TRUST Over IP FOUNDATION

Trust Assurance Companion Guide

Version 1.0
19 October 2021

This publicly available guide was approved by the ToIP Foundation Steering Committee on 19 October 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

Author

Scott Perry — Scott S. Perry CPA, PLLC

Contributors

Line Kofoed — Bloqzone
Jim St. Clair — Lumedic
Sankarshan Mukhopadhyay — Dhiway Networks
Karen Hand — Precision Strategic Solutions
Victor Syntez
Ricky Ng-Adam — Drave Development

Revision History

Version	Date Approved	Revisions
1.0	19 OCTOBER 2021	Initial Publication

Terms of Use

RFC 2119

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet

architecture and to ensure maximal efficiency in operation. IETF has been operating since the advent of the Internet using a Request for Comments (RFC) to convey "current best practice" to those organizations seeking its guidance for conformance purposes.

The IETF uses RFC 2119 to define keywords for use in RFC documents; these keywords are used to signify applicability requirements. ToIP has adapted the IETF RFC 2119 for use in the <name of this document>, and therefore its applicable use in ToIP-compliant governance frameworks.

The RFC 2119[1] keyword definitions and interpretation have been adopted. Those users who follow these guidelines SHOULD incorporate the following phrase near the beginning of their document:

> **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.**

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.

Requirements include any combination of Machine-Testable Requirements and Human-Auditable Requirements. Unless otherwise stated, all Requirements MUST be expressed as defined in RFC 2119.

- **Mandates** are Requirements that use a MUST, MUST NOT, SHALL, SHALL NOT or REQUIRED keyword**.**
- **Recommendations** are Requirements that use a SHOULD, SHOULD NOT, or RECOMMENDED keyword.
- **Options** are Requirements that use a MAY or OPTIONAL keyword.

An implementation which does not include a particular option MUST be prepared to interoperate with other implementations which include the option, recognizing the potential for reduced functionality.

[1] https://datatracker.ietf.org/doc/html/rfc2119. Accessed June 2021.

As well, implementations which include a particular option MUST be prepared to interoperate with implementations which do not include the option and the subsequent lack of function the feature provides.

Executive Summary

The ToIP Trust Assurance Companion Guide (TACG) is intended to introduce the topic of trust assurance and provide ancillary assistance in completing the Trust Assurance and Certification Controlled Documents (i.e., a RECOMMENDED set of controlled documents as specified by the ToIP Governance Metamodel Specification). TACG provides guidance on specific content and intention(s) of the required sections along with examples and references from generally accepted best practices.

Using This Guide

The TACG is designed to be used as a template and guide for writing a Trust Assurance and Certification TAC Controlled Document for a specific governance framework. While most material in this document SHOULD be appropriate for a wide range of governance frameworks, each governance authority will need to tailor the specific content. This MAY involve adding and/or removing material from the template as needed, to accommodate specific needs and constraints.

Purpose

This guide is intended to be used by governance architects and/or trust assurance specialists that are devising a trust assurance scheme for a governance framework using the Trust Assurance and Certification (TAC) Controlled Document template.

The purpose of this document, the ToIP Trust Assurance Companion Guide (TACG), is to provide guidance for ToIP-Compliant Governance Frameworks. TACG can be used as a guide to better understand trust assurance terminology and implementation.

This document is intended for:

- Business leaders and stakeholders building enterprises adopting IT designs around decentralized identity,
- Governance Framework architects,
- Leaders and key stakeholders in a governing authority interested in building a ToIP-compliant governance framework,
- Standard groups and researchers interested in the structure of a governance framework; and
- Service providers participating in ToIP ecosystems and all layers of the ToIP governance stack.

Most importantly, this document encourages emerging digital trust ecosystems to adopt the ToIP Governance Metamodel and thus design governance frameworks, which are aligned and inherently interoperable with those supported, defined and designed by the ToIP community

1. Introduction to Trust Assurance

Trust is a human concept. Trust is difficult to quantify and as humans we are very instinctive when considering the trustworthiness of others. Human society is built on trust, there is implicit and explicit trust in every interaction. There are enough books on the topic to fill a library and yet it seems we have not been able to build a society where trust abounds, and many of us still live in a world without trust.

The ToIP Foundation has advanced the concept of trust assurance in response to increasing concerns on the lack of adherence to security best practices and privacy principles. Diminishing consumer trust, compromised consumers' data and privacy (as the result of unprotected identities), lack of transparency in Internet of things (IoT) and their applications, has resulted in a society of technology adoption hesitancy, avoidance, and hypervigilance - and a failure to realize the socio-economic and environmental benefits of innovative technologies. In the early nineties we witnessed a similar phenomenon with the outcry over the Internet's use of commercial transactions. The risks of e-commerce transactions were very real; however, not enough to heed the temptation of returns awaiting vendors able to generate twenty-four-hour global sales. The cyber commerce industry was born – despite its inherent risks.

Over the last twenty-five years, companies have been allowed to exploit the ubiquitous nature of the Internet to transform daily life despite the collateral damage caused by criminal opportunists, bad actors, and human error/bias. Society has now passed the point of no return regarding the use of public networks - but no longer blindly trusts it. There is a growing societal demand for internet application oversight, transparency and integrity and a need to provide mechanisms for trust, both human and machine. This creates the avenue for self-sovereign identity and verifiable credentials to fill the void.

1.1 Risk Drives the Need for Trust

This guide would not exist if there were no threats to the expected processes of systems and networks. In an Internet that is over fifty years old and a world wide web that is thirty years old, we have high expectations for the online applications we use: systems to be available when we need them, our data to remain secure from prying eyes and our private data to remain private. These conditions do not happen by themselves. They MUST be built in by a cooperative array of information technology providers who design controls to address risk.

The formula for risk definition is rather simple; the determination of risk for the purpose of defining a trust framework is logically complex with a drizzle of art thrown in. Risk is a determination of a threat to a desired condition (e.g., functioning process) multiplied by the possibility of that threat occurring, leading to a (mostly judgmental) qualification of risk (high, medium, low, or potential monetary impact).

Given that the need for verifiable credentials can originate in almost every sector of industry and life's pursuits, no set of risks are the same. While industry has created potential starter sets of risks based on known roles within an ecosystem, the complete set of impactful risks are relevant to the

ecosystem. In one system, the availability of credential issuers could be critical; in another the privacy of credential information MAY constitute a minor risk. Bottom line, the analytical process of a risk assessment as a precursor of a trust assurance framework is mandatory. It is up to the governing entity to determine the process for risk identification and management. A recommended starting point is the ToIP Risk Assessment Worksheet Template and its associated ToIP Risk Assessment Companion Guide.

1.2 How Trust is Created

Trust is defined[2] as the "firm belief in the reliability, truth, ability, or strength of someone or something". Human trust is built from the following components: Inherent Trust; Acquired Trust, Referential Trust, Public Trust, and Game Theory Trust. These components contribute to Transitive Trust (see 1.3)

- **Inherent Trust** stems from our acceptance of the innate laws of nature and established social norms. We have inherent trust that the sun will come up or a bird's ability to fly from birth.
- **Acquired Trust** is gained through direct experience. People or organizations set expectations by stating they will do things and then satisfying the statement by "doing what they say". This adds to the "trust bank" with deposits made for every satisfied commitment. This can work in reverse as trust can be degraded when organizations do not meet stated commitments creating withdrawals from the trust bank.
- **Referential Trust** does not require personal experience with a person or entity. It is established through a trustworthy intermediary transferring trust upon a third party. We experience it in everyday life when Harry says, "Sally, please meet Joe. He'll take good care of you". Sally does not have acquired trust with Joe, but because of the trust Sally has acquired from her relationship with Harry, Sally acquires referential trust with Joe. In business we see it all the time. We trust unknown foods and drugs because they have FDA or USDA approvals. We trust online companies because they have acquired Trust-e or WebTrust seals.
- **Public Trust** is the confidence of individuals in the legal system to enforce contractual obligations, laws and rules in our society.
- **Game Theory Trust** is the trust that planned future repeated interactions that lead to mutual benefit to each one self-interest favors cooperation

In Self-Sovereign Identity (SSI) and Verifiable credential ecosystems, trust is also achieved through the consideration of these factors:

- **Cryptographic Trust**: The reliance on cryptographic technology to gain assurance on the relationship between keys in a public key infrastructure. This allows us to accept cryptographic operations that are inherent to SSI and verifiable credentials such as digital signing actions, key verification, key rotation, and data encryption.

[2] https://www.merriam-webster.com/dictionary/trust

- **Machine – Based Trust**: machine-based systems can invoke programming logic to establish predictable rules within rules engines or smart contracts to produce repeatable and consistent outputs that are correctly following specifications as long as it is developed and maintained by a well-controlled systems development lifecycle.

- **Human Trust through Governance**: While computer technology can enhance trust, trust still needs a human component. While governments have laws, and games have rules, SSI and verifiable credential ecosystems have governance frameworks. The frameworks convey the tailored requirements and guidance of the governed and the parties who rely on them to achieve trust.

1.3 The Requirements of Transitive Trust

In SSI and verifiable credential environments, the term ecosystem has evolved to describe the set of roles, processes, entities, schemas, data, and credentials that are governed under a uniting framework of requirements and guidance. This is led by a governing entity that is empowered by a governing authority. The governing authority plays a leadership role in conveying ecosystem trust. The trust conveyed within the boundaries of an ecosystem is defined as **non-transitive trust,** meaning as the purpose and objectives of a governance framework do not extend past the scope and boundaries of ecosystem components.

The ultimate goal of SSI and verifiable credentials is to achieve **transitive trust** whereby trust can be extended beyond where credentials are issued to achieve a more secure, trustworthy and decentralized upgrade of the Internet itself. In order to realize the full potential of ToIP's vision for enablement of trusted ecosystems (both human and cryptographic) and more broadly, the vision of Society 5.0[3], it is of paramount importance to architect a transitive trust assurance framework to provide emerging and future ecosystems with the necessary guidepost.

What are the constructs of transitive trust? This diagram attempts to encapsulate the major components in a high-level trust assurance model:

[3] Önday, Özgür. (2019). Japan's Society 5.0: Going Beyond Industry 4.0.

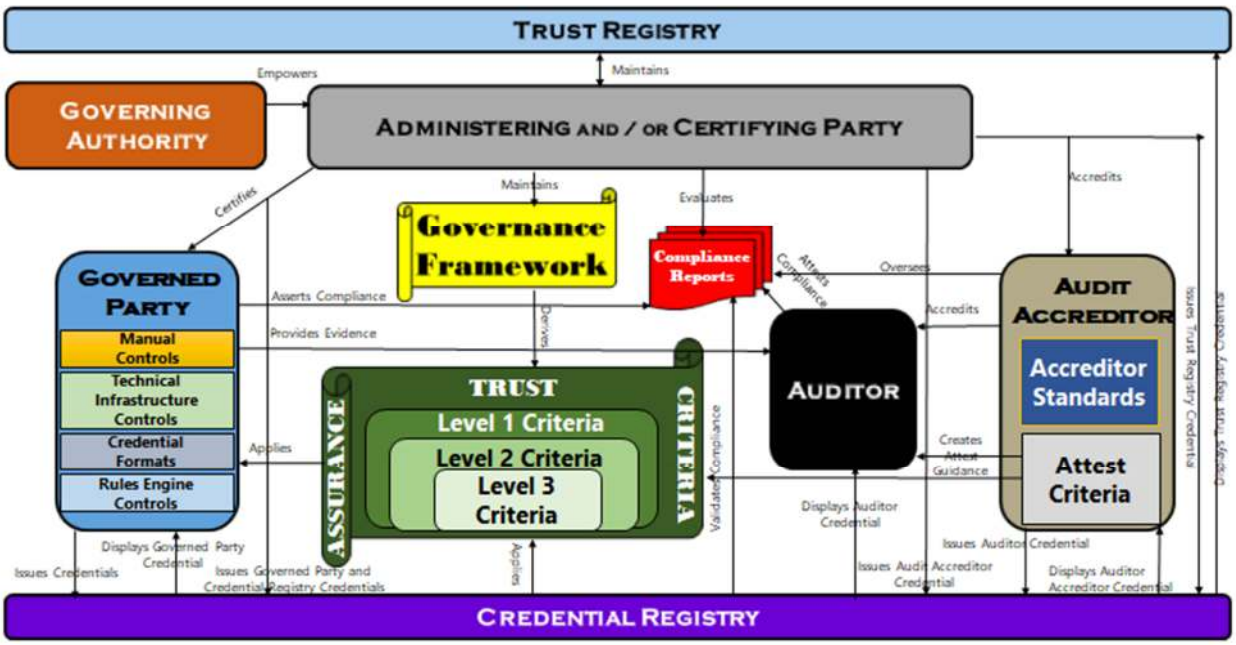


Figure 1: – Transitive Trust Assurance Ecosystem

The ecosystem assures holders of verifiable credentials that vendors are applying generally accepted trust criteria to their products and services by the introduction of accreditation bodies and an independent third-party auditor that acts in the interest of holders and the trust assurance scheme. The holder acquires trust from the ecosystem based on the ability of the actors to follow through on its commitments to comply with a set of issued criteria and the integrity of its decisions. This acquired trust can then be passed referentially to actors who want to be engaged in the ecosystem.

Each participant has a defined role in creating trust in the ecosystem:

- **Governing Authority** is an organization responsible for the trust of the ecosystem. It can empower an Administering Party to manage the ecosystem and certifying entities to convey trust.

- **Governing Party** (either a **Governing Authority** itself or its proxy **Administering Party**) is an organization that defines trust criteria derived from governance framework requirements that mitigate risk dealing with the security, confidentiality, availability, processing integrity and privacy of transactions. They set minimum standards for varying levels of assurance of assets that are transacted in the ecosystem. It recognizes Auditor Accreditors (and issues Audit Accreditor Credentials placing them on a Credential Registry) that set rules for the qualification of auditors and audits to hold ecosystem actors accountable for these minimum standards for levels of assurance. It reviews participating party's performance audits and accredit them as meeting minimum standards for varying levels of assurance and issue credentials and place them on a Credential Registry so relying parties have assurance that they were issued by the

stated governing party.

- **Certifying Party** - is an organization empowered to certify governed parties against a set of trust criteria. It demonstrates compliance by listing the governed party in a trust registry and/or issuing them a trust mark.

- **Governed Parties** which desire to play a recognized role in an ecosystem evaluate the auditable requirements (trust criteria) from Governing Parties and implement manual, technical infrastructure and rules engine controls and credential formats to demonstrate its posture that it is compliant with those criteria. They hold themselves out to a trust assurance scheme which evaluates their criteria conformance resulting in auditor compliance reports used for continuous improvement or actions taken by governing parties to withdraw a party's right to participate in their ecosystem.

- **Audit Accreditors** develop audit standards and criteria out of governance framework requirements developed from Governing Parties. They evaluate applicant auditors for their competence, independence and quality control measures and approve them to attest to audit criteria of governed party practices. They issue compliance credentials if approved auditors can attest to audit criteria without qualification and place those credentials on credential registries.

- **Auditors** are independent professionals that are trained in evaluating technology-based evidence provided from governed parties asserting that they are in compliance with audit criteria set forth by Audit Accreditors. They issue reports attesting to their opinions which enables Governing Parties to issue compliance credentials to governed parties and place them on Credential Registries and add their entry to the Trust Registry.

- **Trust Registries** are repositories of Governed Parties that are recognized by a Governing Party of an Ecosystem as compliant to the trust criteria of its Governance Framework for reliance within and outside of ecosystem boundaries.

- **Credential Registries** are publicly accessible repositories of credentials issued by parties in and accessed by Verifiers during the process of validating trust. They apply Trust Assurance Criteria to the protection of Credentials in the Registry subject to audit. A Credential Registry is an optional component of the Ecosystem

1.4 How Trust Assurance Interoperates with Risk Assessment

The ToIP RECOMMENDED Risk Assessment process allows for:

- Proper consideration and identification of potential risks,
- Critical analysis of potential risks in terms of likelihood and severity needed to calculate a systematic risk impact score,
- Triage of risks for further treatment,

- Treatment of the risks using a variety of options that include creation of risk mitigation requirements as part of the governance framework; and
- Performance of an annual review of risks to ensure criticality of current risks and the consideration of new or emerging risks.

One of the risk treatment options is to mitigate risk by creating mandates on the governance framework. Typically, this is described as a MUST statement in the governance framework which drives the mandate to be complied. The degree of compliance is dependent on the trust assurance framework in place to hold governed parties accountable to that requirement and the degree of effectiveness that the trust assurance framework has in reducing the risk to an acceptable residual level.

Therefore, the trust assurance framework assesses the design (at a point of time) of a governance framework's risk mitigation scheme and its operational effectiveness over time. Without it and other risk treatment options, risk cannot be lowered below an inherent (untreated) risk impact score.

2. Trust Assurance and Certification Controlled Document Sections

The following sections within this chapter provides specific guidance directed at defined sections in the Trust Assurance and Controlled Document Template. The Template SHOULD be used in conjunction with this chapter.

2.1 Introduction

This section sets the tone for the Trust Assurance Framework. It might be beneficial here to describe the concept of Trust Assurance (borrowing from content in section 1 of this Guide) to explain to those new to the topic of trust assurance why this document is important to the Governance Framework.

It also would be pertinent to discuss the risk, industry and regulatory landscape in which the governance framework operates. It affects the choices made within the trust assurance framework.

2.2 Purpose

This section describes the underlying reasons that this Controlled Document is part of the governance framework. The suggested verbiage describes the relationship trust assurance has with governance frameworks acting as an extension of the mandates (MUST statements) to drive accountability to all governed parties that have a role within the framework.

2.3 Version

Including a detailed history of changes and versions of the Controlled Document helps users understand changes in the trust assurance framework. Some of these changes include:

- Changes in Governance Framework mandates causing changes to the trust assurance criteria (Section 5)
- Changes in roles in the trust assurance framework (Section 3.1)
- Changes in trust processes in the trust assurance framework (Section 3.3)
- Changes in the Level of Assurance asserted by the Governance Framework (Section 4)
- Changes in the trust processes used to assure accountability (section 6)

2.4 Contact

It is critical to maintain a central contact point for any issues that arise from the trust assurance framework. At minimum, an email SHOULD be cited.

2.5 Concepts and Terminology

2.5.1 The Concept of Trust Assurance

The Template contains starter verbiage that can be used to explain the concept of trust assurance to new readers. Information derived from section 1 of this Guide can augment the content of this section.

2.5.2 The Interrelation between Trust Assurance and Risk

The Template contains starter verbiage that can be used to explain the concept of trust assurance to new readers. Information derived from section 1 of this Guide can augment the content of this section.

2.5.3 Key Terms

The Template contains a starter set of key trust assurance framework terms. As part of developing a trust assurance framework using the Template, key terms will surface that will be needed to be defined in this section. Material from this Guide and the ToIP Glossary can augment the content of this section.

2.5.4 RFC 2119

RFC2219 provides the following guidance and security considerations in using these normative terms[4]:

Imperatives of the type defined in this memo MUST be used with care and sparingly. In particular, they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions) For example, they MUST NOT be used to try to impose a particular method on implementers where the method is not required for interoperability.

These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD or doing something the specification says MUST NOT or SHOULD NOT be done MAY be very subtle. Document authors SHOULD take the time to elaborate the security implications of not following recommendations or requirements as most implementers will not have had the benefit of the experience and discussion that produced the specification.

[4] https://datatracker.ietf.org/doc/html/rfc2119

3. Scope

The Scope section defines the WHAT. What is the subject and contents of the components of the trust assurance framework? The scope would be a subset of the scope section in the Primary Document of the Governance Framework. The following subsections provide guidance to each component.

3.1 Governed Roles

These are the roles that are the target of accountability of the governance framework. They implement trust processes to assert compliance with mandates of the governance framework as defined in section 6 of the trust assurance framework. These processes can range in accountability from pledges to full-scale certification. A detailed set of Roles to choose can be found in Appendix A of the Governance Metamodel Companion Guide.

3.2 Other Relying Parties and/or Stakeholders

These are the non-governed, interested parties that are affected by the trust assurance framework in their evaluation of the trustworthiness of a governance framework. These include Holders of verifiable credentials, roles in other ToIP stack layers of a stack level governance framework and other ecosystems that establish a TSS (ToIP Standard Specification) that defines the standard requirements for the Governance Authority to conform for the purpose of transitive trust.

3.3 Governed Processes

These are the processes that are the target of accountability of the governance framework. Trust processes (Section 6) are applied to governed processes to assert compliance with mandates of the governance framework as defined in section 6 of the trust assurance framework. These trust processes can range in accountability from pledges to full-scale certification. A detailed set of candidate governed processes within a governance framework can be found in Appendix A of the Governance Metamodel Companion Guide.

3.4 Artifacts

These are the *key components of the governance framework such as credential types, repositories and other artifacts* that are the target of accountability of the governance framework. Trust processes (Section 6) are applied to these artifacts to assert compliance with mandates of the governance framework as defined in section 6 of the trust assurance framework. These trust processes can range in accountability from pledges to full-scale certification.

4. Level of Assurance

A level of assurance (LOA) is the certainty with which a claim made on a verifiable credential during verification can be trusted to actually be the truth. Higher levels of assurance reduce the risk of fraud and increase the security of transactions, but also can increase the cost and inconvenience to holders and relying parties, which could lead to exclusion. It is therefore imperative that practitioners consider the varying requirements of different use cases with respect to LOA. For example, biometric-based authentication is likely to be inappropriate for use across all use cases because some transactions (e.g., scheduling a medical appointment through a website) carry less risk.

Assurance levels depend on the strength of the credential claim verification process and the types of credentials and verification mechanisms used during a transaction.

The level of assurance depends on the method of verification (e.g., in-person vs. remote), the attributes collected, and the degree of certainty with which those attributes are verified (e.g., through cross-checks and deduplication). For verification, the level of assurance depends on the type of credential(s), the number of authentication factors used (i.e., one vs. multiple), and the cryptographic strength of the transaction.

Both eIDAS (*EU 2015*) and *ISO/IEC 29115* have developed standards to classify levels of assurance based on these processes and technologies.1 In addition, recent guidelines from the U.S. National Institute of Standards and Technology (NIST) (*NIST 800-63-3*) have adapted this framework to separate out assurance levels for identity proofing ("identity assurance level" or IAL) and for authentication ("authenticator assurance level" or AAL).

5. Trust Criteria

Trust criteria is the set of mandates within a governance framework which are ascribed by governed roles within the governance framework. They comprised the set included in section 5.1 augmented by either jurisdictional criteria (section 5.2) and/or industry criteria (section 5.3) and/or generally accepted information trust criteria (section 5.4).

5.1 Governance Requirement Criteria

The set of governance criteria is derived from all governance framework mandates (MUST statements). It SHOULD be compiled into a workable set of assessable criteria in an accompanying Trust Criteria Matrix so it can be further disseminated to all trust roles (e.g., Governed Roles, Auditors, etc) that will need to use these criteria to assert or attest compliance. The ToIP Trust Criteria Matrix Template and the ToIP Trust Criteria Companion Guide can be used to develop trust criteria.

The following are examples of specific applications or business processes that require its own set of criteria or operating principles for specific purposes:

- **CA/B Forum Baseline Requirements** – The Certification Authority Browser Forum, aka CA/Browser Forum, is a voluntary consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI (Encrypted) applications that make the industry guidelines. It governs the issuance and management of SSL/TLS and Code Signing digital certificates that chain to a trust anchor root that is embedded in such applications.
- **US DEA E-Prescriptions Trust Criteria** - The United States Drug Enforcement Administration requires specific trust criteria and assurance mechanisms to protect electronic orders and prescriptions for controlled substances.
- **SHAKEN/STIR** - is a telecommunications industry-developed framework of protocols and operational procedures for providing call authentication services. SHAKEN/STIR is an acronym of two sets of technical specifications: The Secure Telephone Identity Revisited (STIR) protocols defined by the Internet Engineering Task Force (IETF); and the Signature-based Handling of Asserted information using toKENs (SHAKEN) specifications defined by an industry task force.

5.2 Jurisdictional Criteria

Jurisdictional Criteria is a set of requirements mandated by a jurisdiction that are within the scope of a governance framework and its associated trust assurance framework. Jurisdictional criteria MAY require a specific and separate set of trust processes to demonstrate compliance. The following are examples of existing jurisdictional trust criteria:

- **US Federal Public Key Infrastructure** - The Federal Public Key Infrastructure Program provides US Government agencies and affiliated actors with a trust framework and infrastructure to administer digital certificates and public-private key pairs. The Federal Trust Framework consists of policies, standards, governance processing and assurance mechanisms.

The participating certification authorities (trust anchors of the network), their Policies, Processes, and Auditing of all the participants are referred to as the Federal Public Key Infrastructure (FPKI).

- eIDAS (electronic IDentification, Authentication and trust Services) - is both a EU regulation and a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.
- Pan-Canadian Trust Framework ™ (PCTF) - is an economic benefit focused set of resources that are developed in collaboration in the Digital ID & Authentication Council of Canada (DIACC)'s Trust Framework Expert Committee (TFEC), published by the neutral governance of the DIACC, and benefit from broad input of the economic sector and from Canada's federal, provincial, and territorial input of the Joint Councils Identity Management Subcommittee (IMSC).
- Australian Digital Identity Network - This Trusted Digital Identity Framework sets out the rules and standards that will build a nationally consistent approach to digital identity in US Federal Public Key Infrastructure Australia. The framework now consists of 16 documents including an overview and glossary.

5.3 Industry Criteria

In most cases, generally accepted trust criteria will be insufficient to the needs of the ecosystem. Industry specific trust criteria MAY be more pertinent to the industry or jurisdiction of the ecosystem, or the specific set of services it offers its actors and relying parties. Below are examples of each.

- HITRUST - Since it was founded in 2007, the HITRUST Alliance has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks, related assessment, and assurance methodologies. While the criteria are not industry specific, it has been widely adopted by the healthcare industry as an industry standard trust assurance framework.
- FFIEC IT Examination Handbook - The Federal Financial Institutions Examination Council Information Technology Examination Handbook has served the banking industry almost since the FFIEC was established in 1979. It has taken generally accepted trust criteria and modified them for the banking industry. Banking regulators and auditors typically use its guidance in their audits.
- Payment Card Industry Data Security Standard (PCI DSS) - Payment card companies had their own individual set of trust criteria until they were aligned by a domain Governing Entity called the Payment Card Industry Security Standards Council (PCI SSC). MasterCard, American Express, Visa, JCB International and Discover Financial Services established the PCI SSC in September 2006 as an administration/governing entity which mandates the evolution and development of the PCI DSS. The PCI DSS suite of trust criteria is now the industry standard for the credit card payment ecosystem.

- NAESB WEQ-12 - The North American Energy Standards Board is a Governing Entity that serves as an industry forum for the development and promotion of standards which will lead to a seamless marketplace for wholesale and retail natural gas and electricity, as recognized by its customers, business community, participants, and regulatory entities. The WEQ-12 is specific to its industry.
- DirectTrust - The Direct Project launched in March 2010 to specify a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet as part of what was known as the Nationwide Health Information Network. The Direct Project was structured as a consensus-based standards development organization since its inception, with participation and sanction from the Department of Health and Human Services (HHS) and the Office of the National Coordinator of Health IT (ONC), but with no affiliation with an accrediting authority.

5.4 Generally Accepted Information Trust Criteria

General accepted information trust criteria are a set of requirements mandated by a recognized standards authority that are within the scope of a governance framework and its associated trust assurance framework. General accepted information trust criteria MAY require a specific and separate set of trust processes to demonstrate compliance. The following are examples of existing general accepted information trust criteria:

- AICPA Trust Services Criteria - In 2017, the American Institute of Certified Public Accounts (AICPA) updated its published set of trust criteria for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy over information and systems (a) across an entire entity; (b) at a subsidiary, division, or operating unit level; (c) within a function relevant to the entity's operational, reporting, or compliance objectives; or (d) for a particular type of information used by the entity.
- ISO/IEC 27001:2013 – This global standard formally specifies an Information Security Management System (ISMS), a suite of activities concerning the foundational management of information risks (called 'information security risks' in the standard). The ISMS is an overarching management framework through which the organization identifies, analyzes, and addresses its information risks.
- ISO/IEC 29115:2013 - This global standard provides a framework for managing entity authentication assurance in a given context. Specifically, it:
  - specifies four levels of entity authentication assurance,
  - specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance,
  - provides guidance for mapping other authentication assurance schemes to the four levels of assurance (LoAs),
  - provides guidance for exchanging the results of authentication that are based on the four LoAs, and

- provides guidance concerning controls that SHOULD be used to mitigate authentication threats.

This document is becoming a common reference to create commonality of identity requirements between jurisdictions where identity laws and evidence vary greatly.

- NIST SP 800-63-3 - The United States National Institute of Standards and Technology (NIST) has issued a revised version of its Digital Identity Guidelines. These guidelines provide technical requirements for federal agencies implementing digital identity services. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.

While it is intended for government entities, it has been accepted by government service providers, contractors, and leading players in the identity industry as the de facto identity standard.

5.5 Trust Evidence

Trust assertions are empty without evidence to support it. Trust evidence is the set of all the information used by a Party in supporting their conformance to trust criteria. According to generally accepted audit standards, evidence MUST be sufficient, appropriate, and persuasive to support the assertion.

- Sufficiency - is the measure of the quantity of trust evidence.
- Appropriateness - is the measure of the quality of trust evidence, that is, its relevance and its reliability in providing support for, or detecting deviations in its assertions.
- Persuasiveness - measures how compelling evidence is to a reasonable person supporting an assertion of compliance. This is often used in trials to persuade juries to a particular verdict.

The Governed Party and auditor should consider the sufficiency, appropriateness and persuasiveness of trust evidence when presenting evidence that the party is conformant with criteria over a stated period of time. The quantity of trust evidence needed is affected by the risk of deviation for the trust criteria (the greater the risk, the more trust evidence is likely to be required) and by the quality of such trust evidence (the higher the quality, the less the trust evidence that MAY be required). The bar to cross makes the evidence persuasive. Accordingly, the sufficiency and appropriateness of trust evidence are interrelated. However, merely obtaining more trust evidence MAY not compensate if it is of a lower quality.

The following are examples of trust evidence that can be used to support trust assertions in a trust assurance framework:

- Signed Contracts and Agreements - This evidence is typical in agreements with Authoritative Issuers and Holders of credentials. It also MAY be in operating agreements between a Governing Party and its members, contractors with subcontractors, entities, and its vendors. In some jurisdictions, signed contracts and agreements take precedence

over the rule of law. Signatures must be legal (some jurisdictions MAY NOT accept some forms of electronic or digital signatures).

- **Computer configurations** - In computer systems and networks, often the most definitive evidence of the state of operational parameters are located on configurable settings of the operating system, application, or device. Often system monitors have controls in place to detect changes of system configurations. If there is sufficient evidence of configuration change control, there SHOULD be sufficient and appropriate evidence that systems were operating in the manner it was configured.
- **Certifications / Accreditations** - are tangible evidence that a standard has been met by an organization, process person or thing. Certificates that attest to the certification or accreditation can be in paper form or stored digitally. Based on the certifier/accreditor, this can be a persuasive form of trust evidence. An example is an electrical appliance certified by United Laboratories (UL)
- **Signed Approvals** - While less formal and authoritative than signed contracts, signed approvals of control processes demonstrate compliance to processes, especially manual processes.
- **Demonstrations of Compliant Processes** - When organizations can demonstrate, on demand, their compliant processes, it creases persuasive evidence. Demonstrations can be visual or through computer processes. Screenshots MAY augment the evidentiary package. Typically, this evidentiary documentation is supported by an organization's certification. For example, an ISO certified organization can be trusted in its evidentiary documentation of a compliant process.
- **Policies, Practices, and Operating Procedures** - While this evidence does not ensure that compliance procedures are operating, it does convey management's intention and clarifies to personnel what is expected and how compliance is achieved. Additionally, they MAY be explicitly documented to show compliance with a trust framework or certification requirement. For example, an organization MAY use NIST or ISO as the template basis for its compliance procedures.
- **Computer and Manual Logs** – provide a record of actions taken by people, devices, and processes. If logs are restricted from tampering, it can be an effective repository of trust evidence. Logs also provide the basis of auditability on a certified process or procedure.

6. Trust Assurance Processes

6.1 Trust Assurance Scheme

Depending on risk, capital and cooperation, the following are trust schemes that a governing authority takes to assure trust. They MAY be deployed by itself or in combination. Each mechanism mitigates varying levels of risk so each mechanism SHOULD be adopted after a proper risk assessment to justify its posture.

- Contracts and Agreements - can be established between Governed Parties and the Governing Party and between Authoritative Issuers and Holders. They SHOULD be signed and, in a format, recognized within an authoritative jurisdiction. Breaches of contracts would be mediated within the jurisdiction's judicial process.
- Pledges - Governed Parties can declare that they plan to or are committed to be in compliance with trust criteria. This is considered a Pledge. A Pledge lacks action and any means of validation, but a recognized intent MAY signify more assurance than not overtly stating any intent.
- Self-Assertion - Actors can declare, without attestation, that they are in compliance with trust criteria. They risk reputational damage if whistle blowers act to dispute their assertion since there is limited assurance over their assertion. They MAY be required to provide evidence to support their self-assertion either publicly or to a governing authority. That would add a degree of assurance.
- Auditor Attestation - provides a commonly accepted form of reasonable, but not absolute assurance that roles are meeting their trust criteria. This can be solidified with the addition of an auditor accreditor, which accredits auditors based on their competence, independence, and consistent practices.
- Certification - Governing authorities MAY, in addition to accepting auditor attestations, perform certification processes of roles against trust criteria. They can do this themselves or deploy accredited certifying parties.
- Trustmarks – are a publishable, graphic representation of conformance to a set of trust criteria. It MAY be linked to another artifact, such as an Auditor opinion report or Certifying Party certificate. In SSI or verifiable credential ecosystems, trustmarks are contained in a credential and located on a Credential Registry.

6.2 Trust Assurance Oversight Governance

The following are examples of oversight processes deployed by a governing authority to manage the trust assurance framework. The following are examples:

- Risk Assessment - A subjective process to identify potential threats of a Governance Framework's scope upon its purpose and objectives and derive a proportionate plan to address them.
- Governing Authority Oversight processes:
  - Governing Authority Establishment - activities to convene stakeholders aligned to oversee a layer of the ToIP stack.

- ❖ Governance Framework Establishment - activities used to draft and enact an initial document containing key directives of a Governance Authority.
- ❖ Governance Framework Government processes
  - Member Application
    - Member Contracting - the presentment and agreement of terms that a Governing Authority has with its participating members.
    - Member Fee Management - the billing and collection of financial obligations required by a Governing Authority with its members.
  - Member Vetting - the unbiased due diligence of prospect members against a set of acceptance criteria.
  - Member Voting - collecting and tabulating definitive choices made to members on proposed Governing Authority actions.
- ❖ Policy Management
  - Policy Establishment - activities used to draft and enact an initial set of requirements and guidance a Governing Authority has upon its scope aligned with its purpose and objectives.
  - Policy Adoption - the acceptance of rules and guidance that a Governing Authority presents to itself and its members.
  - Policy Enforcement - activities that a Governing Authority takes to hold itself and its members accountable for its rules and guidance.
  - Policy Amendment - The re-evaluation and change of previously established rules and guidance.
- ❖ Governance Authority Communication
  - DID Publication - The presentment of availability of a decentralized identifier.
  - DID Whitelisting - The collection and enablement of decentralized identifiers specifically allowed actions specified by a Governing Authority.
  - Verifiable Credential Publication - the availability of verifiable credentials to stakeholders within an ecosystem.
  - Levels of Assurance - the pre-defined tiers of risk mitigation afforded a class of transactions within an ecosystem.

- Member Directory Designation and Recognition - The collection and enablement of approved Member entries available for transaction consideration within a Governance Authority.
- Credential Registry Designation and Recognition - The collection and enablement of approved Credential Registries for transaction consideration within a Governance Authority.
- Authoritative Issuer Designation and Recognition - The collection and enablement of approved Authoritative Issuers for transaction consideration within a Governance Authority.
- Authoritative Verifier Designation and Recognition - The collection and enablement of approved Verifiers for transaction consideration within a Governance Authority.
- Verifiable Credential Standards - The set of rules enacted by a Governing Authority that apply to a set of verifiable credentials under its scope.
- Governance Trust Assurance Processes - The set of governance activities enacted by a Governing Authority to hold its stakeholders accountable for its governance rules.

6.3 Governed Party Processes

This section includes the set of trust processes used based on the trust scheme (section 6.1) deployed by Governed Parties (section 3.1).

6.4 Auditor Processes

Auditor processes the set of accepted practices guiding the attestation of an entity's assertion over its compliance with established Governing Authority trust criteria. Most audit methodologies have processes with the following phases:

- **Risk Assessment and Planning** - Processes intended to educate the auditor on the control environment governing the trust criteria, gauging the risk of Governed Party assertions of conformance and tactically planning the details of the audit.
- **Audit Fieldwork** - The process of gathering and analyzing trust evidence (see 5.5) to determine its conformance to the stated criteria
- **Audit Reporting** - The dissemination of audit exceptions and the results, both verbal and written.

6.5 Audit Accreditor Processes

These include the evaluation and oversight activities enacted by an Auditor Accreditor to approve and regulate auditors for a Governing Authority. ISO/IEC 17024[5] contains principles and requirements for a body certifying persons against specific requirements and includes the development and maintenance of a certification scheme for persons. In the marketplace, various Audit Accreditors operate contingent with the trust criteria it supports such as:

- WebTrust auditors are accredited by CPA Canada for use in auditing CA/Browser Forum trust criteria
- Kantara Initiative and SAFE-BioPharma accredits auditors for their NIST 800-63 conformance criteria
- tScheme accredits auditors under its approved trust criteria
- The EU Member States have their own national accreditation bodies that accredit auditors (conformity assessment bodies) for the eIDAS standard.[6]

6.5 Certification Body Processes

ISO/IEC 17065 is a global standard containing conformity assessment requirements for bodies that certify products, processes and services[7]. Certification is a means of providing assurance that

[5] https://www.iso.org/standard/52993.html
[6] https://tcab.eu/list-of-accredited-conformity-assessment-bodies-eidas/
[7] https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en

Governed Parties comply with trust criteria. Certification schemes MAY include initial testing or inspection and assessment of Governed Party's quality management systems, followed by surveillance that takes into account the quality management system and the testing or inspection of samples from the production and the open market. Other schemes rely on initial testing and surveillance testing, while still others comprise type testing only. We RECOMMEND seeking services from an ISO Accredited Certification Body if certification is to be part of the trust assurance framework.

6.6 Trust Mark Processes

The fundamental purpose of trust marks is to provide trusted, 3rd-party attestation that a Governed Party upholds a specific set of characteristics that are important to a Relying Party. This makes the trust mark concept a very powerful tool for communicating trust assurance.

Figure 2 - Trust Mark Examples. Source: Shopify

In developing a Trust Mark scheme, the following processes SHOULD be considered:

- **Trust Mark Scheme Definition** - The set of activities a Governing Authority defines to establish and regulate its issuance of Trust Marks.
- **Trust Mark Vetting Process** - The evaluation of candidate actions against a predefined set of criteria to determine their eligibility for trust mark issuance.
- **Trust Mark Issuance Process** - The presentment of Trust Marks to approved recipients.
- **Trust Mark Discovery Process** - The search and identification activities of interested parties of a Governing Authority's Trust Marks
- **Trust Mark Revocation** - The rescindment of a previously approved Trust Mark by a Governing Authority
- **Trust Mark Expiration** - The state when a Trust Mark exceeds its stated approval period enacted by a Governing Authority

7. Trust Assurance Implementation Methodology

When an Ecosystem wants to implement a Trust Assurance Framework, it SHOULD follow the following steps:

1. Ecosystem Risk Assessment
2. Identify Ecosystem Parties
3. Choose Level(s) of Assurance
4. Identify Trust Criteria
5. Identify Trust Schemes
6. Select External Resources
7. Document and Publish Trust Criteria Matrix
8. Communicate the Scheme
9. Put the Framework into Operation

7.1 Ecosystem Risk Assessment

A diligent risk assessment attempts to identify inherent threats to network performance, application viability and compliance. Each interoperable governing authority has their own list of threats depending on their domain.

ToIP has created a Risk Assessment Worksheet Template and a Risk Assessment Companion Guide that provide a generally acceptable method of performing a risk assessment.

7.2 Identify Ecosystem Parties

Ecosystems are not one size fits all. There is a myriad of ways that verifiable credentials will be implemented. More than we can even imagine today. However, it is likely that there will be Issuers, Verifiers, Credential Registries, Trust Registries and a Governing Party in place to manage it all.

An implementation consideration is: what will it take to be a qualified ecosystem role and what vetting mechanism will be put in place by the Governing Party to implement it? Are there barriers to entry for Ecosystem Roles? Will previous experience be required? There are many public Certification Authorities in existence today which already act as functioning roles in domains. Are they candidates for your Ecosystem?

7.3 Choose Level of Assurance

A Level of Assurance conveys the trustworthiness of a credential. The Ecosystem's Risk Assessment will drive the level of assurance needed for its own domain. But what if the Ecosystem wants its credential to be trusted outside its domain into the Network of Networks? It needs to consider the highest level of assurance it feels it can support.

For example, a national chain of gym clubs MAY want to create an id credential for access and services in gyms around the country. By itself, it MAY only require a low level of assurance (Class 1 – IAL1, AAL1) for its members. However, if the credential becomes such a utility for its members that millions have it and the Gym Association wants to repurpose the credential for other services, the level of assurance will limit the service potential.

Therefore, long-range planning SHOULD be considered when establishing acceptable levels of assurance. A minimum of Class 2 (IAL2, AAL2) assurance SHOULD be adopted by the domain wanting to exact a minimum, commercial-grade degree of trust.

7.4 Identify Trust Criteria

This document has illustrated several viable trust criteria. The key in determining what would be required for an Ecosystem is the level of specificity. What is particularly unique about the domain that requires unique consideration? If there is none, DO NOT deploy unique governance requirements because the governing authority will have to maintain it. There are ample generally accepted and industry requirements that SHOULD cover 80% of your domains needs. Start with them.

There MAY be a variety of schemes in place for a domain. Issuers MAY be required to follow identity proofing and authentication criteria; Credential Registries MAY be required to adhere to SOC 2 requirements., etc. Looking at the requirements holistically from the top down MAY ensure that there are no holes in trust coverage.

7.5 Identify Trust Schemes

Similar to identifying levels of assurance, identifying trust schemes SHOULD map to the risk assessment and levels of assurance put into operation. Lower assurance credentials MAY not need more than contracts and self-assertion mechanisms. Medium-level credentials might not need more than periodic audits from recognized audit/assessor firms. Whereby higher-assurance credentials MAY require full certification with audit accreditors vetting the qualification of audit/assessors.

The trust scheme SHOULD equate to the level of trustworthiness the domain wants in its credentials and the accountability of Ecosystem Roles in asserting that trust.

Another factor is cost. Trust schemes that convey even a medium level of assurance cost money. Certifying Parties, auditors, audit accreditors do not work for free. The cost of compliance SHOULD equate the level of trust and acceptance for the credentials and the supporting network conveying that trust.

7.6 Select External Resources

If the trust scheme selected in the last section requires the involvement of external resources, they need to be identified, courted, contracted and deployed. The Governing Party MAY want to initially outsource some activities and then bring them in-house to save cost. Each external resource has their own cost, experience, reputation and marketplace reach. It is critical to invoke an unbiased

collaborative method of engaging with external resources or the trustworthiness of the domain MAY be tainted. Some factors to consider are:

- What credentials are required to audit within the domain?
- Are there qualified auditors/assessors located within jurisdictions of Roles?
- Is there a need for an Audit Accreditor to vet auditor/assessors?
- Is an ISO-accredited Certifying Body appropriate for the Ecosystem's needs?

If external resources are deployed, contracts specifying performance and liability MUST be drafted and agreed to by all parties.

7.7 Document and Publish Trust Assurance Framework

A method of memorializing decisions made by the Governing Party on the trust assurance process is to draft and publish a Criteria and Methodology document to all stakeholders. Submitting a draft for comments will allow proper dissemination and buy-in of accountability of actions for all Ecosystem Roles. The Trust Assurance and Certification (TAC) Controlled Document is an excellent starter template to complete a Trust Framework. Combined with the contents of this Guide SHOULD assist in creating a draft for comment

7.8 Communicate the Scheme

The Trust Assurance Framework is a living process. The viability of this process is determined by all stakeholders understanding its tenets and being accountable for their role in it. It all starts with open, clear and consistent communication. Having Ecosystem Roles participate in the formation of the Framework will hedge its success. All parties SHOULD agree to their roles as part of the acceptance process into a permissioned network. There cannot be any surprises when it is time to demonstrate accountability.

Communicating the scheme included in the Trust Assurance Framework document is a way of attracting relying parties to the governance domain. The Framework itself is a competitive advantage engaging participants to perceive greater trust in credentials that are issued and verified under its methodology. The Governing Authority must allocate sufficient funds to properly convey and advertise the objectives of its Trust Framework and how that level of trust is to be achieved.

7.9 Put the Framework into Operation

At some point, it will be time to put the framework into operation. If attestation schemes are in place, there will need to establish a baseline of trust at documented points of time through review of the design of control processes prior to operation. The Governing Authority will have an entity established to deal with compliance issues and review audit reports from the field. A mechanism of discontinuance should be in place that will eliminate unaccountable Ecosystem Roles from continuing to participate in the Framework. Periodic communication vehicles will be set up and groups will meet to discuss trust issues on a cyclical basis.

7.10 Implementation Considerations

The value of an Ecosystem is highly dependent on the integrity of the participating parties. Conflicts of interest MUST be identified and eliminated. Procedures driving compliance MUST be fair, open, clear, and timely. All Governed Parties need to be engaged and MUST feel that it is a strategic advantage to participate – not an obligation. Costs, both for certification fees and auditor engagements MUST be reasonable and matched to the value they carry.

The trust criteria itself MUST have clear and cost-effective practices available to demonstrate compliance. The total compilation of compliance costs of all Governed Parties in aggregate MUST be less than the value individual Governed Parties perceive or commercially realize, or they will refuse to participate.

In our litigious society, all Governed Parties in a trust assurance framework are risk averse. It is critical that each Governed Party remains only accountable to the risk reasonably afforded to them. For example, the public cannot hold Governed Parties accountable for more than its participation in the process. Here are other assumptions:

- Governed Parties MUST be accountable only for their compliance assertion.
- Governing Parties MUST be accountable for the efficacy of trust criteria.
- Governing Parties MUST be accountable for their fair and open accreditation of Audit Accreditors and Actors.
- Auditors MUST be accountable for their attestation opinions.
- Certifying Parties MUST be accountable for their certification of Governed Parties
- Audit Accreditors MUST be accountable for their accreditation of auditors.
- Audit Accreditors or Governing Parties MUST be accountable for the issuance of Trustmarks.

The model MUST be able to weed out nonconformance and apply right-sized penalties when challenged. Accreditation SHOULD NOT be easy but not overly onerous. Relying Parties and their advocates recognize when rubber-stamping is the norm.

The accreditation process itself SHOULD be continuously monitored so it can evolve with changing technical advances and societal needs. Feedback loops SHOULD be established to assess the process from all Actors so continuous improvement can be reengineered into the model.

7.11 Critical Success Factors for Trust Assurance Governance

In order for ecosystem trust assurance governance to work successfully, it needs:

- Independence from vendors,
- Credible and experienced actors engaged in the accreditation process,
- Adequate funding,
- The ability to exude referential trust to the relying consumer public,
- Relationships with audit accreditation bodies, and
- Experience in the accreditation process

A trust assurance framework needs competent, independent, and trustworthy individuals to govern the process. There MUST be reasonable separation to allow Governing Parties and Audit Accreditors to both play and maintain independent roles. The Governing Authority SHOULD recognize and approve competent and experienced Governed Parties to operate within the Ecosystem. It SHOULD create trust criteria that mitigates its risk, are reasonable and cost-effective for actors to comply with. The scheme MUST be flexible and SHOULD mature over time using feedback loops and advances in innovation.

7.12 Trust Assurance Implementation Strategy

Before deploying a successful trust assurance implementation strategy, key components of an Ecosystem Governance Framework MUST be initially established. Master elements of a governance framework MUST be defined, such as: Introduction, Purpose, Scope, Principles, Objectives, General Requirements, Revision Strategy and Extensions (see ToIP Governance Metamodel Specification). Also, the Governing Party SHOULD conduct an Ecosystem Risk Assessment to determine the set of requirements key to personalizing the Trust Assurance Framework. Once those components are in place, the following are highly RECOMMENDED factors in Trust Assurance Framework development:

- The Ecosystem SHOULD establish a Trust Assurance Working Group composed of experienced professionals to perform the Ecosystem Risk Assessment and create the Trust Framework components of: Trust Criteria, Trust Parties, Levels of Assurance, and Trust Mechanisms.
- The Trust Criteria SHOULD be segmented into multiple options to actors based on complexity, risk, and assurance to the relying public.
- The Trust Assurance Working Group SHOULD engage the audit and security compliance professional community about their interest to play a role in the assurance process.
- The Governing Authority SHOULD establish criteria and levels of assurance which provide actors economic justification to participate.
- The Governing Authority SHOULD set requirements upon Auditors, Audit Accreditors and/or Certifying Parties for what is needed for acceptance and recognition of their requirements. Once accepted and recognized, they SHOULD evaluate their performance annually.
- The outgrowth of this model SHOULD be formalized to show confidently how it can be established, grown, and maintained through self-funding.
- The process SHOULD be evangelized to relevant commercial, consumer and governmental representatives to anchor the process of public trust.

The Trust Assurance Working Group defines baseline requirements of all entities to address security, confidentiality, availability, processing integrity and privacy risks of transactions in the Ecosystem. It defines encapsulated services delivered by Governing Authorities that can be verified by independent, competent Auditors. It defines criteria for the acceptance of Audit Accreditation Bodies and their monitoring. It displays accredited Audit Accreditors and Actors (specified by their compliant component) on its public website.

The Trust Assurance Working Group MAY align with existing trust framework providers to approve an acceptable audit accreditation scheme. This would include the following elements:

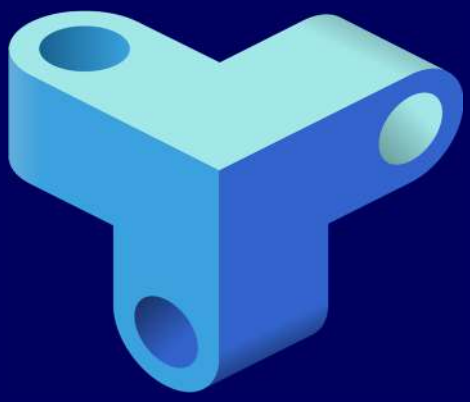
- Qualifications (Certification and experience to qualify to perform the work) of audit personnel,
- Suggested evidence that would successfully demonstrate the actor's conformance to criteria elements (i.e., what does success look like?),
- Templates of reports to be issued, and
- Additional guidance that would streamline and make the audit process consistent.

The Trust Assurance Working Group establishes its requirements for initial accreditation which SHOULD include an initial point-in-time audit. This audit is best segmented to an assertion/attestation process which delineates the role and therefore the risk each plays within its responsibility.

The Ecosystem maintains a list of Auditors and Audit Accreditors, and the expectations needed from Ecosystem Actors for their initial (and subsequent) audits.

Concluding Summary

Trust assurance is a critical part of any SSI or verifiable credentials ecosystem. It is often overlooked and underfunded, yet its value is only truly appreciated when it breaks down and assurance by Relying Parties are openly questioned. The recipe for long-lasting digital trust is to build in trust assurance at the beginning of Ecosystem formation and create a quality management system for continual improvement as a core element of its existence.



TRUST Over IP FOUNDATION

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