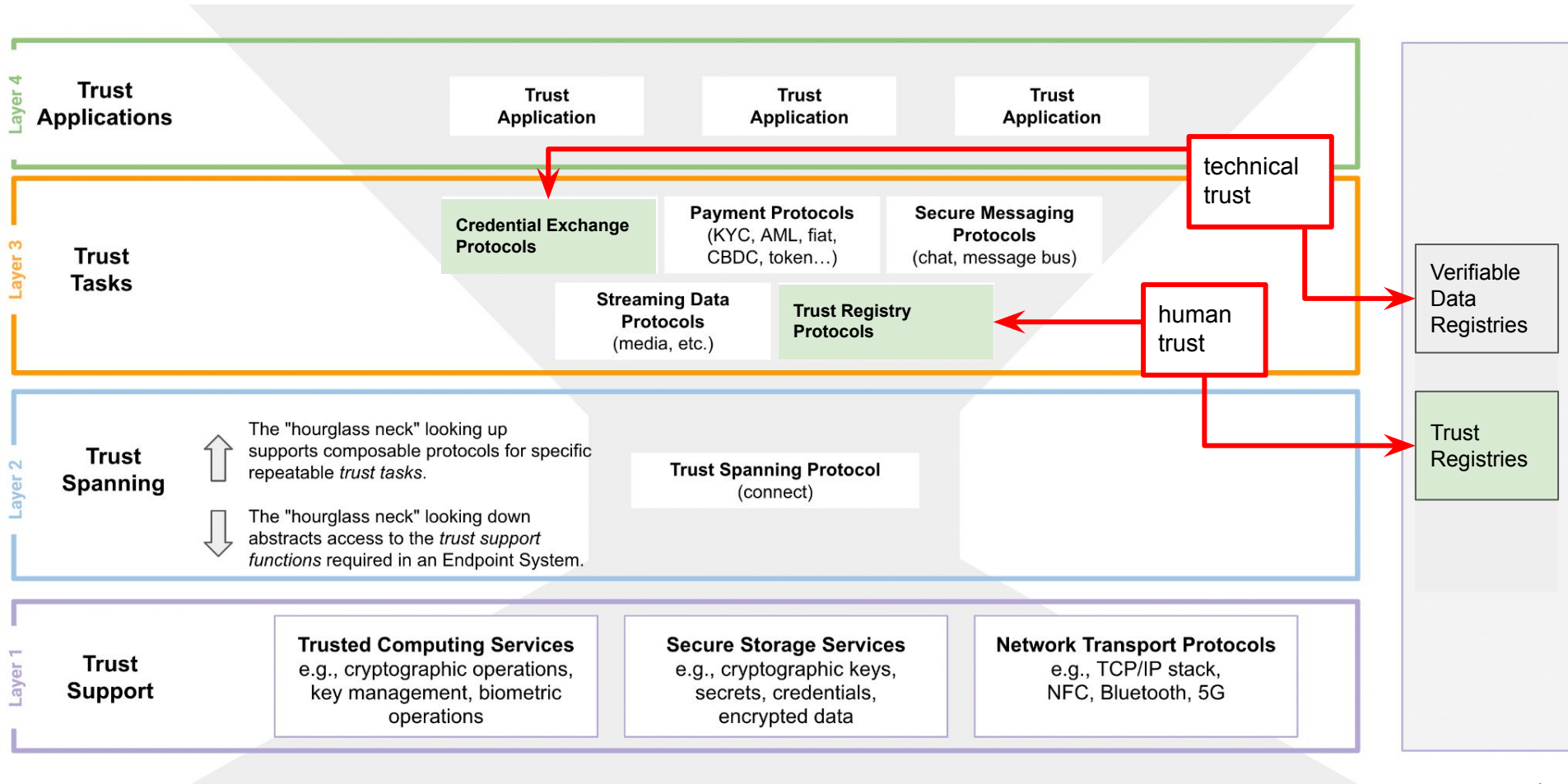
2. That a claim has accurate representation

(AuthN, DID ownership/control)

3. That a claim has been issued by an authority

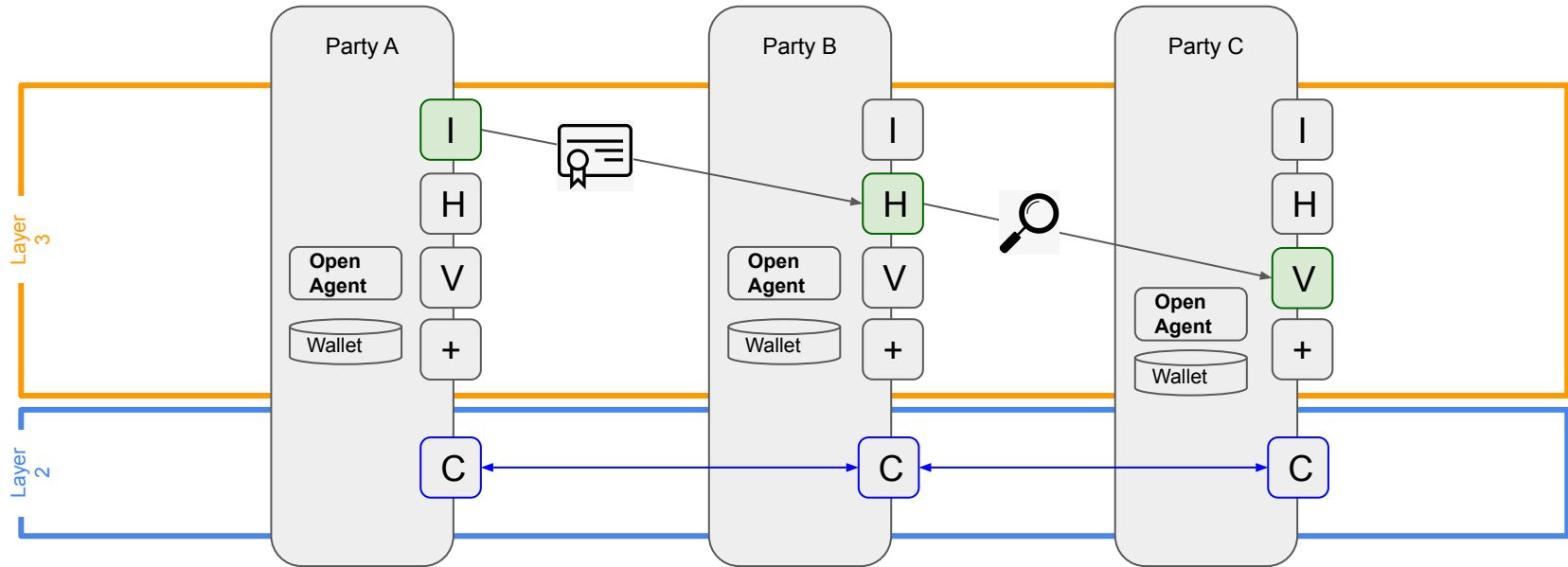
(AuthZ, trust registries/trust lists)

= human trust



A typical credential exchange

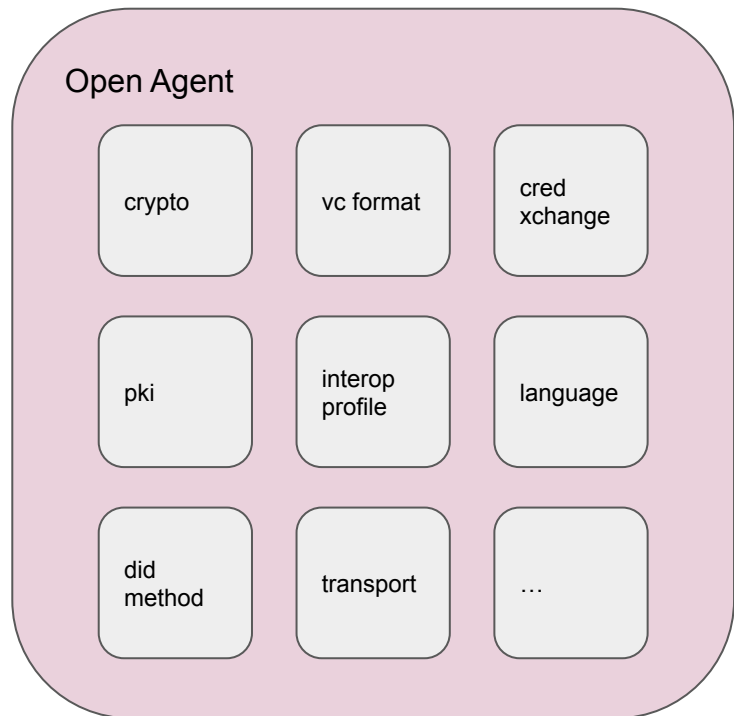
Utilizing credential exchange protocols to achieve *technical trust*







- C: Peer-to-peer connection protocol
- I: Credential issuance protocol
- H: Credential holder protocol
- V: Credential verification protocol
- +: Other protocols

Open Agents

- Open agents are agnostic to protocol implementations
- These different capabilities offer various features that are perhaps better suited for one use case over another.
- Aries is an open agent.
 - Aries can be implemented in languages such as JavaScript and Python,
 - Open *agent test harnesses* to test interoperability and compliance with various protocols and **RFCs**.
- Open agents could be viewed as enablers for various trust tasks by mix and matching protocols to suit the use cases.
- By implementing these, wallets can be built, all based on open source, which is a critical part in establishing a network effect, including the ability to speak multiple protocols in the early days.



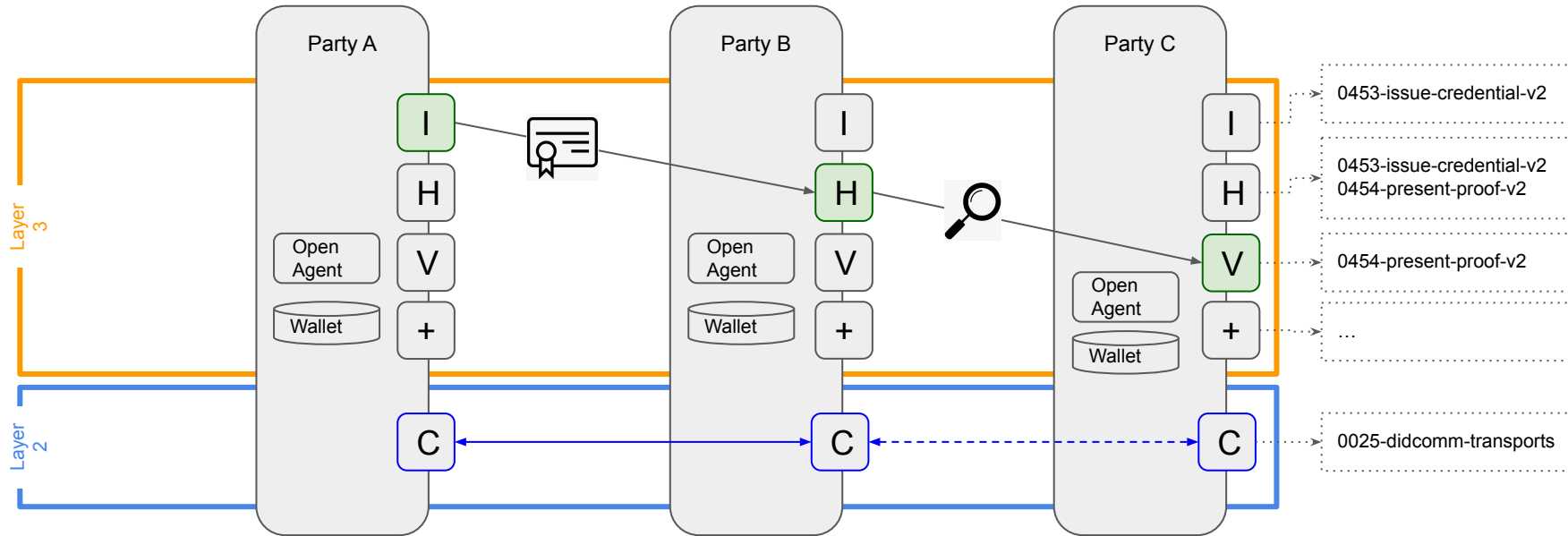
Aries RFCs - some examples..

RFC/Link to RFC Version	Note
0023-did-exchange	
0025-didcomm-transport	AIP V1.0, Minimally Updated
0035-report-problem	AIP V1.0, Updated
0183-revocation-notification	
0434-outofband	
0453-issue-credential-v2	Update to V2 Protocol
0454-present-proof-v2	Update to V2 Protocol
0999-trust-registry???	

<https://github.com/hyperledger/aries-rfcs/blob/main/index.md>

A typical credential exchange

Utilizing credential exchange protocols to achieve *technical trust*



- C: Peer-to-peer connection protocol
- I: Credential issuance protocol
- H: Credential holder protocol
- V: Credential verification protocol
- +: Other protocols

When a party is presented with a *verifiable* claim, there are three things that they will want to ensure:



1. That a claim hasn't been altered/falsified at any point in time

(cryptographic verifiability, verifiable data registry)

= technical trust



2. That a claim has accurate representation

(AuthN, DID ownership/control)

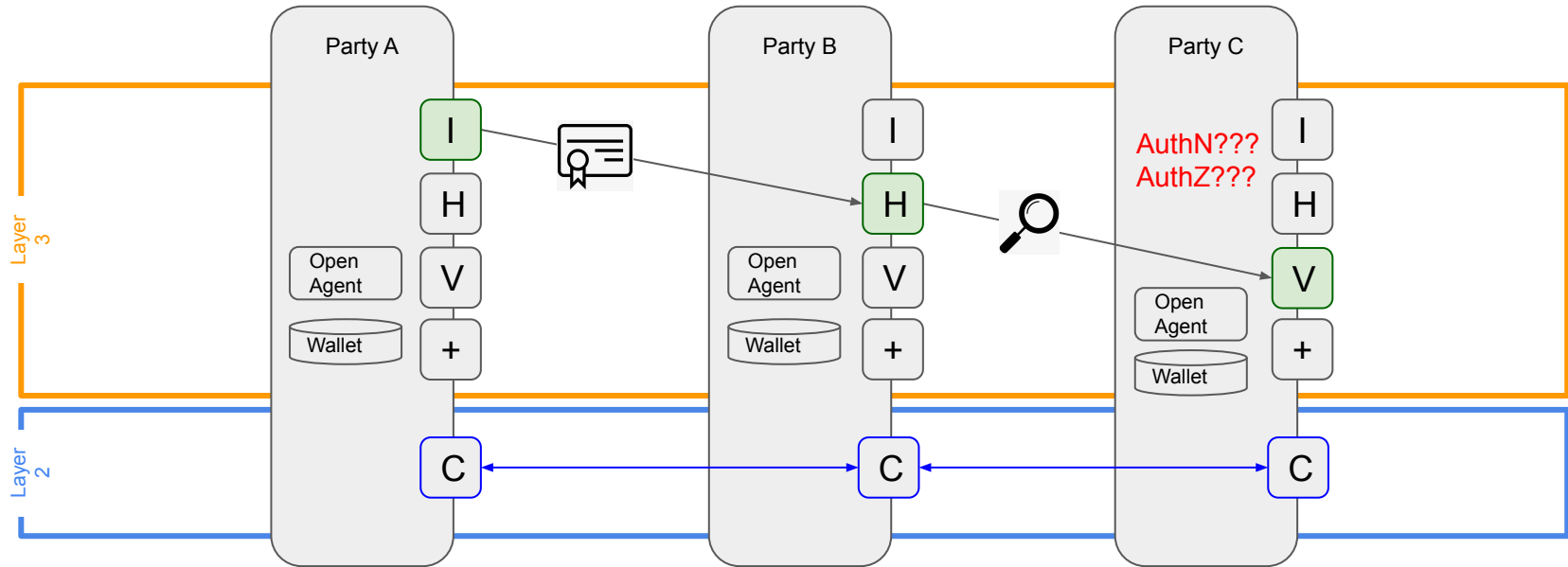
3. That a claim has been issued by an authority

(AuthZ, trust registries/trust lists)

= human trust

A typical credential exchange

Helping with the establishment of *human trust*

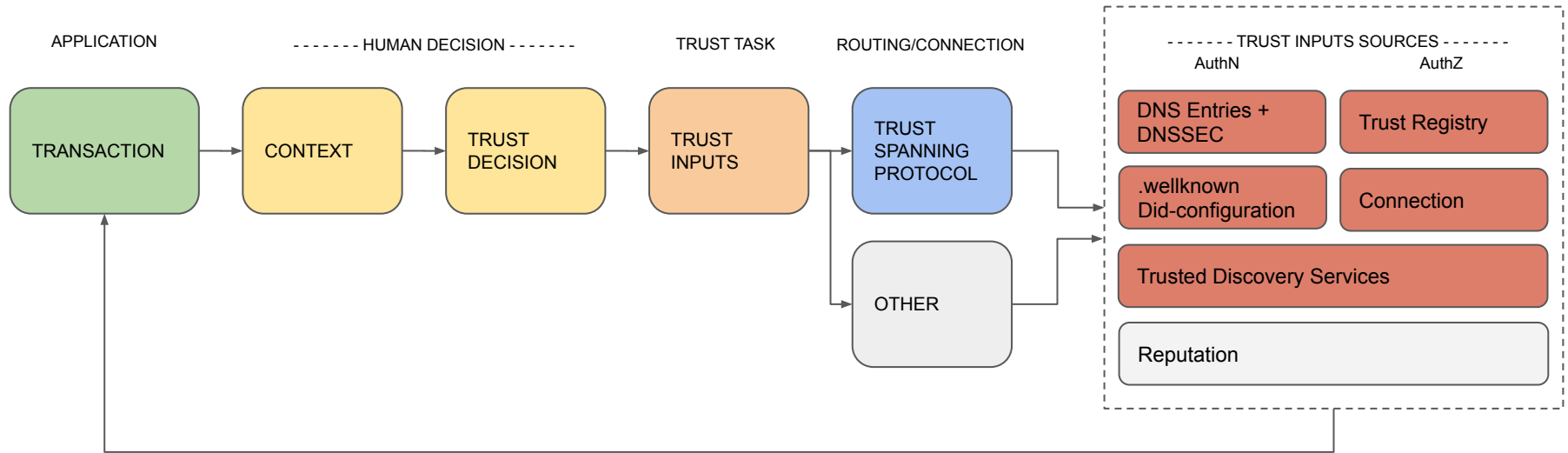


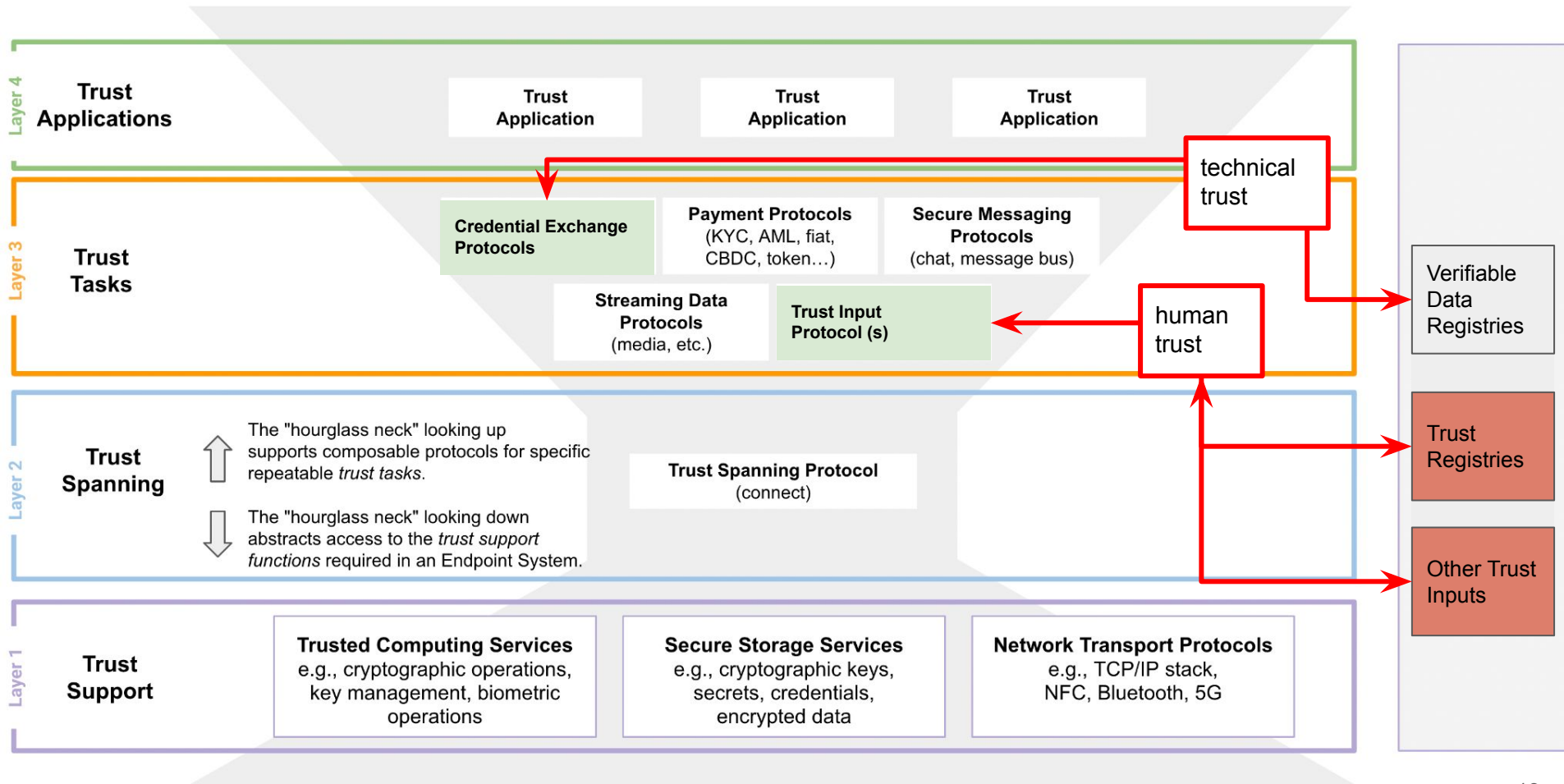
- C: Peer-to-peer connection protocol
- I: Credential issuance protocol
- H: Credential holder protocol
- V: Credential verification protocol
- +: Other protocols

Some definitions

- **Trust Decision:** A decision one party needs to make about whether to engage in a specific interaction or transaction with another entity that involves real or perceived risks. (ToIP Glossary)
- **Trust Inputs:** Any source of information that can assist a party in making a trust decision.
- **Reputation:** The reputation or prestige of a social entity (a person, a social group, an organization, or a place) is an opinion about that entity - typically developed as a result of social evaluation on a set of criteria, such as behavior or performance. (Wikipedia)

Providing Trust Inputs to assist with Trust Decisions





Trust Decision are facilitated by *reputable* Trust Inputs

Wikipedia: The reputation or prestige of a social entity (a person, a social group, an organization, or a place) is an opinion about that entity - typically developed as a result of social evaluation on a set of criteria, such as behavior or performance.

- I get a bunch of inputs, but based on *transaction* and *context* I'm able to draw my trust line and make my *trust decision*
- If your trust inputs have high reputation, then they are more likely to help you make a good trust decision, according to you

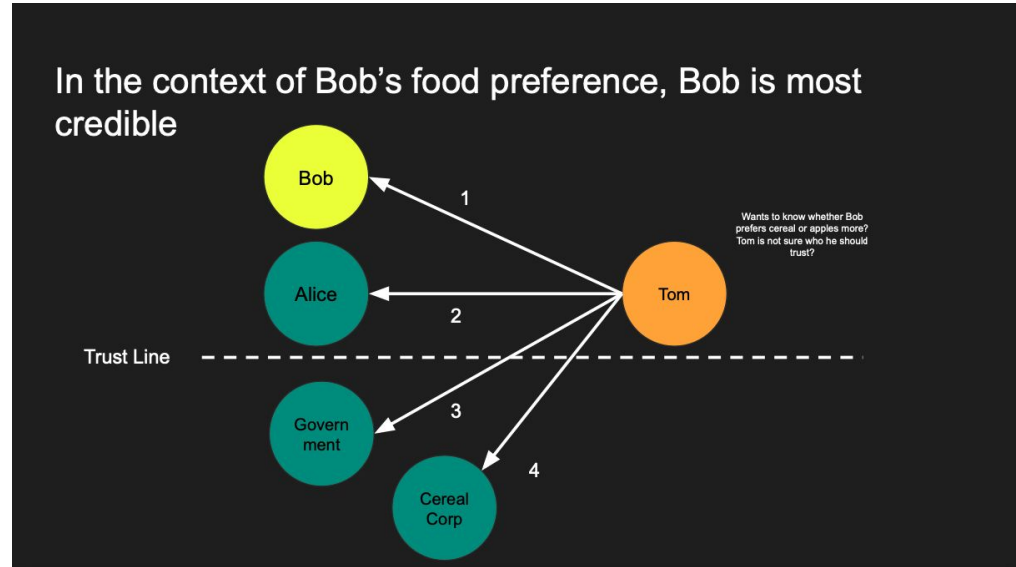
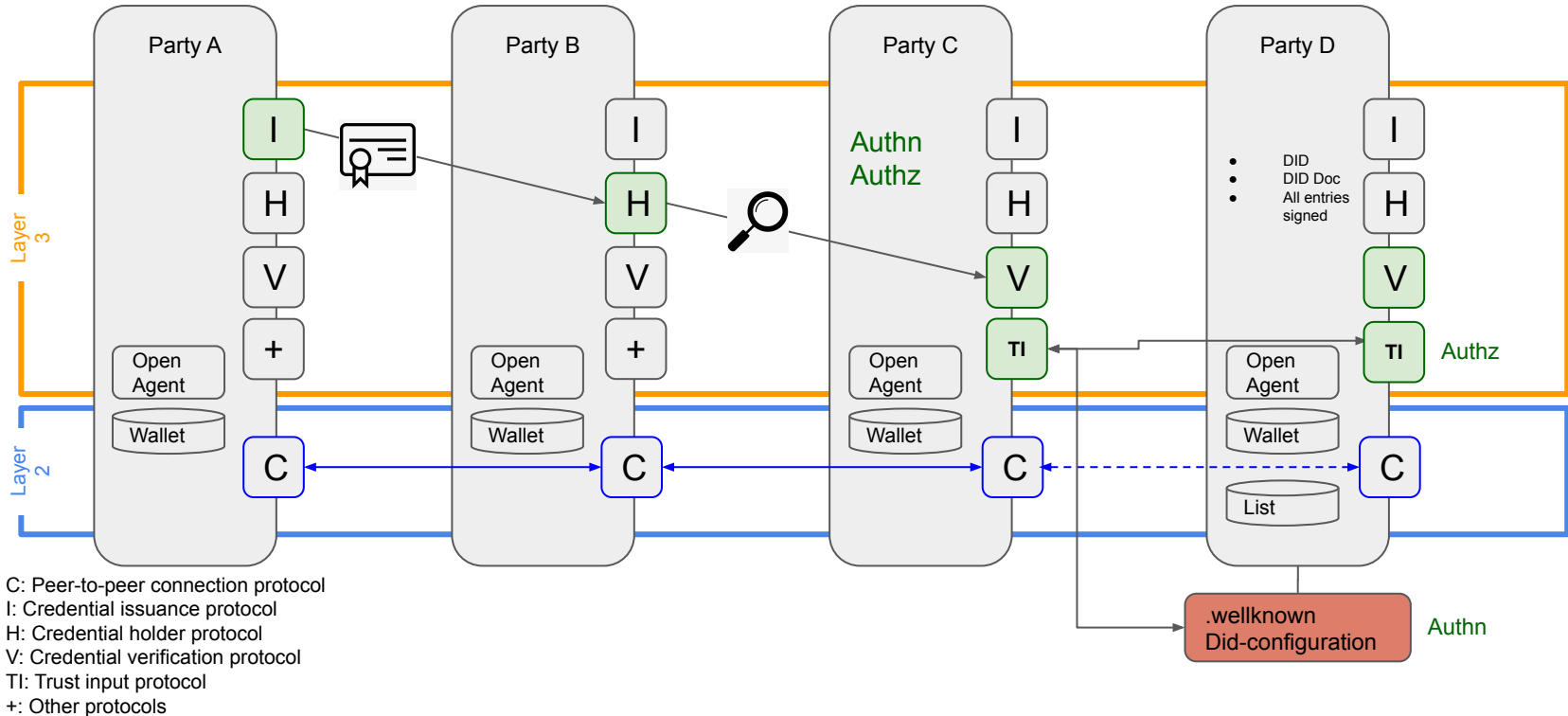


Image taken from "Interop Profiles Oh My : Andor's Proposal":
<https://github.com/trustoverip/tswg-trust-registry-tf/discussions/96>

A typical credential exchange

Using the Trust Input Protocol to help establish *human trust*



Providing trust inputs to the trust decision maker

Party C



The screenshot displays the 'Trust Decision Helper' interface within the Concordia University system. The interface is titled 'Trust Decision Helper' and shows 'Step 3/3 - Verify their information against their DNS records.' The main content area is divided into three sections:

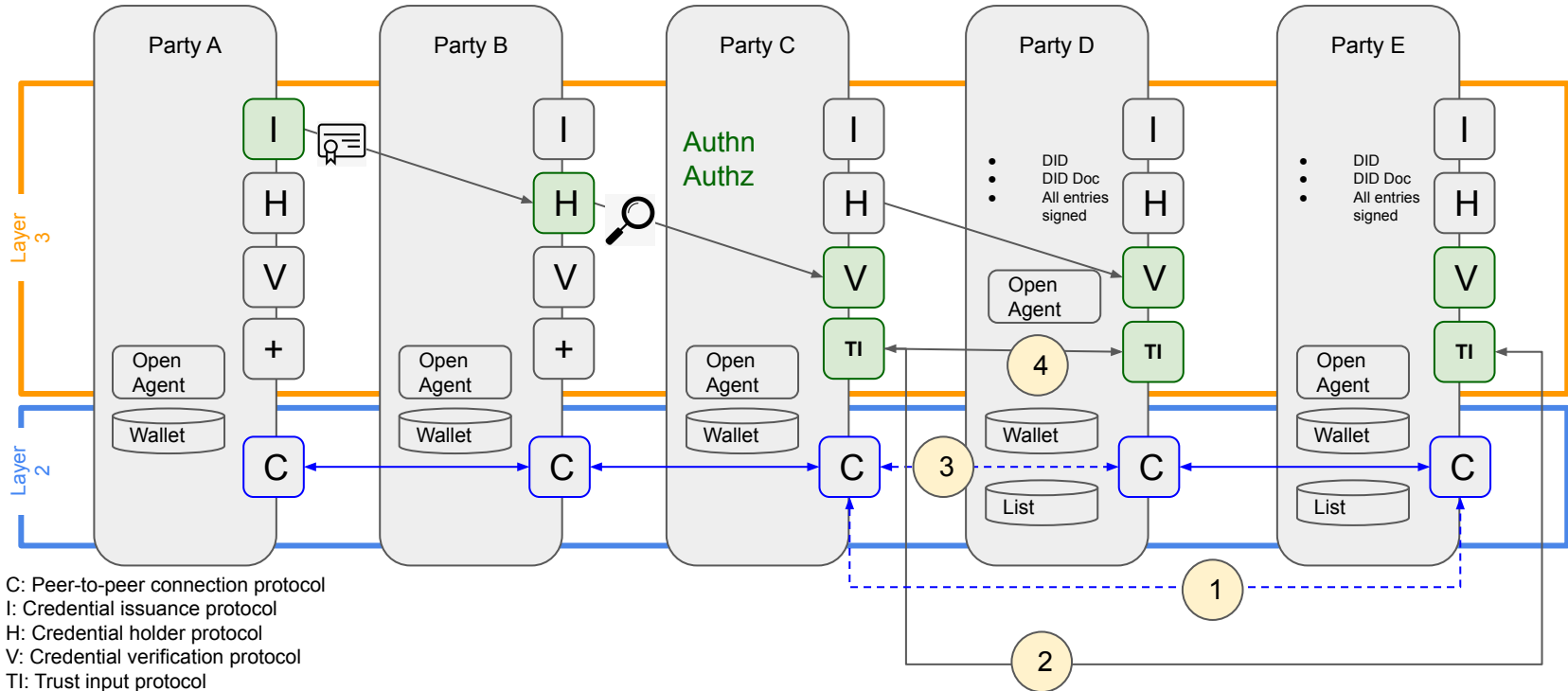
- You have received a credential offer from your connection:** Ville de Montreal
- Information Retrieved from their DID Document:** Name: Ville de Montreal, Public DID: did:sov:QgrV9BWin8bcm8KBHPzLY, Domain Name: nborbit.io
- Information retrieved from their DNS Records:** Name: Ville de Montreal (Match), Public DID: did:sov:QgrV9BWin8bcm8KBHPzLY (Match)
- Information retrieved from Trust Registry:** Trust Registry Consulted: http://trustregistry.nborbit.io:4000, Public DID: did:sov:QgrV9BWin8bcm8KBHPzLY, Credential Authorized to Issue: Business_Licence_Montreil (Match), Authorized (Authorized)

At the bottom, there is a 'Business_Licence_Montreal' credential offer button and a 'CONTINUE' button.

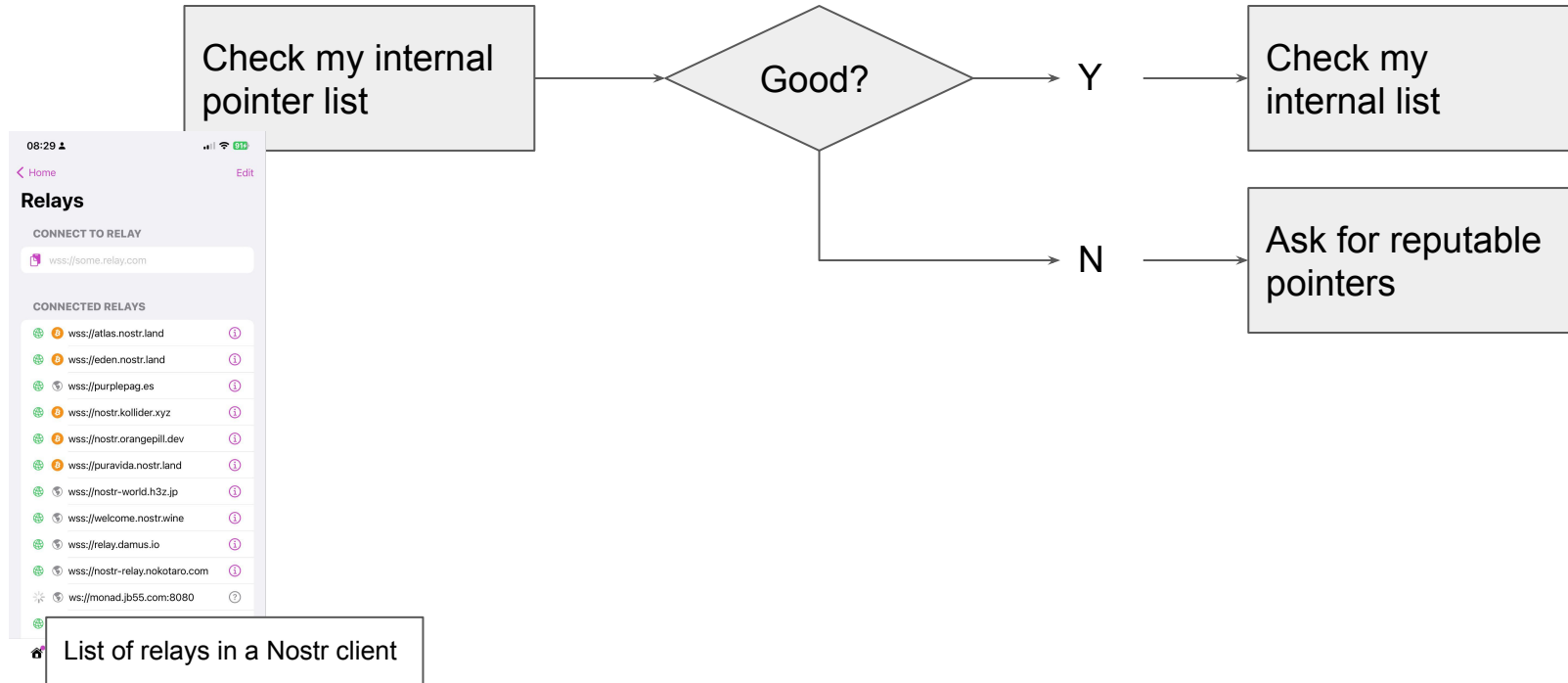
Demo here: <https://youtu.be/oTwbYGYJobQ>

A typical credential exchange

Using the Trust Input Protocol to help establish *human trust*

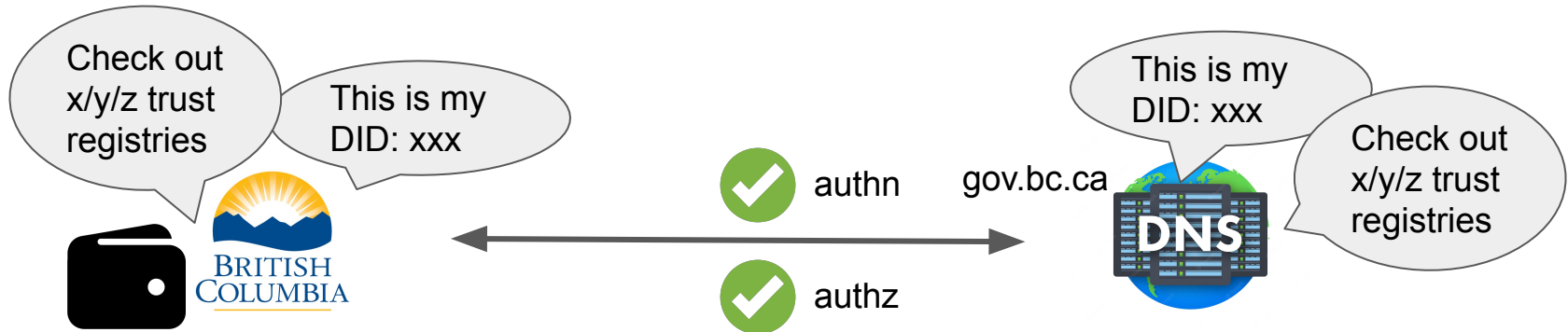


When seeking to make a trust decision (needed discovery) E.g., being presented with a proof



How DNS can be used as a reputable tool for Discovery

- We can assume that organizations/public parties will have stable DNS.
- There's trust built in to the fact that Canada Post owns <https://www.canadapost-postescanada.ca/> and that BC owns gov.bc.ca
- ccTLD administrators such as CIRA have strong governance processes that help build trust on the Internet for Canadians



When a party is presented with a *verifiable* claim, there are three things that they will want to ensure:



1. That a claim hasn't been altered/falsified at any point in time

(cryptographic verifiability, verifiable data registry)

= technical trust



2. That a claim has accurate representation

(AuthN, DID ownership/control)

= human trust

3. That a claim has been issued by an authority

(AuthZ, trust registries/trust lists)

Action Items for Quick MVP

- Design Trust Input Protocols for Open Agent consumption
- Trust Input Protocol is a query language
 - Proposed RFCs (Read)
 - Give me an answer to my question
 - Help me discover list of TRs
- 2nd Proposed RFC: Entering data into the list (Create, Update, Delete)
- One way for discovery - Proposed .wellknown Did-configuration

end