

Trust Registry Protocol v2 - Loose Capture

Christine Martin we will capture high-level requirements and tasks here.

The v1 protocol provides answers for three main questions

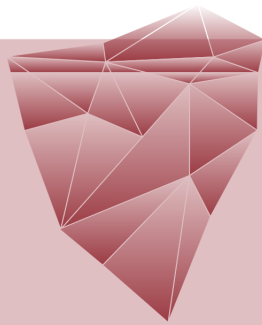
- Is this Issuer Authoritative to issue a particular credential type under a governance framework.
- Is a Verifier Authorized to request a presentation under a governance framework.
- Does the answering Trust Registry acknowledge another Trust Registry under a governance framework.

The analogy we have been using about the v1.0 protocol is that it handles the simplest (but powerful) questions - it is the tip of the iceberg.

V1.0

- Authoritative Issuers
- Authorized Verifiers
- Other Trust Registries

Where Are We Now?



vFuture

- Many more things...
- Schemas, Credential Types, Messaging,

Key Areas to Consider for v2:

- **Trust Registry Metadata** - what data are needed by systems to understand a Trust Registry
- **Centralized / Decentralized** - what does this question even mean?
- **Credential Information/Metadata** -
 - Credential Names - how do we name these things?
 - Credential Types - JWT, JSON-LD, AnonCreds, SD-JWT, etc.
 - There are numerous flavours of VCs and much debate. This is a problem that Trust Registries can help. They can provide answers where there aren't any in the "we are compliant with W3C Verifiable Credentials" statement.
 - The use of Credential Types in Trust Registries will answer the question of "what credential format are ACTUALLY used?"
 - Schema Definitions - provide the data or a pointer to the data (e.g. on ledger)
 - Credential Definitions if required (AnonCreds requires) - provide the data or a pointer to the data
- **Proof/Presentation Metadata**
 - What proof/presentation requests are supported and by whom can they be made? e.g. the overused driver license - who can request the full DL, versus an "age of majority" ZKP or some selective disclosure profile.
 - What should be done for inappropriate requests - should they be reported?
- **DID Metadata**
 - What DID Methods are supported
 - What other expectations are at play (e.g. must support `did:method:identifier:GetCapabilities` or something similar.
- **Wallet Metadata**
 - What wallets are approved (and how) in the ecosystem
- **Holder Metadata**
 - A
- **Other technical things**
 - Key Bindings
 - DIDAuth - is DIDAuth (its real-world implementations)
 - Service Discovery -

BACKGROUNDS:

- Trust Continuum - Scott Perry's - Trust Decision...
- Trust Assurance Companion - <https://trustoverip.org/wp-content/uploads/ToIP-Trust-Assurance-Companion-Guide-V1.0-2021-10-19.pdf>
- Trust Assurance & Certification - <https://trustoverip.org/wp-content/uploads/ToIP-Trust-Assurance-and-Certification-Controlled-Documents-Template-V1.0-2021-10-19.pdf>

2022-11-24

- Antti - connection is underlying

- TRs help create context for connection (and more)