

Trust Registries Drafting Group

Objective

Good Health Pass compliant implementations must be able to quickly and safely verify authorized issuers and verifiers.

The term “trust registry” is not intended to suggest a specific solution to this problem. Rather, we use the term to suggest that – at the scale of the Good Health Pass digital trust ecosystem – some mechanism(s) will be required for verifiers to make this trust decision. Such a mechanism could be centralized, federated, or decentralized – or any combination that solves the problem.

The primary challenge of a centralized trust registry, operated by a single governance authority, is that it requires the trust of all verifiers. While this may be possible with a subset of verifiers in the Good Health Pass ecosystem, it is unlikely to work for all verifiers. However, a reasonably constrained set of centralized trust registries that collectively serve all verifiers might work.

Federated trust registries are another solution commonly used for PKI certificate chains. A root certificate authority (CA) self-signs its own digital certificate together with the certificates of its delegates. They, in turn sign the certificates of their delegates, and so on. Verifiers “walk the chain” back of digital certificates back to a root CA they trust. The World Health Organization has already indicated it intends to implement a federated public key directory (PKD) for its Smart Vaccination Certificates (SVCs).

Decentralized trust registries are a well-known solution in decentralized digital trust architectures. They are a particular focus of the Governance Stack Working Group (GSWG) at the Trust Over IP (ToIP) Foundation. The draft ToIP Governance Architecture specification recommends the use of trust registries that leverage decentralized identifiers (DIDs) based on the W3C DID Core 1.0 Specification. DIDs are cryptographically verifiable, globally unique identifiers that can be generated directly by an individual or organization for their own use and do not require the use of a centralized registry provider.

If authorized Good Health Pass credential issuers and verifiers have their own public DIDs, registered on an authorized verifiable data registry, DID-based trust registries can be implemented in several different configurations:

1. **Simple DID trust registries** are lists of the DIDs the issuers and verifiers authorized by a particular governance authority. They may be hosted on any suitable verifiable data registry designed by that governance authority.
2. **Federated DID trust registries** work the same way as conventional federated PKI registries, except that they use DIDs instead of digital certificates. Verifiers can walk the path of DIDs to the root DID of a governance authority they trust.
3. **DID web-of-trust registries** are a combination of simple DID trust registries and/or federated DID trust registries that have mutually-verifiable trust relationships (“cross-registrations”). Thus, they do not need to be organized into a specific hierarchy.

Key Resources:

- [GHPC Blueprint Outline v2](#) - The Trust Registries section is detailed on pages 25-26.

Terms of Reference

- **Key Questions** we need to answer:
 1. Is there a way to establish transitive trust between different subsets of the Good Health Pass digital trust ecosystem that can still result in global interoperability?
 2. If so, what is the recommended technical architecture to support this solution or solutions?
 3. How should this be reflected in the Good Health Pass Ecosystem Governance Framework and in any delegated governance frameworks?

Responsibilities and Deliverables

1. (TBC)

Chairs/Conveners

- Darrell O'Donnell - Chair
- Todd Gehrke - PM

Members

Only members of the Trust Over IP Foundation who have signed the necessary agreements and charters are permitted to participate in this Drafting Group and contribute to its deliverables.

Please add your name to the list below to indicate you have joined the Drafting Group:

- TBC

Meeting Schedule

The Drafting Group meets twice Weekly on Tuesdays and Thursdays at 7am PT/ (Weekly/Bi-Weekly) on (Day) at XY PT / XY UTC.

Meeting Page

Please find agendas, presentations, notes and recordings for all Drafting Group meetings [HERE](#).

Communications

The Slack channel for this Drafting Group (trustoverip.slack.com) is #ghp-wg-trust-registries