An Overview of all SSI Standardization
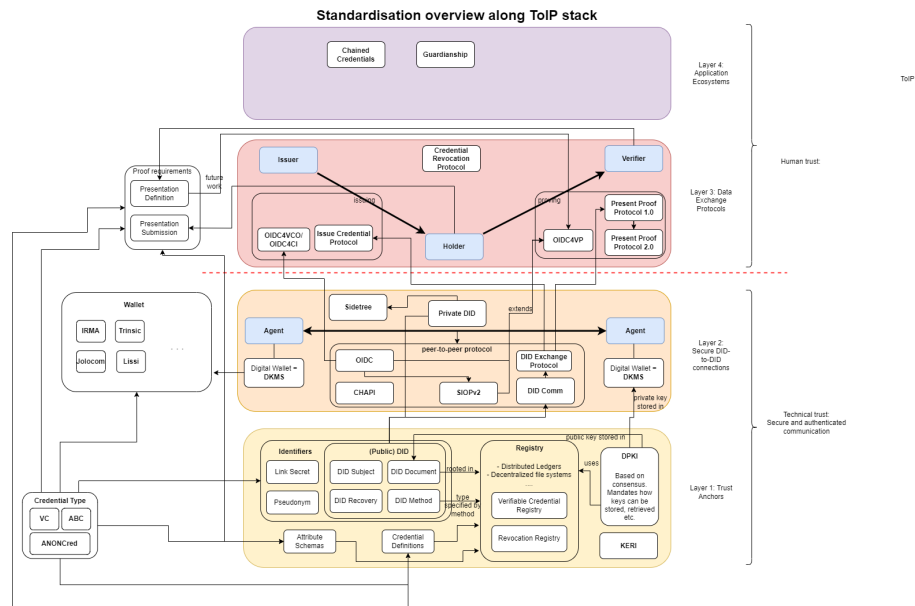
By Maaike van Leuken (TNO)
Date: 26-07-2022

Introduction

Various groups of people, such as DIF, W3C, eSSIF-Lab, Sovrin, etc. are working on standardizing SSI-related technologies. We see work being done that ranges from high-level concepts such as guardianship, to models (ToIP, VC Data Model, eSSIF-Lab mental models) to actual technology such as peer-to-peer protocols (DIDComm), DIDs, etc. Currently, it can be quite a task to figure out how one standard x connects to another y. Can standard x be used for SSI? Are standards x and y competing with each other? Is standard x dependent of y? By making an overview of SSI-related standards and by making connections between the standards, these questions can be answered more easily.

Making an Overview

Below you can see my first attempt to create an overview of the standards I have encountered so far, structured along the ToIP stack. The ToIP stack is divided into four layers, as can be seen on the right of the image. In **layer 1: trust anchors**, we have various technologies that serve as a trust anchor for the higher layers. The type of identifier (DIDs, link secrets, . . .) and registry (blockchain, no blockchain, Ethereum blockchain, . . .) influence the type of peer-to-peer protocol that is used in **layer 2: secure DID-to-DID connections** which in turn influences the choice of issuing or verifying protocol in **layer 3: data exchange protocols**. Whether one choice of technology influences another, how much and in what way is to be investigated.

Standardisation overview along ToIP stack

Chained Credentials

Guardianship

Layer 4: Application Ecosystems

ToIP

Human trust:

Issuer

Credential Revocation Protocol

Verifier

Layer 3: Data Exchange Protocols

Proof requirements

Presentation Definition

Presentation Submission

future work

Issuing

Present Proof Protocol 1.0

Present Proof Protocol 2.0

OIDC4VCO/ OIDC4CI

Issue Credential Protocol

Holder

OIDC4VP

Wallet

IRMA

Trinsic

Jolocom

Lissi

. . .

Sidetree

Private DID

extends

Agent

Agent

Layer 2: Secure DID-to-DID connections

Technical trust: Secure and authenticated communication

Digital Wallet = DKMS

OIDC

peer-to-peer protocol

DID Exchange Protocol

Digital Wallet = DKMS

CHAPI

SIOPv2

DID Comm

private key stored in

Credential Type

VC

ABC

ANONCred

public key stored in

Identifiers

Link Secret

Pseudonym

(Public) DID

DID Subject

DID Document

DID Recovery

DID Method

rooted in

type specified by method

Registry
- Distributed Ledgers
- Decentralized file systems

Verifiable Credential Registry

Revocation Registry

uses

DPKI

Based on consensus. Mandates how keys can be stored, retrieved etc.

KERI

Layer 1: Trust Anchors

Attribute Schemas

Credential Definitions

This overview is not complete and it needs to be checked for correctness. I could use the help of the RWOT community to come to a correct and complete overview.