# Governance Stack Design Principles

* Authors: Drummond Reed, [Victor Syntez](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ)
* Deliverable Type: Recommendation - Design Principle
* Status: [PROPOSED](https://hackmd.io/README.md" \l "proposed)
* Since: 2020-11-04
* Status Note: Draft
* Supersedes: N/A
* Start Date: 2020-11-04
* Tags: (see …/…/…/tags.md)
* [Governance Stack Design Principles](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Governance-Stack-Design-Principles)
  + [Summary](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Summary)
  + [Motivation](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Motivation)
  + [Scope](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Scope)
  + [Important concepts](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Important-concepts)
  + [Trust Over IP Stack Governance Frameworks description](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Trust-Over-IP-Stack-Governance-Frameworks-description)
  + [Design Goals](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Design-Goals)
  + [List of Principles](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "List-of-Principles)
    - [1. Interoperability and Portability](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "1-Interoperability-and-Portability)
    - [2. Equity and Inclusion](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "2-Equity-and-Inclusion)
    - [3. Security and Privacy.](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "3-Security-and-Privacy)
    - [4. Transparency in governance and operation](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "4-Transparency-in-governance-and-operation)
    - [5. User control and consent](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "5-User-control-and-consent)
    - [6. Rights and Obligations](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "6-Rights-and-Obligations)
    - [7. Independent audit and assessment](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "7-Independent-audit-and-assessment)
    - [8. Human Integration for continuous feedback and consistent experience](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "8-Human-Integration-for-continuous-feedback-and-consistent-experience)
    - [9. Minimal Disclosure for a Constrained Use](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "9-Minimal-Disclosure-for-a-Constrained-Use)
    - [10. Open and Automated systems](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "10-Open-and-Automated-systems)
  + [Synopsis](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Synopsis)
  + [Relevance](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Relevance)
  + [Trade-offs](https://hackmd.io/MN_DJeVDQv-UWZ7JRvPGEQ" \l "Trade-offs)

## Summary

This document is a template for TOIP Governance Stack Design Principles that might be used throughout all or any of the Trust Over IP Layers. It is based on several works:

1. Laws of Identity by [Kim Cameron](https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf)
2. Presidio Principles by [WEF](http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf)
3. The Principles of SSI by Sovrin [(current version)](https://docs.google.com/document/d/1GhcLeZEujX9h5gqrFNP-C1dMrS71EdCY4Uc1hGQbqI0/edit" \l "heading=h.jkpp8prq58uk)
4. Guiding Principles of the [PCTF](https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf)
5. Seven Principles of Universal [Design](http://universaldesign.ie/What-is-Universal-Design/The-7-Principles/)

## Motivation

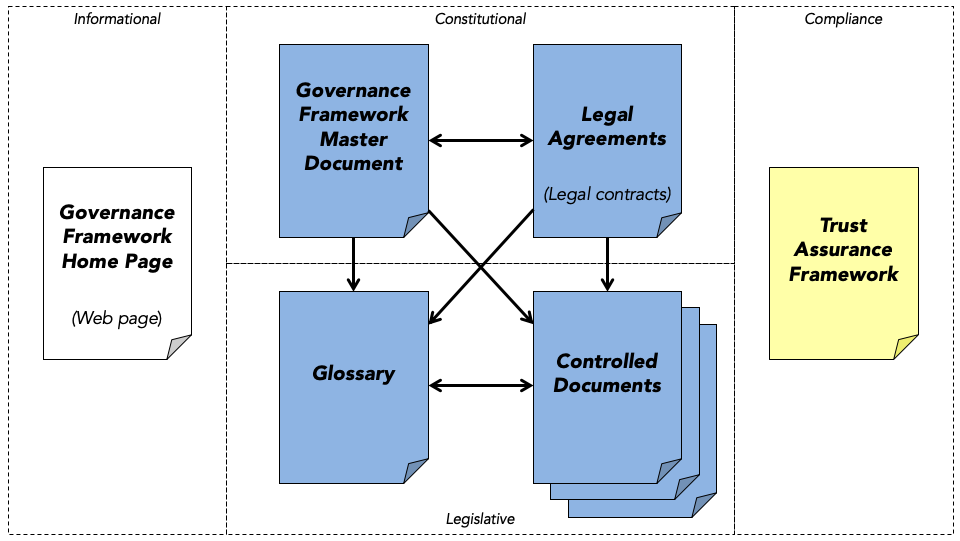
We see our task for creating this document in outlining TOIP Governance Stack Design Principles. These principles are needed for creating governing documents that will enable business, legal and social trust between entities engaged in any activity related to digitally verified credentials. By defining these principles we hope to assist in creating governance documents for user-centric, secure, accountable, interoperable, transparent and accessible utilities, protocols, applications, and ecosystems around verified credentials. Our goal lies in proposing not only the content of governance frameworks but also the way, how this content is organized for the future reading and use by humans and/or machines. We would like to highlight that these Design Principles are recomendations on HOW to create governing documents and WHAT these governing documents will contain.

## Scope

This document serves to provide an opportunity to discuss how further mentioned Design Principles MUST or SHOULD, or MAY be applicable on all or any layer of TOIP Governance Stack.

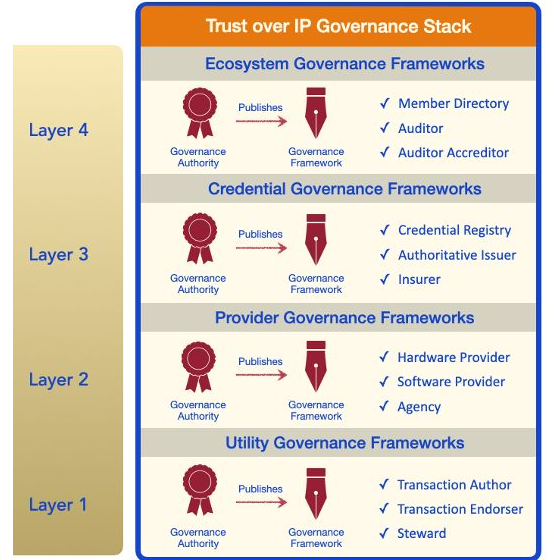
In many standards track documents words MUST, SHOULD, and MAY are used to signify the requirements in the specification. This document use these words according to IETF [RFC2119](https://tools.ietf.org/html/rfc2119).

## Important concepts

* Verified Credential. A Credential that includes a Proof from the Issuer. Typically this proof is in the form of a digital signature. In Sovrin Infrastructure, a Verifiable Credential uses Zero Knowledge Proofs by default and can usually be verified by the Issuer Public Key stored in the Credential Definition on the Sovrin Ledger. Based on the definition provided by the W3C Verifiable Claims Working Group. (from Sovrin [glossary](https://github.com/trustoverip/concepts-and-terminology-wg/blob/master/submissions/sovrin/Governance_Framework.md)).
* Credential Verification is the evaluation of whether a Verifiable Credential or Verifiable Presentation authentically and accurately represents the Issuer or Presenter. This includes verification that the proof is satisfied (normally via cryptographic validation), confirmation the Credential or Presentation is valid (e.g., is not suspended, revoked, or expired), and that the Credential or Presentation conforms to relevant specifications and/or standards. (from [PCTF Credential](https://diacc.ca/wp-content/uploads/2020/09/PCTF-Credentials-Relationships-Attributes-Component-Overview-Final-Recommendation-V1.0-1.pdf))
* Governance Framework - The set of business, legal, and technical definitions, policies, specifications, and contracts by which the members of a Trust Community agree to be governed in order to achieve their desired Levels of Assurance. Typically divided into a Master Document and a set of Controlled Documents. A Governance Framework is itself governed by a Governance Authority. A Governance Framework is also known as a Trust Framework. (from Sovrin [glossary](https://github.com/trustoverip/concepts-and-terminology-wg/blob/master/submissions/sovrin/Governance_Framework.md)) 
* Design - A design is a plan or specification for the construction of an object or system or for the implementation of an activity or process, or the result of that plan or specification in the form of a prototype, product or process.

## Trust Over IP Stack Governance Frameworks description

The ToIP stack does not define specific governance frameworks. Rather it is a metamodel for how to design and implement digital governance frameworks that can be universally referenced, understood, and consumed in order to facilitate transitive trust online. The ToIP governance stack is designed to be compatible with—and an implementation vehicle for—national governance frameworks as well as for regional and local governance frameworks of all kinds.



TL4: Ecosystem Governance Frameworks. Layer Four is where humans will directly experience the ToIP Governance Stack—specifically the trust marks and policy promises of ecosystem governance frameworks. These specify the purpose, principles, and policies that apply to all governance authorities and governance frameworks operating within that ecosystem—at all four levels of the ToIP stack. Any group of issuers who want to standardize, strengthen, and scale the credentials they offer can join together under the auspices of a sponsoring authority to craft a governance framework. No matter the form of the organization—government, consortia, association, cooperative—the purpose is the same: define the business, legal, and technical rules under which the members agree to operate in order to achieve trust.

TL3: Credential Governance Frameworks. This is the layer where governance frameworks become a critical component for interoperability and scalability of digital trust ecosystems. Credential governance frameworks can be used to specify:

* Credential schema definitions.
* The rules governing who can serve as the authoritative issuers for those credentials.
* The policies those issuers must follow to issue and revoke those credentials.
* Applicable business models, liability frameworks, and insurance models.

TL2: Provider Governance Frameworks. At Layer Two, governance is needed primarily to establish interoperability testing and certification requirements, including security, privacy, data protection, for the following roles: Hardware Developer, Software Developer, Agencies.

TL1: Utility Governance Framework. A Layer One public utility may choose any governance model suited to the the constraints of its business model, legal model, and technical architecture. All ToIP architecture requires is that the governance model conform to the requirements of the ToIP Governance Stack to support both interoperability and transitive trust. This includes transparent identification of the governance authority, the governance framework, and participant nodes or operators; transparent discovery of nodes and/or service endpoints; and transparent security, privacy, data protection, and other operational policies.

## Design Goals

For designing this document we will try to use 4 principles of universal design. Our goal is to make this document perceptible for future use outside of the Trust Over IP community. For this we seek to implement below principles:

1. Equitable Use. This document is useful and marketable to people with diverse abilities and backgrounds.
2. Flexibility in Use. This document accommodates a wide range of individual preferences and abilities.
3. Perceptible Information. This document communicates necessary information effectively to the user.
4. Size and Format for Read and Use. Appropriate size and format is provided for reading, manipulation, and use keeping in mind diversity of knowledge about verified credentials among future consumers of the document.

One of the design tasks will be to organize mentioned DP for GF in the order of their importance, in the order of their implementation and consideration. Another design task will be to use relevant verb MUST/SHOULD/MAY for every principle described.

## List of Principles

Below you will find principles and their meaning. Principles are mentioned without any particular order.

### 1. Interoperability and Portability

* Capability to port data between interoperable systems or parts of a system.
* Capability to have access to information sufficient to facilitate system interoperability.
* Capability to use various verifiable data structures, wallets, or cloud service providers to manage and use verified credentials.
* Ensuring users’ identification/authentication portability and interoperability, allowing for separating the data from the application and for the user to have the right to decide where to store the identification/authentication data.
* Promoting different identity providers offering different features. VC ecosystems must be polycentric and also polymorphic.

### 2. Equity and Inclusion

* Identification and mitigation of legal, procedural, and social barriers in VC ecosystems, with special attention to groups who may be at risk of exclusion for cultural, political or other reasons.
* VC ecosystems should not be used as a tool for discrimination or infringement on individual or collective rights.
* Hardware and software should be common and affordable while allowing for sufficient speed and security.
* VC ecosystems should not exclude or discriminate against any groups within its governance scope.
* VC ecosystems should to be easy to access and simple to understand.

### 3. Security and Privacy.

* Data protection MUST be in accordance with internationally recognized technical security standards.
* VC ecosystems MUST have safeguards against tampering, VC theft, data misuse.
* MUST: Establishing tools for end-to-end encryption.
* MUST: Verification that operations have been completed and confirmed in accordance with the system’s rules.
* Security of VC at rest and during exchanges.
* Protection of VC security and privacy through VC ecosystem design. Information SHOULD be protected from improper and unauthorized use by default, through both technical standards and preventative business practices.

### 4. Transparency in governance and operation

* MUST: Capability to assess and verify the information necessary to understand the incentives, rules, policies, and algorythms under which VC systems participants operate.
* MUST: Open publication of the governing documents among them principles, policies, regulations, institutional mandates, etc.
* SHOULD: Availability of the system performance metrics and critical points in service delivery system.

### 5. User control and consent

* SHOULD empower VC ecosystems participants to exert their control over VC by employing and/or delegating to the agents and guardians of their choice, including individuals, organizations, devices, and software.
* VC ecosystems SHOULD provide capability for explicit and informed consent from its participatns.
* The VC ecosystems MUST inform the participant whether his or her VC will be tracked and what data from her or his VC is used and released.
* The VC ecosystem SHOULD reinforce the sense that the participant is in control regardless of context. It SHOULD support user consent in enterprice as well as consumer environment.

### 6. Rights and Obligations

* SHOULD: Transparency around the roles and responsibilites of VC ecosystem participants.
* MUST: Clear description of potential risks and benefits of a VC ecosystem.
* MUST: Clear specification of the terms and conditions governing VC ecosystem participants relationship.

### 7. Independent audit and assessment

* MUST: Creation of the independent oversight body (e.g. a national privacy commission) with appropriate powers to protect VC ecosystem participants against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or legimate purpose.
* Ecosystem-wide trust frameworks MUST establish and regulate governance arrangements for VC ecosystems.
* VC ecosystems SHOULD be independantly monitored for effeciency, transparency, exclusion, misuse, etc.
* Disputes regarding VC and their use that are not satisfactorily resolved by the providers SHOULD be subject to rapid and low-cost review by independent administrative and judicial authorities with authority to provide suitable redress.
* SHOULD: On-going, functionally independent, and third-party assessments provide one way to ensure that ecosystem participants adhere to the Trust Framework requirements.

### 8. Human Integration for continuous feedback and consistent experience

* Public and private stakeholders SHOULD be engaged throghout planning and implementation of VC ecosystem.
* The VC ecosystem SHOULD extend to and integrate the human user.
* SHOULD: Maximization of usability and consistency of VC user experience.
* MUST: Capability to opt-out of not participation in the VC ecosystem that doesn’t treat data in accordance with internationally recognized governance and data protection standards.
* MUST: Necessity for VC players to be flexible, scalable, and meet the needs and concerns of people (users) and relying parties (e.g., public agencies and private companies).

### 9. Minimal Disclosure for a Constrained Use

* VC ecosystem provider SHOULD disclose exactly the amount of information necessary for each interaction between only the required parties in the context of the service provided, in compliance with the applicable data protection rules.
* VC ecosystem provider SHOULD not disclose any personal information unless otherwise required.
* VC ecosystem provider SHOULD accept users who want to preserve high level of privacy and anonymity, e.g. by using pseudonym and/or other privacy-by-design mechanisms, associated in a trustworthy manner to their government-issued/recognized ID.
* VC ecosystem provider SHOULD provide a possibility to revoke consent for future data collection system and support user’s “right to be forgotten”.
* VC ecosystem provider SHOULD provide capabilities for users not to be subject to automated-decision making.

### 10. Open and Automated systems

* Maintance of VC ecosystems neutrality, openness and innovation.
* VC ecosystems SHOULD use open standarts and applicable open practices.
* Avoidance of vendor or technology lock-in.
* Enabling open design principles for market-based competition and innovation.

## Synopsis

## Relevance

We consider that there is a need in documents highlighting not only the very principles of verified credentials governance but also organizing these principles in clear, consise, and appealing way. Therefore we wish that this document will create an emotional feedback from its consumers. We need to remember that for a product to be accepted by corresponding public it has to be of high quality and it has to be wrapped appropriately.

## Trade-offs