34

Trust assurance in SSI ecosystems

Scott Perry CPA, CISA

In Chapter 11 on governance frameworks, we explain how the trustworthiness of digital transactions is assured through a framework of policies, accountability requirements, and skilled participants who play contributing roles for the benefit of all members of a digital trust ecosystem. This chapter explores how digital trust is created and maintained in such an ecosystem through the development and operationalization of a trust assurance framework to achieve the appropriate risk mitigation for all stakeholders. Scott Perry is the founder of a nationally-operating U.S. CPA firm specializing in cybersecurity consulting and auditing—and one of only a handful of CPA firms licensed to issue WebTrust opinion reports over Certificate Authorities who issue digital certificates to websites. Among his many other roles, Scott is also co-chair of the ToIP Governance Stack Working Group.

Introduction

"Trust is like blood pressure. It's silent, vital to good health, and if abused it can be deadly."
--Frank Sonnenberg, - Follow Your Conscience

Trust is a human concept. It is hard to quantify, yet humans clearly know if it's not there. It binds people together stronger than commercial adhesive, yet you cannot see it, touch it, or taste it. There are enough books on the topic to fill a library, yet it seems that we still live in a world without trust.

This chapter responds to the increasing concerns about the lack of adherence to security best practices and privacy principles. The resulting diminishing trust among consumers—who suffer constantly from compromises of their data and privacy as the result of unprotected Internet devices and applications—threatens the very benefits this technology promises to deliver.

In the early nineties, there was a similar outcry over the Internet's use of commercial transactions. The risks of e-commerce transactions were very real at the time. However, the treasures awaiting vendors generating 24-hour-a-day sales from the far reaches of the globe were too tempting to heed the risks. This ecommerce industry was born – despite its inherent risks.

Over the last 25 years, companies have continued to exploit the ubiquitous reach of the Internet despite the collateral damage caused by criminal opportunists and human error. Society has passed the point-of-no-return of using a public network—but also no longer blindly trusts it. Demand for oversight and integrity of the Internet is growing. It appears the usual suspects for generating societal trust are reluctant to step forward. This creates an avenue for SSI and verifiable credentials to fill the void.

Risk Drives the Need for Trust

This chapter would not exist if there were no threats to systems and networks operating as expected. In an Internet over 25 years old, we expect apps to function as designed, systems to be available when we need them, data to remain secure from prying eyes, and our private data to remain private. But these outcomes do not happen by themselves. They must be consciously built-in to our infrastructure by a cooperative array of information technology providers who design the controls necessary to address risk.

The formula for defining risk is rather simple: it is a determination of the threat to a desired condition (e.g., a functioning process) multiplied by the possibility of that threat occurring. The result is a judgement about the potential monetary impact of the risk as *high*, *medium*, or *low*.

Given that the need for SSI verifiable credentials is nearly universal across business, commerce, and social use cases, there is no single universal set of risks. While the SSI industry has identified potential starter sets of risks based on well-known roles within an digital trust ecosystem, the complete set depends on the particular ecosystem. In one ecosystem, the availability of credential issuers could be critical but privacy of credential data might be a minor factor; in another ecosystem, it could be just the opposite. The bottom line is that performance of a risk assessment as a precursor to producing a trust assurance framework is mandatory.

How Trust is Created

Trust is defined as the "firm belief in the reliability, truth, ability, or strength of someone or something". Human trust is built from three main components: Inherent Trust; Acquired Trust and Referential Trust.

- **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 that people communicate in generally acceptable languages.

- **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.

In 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 enables us to accept the cryptographic operations inherent to SSI, such as digital signatures, key verification, key rotation, and data encryption.
- **Machine–Based Trust**: Computers systems can follow programming logic encoded in machine-readable rules enforced by rules engines or smart contracts that work consistently when they follow a well-managed systems development lifecycle.
- **Human Trust through Governance**: While computer technology can enhance trust, it ultimately depends on human decisions. Governments have laws and games have rules—SSI and verifiable credential ecosystems have *governance frameworks*. As explained in chapter 11, these frameworks capture the requirements of the governed parties and other stakeholders who rely on them to achieve trust.

The Requirements of Transitive Trust

In SSI and verifiable credential environments, the term *digital trust ecosystem* (or just *ecosystem* for short) has emerged to describe the set of roles, processes, entities, schemas, data, and credentials that are governed under a governance framework. This is led by a *governing authority* who plays a leadership role in conveying ecosystem trust. The trust conveyed within the boundaries of an ecosystem is called *non-transitive trust* because it does not extend past the scope and boundaries of the ecosystem.

The ultimate goal of SSI and verifiable credentials is to achieve *transitive trust*—trust can be extended from one digital trust ecosystem where credentials are issued to another where those credentials are accepted by verifiers. Transitive trust is how we can achieve a more secure, trustworthy and decentralized Internet.

Figure 34.1 encapsulate the major components of a digital trust ecosystem:

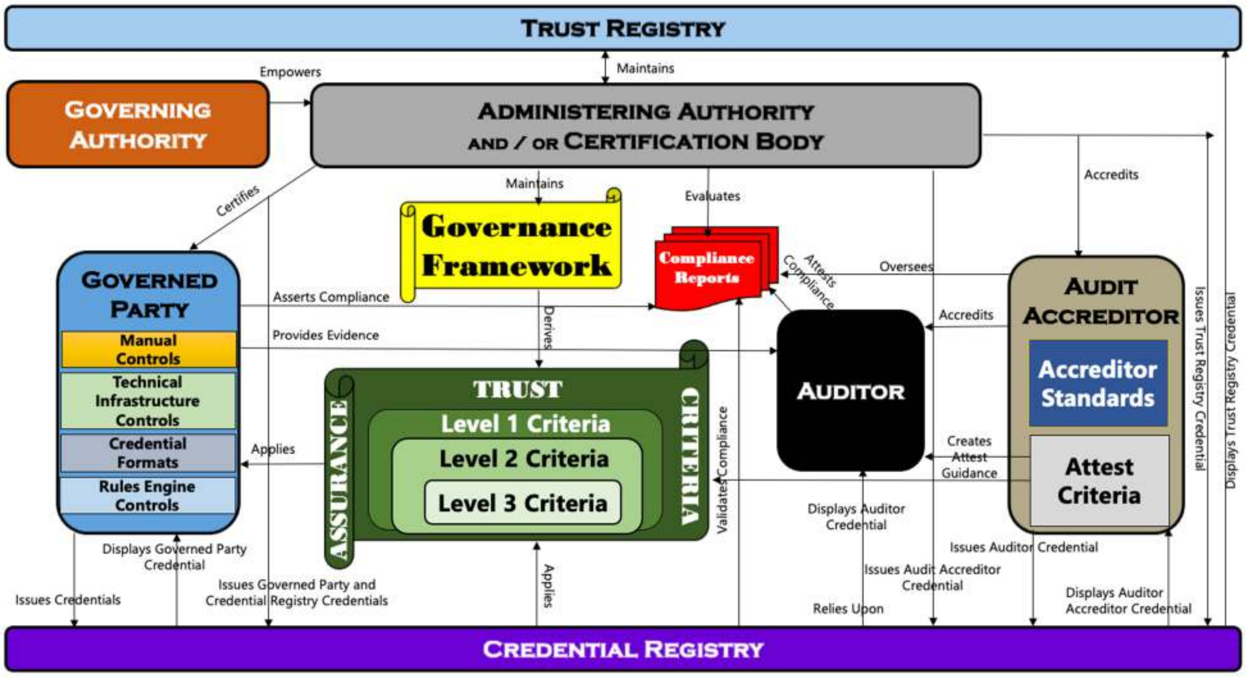

Figure 34.1: The components of a complete digital trust ecosystem designed to achieve transitive trust

The ecosystem creates assurance for all stakeholders that participants are applying generally accepted trust criteria to their products and services by introducing accreditation bodies and independent third-party auditors that enforce the trust assurance scheme. Stakeholders acquire trust from the ecosystem based on the ability of the participants to follow through on their commitments to comply with the governance framework. This acquired trust can then be passed referentially to others inside or outside the ecosystem.

Each participant has a defined role in creating trust in the ecosystem (*note that in these definitions and descriptions we will use First Letter Capitals for all formally defined roles*):

- **Governing Authorities** are the organizations responsible for ecosystem-wide governance. They operate on behalf of a trust community to define governance framework requirements and trust criteria 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. A Governing Authority may also serve as its own Administering Authority, or it may delegate to an Administering Authority to manage the ecosystem and Certification Bodies to convey trust. They set rules for the qualification of Auditors and audits to hold ecosystem actors accountable for these minimum standards for levels of assurance. They recognize Auditor Accreditors, issue them credentials, and place them on a Credential Registry. A Governing Authority may also issue a Governing Authority Credential to another Governing Authority to propagate risk assurance to a different ecosystem.

- **Administering Authorities** are organizations appointed by Governing Authorities to administer the operational components of a governance framework. They can take on many different duties as required by the Governing Authority, such as reviewing a Governed Party's performance audits and accrediting them as meeting minimum standards for varying levels of assurance. They can also issue credentials and place Governed Parties in a Trust Registry and/or a Credential Registry.
- **Certification Bodies** are organizations authorized by a Governing Authority to certify Governed Parties against a set of trust criteria. They demonstrate compliance by listing the Governed Party in a Trust Registry and/or issuing them a trust mark. PECB and BSI are examples of Certification Bodies. Certification may also be called *registration*; Certification Bodies may also be called *registrars*. Certification is the provision by an independent body of written assurance (a certificate) that a product, system, or services meets specific requirements. In this scheme, Governed Parties would be certified to meet trust criteria established by the Governing Entity. The International Standard ISO/IEC 17021:2015 guides Certification Bodies in the role of certifying systems under ISO/IEC standards. These Certification Bodies are accredited by ISO Accreditation Bodies (e.g., IAS, ANSI, ANAB, and UKAS) and have been evaluated against the ISO/IEC 17021 standard. This includes provisions for impartiality, independence, policies, practices, procedures, training, etc.
- **Governed Parties** are organizations or individuals who wish to play a recognized role in an ecosystem. They evaluate the auditable requirements (trust criteria) from the governance framework and implement manual procedures, rules engines, and other technical infrastructure in compliance with the trust criteria. They hold themselves out to a trust assurance framework which evaluates their criteria conformance resulting in Auditor compliance reports used for continuous improvement or actions taken by Administering Authorities to withdraw a Governed Party's right to participate in their ecosystem.
- **Audit Accreditors** are organizations authorized by a Governing (or Administering) Authority to approve and issue Auditor credentials under a particular governance framework. Auditor accreditation involves assessing the competence and qualifications of Auditors accepted within the relevant jurisdiction of the ecosystem against generally accepted audit standards. Audit Accreditors assert that their method of evaluating auditors meet global standards for competence, independence, and consistency. ISO/IEC 17024 specifies the criteria for an organization that conducts certification of persons in relation to specific requirements, including developing and maintaining a certification scheme for persons.
- **Auditors** are independent professionals trained in evaluating technology-based evidence provided by 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 Administering Authorities to issue compliance credentials to Governed Parties and place them on Credential Registries and Trust Registries. Confidence in an Auditor is based on their competence, period of audit and the

auditing methodology employed. The Auditor carries only *audit risk* (the risk of a misstated opinion) which is substantially less risk than the *assertion risk* that a Governed Party takes in asserting conformance over the trust criteria if they are not in fact conformant.

- **Trust Registries** are machine-readable registries of Governed Parties that are recognized by an Governing Authority as compliant with the trust criteria of the governance framework. Trust Registries can be as simple as verifiable lists of the decentralized identifier (DID) of each authorized Governed Party. Typically, they are publicly available for use by Verifiers whether operating inside or outside of the ecosystem.
- **Credential Registries** are publicly accessible repositories of credentials issued by Governing Authorities or Administering Authorities (or in some cases Governed Parties) and accessed by Verifiers during the process of validating trust. A Credential Registry is typically a publicly searchable directory with more attributes and information about the credential subjects than a Trust Registry. Therefore, a properly designed Credential Registry may also serve as a Trust Registry. The additional features of a Credential Registry are not always required in a digital trust ecosystem.

Governed Parties in a Trust Assurance Framework

The three main Governed Parties in a digital trust ecosystem are the three corners of the verifiable credential "trust triangle" described in chapter 1:

1. **Authoritative Issuer** - this Governed Party must assert conformance to trust criteria for the issuance of credentials. For example, if the stated level of assurance requires implementing identity proofing measures to a certain level of assurance prior to issuance of a credential, Authoritative Issuers must assert that their practices meet controls that satisfy those requirements. Typically, Authoritative Issuers transfer responsibility over the usage of credentials to Holders based on a contractual agreement to reduce their ongoing liability.
2. **Holder** - A party who is issued a Credential by an authorized Issuer. The Holder may or may not be the Subject of the credential. (There are many use cases in which the Holder is not the Subject, e.g., a birth certificate where the subject is a child, and both the mother and father may be Holders. Another case is a Credential Registry which serves as a secondary Holder for publicly searchable credentials.) If the credential supports zero knowledge proof (ZKP) cryptography, the Holder is also the Prover. These roles often assert trust based upon contractual agreements that transfer trust responsibility to the Holder for liability mitigation purposes.
3. **Verifier** - A party who requests proof of a credential from a Holder and verifies it to make a trust decision. Similar to an Authoritative Issuer, a Verifier can make trust assertions about its verification and data usage practices—usually a combination of generally accepted identity, industry, or ecosystem-specific trust criteria.

Trust Criteria

The Ecosystem’s Trust Criteria may consist of any combination of: 1) generally accepted trust criteria, 2) industry- or jurisdiction-specific trust criteria, and 3) ecosystem specific trust criteria.

Generally Accepted Trust Criteria

The following are widely accepted standards for asserting trust.

- **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 harmonize 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 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.

Industry-Specific Trust Criteria

In most cases, generally accepted trust criteria alone will not be sufficient to meet the needs of an ecosystem. It will also require industry-specific trust criteria such as the following:

- **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 highly industry specific, it has been widely adopted by the healthcare industry as an industry standard trust assurance framework.
- **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.
- **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 Authority that serves as an industry forum for the development and promotion of standards enabling a seamless marketplace for wholesale and retail natural gas and electricity. These standards are widely recognized by customers, business community, participants, and regulatory entities.

Jurisdiction-Specific Trust Frameworks

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

Ecosystem-Specific Trust Criteria

The set of mandates (MUST statements within a governance framework) can constitute its own set of trust criteria. The following are other examples of applications or business processes that require their 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 vendors. 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 applications such as Internet browsers.
- **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.

Assurance Levels

Several accreditation models have been successful in segmenting trust criteria to a few discrete assurance levels based on risk. The number of levels varies but is generally between two and four. This allows relying parties to subscribe only at the complexity, cost and assurance level that makes sense for their business. Risk and assurance must be assessed holistically given the product, the company, and the risks being addressed.

The US National Institute of Standards (NIST) has developed probably the most exhaustive analysis of levels of assurance in its revised publication, Digital Identity Guidelines (NIST Special Publication 800-63-3, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. It has become a widely accepted standard for identity trust frameworks. It defines two assurance level categories: Identity Assurance Level (IAL) and Authentication Assurance Level (AAL). It also established a "Federated Assurance Level (FAL)", however this may not be applicable in an SSI ecosystem.

While these levels may not fit perfectly into all ecosystems, the concept of levels of assurance still applies to SSI verifiable credentials since the level of assurance asserted in the issuance needs to match the level of assurance required by verifiers.

Recently, trust assurance innovators have begun exploring the use of a continuum of risk assurance levels by using an algorithmically produced assurance score. This approach is intriguing and one to monitor in the future.

Trust Evidence

Trust assertions are empty without evidence to support it. Trust evidence is the set of all information used by a party in support or 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 jurors towards a particular verdict.

The audited party and auditor should both consider all three of these 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). Thus the sufficiency and appropriateness of trust evidence are interrelated; the bar to cross is the combination that makes the evidence persuasive. For example, merely obtaining more trust evidence may not compensate if it is of low quality.

The following are examples of trust evidence that can be used to support trust assertions in ecosystems.

- **Signed contracts and agreements** - These are typical in operating agreements between a Governing (or Administering) Authority and its Governed Parties (members, contractors, subcontractors, vendors, etc). They are also typical between Authoritative Issuers and Holders of credentials. 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).
- **Signed approvals** - While less formal and authoritative than signed contracts, signed approvals of control processes demonstrate compliance to processes, especially manual processes.
- **Computer configurations** - In computer systems and networks, often the most definitive evidence of the state of operational parameters are 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 configured.
- **Certifications or accreditations** are tangible evidence that a standard has been met by an organization, process, person or thing. Certificates may be in paper form or stored digitally.
- **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.
- **Published policies, practices, and operating procedures** - While this evidence does not ensure an entity is compliant, it does convey management’s intention and clarifies to personnel what is expected and how compliance is achieved.
- **Computer and manual logs –** these 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.

Trust Mechanisms

The specific mechanisms an ecosystem can use to assure trust vary by risk, capital and cooperation. They may be deployed singly or in combination. Each mechanism mitigates varying levels of risk so each mechanism should be adopted after a proper risk assessment.

- **Contracts and agreements** should be formatted and signed as required by the authoritative jurisdiction. Breaches of contracts are mediated within that 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 called a *pledge*. A pledge lacks an explicit means of validation, but a recognized intent may signify more assurance than not overtly stating any intent, and a pledge that is explicitly broken by the pledging entity can entail legal liability.
- **Self-Assertion** - Governed Parties can declare, without independent attestation, that they are in compliance with trust criteria. They may be required to provide evidence to support their self-assertion either publicly or to a governance body (which would add some degree of assurance). A Governed Party risks reputational damage if a whistle blower disputes their assertion and it could result in legal action for misrepresentation or fraud.
- **Auditor attestation** is a commonly accepted form of reasonable—but not absolute—assurance that a Governed Party in a specific role is meeting the applicable trust criteria. An auditor attestation is stronger if the Auditor itself is accredited by an Auditor Accreditor for its competence, independence, and consistent practices.
- **Certification** - The step beyond Auditor attestations is for Governing (or Administering) Authorities to define complete certification programs for Governed Parties performing specific roles in a governance framework. They can do this themselves or deploy accredited Certification Bodies.
- **Trust marks** – are publishable, graphic representations of conformance to a set of trust criteria. A trust mark may be linked to another artifact, such as an Auditor opinion report or Certification Body certificate. In SSI or verifiable credential ecosystems, trustmarks can be asserted in a credential and stored in a Credential Registry.

Accountability and Value

"When the trust account is high, communication is easy, instant, and effective."
--Stephen R. Covey

The value of a digital trust 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 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, Governed Parties are risk averse. It is critical that each Governed Party remains only accountable to the risk reasonably afforded to them. For example:

- Governing (or Administering) Authorities must be accountable for the efficacy of trust criteria.
- Governing (or Administering) Authorities must be accountable for their fair and open accreditation of Audit Accreditors and Actors.
- Governed Parties must be accountable only for their asserted compliance to the trust criteria for the role they are serving as defined in the relevant governance framework
- Auditors must be accountable for their attestation opinions.
- Certification Bodies must be accountable for their certification of Governed Parties.
- Audit Accreditors must be accountable for their accreditation of auditors.
- Governing (or Administering) Authorities and Audit Accreditors must be accountable for the issuance of trust marks.

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 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 with inputs from all participants so continuous improvement is engineered into the model.

Steps to Implementing a Trust Assurance Strategy

The first step in implementing a successful trust assurance strategy is for the Governing Authority to develop the core elements of its governance framework (see chapter 11, in particular the section on the ToIP Governance Metamodel).

The second step is for the Governing Authority to establish a **Trust Assurance Working Group (TAWG)** consisting of both subject matter experts from the ecosystem and experienced risk management professionals.

The third step is for the TAWG to conduct an *ecosystem risk assessment* to determine the prioritized set of risks to be addressed by the trust assurance framework.

At that point, the TAWG can push forward with the rest of the tasks required to complete the trust assurance framework, including:

- Defining the trust criteria for each Governed Party role based on complexity, risk, and assurance to the relying public.
- Defining the required trust mechanisms and levels of assurance.
- Defining the requirements for Auditors, Audit Accreditors and/or Certification Bodies and how to evaluate their performance annually.
- Defining the reasonable costs and business model for trust assurance to be economically sustainable.

- Publishing the governance framework and trust assurance framework for public review by all relevant stakeholders.
- Publishing the approved governance framework and trust assurance framework and listing the initial Governed Parties, including any Auditors, Auditor Accreditors, and Certification Bodies.
- Evangelizing the governance framework and trust assurance framework to relevant governmental, commercial, and consumer stakeholders to anchor the process of public trust.

Conclusion: Critical Success Factors for Ecosystem Trust Assurance

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/or certification bodies, and
- Experience in the accreditation process

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 relying parties begin openly questioning whether they can trust the ecosystem. The recipe for long-lasting digital trust is to build in trust assurance when a digital trust ecosystem is formed and then manage quality and continual improvement as a core element of the program.