Saturn-V TIP

The **Saturn-V** TIP is a recommendation of the ToIP Foundation.

A *ToIP Interoperability Profile (TIP)* is a deliverable of the ToIP Technology Stack Working Group.

Audience

ToIP Layer 4 Ecosystem Projects that follow the guidance of the ToIP Ecosystem Foundry Working Group will make decisions during the `DEFINE` and `CREATE` workflow swimlanes that will allow them to articulate specific technology requirements. They can use these requirements to help in their selection of which ToIP TIP they seek to leverage.
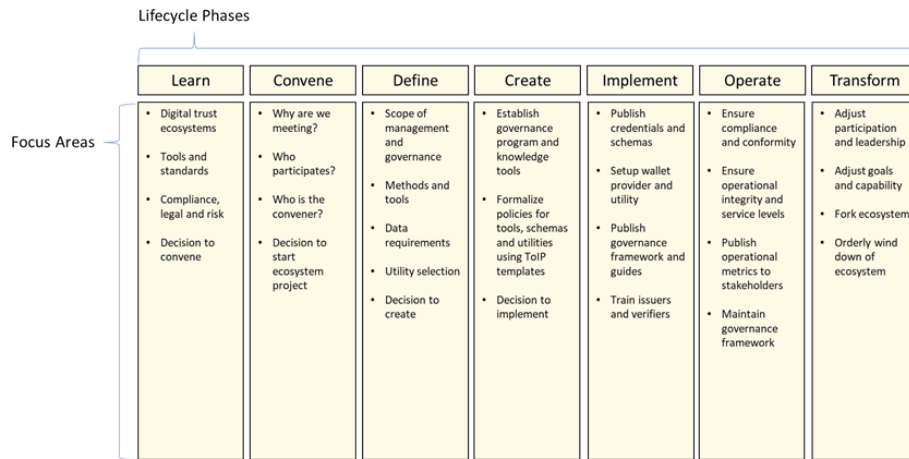

Figure 1: efwg-workflow

Figure 1: ToIP EFWG Workflow Swimlanes

As stakeholders in a specific Ecosystem Project consider the various technology ingredients associates with a solution architecture, they may appreciate the guidance of ToIP TIPs that have formulated a very specific solution recipe containing a profile of use cases backed by technology that has been implemented and tested by a community of vendors.

The Saturn-V TIP represents one such solution recipe.

Name

This TIP represents the next evolutionary step towards the *moon shot* known as decentralized identity. Acknowledging the recently successful NASA/Space-X mission that has revitalized attention to space exploration, history reveals

that our early success in space was significantly aided by the **Saturn V** multi-stage rocket platform. The *Saturn V* three-stage rocket served as a *Heavy Lift Vehicle* for space exploration. It was the most powerful rocket that had ever flown successfully. The *Saturn V* was used in the Apollo program in the 1960s and 1970s. It also was used to launch the Skylab space station. Containing three (3) powerful fuel-stages, this massive rocket was used to propel man to the moon.

Since we are in the early stages of the technology adoption lifecycle for decentralized identity, we seek a technical architecture (recipe) to bootstrap an interoperable digital trust marketplace. Analogous to the first three layers of the ToIP Technology Stack, this TIP represents an exemplar of a technical collaboration to help propel decentralized identity into mainstream adoption.
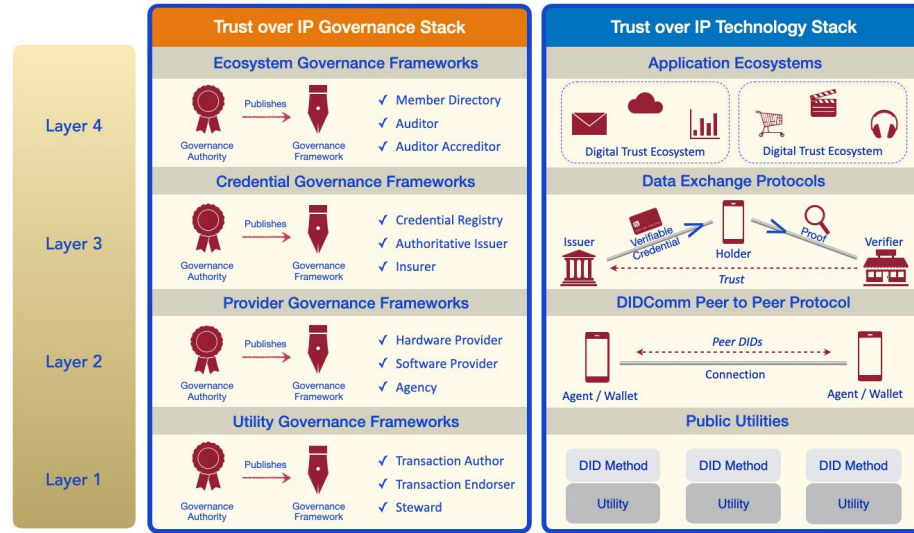

Figure 2: toip-stack

In fact the *Saturn V* project required that three separate companies, each responsible for a separate fuel-stage, collaborated to integrate their fuel-engines into a single interoperable rocket platform that would propel the Appolo and Skylab missions. Today, we seek to integrate technology for three ToIP Layers to achieve a common goal – **help propel the adoption of digital credentials**.

Purpose

Today, the decentralized identity community continues the *moon shot* started by the *Sovrin Foundation* towards self-sovereign identity. This proposal is unique as it represents a vertical interoperable stack that is already familiar to most industry participants. This proposal is effectively receiving the baton that began

with the Sovrin Network and will focus on evolving that effort into a network of networks model.

Convener(s)

- Richard Esplin
- Dan Gisolfi

Stakeholders

The following entities are supporters and contributors to the this TIP:

Vendors

- esatus
- Evernym
- Main-Incubator (R&D Unit of Commerzbank Group)
- SCOIR

Other Contributors

- Dan Gisolfi

Key Motivators

List the reasons that triggered the proposal.

1. We need to describe an example TIP that is of interest to many in the ToIP Foundation.
2. As the Sovrin Community transitions under the broader umbrella of the ToIP Foundation, we need a description of the architecture in which the community desires to embrace.

3. We need a methodology that will allow alternative TIPs to be compared to the one most familiar with many in the ToIP Foundation.
4. We need a forum for the Indy Interop-athon events that are focused on making the network of networks concepts reality of public identity utilities based on Hyperledger Indy.

Use cases to be validated

In addition to the common business patterns associated with decentralized identity, namely `password-less auth` and `digital onboarding`, this TIP will build on existing proof-points to establish a generalized list of uses-cases that will help to demonstrate cross-industry adoption.

Core Principles

This TIP provides a set of gGuidelines for how market requirements should be translated into architecture and technology decisions.

Evaluators of this TIP should look at each of these suggested design principles and consider the ramifications for supporting or not-supporting each.

The vendors supporting this TIP have incorporated these design principles into their software solutions.

Laws of Identity

The seven (7) principles outlined by in 2006 and captured in the ToIP Design Principle Recommendation - DP0003: Laws of Identity are foundational principles for this TIP.

Privacy by design

The seven (7) principles outlined by in the ToIP Design Principle Recommendation - DP0004: Privacy by Design are foundational principles for this TIP.

Self-sovereign identity (SSI)

This TIP is purpose built to provide the foundational infrastructure necessary to support the 10 Core Principles that were adopted by the Sovrin Foundation in support of SSI.

Principle	Description
Existence	Users must have an independent existence.
Control	Users must control their identities.
Access	Users must have access to their own data.
Transparency	Systems and algorithms must be transparent.
Persistence	Identities must be long-lived.
Portability	Information and services about identity must be transportable.
Interoperability	Identities should be as widely usable as possible.
Consent	Users must agree to the use of their identity.
Minimization	Disclosure of claims must be minimized.
Protection	The rights of users must be protected.

Decentralization by Design

The ToIP Design Principle Recommendation - DP0005: Decentralization by Design provides a spectrum of considerations to be considered when solution architectures are contemplating the degree of decentralization that is required.

This TIP minimally specifies that the root of trust MUST be managed in a

decentralized manner, preferably by one or more decentralized public identity utilities.

When the technology has matured, this TIP will be modified to REQUIRE stronger decentralization technics for the root of trust by combining a decentralized ledger with Key Event Receipt Infrastructure (KERI). Refer to advancements in the Indy DID Method.

ENTER CONTENT HERE

ENTER CONTENT HERE

Evernym { #.-interop-evernym-evernym }

- **Product**: Verity
- **Product URL**:
- **Region**: NA/USA

Contact Info { #.-interop-evernym-contact-info }

- **TIP Focal Point**: Richard Esplin
- **TIP Focal Point eMail**: TBD

TIP Support Proclamation { #.-interop-evernym-tip-support-proclamation }

Plans of Record

The vendors supporting this TIP have outlined test plan milestones to help interested parties to understand the state of interoperability testing.

Wave 1

Our initial plan milestone will be for each vendor to demonstrate interoperability against the following:

1. Validation against Aries Protocol Test Suite for Aries Interop Profile v. 1.0
2. Core Aries Interop Profile v. 1.0 - See Aries RFC 302
3. DIDComm (did:sov)
4. Connection
5. Credentials
6. Proofs
7. Ephemeral Proofs: receive only
8. Service decorator
9. Needed for VC-Authn-OIDC (used by BC.gov)
10. Transition Message Type to HTTPs: receive
11. Aries RFC 348: Can receive messages with protocol definition of type http://didcomm.org

Wave 2

Our second milestone will be for each vendor to tackle the goals of AIP 2

- Aries PR 579 for RFC 302 - AIP 2.0
- Notes AIP 2.0
- Slide deck with current thinking
- Discussion in Aries WG B 2020-12-02
- Discussion in Aries WG B 2020-12-09

User Stories

- Able to provide a proof without creating a persistent connection.
    - Out-of-Band Protocol

Other Technical Requirements

- Transition Message Type to HTTPs: send/receive
    - Aries RFC 348: http://didcomm.org

Further Ideas

- Core Aries Interop Profile v. 2.0 (TBD)
    - Out Of Band
    - DID Exchange
    - Credential Exchange Protocols (v2)
    - feature discovery v2
    - mime-types (to help transition to didcomm v2)
    - Signed attachments
- New MIME Types
- BC-Gov Test Suite

Peer Certifications

This TIP leverages public peer-to-peer attestations where vendors can publicly certify their completion of interoperability testing with peer stakeholders.

Wave 1

Enterprise Agent	Holder	Peer Certification
IBM	Evernym	IBM(EA) :: Evernym(H)

Wave 2

Enterprise Agent	Holder	Peer Certification

ENTER CONTENT HERE

ENTER CONTENT HERE

ENTER CONTENT HERE

Org-Name

Contact 1

Email xxxxxxxxxxxxx

Contact Authors

Email xxxxxxxxxxx