2023-01-24 DMRWG Meeting Notes

Meeting Date

01 Nov 2022 The DMRWG meets bi-weekly on Tuesdays at 12:00-13:00 PT / 16:00-17:00 UTC. Check the ToIP Calendar for meeting dates.

Zoom Meeting Link / Recording

- Recording link

Attendees

- Neil Thomson
- Steven Milstein
- Burak Serdar
- Carly Huitema
- Mattia Zago

Main Goal of this Meeting

Modify the mandate of the Data Modelling & Representation WG to cover the Data, Authentic Data/Provenance Chains and Data Governance aspects of ToIP, its projects, working groups and task forces.

The immediate task is looking at the Data Requirements of the ToIP Trust Registry TTF

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 mins	Review of action items from the previous meeting	Chairs	
5 mins	Announcements	TF Leads	News or events of interest to Governance Stack WG members:

20 mins	Data Requirements	Chair	What are the Data requirements of Trust Registries?
			• Create a list of topics of which the following is a starter set
			  ◦ What is the data (or data API(s)), data structure, etc., required for a ToIP entity (organization, person, thing):
			  ▪ For Entities to be searchable within the registry
			  ▪ To support verifying an Entity's authentic providence chains of data and identity.
			  ▪ Other data aspects driven by other Trust Registry requirements.
			  • Management of entities, admission and updates to the TR for the entity
			  ◦ Revocation or suspension (change of status)
			  ◦ Governance of data access - dealing APIs and protocols for data access (CRUD) with particular attention to potentially sensitive data of a "Registrant" (SSI object registered in a Registry) within a TR context, which is made accessible and managed by the TR
			  ◦ ...
			Some specifics from the discussion:

- What evidence (and critieria) are required to be admitted to a given registry (KYR - Know Your Registrant)
- What Registration info/data is required:
  - For operation/management of the TR
  - For TR clients to access via the TR APIS
  - For TR clients to access via direct interfacing (OOBI) against the Registrant
    - Is the Registrant direct data access API a requirement of being registered or can that interface be a TR Client/Registrant issue?
- TR functionality for audit trail
  - Audit the onboarding process (significant events and data during onboarding of Registrant
  - Auditing the access (who asked what via the TR APIs),
- Verification of what the TR holds about you (access to data held by third parties)
  - Verification by other parties about you?
  - Who has viewed your profile - back to Governance -
  - May get an event about type of person who asked for information about.

DR. Mattia Zago - PhD in CyberScience - working from Italy on cyber security working with/for [Monokee](https://monokee.com/en/homepage/)mattia.zago@monokee.com. Monokee is building an orchestrator for identity access management.
What is a Trust Registry?

- It is a data store (with various APIs) which contains and manages entries for SSI Entities (organizations, people, things) which are considered trustworthy based on criteria defined by the ecosystem (e.g., law society, health care). Criteria includes
  - Verifiable identifiers, identity (through qualifying criteria (VCs?)) and data/verification lineage
  - Subject to evidence (sign-off) of governance of how verification is achieved by qualified governance stewards

Similarly, a Data Registry is about Data stores or Data access interfaces, for which the data content meets data credibility and traceability criteria for a given data hub's purpose within an ecosystem (e.g., health records for pharma research). Associated with a Data Registry Registrant would be verifiability of the data producer (entity responsible for collecting, processing and publishing the data) and (data) governance steward ([Wikipedia](https://en.wikipedia.org/wiki/Data_steward))

What information is in a Trust Registry vs the Object listed in the Registry :

- A link, reference or SAID is stored in the Registry for each object.
- Properties specific the object with respect to trust and trust status (e.g., is currently trusted, under review or revoked)
  - Links/references to any registry specific on how the object was acreditted
- Object data and access to that data is rovided by and integral to the object
  - It is expected that the Object must have integral ability to provide it's own authentic audit trail (ACDC lite)
- It is expected there is tight binding of the listed Object and the Registry such that a substitue will fail. For example, the SAID of the object is capable of proof of ownership of the PKI pair which produced the SAID crypto hash on demand (e.g., survives key rotation) - this is both a dynamic and static proof
  - e.g., the public key of the object is a property stored in the trust registry along with the object.

To put in ToIP terms, a Register is like (in concept) to a LDAP server (and its' protocol), which includes Active Directory, were in both cases, these directory servers are authorities of trusted data on network components and users as trusted entities from an Authentication and Authorization perspective.

What is new is the use of a cryptographic signing on the object's data, plus an audit trail and connection of both data processing and governance which are traceable to cryptographic and governance roots of trust.

Comment: Mattia if it's like LDAP, then there can be private data for individuals (as users in a User Registry)

Response: A key difference between LDAP and an SSI Registry is that - in the case of an individual (User)

a) The Registry will contain a list of User objects, where access to data within the User object is via the User Objects interface. This is in contrast to LDAP having personal data within the LDAP records themselves.

b) The Registry is a list of SSI and Data objects that have passed a series of requirements, specified by the Ecosystem that defines the trust criteria for objects of that class (e.g., Users, Issuers, Verifiers, ...). It also provides interface(s) to validate the trust/proof audit trail

Another question - (which will not be answered here) - is how will ToIPs view of a Trust/Verifiable Data Registry differ from those being developed elsewhere? That includes the (messaging protocol) and how ToIP will interoperate with other technologies

What determines trust? I is likely built on Verifiable Credentials and/or processes very similar to Verifiable Credentials that may involve a combination of KYC/E (Know Your Customer/Etity) governance and technical techniques (crypto signing), which are specified by each Ecosystem and may be an Out Of Band (OOB) process. Ultimately, this is likely a "business" validation process vs. a (purely) technical one.

Mattia - which is like a Certification authority - get a "green sticker" for your website if your - have to go through a business validation process to be issued an SSL Certificate

Neil: an example of a business process to issue an Identifier is the [GLEIF VLEI project.](https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei). the GLEIF organzation issues a verifiable Legal Entity Identfier, which a cryptographically verifiable Legal Entity Identifier which is globally unique number, which requires meeting business accreditation criteria.

Expectation of if I put my ID in a Trust Registry how do you avoid exposing personal information

Catalogs of DIDs (or verifiable identifier) - those identifiers

Partitioning of functionality of data access between TR and Trusted Entity.

Discussions on ToIP GitHub (you will need a GitHub account)
- [Trust Registries](https://github.com/trustoverip/tswg-trust-registry-tf/discussions)
- [Trust Spanning Layer](https://github.com/trustoverip/trust-spanning-protocol/discussions)

Governance will be "centralized' in that an ecosystem will defined the rules/accreditation on what objects can be listed in a Trust Registry

			Trust registries themselves will be distributed (replications) and will interact with each other by inter-registry trust protocols, rules and accreditation - so they are decentralized. Example. A Canadian Trust Registry may list entities that it lists based on a entry that was accredited by an EU registry. [Continuum Loop Blogs](https://www.continuumloop.com/blog/) - PodCasts and videos - [SSI Orbit Podcast - Trust Registries](https://www.continuumloop.com/ssi-orbit-podcast-trust-registries/) - [Trust Registries - Beyond the Basics](https://www.continuumloop.com/trust-registries-beyond-the-basics/) [eIDAS view on Trust Registries](https://sgmconsultingservices.com/wp-content/uploads/2022/04/Comments-on-ARF-Document-April-15-2022.pdf) suggest (in a eIDAS Wallet ARF - Architecture and Reference Framework suggests that a trust registry can be for multiple roles, including Verifier, Holder and Issuer. And frankly that could extend to any component, including an executable (e.g., selective disclosure processing toy
15 mins	Working relationships with other ToIP Task Forces and Working Groups	Chair	It's becoming clear that the big topics for ToIP WG/TFs in 2023, like Trust Registries and Trust Spanning Protocol, will need companion Governance TFs to provide Governance as a first-class deliverable (ToIP is a dual tech/gov stack). Given that a Trust Registry is a specialization of a Data Registry, which will have very high standards of verifiability, having the Data WG focus on this is a priority.
5 mins	Any other business		
5 mins	• Review decisions /action items • Planning for the next meeting	Chairs	

Screenshots/Diagrams (numbered for reference in notes above)

#1

Decisions

- Sample Decision Item

Action Items

- [ ] Sample Action Item