



TRUST
Over IP
FOUNDATION

ToIP Governance Metamodel Specification Companion Guide

Version 1.0

21 December 2021

This publicly available guide was approved by the ToIP Foundation Steering Committee on 21 December 2021.

The mission of the [Trust over IP \(ToIP\) Foundation](#) is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 300 organizational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Table of Contents

Document Information	4
Authors	4
Contributors	4
Revision History	4
Notations and Abbreviations Used in this Document.....	4
Terms of Use.....	5
1. Introduction	6
2. Purpose and Audience	7
3. Metamodel Structure and Versioning	8
3.1. Modular Architecture	8
3.1.1. Primary Document	8
3.1.2. Controlled Documents	9
3.1.3. Choosing the Structure.....	9
3.2. Versioning.....	9
4. Terminology Guidance	10
4.1. RFC 2119 Requirements Terminology.....	10
4.2. ToIP Requirements Terminology.....	11
4.3. ToIP Glossary Tools.....	12
5. Policy Drafting Guidance	13
5.1. Unique Addressability	13
5.2. Single Normative Statements.....	13
5.3. Nesting Policy Statements.....	13
5.4. Capitalized RFC 2119 Keywords	13
5.5. Informative (Non-Normative) Text	14
5.6. Example	14
5.6.1. Household Policies for Teenagers	14
6. Primary Document	15
6.1. Introduction.....	15
6.2. Terminology and Notation	15
6.3. Localization.....	16

6.4. Governing Authority	16
6.5. Administering Authority	17
6.6. Purpose	18
6.7. Scope	18
6.8. Objectives	19
6.9. Principles	19
6.10. General Requirements	20
6.11. Revisions	21
6.12. Extensions	22
6.13. Schedule of Controlled Documents	22
7. Controlled Documents	23
7.1. Glossary	23
7.2. Risk Assessment	23
7.3. Trust Assurance and Certification	24
7.4. Governance Requirements	24
7.5. Business Requirements	25
7.6. Technical Requirements	25
7.7. Information Trust Requirements	26
7.8. Inclusion, Equitability, and Accessibility Requirements	27
7.9. Legal Agreements	28
8. Additional Resources	28

Document Information

This specification was a deliverable of the [ToIP Governance Stack Working Group](#).

Authors

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

Contributors

- Sankarshan Mukhopadhyay — Dhiway Networks
- Taner Dursun — TUBITAK BILGEM
- Victor Syntez
- Karen Hand — Precision Strategic Solutions

Revision History

Version	Date Approved	Revisions
1.0	21 December 2021	Initial Publication

Notations and Abbreviations Used in this Document

Sections [2](#), [4.2](#), and [5.1](#) of this Companion Guide explain in detail the importance of **terminology** in drafting a **governance framework**. The [ToIP Concepts and Terminology Working Group](#) has developed special tools for this purpose. These tools will soon enable all defined **terms** within any **ToIP deliverable**, **governance framework**, or other documents to be linked directly to their entry in an associated **glossary**. Until these tools are fully operational, all defined **terms** in this Companion Guide will appear in **bold** and can be referenced in one of the ToIP **glossaries** listed in section [2.3](#).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#).

In addition, certain words, phrases, and abbreviations are used frequently enough in this document that we will define them once here. Note: these abbreviations will *not* appear in bold.

Abbreviation	Stands for
ToIP	Trust Over IP (and the ToIP Foundation)
GSWG	Governance Stack Working Group
TSWG	Technology Stack Working Group
CTWG	Concepts and Terminology Working Group
GF	governance framework

Terms of Use

These materials are made available under and are subject to the Creative Commons Attribution 4.0 International license (<http://creativecommons.org/licenses/by/4.0/legalcode>).

THESE MATERIALS ARE PROVIDED "AS IS." The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series ("ToIP"), and its members and contributors (each of ToIP, its members and contributors, a "ToIP Party") expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1. Introduction

The mission of the Trust over IP Foundation (ToIP) is to define a complete architecture for Internet-scale digital trust that enables interoperable **digital trust ecosystems** of all types and sizes. A hallmark of this architecture is that it combines the “tools” for technical interoperability with the “rules” individuals and organizations need to meet their legal, business, and social requirements for trust.

In digital trust infrastructure, these “rules” are formally known as a **governance framework** (GF). A core thesis of ToIP architecture is that interoperability of GFs is just as important—if not more so—than interoperability of the technical protocols. This is the rationale for the “dual stack” design of ToIP shown in figure 1. For more about this design, see the [Introduction to ToIP](#) white paper and the [Design Principles for the ToIP Stack](#).

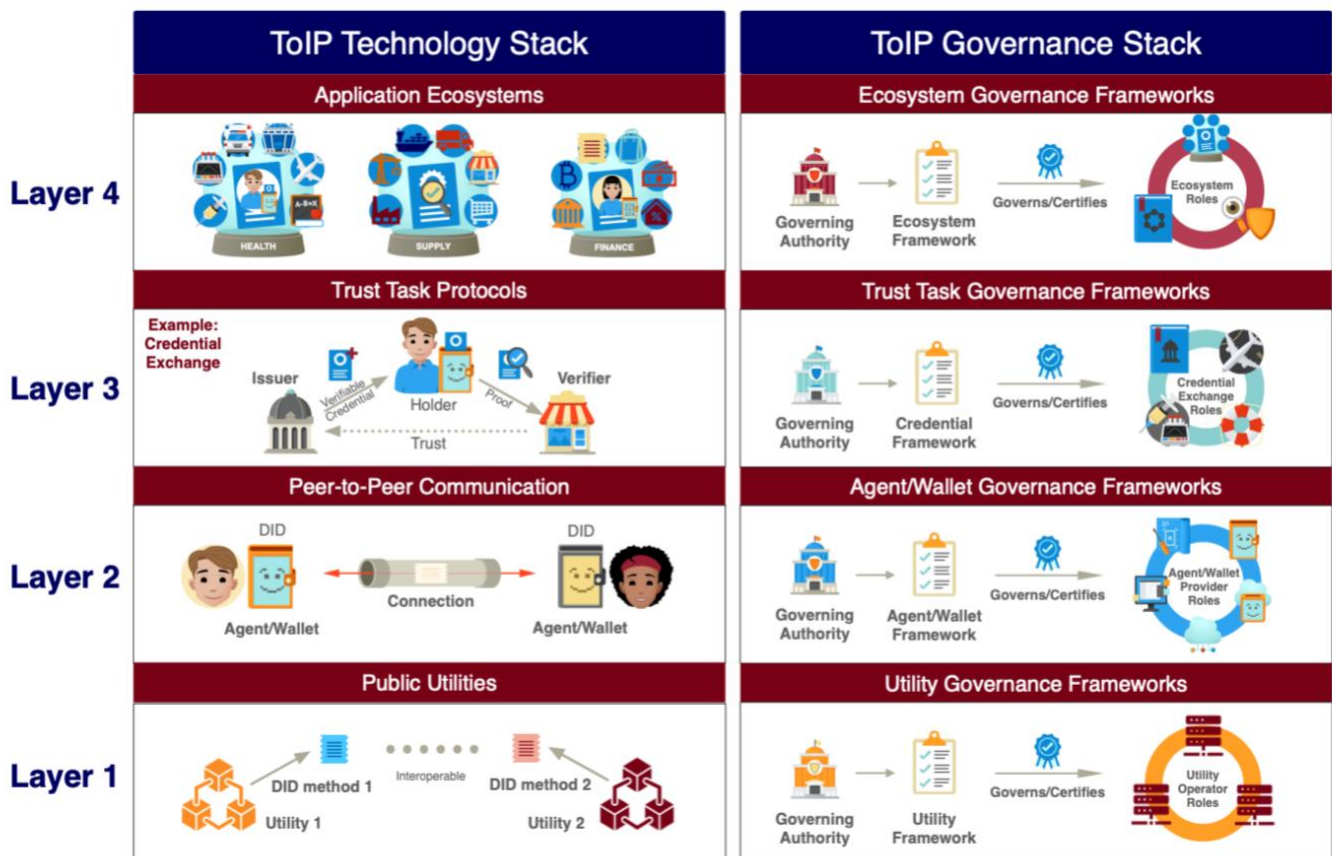


Figure 1. The ToIP Stack

Although figure 1 shows four different kinds of GFs at the four different layers, ToIP determined that the foundation for all ToIP-compliant GFs should be set forth in two specifications:

1. The [ToIP Governance Architecture Specification](#) which defines how the ToIP governance stack interoperates with the ToIP technology stack.
2. The [ToIP Governance Metamodel Specification](#) which defines the requirements common to all ToIP-compliant GFs.






2. Purpose and Audience

The purpose of this document, the **ToIP Governance Metamodel Companion Guide**, is to serve as the “user’s manual” for the [ToIP Governance Metamodel Specification](#). The audience is authors who need to design, draft, review, and publish a ToIP-compliant GF at any of the four layers of the **ToIP stack** (utility, agent/wallet, credential, ecosystem).






A good analogy is the construction of a house or an office building. First, an architect needs to construct plans and drawings—*blueprints*—so that a coordinated group of tradesmen, typically led by a general contractor, can construct the building. These blueprints must *themselves* follow a set of standards—layout, measurements, symbols, even pen color—so that contractors, tradesmen, suppliers, and even building inspectors can all read and interpret them the same way.

A governance framework (GF) is a *blueprint for building a digital trust community* based on the **ToIP stack**. [The ToIP Governance Metamodel Specification](#) is a set of standards for these blueprints. This guide is a handbook for how to use these standards.

A secondary purpose of this guide is to serve as a tool in the development of (ToIP stack) **layer-specific templates** for each of the four layers of ToIP GFs. Each template defines a specific instance of the metamodel that includes:

-  Standard ToIP **roles** for that layer.
-  Standard ToIP **processes** in which **actors** in those roles will be engaged.
-  Recommended **requirements** for those **processes**.
-  Standard **risks** against which **risk assessment** should be performed; and
-  Standard elements of a **trust assurance framework** to address those **risks**.

The intended audience for this document includes:

-  **Governing authorities** (of any kind) and their architects, e.g., governments, NGOs, industry consortia, associations, etc.
-  Enterprise CIOs, CISOs, Chief Privacy Officers, Chief Identity Officers, Chief Trust Officers, professional auditors, and other architects of enterprise-level GFs.
-  Identity management professionals designing and building decentralized identity systems (aka “self-sovereign identity” or “SSI”).
-  Service providers participating in ToIP **digital trust ecosystems** and all layers of the ToIP **governance stack**; and
-  Standards bodies and researchers interested in GF architecture and design.

3. Metamodel Structure and Versioning

The ToIP Governance Metamodel has been engineered to meet several goals:

1. To standardize—as much as feasible—the artifacts needed for GFs to succeed in meeting the needs of a diverse set of **trust communities**.
2. To modularize the structure of the artifacts within a GF so **policies, rules** and **controlled documents** can be developed, maintained, and reviewed in the most efficient manner.
3. To standardize the identification and versioning of governance artifacts so both humans and machines can precisely reference the **policies** and **rules** in effect at any one point in time.

3.1. Modular Architecture

The modular architecture of the ToIP **governance metamodel** consists of two main parts:

1. A **primary document** with a standard set of sections.
2. A set of optional **controlled documents** representing standard categories of more detailed GF components.

The main reason for this modular architecture is so the **primary document** and each **controlled document** can be managed and versioned separately. This design enables incremental revisions to be made to specific components of the GF without needing to create a new version of the entire set of documents.

The overall structure of the **primary document** and **controlled documents** is shown below.

3.1.1. Primary Document

1. Introduction
2. Terminology
3. Localization
4. Governing Authority
5. Administering Authority
6. Purpose
7. Scope
8. Objectives
9. Principles
10. General Requirements
11. Revisions
12. Extensions
13. Schedule of Controlled Documents

3.1.2. Controlled Documents

1. Glossary
2. Risk Assessment
3. Trust Assurance and Certification
4. Governance Requirements
5. Business Requirements
6. Technical Requirements
7. Information Trust Requirements
8. Inclusion, Equitability, and Accessibility Requirements
9. Legal Agreements

3.1.3. Choosing the Structure

Every ToIP-compliant GF **MUST** have a **primary document** even though some sections within it are **OPTIONAL**. With a few exceptions, the **controlled documents** are **OPTIONAL** depending on the needs of the **governing authority**.

For a relatively simple GF, it is possible for the relevant **controlled documents** to be logically included within the **primary document** as appendices. However, when a **controlled document** involves sufficient complexity—or when it might need to be revised independently of the rest of the GF—it is **RECOMMENDED** to maintain it as a separate **controlled document**.

3.2. Versioning

The [ToIP Governance Architecture Specification](#) requires that, in order to maintain cryptographically-verifiable [permalinks](#) to GF artifacts:

1. The **primary document** of a ToIP-compliant GF **MUST** be identified with a **DID**.
2. Each **controlled document** **MUST** be identified with either:
 - a) Its own **DID**, or
 - b) A **DID URL** based on the **primary document DID**.
3. Each version of the **primary document** and each **controlled document** **MUST** be identified with a **DID URL** using the versioning syntax in the [W3C Decentralized Identifiers \(DIDs\) 1.0](#) specification.

It is therefore important that strict version control be maintained across all component documents in a GF. The procedure for issuing DIDs, DID URLs, and version identifiers for these documents will depend on the DID method(s) supported by your GF. Consult your DID method specification, your technical architects, and the TSWG for more guidance.

4. Terminology Guidance






4.1. RFC 2119 Requirements Terminology

The Internet Engineering Task Force (IETF), the granddaddy of Internet standards bodies, issues standards called Request for Comments (RFCs). The most widely-cited is [RFC 2119](#)¹ because it defines **keywords** for use in all other RFCs—terms that are used with precision to define conformance levels for specific **requirements**.

ToIP-compliant GFs **MUST** incorporate the following paragraph in their **primary document**. Note that the more recent update to RFC 2119, [RFC 8174](#)², updates this text to clarify that whenever an RFC 2119 **keyword** is used normatively it **MUST** in uppercase:

The key words "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.

RFC 2119 defines these keywords as follows:

-  **MUST:** This word, or the terms "**REQUIRED**" or "**SHALL**", mean that the definition is an absolute requirement of the specification.
-  **MUST NOT:** This phrase, or the phrase "**SHALL NOT**", means that the definition is an absolute prohibition of the specification.
-  **SHOULD:** This word, or the adjective "**RECOMMENDED**", means that there **MAY** exist valid reasons in particular circumstances to ignore a particular item, but the full implications **MUST** be understood and carefully weighed before choosing a different course.
-  **SHOULD NOT:** This phrase, or the phrase "**NOT RECOMMENDED**" means that there **MAY** exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications **SHOULD** be understood, and the case carefully weighed before implementing any behavior described with this label.
-  **MAY:** This word, or the adjective "**OPTIONAL**", means that an item is truly optional. One vendor **MAY** choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor **MAY** omit the same item.

As you have seen, even though this Companion Guide is *not* normative, it will use RFC 2119 keywords in UPPERCASE to illustrate how this nomenclature should be used.

¹ <https://datatracker.ietf.org/doc/html/rfc2119>

² <https://datatracker.ietf.org/doc/html/rfc8174>

4.2. ToIP Requirements Terminology

The [ToIP Governance Metamodel Specification](#) defines the ToIP Governance Requirements Glossary containing the following additional terms describing requirements.

requirement	In the context of a governance framework (GF), a requirement states a condition that an actor (human or machine) must meet in order to be in conformance.
mandatory	A requirement expressed using one of the following RFC 2119 keywords : "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT".
recommendation	A requirement expressed using one of the following RFC 2119 keywords : "SHOULD", "SHOULD NOT", "RECOMMENDED".
option	A requirement expressed using one of the following RFC 2119 keywords : "MAY", "OPTIONAL".
human-auditable requirement	A requirement expressed in a human language that can only be fulfilled by a human actor performing a set of processes and practices against which conformance can only be tested by an auditor of some kind. In a ToIP-compliant governance framework , human-auditable requirements are expressed as policies .
machine-testable requirement	A requirement written in a machine-readable format such that conformance of a software actor implementing the requirement can be tested by an automated test suite or rules engine . In a ToIP-compliant governance framework , machine-readable requirements are expressed as rules in a rules-based language .
policy	A human-auditable requirement that specifies some set of processes and practices that an actor must follow in order to be in conformance with the requirement .
process	A specified set of actions that an actor must take in order to be in conformance with a policy . A process may consist of a set of practices .
practice	A specified activity that an actor must perform as part of a process .
rule	A machine-testable requirement written in a machine-readable language that can be processed by a rules engine .
specification	A document or set of documents containing any combination of human-auditable requirements and machine-testable requirements needed to produce interoperability amongst implementers. Specifications may be included in (as controlled documents) or referenced from a governance framework .

4.3. ToIP Glossary Tools

It is extremely important to use clear, accurate, well-defined terminology in the GF. This is the reason the very first **controlled document** we suggest is the [Glossary](#) (see [section 7.1](#)).

Although a trust community is free to develop its glossary using any tools or techniques its needs, it is the responsibility of the [ToIP Concepts and Terminology Working Group](#) (CTWG) to develop tools and best practices for this purpose.

The CTWG has created a **glossary** development tool called [terms wikis](#). This tooling uses [the built-in wiki capability of GitHub repositories](#) together with CTWG-developed open-source software called the *ToIP Term Tool* to make it easy for any **terms community** to develop and maintain **terminology** for use in **ToIP deliverables**, GFs, or any other ToIP-related documentation.

The ToIP **terms community** along with several ToIP Working Groups have already used this tooling create the following **glossaries** that provide ToIP standard **terms** for use in the GF:

Glossary	Terms Wiki	Purpose
ToIP Core Glossary	ToIP Core terms wiki	Terms intended to have the same meaning across all ToIP-related documents
CTWG Glossary	CTWG terms wiki	“Bootstrap” terms for describing the structure and operation of terms wikis and glossaries
GSWG Glossary	GSWG terms wiki	Terms that have a specific meaning in the context of the ToIP governance stack

Additional specialized glossaries from other ToIP Working Groups, Task Forces, and related **terms communities** are listed in the registry on the [CTWG Terms Wikis page](#).

Even with these standard glossaries already available, development of additional specialized terms needed for a specific GF is a significant component of the work. Please see the [CTWG Terms Wikis page](#) for further instructions about how to use the CTWG tooling to streamline efforts.

5. Policy Drafting Guidance

Aside from general explanatory information or instructions, most of the content of a **primary document** and most **controlled documents** are **policies**. This section contains specific recommendations for **policy** drafting.

5.1. Unique Addressability

The [ToIP Governance Metamodel Specification](#) requires that each individual **policy**, **rule**, or other normative statement within a **primary document** or a **controlled document**:

1. **MUST** be uniquely identifiable with a human-readable addressable identifier.
 - a. For section headings within a document, it is RECOMMENDED to use both a unique number and name.
 - b. For individual policy statements, it is RECOMMENDED to use a unique number.
2. **SHOULD** be uniquely machine addressable with a **DID URL** (i.e., using a [digital bookmark](#) within the document that can be added as a fragment to the **DID URL**).

5.2. Single Normative Statements

To foster clarity and avoid confusion, it is RECOMMENDED to use only one RFC 2119 **keyword** within each uniquely addressable **policy** statement. If a policy needs to use two or more **keywords** (e.g., a **MUST** and a **MAY**), simply break it into nested **policy** statements (see examples below).

5.3. Nesting Policy Statements

It is RECOMMENDED to nest numbered/named policy statements whenever a **policy** contains multiple or branching **requirements**. See the examples in section 5.6 below.

5.4. Capitalized RFC 2119 Keywords

RFC 2119 **keywords** **MUST** be capitalized when using it normatively. This not only makes it easier for readers to spot normative **requirements**, but it also eliminates any ambiguity about whether a keyword is normative.

5.5. Informative (Non-Normative) Text

Whenever it is helpful to clarify the context, purpose, intent, or usage of a **policy** by including informative text that is NOT normative, the RECOMMENDED best practices are:

1. *Place the informative text in its own separate sentence, paragraph, or callout.* A common example is including a standalone introductory paragraph immediately after a numbered/named section heading. This is typically followed by named/numbered policy statements.
2. *Never use RFC 2119 **keywords** in informative text.* This avoids confusion with normative policies or rules. If necessary, use some other synonym for a keyword (e.g., “essential” instead of “required”).

5.6. Example

Following is a fictional example of **policy** statements illustrating these recommendations:

5.6.1. Household Policies for Teenagers

These **policies** apply to all household members attending secondary schools (“teenagers”).

5.6.1.1. Waking Up

1. Teenagers:
 - a) **MUST** be out of bed by one hour before departure for school.
 - b) **SHOULD** plan ahead and set an alarm prior to bedtime.
 - c) **MAY** ask their parents to wake them up. Such a request:
 - (1) **MUST** come before the parent’s scheduled bedtime.
 - (2) **SHOULD** come no later than dinnertime of the previous night.
2. If not out of bed on time
 - a) Each week, teenager **SHALL** receive one warning and **MUST** perform additional household chore.
 - b) If it happens a second time in the same week, teenager **SHALL** lose one-half of his/her weekly allowance.

5.6.1.2. Making Their Bed

1. Teenagers **MUST** ensure their beds are made prior to departure for school unless they have verbal permission of an exception from at least one parent.
2. If teenager does not make their bed in the morning, they **MUST** be assigned additional chore for the week (no matter whose turn it is).
3. Teenagers **MAY** contract for a sibling to make their bed.
 - c) A parent **MUST NOT** be responsible for enforcing such contract.
 - d) If the sibling does not follow contract terms, the teenager **MUST** still make their bed.

6. Primary Document

The following sections contain guidance for the completion of governance framework sections according to the [ToIP Governance Metamodel Specification](#). The first requirement is that all ToIP-compliant GFs **MUST** have a primary document. From a Web architecture perspective, this serves as the "home page" for the GF.

Like a home page on the Web, the **primary document** is very likely to be the most-read document in the GF. Therefore, it **SHOULD** be as readable and understandable as possible. This section provides more information and recommendations about each section within the **primary document**. Note that:

1. All sections are normative except the Introduction section.
2. Some sections are optional depending on the usage of a particular GF.

6.1. Introduction

The purpose of this section is simply to orient readers and give them the "big picture" of a particular GF. This is the only section of the document that is purely informative, (i.e., this section **MUST NOT** contain any RFC 2119 **keywords** or normative **policy** statements). It is **RECOMMENDED** to keep it relatively short—ideally just a few paragraphs, but not more than a page.

This section:

1. **SHOULD** contain references to other explanatory materials that will help readers understand the context, purpose, and process surrounding this GF, particularly:
 - a. Websites or microsites about the GF and the governing authority.
 - b. Any white papers about the GF and the **trust community**.
2. **SHOULD** reference the [ToIP Foundation](#), the **ToIP stack**, and the specific version of the **ToIP governance template** upon which the GF is based (if any).
3. **MAY** include an "Acknowledgements" section thanking contributors to the GF.

6.2. Terminology and Notation

Terminology is critically important for all aspects of the **ToIP stack**, but especially in GFs, where **terms** must be accurately understood and interpreted by all stakeholders—from technical architects and developers to lawyers and policymakers.

In the **primary document**, this section normatively defines the terminology used throughout the GF. The [ToIP Governance Metamodel Specification](#) states the following **requirements** for this section. It:

1. MUST explicitly specify the use of the ToIP Governance Glossary (see the [Glossary](#) section above).
2. MUST reference a Glossary **controlled document** (if there is one) for all other **terms** (see the [Controlled Documents](#) section).
3. MAY specify that terms specific to one **controlled document** are defined in that **controlled document**.
4. MUST specify that all RFC 2119 **keywords** used normatively with their RFC 2119 meanings are CAPITALIZED.
5. SHOULD specify any other formatting, layout, or notation conventions used in the **primary document** or **controlled documents**.

As discussed in [section 4.3](#), the [ToIP Concepts and Terminology Working Group](#) (CTWG) has developed tools and best practices to assist in this endeavor. Although the work of the CTWG is ongoing, the best practices it currently recommends are:

1. Use the CTWG's [terms wiki](#) infrastructure to develop the **glossary**.
2. If a **term** is needed to apply to the **ToIP stack** as a whole (and better to use the ToIP definition), include that term from the [ToIP Core terms wiki](#). If that term does not exist yet, please contact the CTWG via the ToIP Slack [#concepts-terminology-wg](#) channel to request that it be added.
3. If specialized **terms** are needed for its own [terms community](#)—and most GFs do—it is RECOMMENDED that an associated [terms wiki](#) is created. It takes only minutes to set up and will give contributors a powerful collaboration tool for collectively developing and generating a distinct **glossary**. See the [CTWG Terms Wiki](#) page for more information.

6.3. Localization

This section is for specifying the official language and translations for the GF. [The ToIP Governance Metamodel Specification](#) requirements for this section are very straightforward—it:

1. MUST specify the official language or languages for the GF.
2. SHOULD use an [IETF BCP 47 language tag](#) to identify each official language.
3. SHOULD specify and provide links to all official translations of the GF.
4. SHOULD specify the **policies** and/or **rules** governing the production of translations.

If usage of the GF is limited to one **jurisdiction** with a fixed language or languages, this will be very simple. On the other hand, if the GF operates globally, consider policies for publishing translations rapidly whenever there is an updated version.





6.4. Governing Authority

The **governing authority** is the **party** legally responsible for developing, maintaining and implementing a GF. Every GF has a **governing authority** regardless of the legal form that **party** takes—government agency, corporation (for-profit, non-profit, benefit corporation, etc.), partnership, association, [decentralized autonomous organization](#) (DAO), or any other formal or informal organizational structure.

The [ToIP Governance Metamodel Specification requirements](#) for this section are defined into two distinct parts:

1. *Information identifying the legal entity and all necessary contact information.* Note that it is HIGHLY RECOMENDED to use a [Legal Entity Identifier \(LEI\)](#) as defined by the [Global Legal Entity Foundation \(GLEIF\)](#).
2. *Information about official publication of the GF.* This includes a list of recommendations for the GF website.

Although a dedicated GF website is optional, the following are RECOMMENDED best practices:

-  Publish a [microsite](#) dedicated to the GF with its own URL and landing page.
-  Include separate HTML pages **and** PDFs for the **primary document** and all **controlled documents**.
-  Post a zip file with the full set of PDFs to make it easy to download a local copy of all the documents (as the legal teams for **governed parties** will want to do).
-  If the GF has an associated **trust mark**, display it prominently on the home page and build it into templates for all other pages.

6.5. Administering Authority

In most cases, a **governing authority** will administer its own GF. However, in some cases the **governing authority** may delegate this job to a separate **administering authority**. For example, a government agency responsible for a particular GF might contract with a non-governmental organization (NGO) to handle day-to-day administration.

If that is not the case, skip this section.

If the GF does have a separate **administering authority**, in this section provide the same type of legal identification and contact information as for the governing authority.




Please clearly state the duties of the **administering authority** and the operational **policies** it must follow. It is important to clearly establish the separation of **roles** between the **governing authority** and the **administering authority**.

6.6. Purpose

The purpose statement is intended to be a very concise summary of the reason the GF was created. Ideally it should be a single sentence, but in no case should it be no longer than one paragraph.

6.7. Scope

Many technical specifications include a scope section that defines as precisely as possible what problem areas are in and out of scope. The same should be done with a GF. Understanding what the GF does and does not cover helps:

-  **Verifiers** and other **relying parties** know what types of **trust decisions** the GF will and will not help them make.
-  **Governed parties** know what **roles** are and are not governed by the GF, and what the duties and responsibilities are for each.
-  **Auditors** know what is inside and outside the boundaries of the **trust community**.

When crafting statements about what is explicitly in scope, consider the following:


1. The key **roles** the GF defines (e.g., issuers, verifiers, insurers, auditors).
2. The key **processes** the parties in these roles will be undertaking (e.g., issuance, verification, underwriting, certification).
3. The key artifacts the GF will be governing (e.g., distributed ledgers, wallets, credentials, trust registries).
4. The types of **trust decisions** the GF is ultimately intended to help parties make.

It is also RECOMMENDED to explicitly specify what is *out-of-scope*. As with technical **specifications**, the exercise of determining what will *not* be covered often helps bring clarity about what should be covered. This is also an opportunity to declare what features or **policies** are planned to be included in future revisions.


6.8. Objectives


The [Scope](#) section defines the boundaries of the GF—what is “in” and what is “out”. The Objectives section is where the concrete outcomes that are trying to be achieved with the GF is stated.


In defining **objectives**, it is RECOMMENDED to use the generally accepted SMART framework: Specific, Measurable, Achievable, Relevant, and Time-Bound³.


 **S: Specific** - In order for an **objective** goal to be effective, it needs to be specific. Do not be afraid to dig into nitty-gritty details. Answer the following questions:

- ❖ What needs to be accomplished?
- ❖ Who is responsible for it?
- ❖ What steps will be taken to achieve it?

 **M: Measurable** — Quantifying **objectives** makes it easier to identify when they have been achieved. Examples might be the number of **issuers** or **verifiers** registered, the number of **credentials** issued, the percentage of **digital wallets** in active use, the decrease in fraud rates.

 **A: Achievable** — **Objectives** should be realistic and attainable — not lofty sky-high targets. Limitations should be carefully considered. GF architects should ask: “Does the GF have the capacity to accomplish this goal?”

 **R: Relevant** — Every outcome should achieve a tangible benefit that provides a serious incentive for some set of participants in the **trust community**. The clearer the benefits, the stronger the stakes for stakeholders.

 **T: Time-bound** — Solid **objectives** do not stretch into infinity—they have an achievable time, horizon, or deadline. Do not hesitate to put stakes in the ground— one, three, five, ten years—so stakeholders know what to expect when.

Lastly, the **objectives** MUST be consistent with the [principles](#).

6.9. Principles

The balance of the GF will consist primarily of **policies**—**human-auditable requirements** expressed using RFC 2119 **keywords**. Each **policy** specifies one or more behaviors the members of the **trust community** agree to follow to achieve the mutual **objectives**.

But before drafting the **policies**, first draft the **principles**. The key difference is that a **principle** is not something against which can directly measure conformance. Rather it states a proposition or a value that is useful in guiding or evaluating the behavior the GF wants to achieve. In short, “**principles** guide **policies**”.

For example, if one of the **principles** is: “Transparency”, it suggests that the GF should include **policies** such as, “All meetings MUST be open to the public” or “All meeting minutes MUST be posted to the public website”.

Other tips on drafting **principles**:

³ <https://www.atlassian.com/blog/productivity/how-to-write-smart-goals>

1. *Keep them short.* Many **principles** can be captured in a single word. Almost any good **principle** can be stated in a single sentence.
2. *Reuse existing principles whenever possible.* No need to reinvent the wheel. Certain **principles**, such as the [Principles of SSI](#), are **ToIP Approved Deliverables** for this very purpose. If some or all the **principles** are already stated in other public documents or GFs, just include references to those.
3. *Test the principle* by seeing if it can answer the question: “If we adopt this **principle**, what must we start doing and/or what must we stop doing?” Try writing a few policies that reflect the proposed **principle**—and then a few **policies** that would break the **principle** (and make sure these counterexamples are indeed unwanted).
4. *Make them timeless.* Good **principles** are enduring—they don’t change with political winds or market conditions.
5. *Make them stand alone.* Avoid overlapping **principles**. The fewer **principles**, the better. Avoid compound **principles**.
6. *Omit needless words.* With apologies to Steve Krug and Chapter 5 of his book on usability: [Don’t Make Me Think](#)⁴.
7. *DO NOT use capitalized [RFC 2119](#) keywords.* **Principles** are NOT normative statements. If an RFC 2119 keyword is used, make sure it is lowercase.
8. **Co-create principles.** The more stakeholders are involved in the trust community in the drafting of **principles**, the better they will work in practice.

Two examples of well-written sets of principles are the Principles of SSI⁵ and the UK Government Digital Service Design Principles.⁶

6.10. General Requirements

The sections up to this point have defined the “superstructure” of the GF. This section is the beginning of the main content—formal **policy** statements.

IMPORTANT: Most **policies**—those that apply to specific **roles**, responsibilities, and functions—should be specified in [controlled documents](#) (see below). This [General Requirements](#) section should be reserved for **policies** that apply generally *to the GF as a whole*, and not just in the context of a particular **controlled document**.

Many GFs have very few general **requirements**. Here are a few tests that can be applied to determine if a **policy** belongs in this section:

1. The **policy** does NOT naturally fit into one of the categories for which there is a **controlled document**.
2. The **policy** applies generally to the entire **trust community**.

⁴ <https://www.amazon.co.uk/Dont-Make-Me-Think-Usability/dp/0321344758>

⁵ <https://sovrin.org/principles-of-ssi/>

⁶ <https://www.gov.uk/guidance/government-design-principles>

3. The **policy** applies to the structure of the GF itself, e.g., it states what **controlled documents** must be specified by whom and applied to whom (but is not a **policy** about amending or extending the GF—those belong in the next two sections).
4. The **policy** guides or constrains more specific **requirements** within the GF's **controlled documents**.

In addition, the [ToIP Governance Metamodel Specification](#) requires this section to include:

1. [Responsible use policies](#) that apply generally to infrastructure governed by the GF.
2. Regulatory compliance **policies** that are not specified within particular **controlled documents**; and
3. A [Code of Conduct](#), if applicable and not included in the legal documents section, that applies to **trust community** members.

6.11. Revisions

A key design **principle** of the **ToIP stack model** (see [Design Principles for the ToIP Stack](#)) is to “design for change”. In most cases GFs are “living documents” that need to evolve as their **trust community** evolves. Therefore, the [ToIP Governance Architecture Specification](#) has strict requirements for document versioning.

This section SHOULD include the **policies** that specifically govern how any revisions or amendments to the GF will be developed, reviewed, and approved. The [ToIP Governance Metamodel Specification](#) requires these **policies** to also specify how all new versions will be identified with a **DID URL**.

It also RECOMMENDS that at least one public review period is held for any GF that will be available to the public. This is consistent with the advice provided throughout this Companion Guide to *involve stakeholders as much as possible in the GF development and review process*, so their needs and interests are incorporated to the greatest extent possible.

This section SHOULD NOT contain any other types of **governing authority policies**—those should be defined within controlled documents in the General Requirements (section 6.10) or controlled documents (section 7) which specify policy requirements.

6.12. Extensions

The goal of the **ToIP model** for decentralized digital trust infrastructure is enabling online **transitive trust** relationships. A key aspect of this interoperability is enabling GFs to “plug in” to each other to maximize the synergy across **trust communities** that are aligned.

While it is not necessary for two or more ToIP-compliant GFs to be explicitly designed to work together, in order to enable **transitive trust** relationships (the baseline of interoperability is achieved by the **ToIP stack** itself) a higher level of interoperability can be achieved if one GF is explicitly designed to “plug in” to another. The GF aligned to “plug in” is called an **extension GF** and the GF being extended is called the **base GF**.

A common example is an **ecosystem GF** that can be extended by new **credential GFs** that add new credential types into the ecosystem.

Any **base GF** that accepts **extension GFs** requiring explicit approval by the **governing authority** **MUST** include **policies** in this section governing:

1. Any **requirements** the **extension GF** must meet for approval.
2. The **process** under which the **extension GF** can be approved.
3. How to register, activate, and deactivate an approved **extension GF**.
4. How the **trust community** shall be notified of activation or deactivation of an **extension GF**.

6.13. Schedule of Controlled Documents

If applicable, the concluding section of the **primary document** **MUST** be an authoritative listing of all **controlled documents** included in the GF. This fulfills the modular architecture explained in section 3.1. It also enables the **primary document** to effectively serve as the “home page” for the entire GF, which adapts well to publishing the GF on a microsite. The **primary document** page can link to all the other **controlled document** pages.

The [ToIP Governance Metamodel Specification](#) requires that this section:

1. **MUST** include authoritative references to all **controlled documents** in the GF.
2. **MUST** identify the exact version of each **controlled document** with a unique, permanent **DID** or **DID URL**.
3. **SHOULD** include a web link to each **controlled document** in the web version of the GF.
4. **SHOULD** include a brief description of the purpose and scope of each **controlled document** to make it easy for readers to navigate the GF.

7. Controlled Documents

7.1. Glossary

[Section 4.3](#) stressed the importance of **terminology**. In the fields of **digital identity**, trust, and **governance**, a well-defined glossary is essential. It is the only way to ensure that all stakeholders— business, legal, technical, operational—share a common understanding of the **terms** used within a GF.

It is strongly RECOMMENDED that a GF includes a **glossary** published as a separate **controlled document** that includes **terms** in the following three general categories:

1. *ToIP core terms* that describe the common components of the ToIP model and MUST be used consistently across all **ToIP deliverables** and ToIP-compliant GFs. These terms are defined in the [ToIP Core Glossary](#).
2. *ToIP governance terms* are specialized **terms** used to describe ToIP governance concepts. They are defined in the [ToIP Governance Glossary](#) (which includes the ToIP Governance Requirements Glossary reproduced in [section 4.3](#)).
3. *GF-specific terms* are **terms** only needed in the context of the GF's specific **trust community**. For these, it is RECOMMENDED to create a separate [terms wiki](#) to publish the GF-specific **glossary**.

Note that ToIP's CTWG [terms wiki](#) tooling enables the combination of terms from all three of these categories into a single document that can serve as the GF's glossary.

Please see the [CTWG Terms Wiki page](#) for further instructions and guidance about creating a GF **glossary**.

7.2. Risk Assessment

The purpose of a GF is to define the **policies** and **rules** the members of a **trust community** agree to follow to minimize the **risks** to achieving their **objectives**. There are **risks** associated with every facet of establishing and maintaining a healthy **trust community**: technical risks, business risks, governance risks, regulatory risks, etc. Assessing the nature and severity of these **risks** requires understanding the potential **threats**: purposeful attacks, human or machine errors, structural failures, environmental disruptions, or any other known or unknown vulnerability that can harm the trust community—and harm its **reputation**.

Therefore, it is strongly RECOMMENDED that the first **controlled document** category developed for the GF along with the **glossary** should be **risk assessment**. ToIP has developed two tools for this purpose: the [ToIP Risk Assessment Worksheet Template](#) and the [ToIP Risk Assessment Companion Guide](#). Please see these two documents for detailed recommendations about how to perform an ISO 27005 (or compatible) **risk assessment**.

7.3. Trust Assurance and Certification

The **risk assessment** ([section 7.2](#)) category will guide the **policies** and **rules** in the GF that **governed parties** need to follow to mitigate against those **risks**. But how are **governed parties** held accountable for compliance? That is the purpose of the *Trust Assurance and Certification* **controlled document**. It specifies the **trust assurance framework**—and if applicable, the **certification** program—by which the GF’s trust community can evaluate the compliance of any particular **governed party**.

ToIP has created two tools for guidance on this topic: the [ToIP Trust Assurance and Certification Template](#) and the [ToIP Trust Assurance Companion Guide](#). Please see these for our in-depth recommendations about American Institute of Certified Public Accountants (AICPA) [trust service categories](#), **roles**, **processes**, **trust criteria**, **trust evidence**, and **levels of assurance**. Also, if the GF includes a **trust mark**, this **controlled document** should also cover the policies for its use.

7.4. Governance Requirements

Trust in a GF begins with trust in its **governing authority**, whatever form that entity may take (see [section 6.4](#) for more details). That trust is rooted in the foundational governance documents for the governing authority itself. Depending on its legal form, these may include:

-  Legislative Acts
-  Charters
-  Bylaws
-  Articles of Incorporation
-  Operating Rules
-  Criteria and Methodologies (“Crits and Methods”)
-  Rules of Order
-  Antitrust Policies
-  Intellectual Property Rights Policies
-  Confidentiality Policies
-  Dispute Resolution Policies
-  Conflict of Interest Policies
-  Codes of Conduct

If these documents already exist and are publicly available—especially via the Web— it is not necessary to include actual copies. A list of links with capsule summaries of the contents of each document will suffice.






If a new governing authority is being created along with the GF, designing the best practices for its governance is a rich and complex topic beyond the scope of this Companion Guide. However, the GSWG has produced two documents to assist in reviewing and assessing how all parts of the GF can work together to provide good governance: the [ToIP Governance Framework Matrix](#) and the [ToIP Governance Framework Matrix Companion Guide](#). It is RECOMMENDED to use these tools at the outset of the GF drafting process to help consider all aspects of governance.

7.5. Business Requirements

Many business requirements will flow directly from **objectives** as discussed in section 6.8. The policies in this category will be the kind of **business rules** common to any business or industry organization. The difference is that these business rules apply in the specific context of the GF in order to govern specific **actions** taken by specific **actors** performing specific **roles** and **processes** within the **trust community**. These business rules can be expressed as human-readable **policies** and/or machine-readable **rules** that can be processed by a **rules engine** or a **decision support system**.

One of the secrets to the success of any trust community is the **incentive model**—ensuring that all governed parties have sufficient incentives to comply with the GF in order to achieve their objectives. Typically, the business rules in a GF will define and govern the value exchange mechanisms designed to provide these incentives. They should also govern how the **governing authority**, **administering authority** (if any), and any other required supporting infrastructure will be sustainable.












Depending on the layer and nature of the GF, business rules might include:

-  Service levels
-  [Contracts \(see section 7.9 on Legal Agreements\)](#)
-  Pricing (but avoid antitrust issues)
-  Liabilities
-  Insurance

7.6. Technical Requirements

The structure of the **ToIP stack** (figure 1) graphically illustrates that governance is only *half* of what is required for interoperability within and between **trust communities**. The other half is *technical interoperability*. This is the responsibility of the [ToIP Technology Stack Working Group](#) (TSWG). Its job is to assemble the necessary tools (standards, **specifications**, **specification profiles**, **recommendations**, **guides**, and [test suites](#)) that are needed for Internet-scale technical interoperability.

The overall goal of these tools is to minimize the additional work needed to specify technical interoperability **requirements** in this category. However, there will most likely be some additional technical **requirements** beyond those defined by the TSWG that apply to the GF's specific **trust community**. Depending on the layer of the GF, these may include:

-  Trust anchor or trust registry **DIDs**
-  **DID document** requirements
-  Website and **service endpoint** addresses
-  Onboarding processes
-  **Agent** and **wallet** requirements
-  Data models and schemas
-  **Credential** schemas
-  User interface / experience requirements
-  **Digital trust ecosystem** application requirements
-  **Trust mark** display requirements
-  GF-specific **test suites** and testing requirements

It is strongly RECOMMENDED that all **terms** used throughout these technical **requirements** be specified in the GF **glossary**.

For more information about ToIP technical interoperability, please contact the [TSWG](#).

7.7. Information Trust Requirements

The members of any digital **trust community** need to mitigate against **risks** from a common set of **threats** affecting the information the members generate, exchange, store, backup, and expunge. The AICPA Assurance Services Executive Committee (ASEC) divides these [trust services criteria](#) into five categories:

1. Information security
2. Information availability
3. Information processing integrity
4. Information confidentiality
5. Information privacy

The mitigations for these risks involve **governed parties** implementing **internal controls** such as those defined by the Committee on the Sponsoring Organizations of the Treadway Commission (COSO) [Guidance on Internal Control](#). **Policies** in this category will likely be driven by Chief Information Security Officers (CISOs), Chief Privacy Officers, Chief Identity Officers, Chief Trust Officers, and other information trust professionals within the **trust community**.

As with technical specifications, it is RECOMMENDED to reference or reuse existing standards and best practices whenever possible. It is also RECOMMENDED to structure these policies according to this [inheritance hierarchy](#):

1. ToIP **specifications and recommendations**.
2. **Other regulatory or industry standards**.
3. GF-defined **policies**.
4. GF-defined **rules** (for use by **rules engines** or **decision support systems**).
5. **Trust community member-specific policies**.
6. **Trust community member-specific rules**.

7.8. Inclusion, Equitability, and Accessibility Requirements

This final category of requirements is especially important for digital **trust communities**—important enough that this category of **controlled document** is REQUIRED in a ToIP-compliant GF.

This is another area where it is RECOMMENDED to consult industry professionals both within and outside the trust community. For a wide-ranging discussion of the many considerations involved on these subjects, the October 2020 Harvard Business Review article [To Build More-Inclusive Technology, Change Your Design Process](#) is RECOMMENDED. It includes the following quote:

In technology, [inherent bias](#) can be hard to root out. Our tech tends to reflect the people who create it — their perspectives and experiences shape how products are designed. Whether you’re talking about a smart city or a smart speaker, the systems that underpin our lives are the sum of designers’ decisions; inequality and exclusion are often the unintentional consequences of those choices.

These unintended consequences can be even more severe when they affect the ability of GF members to have fair and equal access to the resources and benefits of the **trust community**. The policies must reflect the values and practices of the specific trust community. In June 2021, the ToIP Foundation approved the Principles of SSI, originally developed under the auspices of the [Sovrin Foundation](#), as a set of principles recommended for any digital trust ecosystem that wishes to implement the SSI model for decentralized digital identity.

Once more, it is RECOMMENDED to reference or reuse existing policies and best practices in this area, following the same inheritance hierarchy as in [section 7.7](#).

7.9. Legal Agreements

Whether or not the GF requires any legal agreements or contracts depends on the nature of the **trust community**, the ToIP infrastructure, and the **jurisdiction(s)** in which it operates. Some GFs require contractual commitments between the **governing authority** and **governed parties** playing various **roles** such as **node operators** (ToIP Layer 1), **wallet providers** (ToIP Layer 2), **credential issuers** or **verifiers** (ToIP Layer 3), or **trust registry operators** (ToIP Layer 4).

However other GFs designed for decentralized **trust communities** that use permissionless blockchains or other mechanism based on algorithmic governance and built-in incentive mechanisms may not need any legal agreements at all.

In any case, if the GF specifies the need for any legal agreements, to be ToIP-compliant it:

1. MUST include them as **controlled documents**.
2. SHOULD reference the GF [Glossary](#) for all terms not defined internally to the legal agreement.
3. MUST clearly state the **governed parties** to whom these legal agreements apply.
4. MUST define or reference all relevant accountability and enforcement mechanisms.
5. SHOULD reference any other relevant **requirements** in the balance of the GF.

8. Additional Resources

The authors hope this Companion Guide is a helpful tool for interpreting the [ToIP Governance Metamodel Specification](#) (and the [ToIP Governance Architecture Specification](#)) in the development of a ToIP-compliant GF.

Additional resources are listed on the [Deliverables page](#) of the ToIP website.

Please feel free to contact ToIP with any questions or feedback via the [contact page](#). Or reach out to the members individually listed on the ToIP [Confluence wiki](#) for the Governance Stack Working Group or any of the other [ToIP Working Groups](#).



The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- ❖ Specifications to be implemented in code
- ❖ Recommendations to be followed in practice
- ❖ Guides to be executed in operation
- ❖ White Papers to assist in decision making
- ❖ Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, <https://trustoverip.org>.

Licensing Information:

All Trust Over IP Foundation deliverables are published under the following licenses:

Copyright mode: Creative Commons Attribution 4.0 International licenses
<http://creativecommons.org/licenses/by/4.0/legalcode>

Patent mode: W3C Mode (based on the W3C Patent Policy)
<http://www.w3.org/Consortium/Patent-Policy-20040205>

Source code: Apache 2.0.
<http://www.apache.org/licenses/LICENSE-2.0.htm>