SSP C A SCOTT S. PERRY CPA, PLLC

AFFIRMING DIGITAL TRUST

DOMAIN-SPECIFIC TRUST ASSURANCE FRAMEWORK DEVELOPMENT KIT

SCOTT S. PERRY CPA, CISA

JUNE 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"Trust is the lubrication that makes it possible for organizations to work." --Warren Bennis

Trust is defined as the "firm belief in the reliability, truth, ability, or strength of someone or something". Digital trust is built from three main components: *Cryptographic Trust; Human Trust and Referential Trust. Referential Trust* is established through a trustworthy entity transferring trust upon a third party.

For a digital world, trust is an essential. As shown in Appendix D in the Sovrin Glossary, human trust is relied upon in layer three – Credential Exchange and is refined in the Governance Layer (Layer Four) with the introduction of the following roles creating a referential trust ecosystem: Trust Anchor; Credential Registry, Governance Authority, Auditor and Audit Accreditor. The following diagram depicts how these roles interact

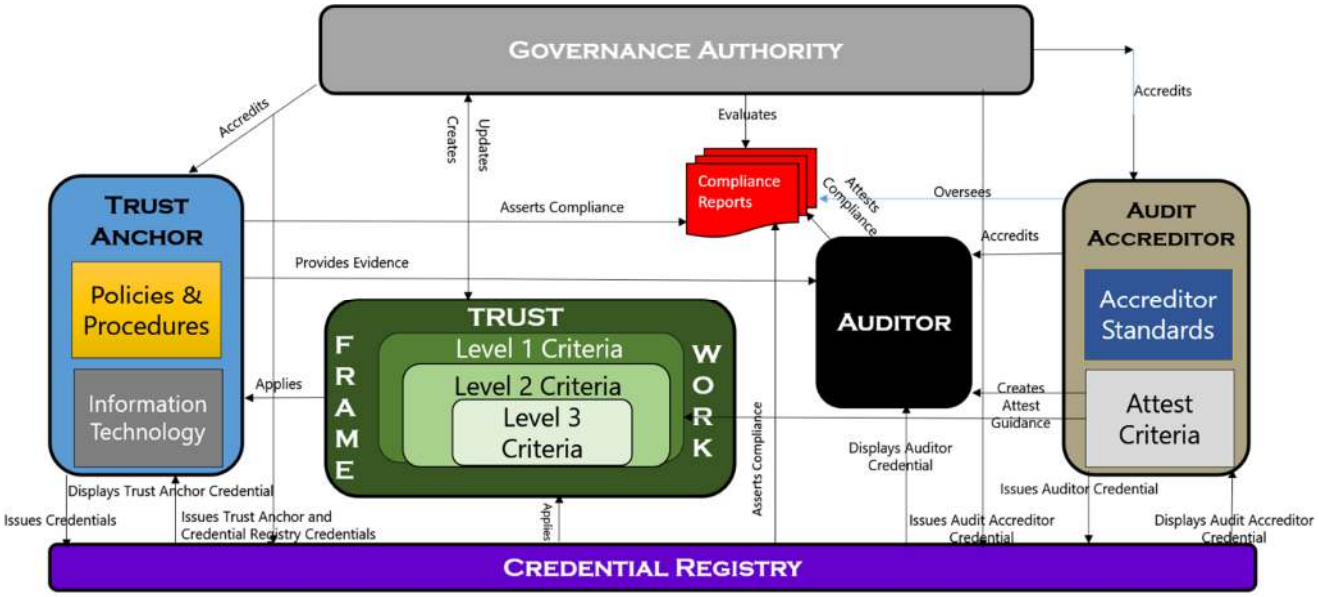

Figure A – Referential Trust Assurance Ecosystem

The ecosystem creates assurance to verifiers, identity owners and relying parties that trust anchors are applying generally accepted trust criteria to their methods and practices by the introduction of accreditation and independent third-party audits that act in their interest. Relying parties acquires trust from the ecosystem based on the ability of the players to follow through on its commitments and the integrity of its decisions. Symbols of this trust are stored on publicly accessible credential registry it can be propagated throughout the ecosystem.

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

- **Governance Authorities** define baseline requirements that mitigates risk dealing with the security, confidentiality, availability, processing integrity and privacy of transactions. They set

minimum standards for varying levels of assurance for participants to operate in the ecosystem. They accredit Auditor Accreditors (and issue Audit Accreditor Credentials placing them on a Credential registry) that set rules for the qualification of auditors and audits to hold trust anchors accountable for these minimum standards for levels of assurance. They review trust anchor performance audits and accredit trust anchors as meeting minimum standards for varying levels of assurance and issue Trust Anchor Credentials and place them on a Credential Registry.

- **Audit Accreditors** develop audit criteria out of baseline requirements developed from Governance Authorities They evaluate applicant auditors for their competence, independence and quality control measures and approve them to attest to audit criteria of trust anchor practices. They issue 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 evidence provided from Trust Anchors asserting that they are in compliance with audit criteria set forth by Audit Accreditation Bodies. They issue reports attesting to their opinions which enables Governance Authorities to issue Trust Anchor Credentials and place them on Credential Registries.
- **Trust Anchors** issue authoritative credentials to identity owners and verifiers based on minimum standards for varying levels of assurance set by a Governance Authority. They must continually assert their compliance with these standards and undergo audits of their compliance by auditors accredited by Audit Accreditors who develop audit criteria to obtain reasonable assurance of this compliance. As a result of these audits they receive accreditation by the Governance Authority as indicated by a credential stored and accessible within a Credential Registry.
- **Credential Registries** are Entities who maintain publicly accessible repositories of credentials issued by actors in this layer and accessed by Identity Owners, Verifiers and Relying Parties in the process of asserting trust. They apply Trust Framework Criteria to the protection of Credentials in the Registry subject to audit. A Credential Registry is an optional component of the Layer.

1 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.

You are reading this because you are interested in building a domain-specific trust framework for self-sovereign identities and verifiable credentials. Self-sovereign means a lifetime portable identity for any person, organization, or thing. It's a smart identity that everyone can use and feel good about. Having a self-sovereign identity allows the holder to present verifiable credentials in a privacy-safe way. These credentials can represent things as diverse as an airline ticket or a driver's license.

We have created this development kit responding to the increasing concerns on the lack of adherence to security best practices and privacy principles. The resulting diminishing consumer trust, and compromises of their data and privacy as the result of unprotected identities Internet devices and their applications, create unexpected and undue threats nullifying the promoted benefits of this technology. In the early nineties, there was a similar outcry over the Internet's use of commercial transactions. The risks of e-commerce transactions were real then. However, the treasures awaiting vendors generating twenty-four-hour sales from the far reaches of the globe were too tempting to heed the risks. 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 and human error. Society is now passed the point of no return of using public networks but no longer blindly trusts it. The demand is now high for oversight and integrity for Internet uses and it seems that the usual suspects for societal trust are reluctant to step forward. This creates the avenue for progress for an independent body such as the Sovrin Foundation to fill the void.

1.1 HOW TRUST IS CREATED

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

Inherent Trust stems from our acceptance of the laws of nature and human nature. We have inherent trust that the sun will come up (even though I don't get to see it in Seattle for three months) or that my heart will continue to beat (until it doesn't).

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 entity 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. The remainder of this kit is attributed to the ecosystem of Referential Trust.

1.2 THE ECOSYSTEM OF REFERENTIAL TRUST

So how does referential trust work in practice? The following diagram depicts the most commonly used model to create referential trust.

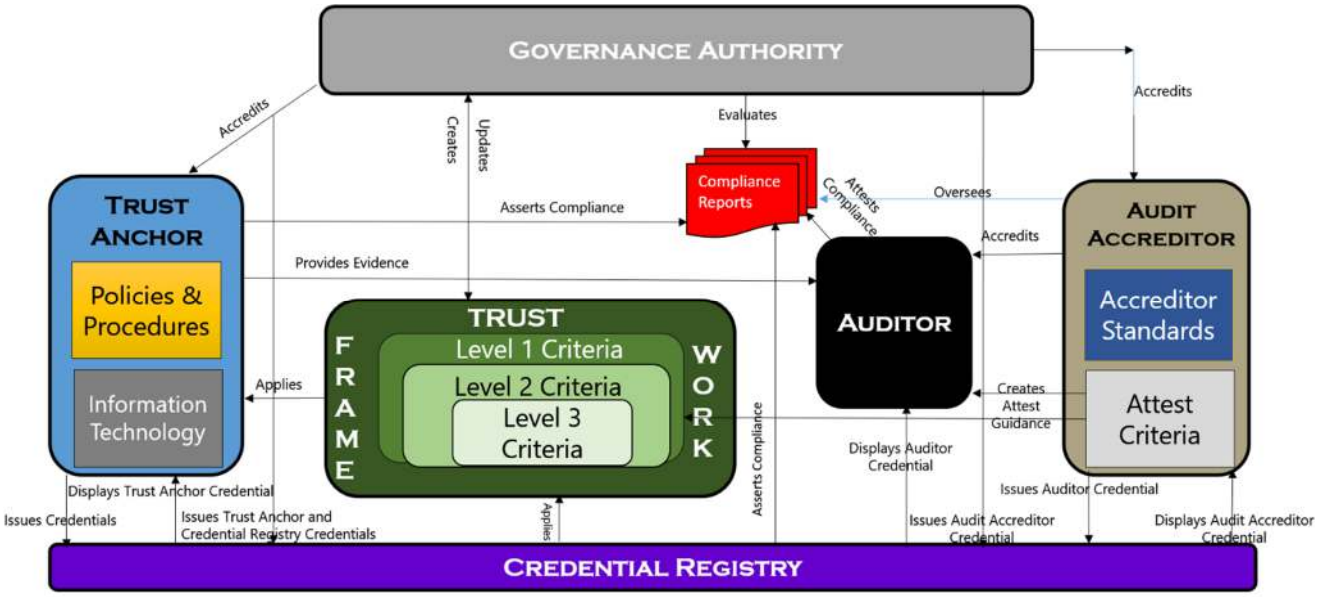

Figure 1 – Referential Trust Assurance Ecosystem

The ecosystem creates assurance to consumers 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 consumers. The consumer acquires trust from the ecosystem based on the ability of the players to follow through on its commitments and the integrity of its decisions. This acquired consumer trust can then be passed referentially to vendors who want to be engaged in the ecosystem.

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

- **Governance Authorities** define baseline requirements that mitigates risk dealing with the security, confidentiality, availability, processing integrity and privacy of transactions. They set minimum standards for varying levels of assurance for participants to operate in the ecosystem. They accredit Auditor Accreditors (and issue Audit Accreditor Credentials placing them on a Credential registry) that set rules for the qualification of auditors and audits to hold trust anchors accountable for these minimum standards for levels of assurance. They review trust anchor performance audits and accredit trust anchors as meeting minimum standards for varying levels of assurance and issue Trust Anchor Credentials and place them on a Credential Registry.
- **Audit Accreditors** develop audit criteria out of baseline requirements developed from Governance Authorities They evaluate applicant auditors for their competence, independence and quality control measures and approve them to attest to audit criteria of trust anchor practices. They issue 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 evidence provided from Trust Anchors asserting that they are in compliance with audit criteria set forth by Audit Accreditation Bodies. They issue reports attesting to their opinions which enables Governance Authorities to issue Trust Anchor Credentials and place them on Credential Registries.
- **Trust Anchors** issue authoritative credentials to identity owners and verifiers based on minimum standards for varying levels of assurance set by a Governance Authority. They must continually assert their compliance with these standards and undergo audits of their compliance by auditors accredited by Audit Accreditors who develop audit criteria to obtain reasonable assurance of this compliance. As a result of these audits they receive accreditation by the Governance Authority as indicated by a credential stored and accessible within a Credential Registry.
- **Credential Registries** are Entities who maintain publicly accessible repositories of credentials issued by actors in this layer and accessed by Identity Owners, Verifiers and Relying Parties in the process of asserting trust. They apply Trust Framework Criteria to the protection of Credentials in the Registry subject to audit. A Credential Registry is an optional component of the Layer.

1.3 EXISTING TRUST ENTITIES

The ecosystem has practical examples. The following are just a few of the security criteria and audit accreditation bodies that subscribe to a security accreditation ecosystem in some variant:

CRITERIA

- ANSI
- CA / Browser Forum
- Payment Card Industry
- Cloud Security Alliance
- NIST

AUDIT

- AICPA
- ISACA
- *t*Scheme
- Kantara
- GIAC

ORGANIZATION	DESCRIPTION
AICPA	The American Institute of Certified Public Accountants. It sets ethical standards for the profession and U.S. auditing standards for private companies, nonprofit organizations, federal, state and local governments. It develops and grades the Uniform CPA Examination, and offers specialty credentials for CPAs who concentrate on personal financial planning; forensic accounting; business valuation; and information management and technology assurance.
ANSI	The American National Standards Institute. Its mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and safeguarding their integrity. It represents the US accreditation body for ISO standards.
CA / BROWSER FORUM	Certification Authority / Browser Forum. Organized in 2005, it is a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing.
CLOUD SECURITY ALLIANCE	Its mission is to promote the use of best practices for providing security assurance within cloud computing and provide education on the uses of Cloud Computing to help secure all other forms of computing.
GIAC	Global Information Assurance Certification (GIAC) is the leading provider and developer of Cyber Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military and industry to protect the cyber environment.
ISACA	Formerly known as the Information Systems and Audit Control Association, ISACA engages in the development, adoption and use of globally

	accepted, industry-leading knowledge and practices for information systems.
NIST	The National Institute for Standards and Technology. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. It creates technology standards for US governmental agencies that have brought acceptance in the world and with the commercial marketplace.
KANTARA	As a global brand, Kantara Initiative Inc is an ethics based, mission-led 501 (c)(6) US nonprofit based organization passionate about giving control of data back to people. Kantara Initiative, Inc. provides real-world innovation and development of specifications and conformity assessment programs for the digital identity and personal data ecosystems. Beyond its flagship eID-assisting Identity Assurance Trust Framework, developing initiatives including Identity Relationship Management, ground-breaking User Managed Access (EIC Award Winner for Innovation in Information Security 2014) baselined for GDPR, Identities of Things, and the GDPR-ready Consent Receipt specification, Kantara Initiative connects a global, open, and transparent leadership community, including CA Technologies, Experian, ForgeRock, Digi.me, Internet Society, Nomura Research Institute and SecureKey..
PAYMENT CARD INDUSTRY	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, JCB, and China UnionPay
tSCHEME	tScheme is the independent, industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve Trust Services. The organization is taking a strong lead in Europe through its commitment to industry-led self-regulation, rather than government-led legislation.

Figure 2 – Trust Assurance Framework Players

2 COMPONENTS OF A DOMAIN SPECIFIC TRUST ASSURANCE FRAMEWORK

"He who does not trust enough will not be trusted." --Lao Tzu

After you have created a risk assessment model and understand the level of risk inherent and driven out of your industry and jurisdiction, the following are trust components that will need to be configured to appropriately meet relying parties needs of a trustworthy system and one that can communicate appropriately outside your domain to the global Web of Trust.

1. The Trust Elements that actors assert in the Domain
2. The Roles in the Domain that assert and rely upon Trust
3. Generally Accepted or Domain Specific Trust Criteria used in the evaluation of trust in the network
4. The Level of Assurance Relying Parties can take in the conformance of Roles for a specified Service
5. Trust Evidence is what trust asserters produce to create assurance regarding their trust assertions
6. The Trust Actors that play a key role in evaluating and opining upon trust assertions made by Domain Roles
7. Trust Mechanisms in place to assert and evaluate trust

2.1 TRUST ELEMENTS

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) Trust Information Integrity Task Force has established ensures the technical accuracy of a set of globally generally accepted set of Trust Services Criteria (TSC) which defines a baseline set of control objectives and procedures needed for trustworthy entities delivering trustworthy services and components. The following are high-level but can be helpful in accrediting entities, services and components where only specific trust principles needed to be assured:

2.1.1 SECURITY

A business's data and computing systems are fully protected against any unauthorized access, unauthorized and inappropriate disclosure of information, and any possible damage to systems that might compromise the processing integrity, availability, confidentiality or privacy of data or systems that may affect the entity's ability to meet its objectives.

2.1.2 AVAILABILITY

All information and computing systems are ready and available for operation and use at all times to meet the entity's objectives.

2.1.3 PROCESSING INTEGRITY

All system processing is complete, accurate, valid, timely and authorized to ensure that the entity meets its objectives.

2.1.4 CONFIDENTIALITY

Any information designated as confidential remains secure to meet the entity's objectives.

2.1.5 PRIVACY

All personal information collected, used, retained, stored, disclosed or disposed of must meet the entity's objectives.

2.2 POTENTIAL DOMAIN ROLES THAT ASSERT TRUST

The following Roles make assertions with regards to the Trust Elements to Relaying Parties of the Domain. For more information, please see the Sovrin Glossary:

2.2.1 GOVERNANCE AUTHORITY –

The Entity (typically an Organization) governing a particular Governance Framework such as a Domain-Specific Governance Framework. Depending on the design of the Governance Framework, the Governance Authority may be responsible for issuing Trust Anchor Credentials, Credential Registry Credentials, Auditor Credentials, or Auditor Accreditor Credentials. A Governance Authority may also issue a Governance Authority Credential to another Governance Authority to cross-link two Governance Frameworks.

Governance Authorities create policies, procedures, agreements and issues authoritative credentials that relying parties accept. It provides oversight into the risk assessment process for the Domain and implements trust assurance mechanisms applicable to mitigate identified risks.

2.2.2 STEWARD

An Organization approved by the Sovrin Foundation to operate a Node. A Steward must meet the qualifications defined in the Steward Business Policies and the technical requirements defined in the Steward Technical Policies (see Appendix A of the Sovrin Governance Framework Master Document). A Steward must also execute the Sovrin Steward Agreement.

Domain Specific Governance Frameworks depend on the underlying operation of distributed ledger nodes. At the Steward layer, Stewards are guided by business and technical policies and must agree to a Steward Agreement. Based on mitigating controls endemic to these controls, Stewards self-assert they are in compliance with their responsibilities to the network.

2.2.3 AGENT

A software program or process used by or acting on behalf of an Entity to interact with other Agents or with the Sovrin Ledger or other distributed ledgers. Agents are of two types: Edge Agents run at the edge of the network on a local device; Cloud Agents run remotely on a server or cloud hosting service. Agents require access to a Wallet in order to perform cryptographic operations on behalf of the Entity they represent.

The Agent Layer is located below the Domain Specific Governance layer and operates using global standards using formats and protocols promulgated by standards authorities such as W3C and the Linux Foundation. There is an implied assertion that agent software has been developed and implemented using a generally accepted software life-cycle methodology with reduces processing errors to an acceptable level.

2.2.4 CREDENTIAL REGISTRY

An Entity that serves as a Holder of Credentials issued by Trust Community Members in order to provide a cryptographically verifiable directory service to the Trust Community or to the public. The term also refers to the actual repository of Credentials maintained by this Entity. An informal Credential Registry may accept Credentials from participants whose purpose is to cross-certify each other's roles in the Trust Community. A formal Credential Registry may be authorized directly by a Governance Authority or Accredited by an authorized Auditor for the relevant Governance Framework.

Credential Registries must assert trust elements over the protection, integrity and availability of its repository. Its asserted trust criteria are likely to be a generally accepted

2.2.5 DEVELOPER

An Individual or Organization that develops hardware or software providing the functionality of any component of Sovrin or Domain-Specific Infrastructure, including Nodes, Wallets, and Agents, Verifiers and Issuers.

There is an implied assertion that developers develop and implement code using a generally accepted software life-cycle methodology with reduces processing errors to an acceptable level.

2.2.6 HOLDER/SUBJECT/IDENTITY OWNER

A role played by an Entity when it is issued a Credential by an 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 baby and both the mother and father may be Holders. Another case is a Credential Registry.) If the Credential supports Zero Knowledge Proofs, the Holder is also the Prover.

These roles usually assert trust based upon terms it contracts with other roles in formal agreements. These agreements are a way for other Roles to transfer trust responsibility for liability purposes.

2.2.7 ISSUER

The Entity that issues a Credential to a Holder.

Issuers must assert trust over practices it deploys in the issuance of credentials. If the stated level of assurance warrants identity proofing measured to be deployed prior to issuance, Issuers assert that their practices meet controls that satisfy the requirements under that level of assurance. Typically, Issuers transfer responsibility over the usage of credentials after issuance to Holders based on a contractual agreement.

2.2.8 VERIFIER

An Entity who requests a Credential or Proof from a Holder and verifies it in order to make a trust decision about a Sovrin Entity

Similar to an Issuer, a Verifier makes trust assertions about its verification practices. Often this is comprised of a combination of generally accepted identity, industry or special purpose trust criteria.

2.3 TRUST CRITERIA

The following is the set of control requirements that comprise the Domain Network. It consists of 1) Generally Accepted Trust Criteria, 2) Sovrin Specific Trust Criteria and 3) Domain Specific Trust Criteria

2.3.1 GENERALLY ACCEPTED TRUST CRITERIA

This section will call out marketplace accepted standards that guide Roles in asserting trust. The following are core examples:

2.3.1.1 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.

It is aligned with the *Internal Control—Integrated Framework,* published by The Committee of Sponsoring Organizations (COSO), a foundational document for digital trust. These principles for the basis of Service Organization Control (SOC) reports that are well established in the marketplace.

2.3.1.2 ISO/IEC 27001:2013

ISO/IEC 27001 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. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts. - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profits), all sizes (from micro-businesses to huge multinationals), and all industries or markets (e.g. retail, banking, defense, healthcare, education and government). This is very generic but has been established as a baseline to establish interoperable trust, especially outside the United States.

2.3.1.3 WEBTRUST FOR CERTIFICATION AUTHORITIES

Many issuers and verifiers of PKI technology are Certification Authorities (CA), entities that issue digital credentials that are relied upon in a domain. While there are varying sets of criteria that have been established to promote trust of these entities, the gold standard is the WebTrust Principles and Criteria for Certification Authorities as promulgated by CPA Canada who oversees the WebTrust program.

The document is a set of Control Objectives and control practices required for a generic CA to operate dependably and consistently in order to be relied upon by accepters of digital certificates it issues.

2.3.1.4 ETSI EN 319 411

The European Telecommunications Standards Institute (ETSI) is a European Standards Organization that promotes standard for telecom, broadcasting and communication networks. It also has created its own set of standards for Certification Authorities that are accepted globally but mostly within the European Union.

2.3.1.5 ISO/IEC 29115:2013

This standard provides a framework for managing entity authentication assurance in a given context. In particular, 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.

2.3.1.6 NIST SP 800-63-3

The United Stated National Institute of Standards and Technology has issued a revised version of its Digital Identity Guidelines. These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. 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.

2.3.2 INDUSTRY SPECIFIC TRUST CRITERIA

In most cases, generally accepted trust criteria will be insufficient to the needs of the domain. Domain specific trust criteria may be specific to the industry the domain acts in, the jurisdiction it operates under or the specific set of services it offers its network platers and relying parties. Below we will show examples of each.

2.3.2.1 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 for the banking section. Banking regulators and auditors typically use its guidance in their audits

2.3.2.2 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Payment card companies had their own trust criteria until they were aligned by a domain governance authority called the Payment Card Industry Security Standards Council. 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 PCI DSS. Independent/private organizations can participate in PCI development after proper registration. Each

participating organization joins a particular SIG (Special Interest Group) and contributes to the activities which are mandated by the SIG

2.3.2.3 NAESB WEQ-12

The North American Energy Standards Board is a governance authority 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.

As the de facto business standard body for North American energy, North American Energy Standards Board (NAESB) created a PKI standard (WEQ -12) to address an ever-increasing cyber threat landscape around one of our most important critical infrastructure sectors, the power grid. High stake energy applications such as energy trading, off-peak consumption, smart metering expansion, and eTagging require strong authentication and encryption provided through NAESB complaint certificates.

2.3.2.4 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. The standards development mission of DirectTrust today grew from those voluntary discussions and workgroup meetings that began in April 2011 among stakeholders eager to develop standards suitable for the growth of such an exchange approach.
The **Direct Standard™** was first formalized in a document called the "Applicability Statement for Secure Health Transport" crafted from the Direct Project and published in April 2011, with updates in 2012 and 2015.

2.3.3 JUDISDICTIONALLY SPECIFIC TRUST FRAMEWORKS

2.3.3.1 US FEDERAL PUBLIC KEY INFRASTRUCTURE

The Federal Public Key Infrastructure (FPKI) Program provides the government 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 CAs and the Policies, Processes, and Auditing of all the participants are referred to as the Federal Public Key Infrastructure (FPKI). The FPKI includes the U.S. Federal, State, Local, Tribal, Territorial, international governments and commercial organizations that work together to provide services for the benefit of the Federal Government.

The FPKI Policy Authority (FPKIPA) maintains two Certificate Policies to which all Certification Authorities map their policies.

To operate a Certification Authority used in the Federal Government and that contains federal data requires the application of NIST Special Publication (SP) 800-53 security controls. The following document contains the additional security controls that all Certificate Practice Statements (CPSs) must address.

The Federal Government uses specially formatted credentials to identify employees and contractors affiliated with agencies. These credentials are issued with the same processes and technology to provide a common baseline for authenticating to government networks, accessing government facilities, and authenticating to cross-government applications. These credentials conform to both the NIST Standards and the FPKI Certificate Policies

2.3.3.2 EIDAS

eIDAS (electronic IDentification, Authentication and trust Services) is an regulation on / a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.

eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. Both the signatory and the recipient can have more convenience and security. Instead of relying on traditional methods, such as mail or facsimile, or appearing in person to submit paper-based documents, they may now perform transactions across borders, like "1-Click" technology.

2.3.3.3 PAN CANADIAN TRUST FRAMEWORK

The 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).

The PCTF describes the roles require and requirements to be agreed on, by participating public and private sector organizations, to meet current and future Canadian innovation needs. The PCTF incorporates DIACC's Digital Identity Ecosystem Principles listed in this document.

The PCTF documents and artifacts are intended to secure interoperability of public and private sector identity capabilities while prioritizing user-centered design, privacy, security, and convenience of use. PCTF Discussion Drafts will be released in a phased approach where all Canadians and international interested parties are invited to submit comments for consideration.

2.3.3.4 AUSTRALIAN DIGITAL IDENTITY FRAMEWORK

The 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. These documents set the standard for:

- how personal information is handled by participating government agencies and organizations
- the usability and accessibility of identity services
- how the identity system is secured and protected against fraud
- how identity services are managed and maintained
- how this framework will be managed

2.3.4 SPECIFIC PURPOSE TRUST CRITERIA

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

2.3.4.1 CA/BROWSER FORUM BASELINE REQUIREMENTS

The Certification Authority Browser Forum, also known as 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 and Code Signing digital certificates that chain to a trust anchor root that is embedded in such applications.

As one of its guiding practices, it has created a set of baseline requirements for the issuance and management of publicly trusted certificates. The criteria set describes a subset of the requirements that a certification authority must meet in order to issue digital certificates for SSL/TLS servers to be publicly trusted by browsers.

2.3.4.2 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.

2.3.4.3 SHAKEN/STIR

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. Essentially, the SHAKEN procedures utilize STIR protocols to allow communications service providers to attest the legitimacy of a calling party's number.

2.4 ASSURANCE LEVELS

Several accreditation models have been successful in segmenting the trust criteria to a few risk and assurance levels. This allows for vendors 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 consumer risk it addresses, etc. The best segmentation is probably two or, at maximum, three tiers of assurance to which vendors could subscribe. These levels would increase in risk, compliance cost, and public assurance.

The US National Institute of Standards (NIST) has done 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 the new standard for identity trust frameworks. In the document, two relevant assurance level categories are defined: Identity Assurance Level (IAL) and Authentication Assurance Level (AAL). It also established a "Federated Assurance Level (FAL)", however that may not be applicable in the Sovrin Model.

- IAL: The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors.
- AAL: The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs)

The document further defines requirements to reach varying levels of assurance:

- IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).
- IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
- IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
- AAL1: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a NIST SP 800-63-3 DIGITAL IDENTITY GUIDELINES vii This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-63-3 wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

- AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.
- AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

While these levels may not fit perfectly into the Sovrin Web of Trust, the concept of levels of assurance should be a required accreditation component since all credentials are not equal and, given the wide range of use cases, there is a need to match utility with cost for web of trust providers.

2.5 TRUST EVIDENCE

Trust assertions are empty without evidence to support it. Trust evidence is all the information used by the Entity is supporting the adherence to the trust criteria. According to generally accepted audit standards, evidence must be sufficient and appropriate 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. The entity should consider the sufficiency and appropriateness of trust evidence to be presented when presenting proof that a complex criterium is in place 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 also by the quality of such trust evidence (the higher the quality, the less the trust evidence that may be required). 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 the marketplace.

2.5.1 SIGNED CONTRACTS AND AGREEMENTS

This evidence is typical in agreements with Issuers and holders of credentials. It also may be in operating agreements between a governance authority and its members, contractors with subcontractors, entities and its vendors. In some jurisdictions, signed contracts and agreement take precedent over the rule of law. Signatures must be legal (some jurisdictions may not accept some forms of electronic or digital signatures.

2.5.2 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.

2.5.3 CERTIFICATIONS

Certifications / Accreditations are tangible evidence that a standard has been met by an organization, process person or thing. Certificates can be in paper form or stored digitally. Based on the certifier, this can be a persuasive form of trust evidence.

2.5.4 SIGNED APPROVALS

While less formal and authoritative than signed contracts, signed approvals of control processes demonstrate compliance to processes, especially manual processes.

2.5.5 DEMONSTRATIONS OF COMPLIANT PROCESSES

When organizations can demonstrate, on demand, their compliant processes, it creases persuasive evidence. Demonstrations can visual or through computer processes. Screenshots may augment the evidentiary package.

2.5.6 POLICIES, PRACTICES AND OPERATING PROCEDURES

While this evidence does not ensure that compliant procedures are operating, it does convey management's intention and clarifies to personnel what is expected and how compliance is achieved.

2.5.7 LOGS

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.

2.6 TRUST ACTORS

The following is the set of entities that play a role in assessing and opining on trust assertions in the domain

2.6.1 DOMAIN SPECIFIC GOVERNANCE BOARD

The Governance Board is responsible for overall trust of their network. It performs a risk assessment over network risk and develops an audit/accreditation scheme that fits the risk assessment. It may perform

certification practices or employ an external certification body to maintain consistent trust. It may directly certify auditors or assessors or may employ external audit accreditors. It may issue their own accreditation credentials or employ external parties to issue them on their behalf.

2.6.2 AUDITOR/ASSESSOR

An Individual or Organization that performs Accreditation on behalf of a Governance Authority.

An Auditor/Assessor asserts attestation over an audited entity's trust criteria based on the auditor's competence, period of audit and the auditing methodology employed. This is substantially less risk than the entity makes in asserting these criteria.

2.6.3 AUDIT ACCREDITOR

An Organization authorized by a Governance Authority to issue Auditor Credentials under a particular Governance Framework. Auditor Accreditation involves assessing the competence and qualifications of Auditors accepted within the relevant jurisdiction 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 relationship to specific requirements, including developing and maintaining a certification scheme for persons.

2.6.4 CERTIFICATION BODY

A Certification Body is an external entity which has been accredited to certify companies against a management system or a specific set of trust criteria. 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, Roles would be certified to meet trust criteria established by the Governance Board.

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.

2.6.5 LEGAL AUTHORITIES

Domain Specific Governance Authorities operating in a jurisdiction must comply with domain laws. Legal compliance may require the deployment of jurisdictional regulators that possess their own accreditation. Certification or audit/assessment schemes.

2.7 TRUST MECHANISMS

Depending on risk, capital and cooperation, the following are actions that the Domain takes to assert and assure trust. They may be deployed by itself or in combination of schemes.

2.7.1 CONTRACTS AND AGREEMENTS

Contracts and Agreement can be established between roles and the Governance Authorities and between Issuers and Holders or credentials. 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.

2.7.2 SELF-ASSERTION

Roles 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 governance body. That would add a degree of assurance.

2.7.3 AUDITOR ATTESTATION

Auditor/Assessor Attestation provides the most generally accepted form of reasonable, 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.

2.7.4 CERTIFICATION

Governance Bodies may, in addition to accepting audit/assessor attestations, perform certification processes of roles against trust criteria. They can do this themselves or deploy accredited certification bodies (see section 2.6.4).

How does a certification body validate if trust criteria are compliant, and how does the Domain Role maintain compliance? The following is a four-phase certification process modeled against the US Federal government to certify compliance with mandated federal controls.

1. Initiation and Planning
2. Audit /Assessment
3. Certification
4. Continuous Monitoring

Each phase has a list of activities that must be completed before beginning the next phase.

2.7.4.1 PHASE I: INITIATION AND PLANNING

The first phase of the process is initiation and planning. In this phase, the Role Sponsor and the Certification Body will formally initiate the process by acknowledging that certification is required, establishing a certification team, developing a project plan with milestones, determining a formal level of assurance classification for the process and deciding what resources are required to perform a certification process.

The Role Sponsor will be responsible for compiling all the required trust evidence and performing a self-assessment. Based on the outcome of the self- assessment, any compliance exception should be detailed and conveyed as part of the audit process (Phase II) A certification readiness package should be completed and reviewed by the Certification Body before moving onto Phase II – Audit / Assessment.

2.7.4.2 PHASE II: AUDIT / ASSESSMENT

In the Audit / Assessment phase, a team of independent auditors / assessors will perform a review of the audit readiness package and audit the domain Role's adherence to the trust criteria utilizing a checklist or methodology to validate that the proper policies, practices, procedures or evidence have been implemented. The independent audit will consist of onsite interviews, examination of documents, and visual inspections and attribute testing. Once the independent audit is complete, the auditors will assemble a formal report package with the results of their evaluation and make a recommendation to the Certification Body on the certification worthiness of the Domain Role.

2.7.4.2 PHASE III: ACCREDITATION

In the Accreditation phase, the Certification Body will review the completed audit package to validate that all the required information is contained within the package before making an accreditation decision. Once the Certifying Body has reviewed the final package and auditor's recommendations, he/she will make a determination to accept any compliance exception risk before granting an accreditation. If the Certification Body concludes that the package contains all the required documentation and there are no unacceptable risks, a formal letter of accreditation will be issued to the Role Sponsor and issue them a certificate or Trustmark evidencing their achievement.

2.7.4.3 PHASE IV: CONTINUOUS MONITORING

In order to maintain the Role's compliant baseline and to detect any new threats to their compliant processes, a process of continuous monitoring must be implemented. Roles should institute processes to monitor ongoing compliance to the trust criteria. By establishing a process to continuously monitor the information system, the Role Sponsor can detect any compromises that may adversely impact their compliance. In addition, Roles may perform internal audits to ensure that they have maintained its compliance baseline.

3 TRUST ASSURANCE IMPLEMENTATION METHODOLOGY

"Trust is not simply a matter of truthfulness, or even constancy. It is also a matter of amity and goodwill. We trust those who have our best interests at heart, and mistrust those who seem deaf to our concerns." – Gary Hamel

When a Domain wants to implement a Trust Assurance scheme, it should follow the following steps:

1. Domain Risk Assessment
2. Identify Domain Roles
3. Choose Level(s) of Assurance
4. Identify Trust Criteria
5. Identify Trust Schemes
6. Select External Resources
7. Document Criteria and Methodologies
8. Communicate the Scheme
9. Put the Framework into Operation
10. Create Continuous Improvement Loop

3.1 DOMAIN RISK ASSESSMENT

A diligent risk assessment attempts to identify inherent threats to network performance, application viability and compliance. Each domain-specific governance authority has their own list of threats depending on their domain. For guidance, all governance frameworks that involve identity and verifiable credentials have these categories of risk:

- Identity and Verifiable Claims specific risks:
  - Imposter Risk
  - Fraud Risk
  - Identity Proofing Risk
  - Identity Authentication Risk
  - Privacy Risk
  - Liability Risk
- Industry Risks:
  - Industry Compliance Risk
  - Application Risks
  - Business Process Risks
  - Liability Risk
  - Economic Risk
- Jurisdictional Risks
  - Litigation Risk
  - Jurisdictional Compliance Risk
  - Liability Risk

- Infrastructure Risks:
  - Security Risk
  - Confidentiality Risk
  - Availability Risk
  - Integrity Risk
  - Privacy Risk
- Interoperability Risk:

These risks (and more) need to be identified and analyzed as to their likelihood of occurrence and dollar impact in order to construct a governance control model that will adequately mitigate risk to acceptable level for all network participants. This exercise will drive a tailored approach to trust assurance as applications that depend on highly authentic identities and verifiable credentials (such as a banking application) will comprise a more comprehensive set of trust components than one that requires less assurance (like a social media application).

There are generally accepted standards for risk assessment. ISO 27005 and NIST 800-37 rev 2 are guidance documents to be considered in performing a risk assessment. ISO 27005 emphasizes the importance of a systematic approach to developing and maintaining an information security risk management (ISRM) process — and reminds stakeholders that risk management must be continual and subject to regular review to ensure continued effectiveness.

NIST 800-37 Rev 2 describes a Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels.

3.2 IDENTIFY DOMAIN ROLES

Domains are not one size fits all. There is a myriad of ways that self-sovereign identities and verifiable credentials will be implemented. More than we can even imagine today. However, it is likely that there will be Issuers, Verifiers, Credential Registries and a Governance Authority in place to manage it all.

An implementation consideration is: what will it take to be a qualified domain role and what vetting mechanism will be put in place by the Governance Authority to implement it? Are there barriers to entry for Domain 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 Domain?

3.3 CHOOSE LEVEL OF ASSURANCE

A Level of Assurance conveys the trustworthiness of a credential. The Domain's Risk Assessment will drive the level of assurance needed for its own domain. But what if the Domain wants its credential to be trusted outside its domain into the Web of Trust. 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 domain wanted to exact a minimum, commercial-grade degree of trust.

3.4 IDENTIFY TRUST CRITERIA

This document has illustrated several viable trust criteria. The key in determining what would be required for your Domain is the level of specificity. What is particularly unique about your domain that it requires unique consideration? If there is none, don't deploy unique requirements because the governing authority will have to maintain it. There is 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.

3.5 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. Class 1 credentials may not need more than contracts and self-assertion mechanisms. Class 2 credentials might not need more than periodic audits from recognized audit/assessor firm. Whereby Class 3 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 Domain Roles in asserting that trust.

Another factor is cost. Trust schemes that convey even a medium level of assurance cost money. Certification bodies, 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.

3.6 SELECT EXTERNAL RESOURCES

If the trust scheme selected in section 3.5 require the involvement of external resources, they need to be identified, courted, contracted and deployed. The Governance Authority 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 Domain Roles?
- Is there a need for an Audit Accreditor to vet auditor/assessors?
- Is an ISO-accredited Certification Body appropriate for the Domain's needs?

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

3.7 DOCUMENT CRITERIA AND METHODOLOGY

A method of memorializing decisions made by the Governance Authority 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 Domain Roles.

This document should state its objective to create trustworthiness of credentials issued and verified within its domain, the process to become a role in the domain and the summary of choices the domain makes about assurance. The following should be described:

1. Results of a Domain Risk Assessment
2. Domain Roles
3. Level(s) of Assurance Allowed
4. Trust Criteria being used by Roles
5. Methodology of Trust Schemes in place
6. External Resources contracted to operate the Scheme

3.8 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 Domain 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. They cannot be any surprises when it time to demonstrate accountability.

Communicating the scheme included in the Criteria and Methodology document is a way of attracting relying parties to the Domain. The Framework itself is competitive advantage engaging participants to perceive greater trust in credentials that are issued and verified under its methodology. The Governance 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.

3.9 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 point of time through review of the design of control processes prior to operation. The Governance Authority will have an entity establish to deal with compliance issues and review audit reports from the field. A mechanism of discontinuance should be in place that will eliminate unaccountable Domain 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.

The following is an illustrative Framework in operation. It involves Issuers, Verifiers, a Governance Authority, Holders and Insurers (A service provider who provides insurance to Issuers for the potential liability of asserting a Credential or to Verifiers or Relying Parties for the potential risk of relying on a Credential)

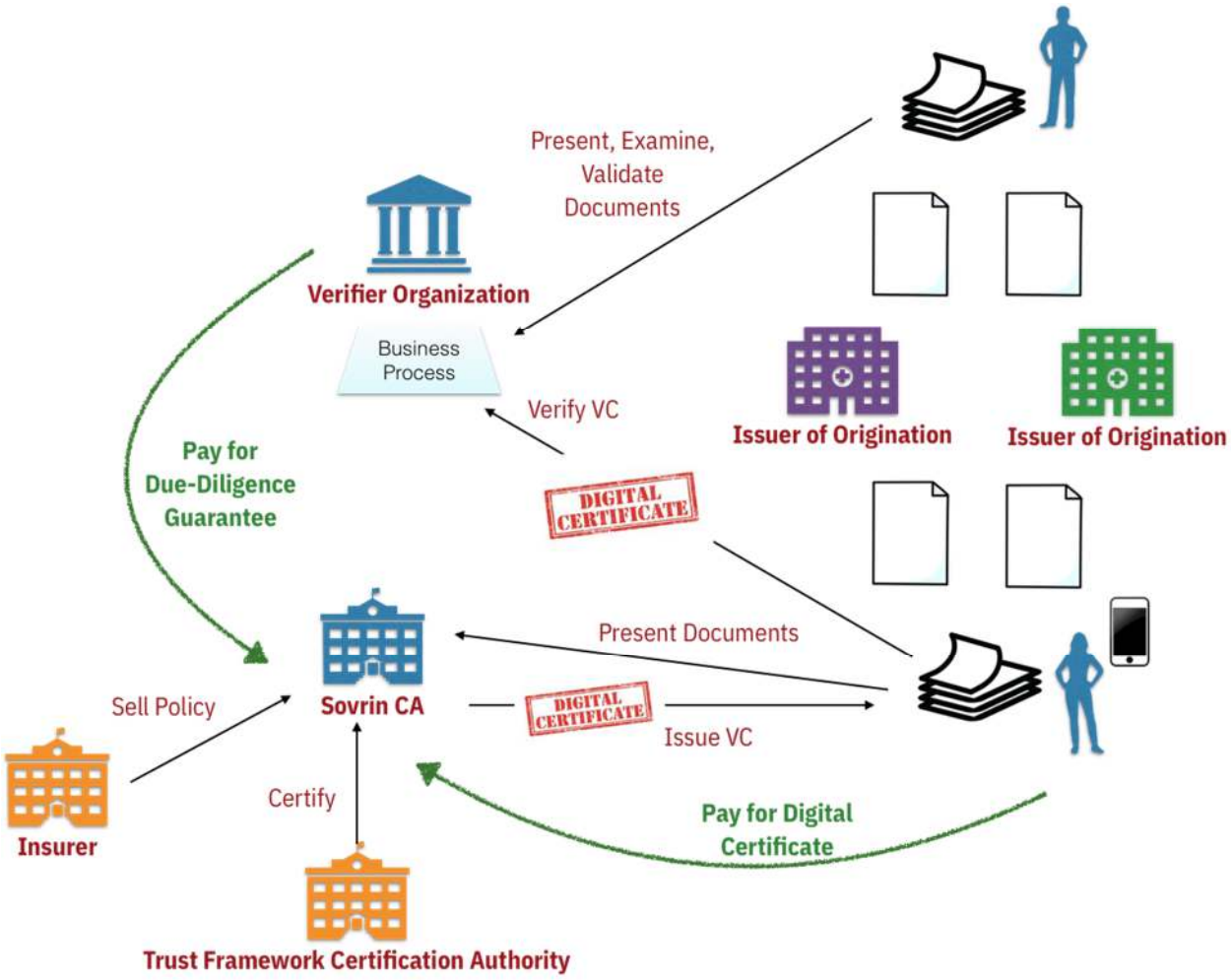

DIAGRAM COURTESY OF DAN GISOLFI, IBM

The key factor in relying upon the Governance Authority, services and Domain Roles is through legal contracts and verifiable audits. The challenge is that all pieces provide varying flavors of assurance including the following: assurance levels, technical nature, business process and certification orientation. It will require a hybrid method of multiple attestations depending on the trust being promoted into the ecosystem.

In this scenario where a Sovrin Certification Authority is vetting identity for use in industry dependence, The Trust Framework Certification Authority needs to establish minimum accreditation standards needed to be able to rely on the stakeholders in this diagram. Variants of established trust criteria are likely to be needed since this ecosystem creates novel interactions.

Whereas CAs use WebTrust for CAs (and ETSI) as their accreditation model for the issuance of client and server authentication certificates, there will likely be a need to produce a variant for these digital certificates.

While NIST 800-63-3 is new, it was not created with this Framework in mind. It is likely that there will be modification needed in digital identity standards to work within this domain so CAs or Issuer/Verifiers can be trusted globally.

Agent developers must adhere to trust criteria of processing integrity in the systems development life cycle processes and obtain trustworthy code signing certificates, so their applications can be trusted.

The foundation of trust must be established for token reliance before it can be used for a measure of value exchange. The domain cannot be exploited by bad actors as we have seen in cryptocurrency exchanges if tokens will be used for digital certificates and verifiable claims. While there are emerging standards for cryptocurrencies, it needs an accountable trust scheme to ensure token issuers and exchangers are meeting minimum standards.

Industry standards must evolve to incorporate these types of domains without adding unnecessary burden needed to operate use cases and realize their potential.

Insurance policies and legal contracts must take advantage of established concepts, laws and regulations and interpret then in a novel way, so they can function in this decentralized domain.

3.10 CREATE CONTINUOUS IMPROVEMENT LOOP

Like any world-class management system, the Domain's Trust Framework must gather feedback on its effectiveness and deploy improvement strategies to refine its shortcomings. It must convey this effort openly to stakeholders, so accountability of the Governing Authority is maintained.

4 SOME FINAL RECOMENDATIONS

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

The value of the ecosystem is highly dependent on the integrity of the players. Conflicts of interest must be identified and eliminated. Procedures driving compliance must be fair, open, clear and timely. All players 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 engagement must be reasonable and matched to the value they assert.

The criteria itself must have clear and cost-effective practices available to demonstrate compliance. The roll-up of the totality of compliance costs must be less than the value the vendors commercially realize, or they will refuse to participate.

In our litigious society, all parties in a trust assurance model are risk averse. It is critical that each player remains only accountable to the risk reasonably afforded to them. For example, the public cannot hold the following players accountable for more than its participation in the process:

- Domain Roles must be accountable for their compliance assertion;
- Governance Authorities must be accountable for the efficacy of baseline requirements.
- Governance Authorities must be accountable for their fair and open accreditation of Audit Accreditation Bodies and vendors;
- Auditors must be accountable for their attestation;
- Certification Bodies must be accountable for their certification of Domain Roles.
- Auditor Accreditation Bodies must be accountable for their accreditation of auditors.
- Auditor Accreditation Bodies must be accountable for the issuance of Trust Marks or Seals.

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. Consumers and its 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 players so continuous improvement can be reengineered into the model. Components of a Domain Specific trust assurance framework

4.1 SHOULD SELF-CERTIFICATION BE ALLOWED?

Many models include the practice of self-certification. Frankly the term is an oxymoron. Self-certification is another term in the ecosystem for an assertion which, by definition, does not contribute to referential trust. It creates only an illusion of trust especially if seals are displayed but the domain's security trust should strive for higher trust and assurance.

4.2 WHERE TO LOOK FOR SPECIALTY TRUST ASSURANCE SERVICES?

So how can a domain role who does not operate a complex component or process and only needs to subscribe to a portion of the Domain Trust Assurance Framework get certified? The answer is in component services and assurance levels.

The following are component services presently in the market that can play a role in the Domain Trust Assurance Framework.

- Credential Services Provider
- Token Services Provider
- Data Custodian
- Certification Authority
- Identity Proofer
- Token Issuer
- Physical Security Hosting Facility

4.3 WHAT ARE THE CRITICAL SUCCESS FACTORS FOR DOMAIN GOVERNANCE?

This is the most difficult question to answer but the requirements are clear. In order for Domain governance to work, it needs:

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

For a trust framework to work, it needs competent, independent and trustworthy individuals to govern the process. I believe that there is a reasonable separation to allow Governance Authorities and Audit Accreditation bodies to both have key roles. The Domain recognizes and approves direct entities to operate in the Domain. It creates baseline criteria that it expects participants to comply with. It approves and monitors audit accreditation bodies to audit entities in the Domain.

Audit Accreditation Bodies derive audit criteria based on the baseline requirements. It applies and is recognized by the Domain to audit Domain Roles and issue Trust Marks or Seals.

4.4 HOW DOES THE AUDITOR COMMUNITY GET ENGAGED?

Commercial auditors, while maintaining accountability to public trust are still businesspeople. There needs to be a profit incentive to become engaged. Profits are realized through auditor training and

certification as well as vendor attestation engagements. The silent determining factor lies in whether auditor involvement is required within the process. In many certification schemes, the first cost reduction seems to be the diluted rigor or extended timelines of audits which eventually erodes the entire model. Therefore, requiring rigorous, frequent and mandatory audits will get the profession's attention.

4.5 TRUST ASSURANCE FORMATION STRATEGY

- The Domain should establish a work group comprised of experienced professionals to create its Trust Framework baseline requirements definable roles, schemes, levels of assurance, and trust mechanisms.
- The trust criteria should be segmented into multiple tiers which offer choices to vendors based on complexity, risk and assurance to the public.
- The Domain Governance Work Group should engage the audit and security compliance professional community about their interest to play a role in the assurance process.
- The Governance Authority should establish criteria it expects component vendors to adhere to at the level of assurance needed for reliance
- The Governance Authority should set requirements upon accreditation bodies on what is needed for acceptance and recognition of their schemes. 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 Domain Governance Work Group takes its Trust Assurance Framework and defines baseline requirements of all entities to address security, confidentiality, availability, processing integrity and privacy risks of transactions in the Domain. It defines encapsulated services delivered by entities 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 Accreditation Bodies and Entities (specified by their compliant component) on its public website.

The Domain Governance Work Group can align with existing trust framework providers (Kantara, AICPA – see list above) to approve an acceptable audit accreditation scheme. An audit attestation scheme would include the following elements:

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

The Domain Governance Work 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 Domain, in its registration guidance, includes a list of audit accreditation bodies and the expectations needed from the applicant for their initial (and subsequent) audits.

4.6 ROLE OF AUDIT ACCREDITATION BODY

The Audit Accreditation Body applies to the Domain Governance Work Group or its proxy to provide audit services and issues Trust Marks for component services of Domain Roles. It derives auditable criteria from the Baseline Requirements for components it chooses to offer Trust Marks or Seals. It creates criteria for the evaluation and accreditation of independent and competent auditors it relies upon for the issuance of Trust Marks or Seals. It does its due diligence to validate whether the auditor applicant meets the qualification criteria published in its public literature. If accepted, the audit accreditation body contracts with the audit firm and an accreditation fee could be charged then or at the issuance of an audit report for a Domain component vendor.

4.7 ROLE OF DOMAIN ROLE

The Domain Role offers services that promote the overall trustworthiness of the Domain. It develops policies, procedures and implement technology controls that address to address security, confidentiality, availability, processing integrity and privacy risks of transactions in the Domain. It asserts that these controls comply to baseline requirements and allow independent auditors to perform validation activities on their practices in order to attest to them. It displays Trust Marks or Seals in order to make the public aware of their compliant status.

The Domain Role will seek security accreditation for their product or service in order to enhance consumer acceptance or to satisfy a regulatory mandate. The vendor reaches a registration web page on the Governance Authority website, downloads registration /accreditation literature and submits a registration form to initiate the process indicating their company and representative, their product/service and the level of assurance (i.e. security criteria level) they seek. The Governance Authority could collect a registration fee at that time.

The Governance Authority acknowledges receipt of the registration and fee and sets expectations for initial accreditation including a "zero-day" point-in-time audit of their compliance to the security criterial level they want to assert. This process is enabled by approved Audit Accreditation Bodies. Accreditation may also include other requirements imposed by the Audit Accreditation Bodies in addition to an independent audit such as their own proprietary tests.

The Domain Role reviews the Baseline Requirements and the Audit Accreditation Body Trust Criteria then chooses the level it wants to assert to the public. It reviews available Domain guidance on how to comply,

then builds processes, practices and technical controls to satisfy security criteria requirements. When the Domain Role feels it can demonstrate its compliance to the criteria in a pre-operational test environment or in operation, it contracts with an accredited auditor for them to perform an attestation of their assertion.

The Domain Role supplies its Attestation Package (the Attestation Letter, the Assertion Letter, and the Exceptions List with Mitigation Plans) to the Audit Accreditation Body. The Audit Accreditation Body evaluates the package and either accepts it, rejects it or creates an alternative path to accreditation.

Once the Audit Accreditation Body is satisfied with the Domain Role submission, it acknowledges accreditation. This can be supplemented with an accreditation fee, a visible Trustmark/seal or some report. All records substantiating their accreditation of the vendor must be retained for a stated archival period to defend against potential claims.

Accreditation should be valid for an initial period of time until that time when re-accreditation should be obtained. This should be accompanied by a period-of-time audit asserting and attesting conformance of the security criteria for that period.

4.8 ROLE OF AUDITOR

Potential Domain audit firms would review public information on the process, gauge the fiscal potential for audit business, and submit an application to be an accredited auditor. A registration fee could complement the submission.

It evaluates qualifications from audit accreditation bodies to determine if it meets their acceptance criteria or it needs training or other investment. When applicable, it applies to audit accreditation bodies for accreditation by submitting its qualifications to audit the Domain Roles for services or components and their respective levels of assurance

During the audit, the Domain Role provides evidence of conformity by providing or allowing the auditor to perform the following regarding the evidence of practices that meet the security criteria:

- Documentary evidence
- Observation
- Physical testing of the product and its functions
- Corroborative inquiry of key vendor players

At the point-of-time that the Domain Role wants to assert its compliance, it issues a letter to its auditor documenting its assertion of compliance as of that date (the Assertion Letter).

The auditor evaluates the evidence it obtains/derives from the Domain Role and assesses it against the security criteria the vendor asserts. Typical attestation letters from CPA firms attest compliance at "a material level" which may or may not suffice the non-profit. My suggestion is that this level of disclosure would be acceptable for the public, but the non-profit may want more granular disclosure about

exceptions the auditor found ("Exceptions List"). To reduce risk of all concerned, the disclosure of these lower level exceptions/risks may be limited to the Domain Role and the Audit Accreditation Body. All exceptions need reasonable response/mitigation plans from the Domain Role and the auditor should affirm their reasonableness.

5. FINAL QUOTES

"Leadership requires five ingredients--brains, energy, determination, trust, and ethics. The key challenges today are in terms of the last two--trust and ethics." --Fred Hilmer

"The glue that holds all relationships together--including the relationship between the leader and the led--is trust, and trust is based on integrity." --Brian Tracy

"Trust each other again and again. When the trust level gets high enough, people transcend apparent limits, discovering new and awesome abilities of which they were previously unaware." --David Armistead

Scott Perry is the Principal of Scott S. Perry CPA, PLLC, a Washington State CPA firm specializing in cybersecurity audits. He is an accredited auditor/assessor of WebTrust, the Federal Bridge Policy Authority, SAFE-Bio-Pharma and ISO 27001. He has served ISO performing a Study Period on trusted third party and PKI standards and is an active member of the Federal Government PKI Certificate Policy Working Group, Sovrin Domain-Specific Governance Working Group and Sovrin Web of Trust Working Group.