ToIP Governance Architecture Specification

This is the home page of the **ToIP Governance Architecture Specification**, a **draft deliverable** of the ToIP Governance Stack Working Group (GSWG). When this specification becomes a **ToIP Approved Deliverable**, it will be published as a PDF in the Tools and Specifications section of the ToIP website.

Contributors

To comply with the intellectual property rights protections in the charter of the ToIP Foundation (as required by all Joint Development Foundation projects hosted the Linux Foundation), all contributors to this draft deliverable MUST be current members of the ToIP Foundation. The following contributors each certify that they meet this requirement:

- Drummond Reed, Evernym
- Scott Perry, Scott S. Perry CPA PLLC

Terminology and Notation

The **keywords** "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

All terms appearing in **bold** on this page are listed in either the ToIP Core Glossary (based on the ToIP Core terms wiki) or the ToIP Governance Glossary (based on the GSWG terms wiki.) For more information see the Terms Wiki page of the Concepts and Terminology Working Group.

Purpose

The purpose of this ToIP **specification** is to specify the standard **requirements** that apply to all ToIP-compatible **governance frameworks** (GFs) regardless of their layer in the **ToIP stack**.

> **Note**
>
> The technical counterpart to this **specification** is the ToIP Technology Architecture Specification.

Motivations

The overall purpose of the **ToIP governance stack** is to enable users of the **ToIP technology stack** to make **trust decisions** (especially those requiring **tr ansitive trust**) based on GFs that include both **human-auditable requirements** and **machine-testable requirements**. While GFs are expected to be specialized for all four layers of the **ToIP stack**, certain interoperability **requirements** apply to all ToIP-compliant GFs regardless of layer. The goal of this **s pecification** is to specify those interoperability requirements in one place.

ToIP Governance Metamodel Specification

The GSWG has developed a single metamodel for GF documents called the **ToIP governance metamodel**. Because it brings together all **requirements** for the structure and content of ToIP-compliant GFs in one place, it is defined in a separate **specification**. All ToIP-compliant GFs MUST conform to the **re quirements** of the ToIP Governance Metamodel Specification.

Identification Requirements

To support **transitive trust** across trust boundaries, ToIP-compliant GFs and their components and **authorities** need to be identified by persistent, verifiable globally-unique identifiers.

1. The following MUST have **public DIDs** compliant with the ToIP Technology Architecture Specification:
    a. **Governing authorit(ies).**
    b. **Administering authority** (if any).

    c. **Primary document.**
    d. All **governed parties** fulfilling **roles** defined in the GF (e.g., **issuers**, **verifiers**, **trust registries**).
2. The following SHOULD have **public DIDs** or **DID URLs** compliant with the ToIP Technology Architecture Specification:
    a. Each **controlled document.**
    b. Each **policy**, **rule** or other normative subcomponent of a **controlled document.**
3. All **DIDs** and **DID URLs** specified in this section are subject to the following **policies**:
    a. The **DID** for a GF document MUST remain the same for all versions of the document it identifies.
    b. A new `versionId` parameter value MUST be assigned for every version of the identified document.
4. The GF MUST include one or more **policies** specifying the format for version identifier values and the **process** for assigning them.
    a. These **policies** SHOULD be the same for all versions of all documents in the GF.
    b. It is RECOMMENDED to use sequential integers for every version starting with "1".
    c. The use of minor version numbers (e.g., "1.1", "1.2", "1.3") is NOT RECOMMENDED.
5. A **DID URL** that includes a `resource` parameter with a value of `true` MUST return the identified document directly.
    a. If this **DID URL** does not include a `versionId` parameter value, it MUST return the current version of the identified document
    b. If this **DID URL** includes a `versionId` parameter value, it MUST return the identified version of the identified document.
    c. If this **DID URL** includes a `versionId` parameter value for a version that does not exist, it MUST return a "Resource Not Found" error.

Verification Requirements

To support the verifiability needed for **transitive trust**, the following verification **requirements** apply to ToIP-compliant GFs:

1. The **governing authority** SHOULD publish a digital signature in its current **DID document** over the hash of the current version of its **primary document**.
2. The **governing authority** or **administering authority** SHOULD:
    a. Register the public DID and all authorized **roles** for a **governed party** in a **trust registry**.
    b. Issue **verifiable credentials** to all **governed parties** serving in a **role** defined by the GF.
    c. Issue those same **verifiable credentials** in a publicly-available **credential registry** as specified by the GF.
3. If the GF includes **certification policies,** the qualified **certifying parties** SHOULD:
    a. Issue **certification credentials** to **governed parties** as directed by the GF.
    b. Issue those same **verifiable credentials** in a publicly-available **credential registry** as specified by the GF.

Transparency Requirements

To support the transparency needed for **transitive trust**, a publicly-available ToIP-compliant GF:

1. MUST be published at a publicly-accessible URL.
2. MUST have a **DID.**
3. MUST publish the following in the corresponding **DID document:**
    a. An `alsoKnownAs` property whose value is the publicly-accessible URL.
    b. The public key(s) for the DID.
    c. All **service endpoints** specified in the GF.
4. SHOULD be localized into all human languages required by its **trust community**.
5. SHOULD be accessible under the W3C Accessibility Guidelines.

Technical Interoperability Requirements

To support the interoperability needed for **transitive trust**, a publicly-available ToIP-compliant GF:

1. MUST specify technical interoperability **requirements** using ToIP **specifications** and **recommendations** whenever possible.
2. SHOULD specify any additional technical interoperability **requirements** using publicly available open standard **specifications** or **specification profiles**.