

A Framework for Evaluating Layer 1 Utilities

Authors: Jessica Townsend (Accenture)
Lynn Bendixsen (Indicio)
Alex Tweeddale (cheqd)
Mathieu Glaude (Northern Block)

Publication date: TBD
ToIP draft approval: TBD
UFWG draft approval: TBD
All Member review: 4/5/22-4/12/22
UFWG draft review request: 4/4/22

Reviewers: Judith Fleenor
Jim St. Clair
Anita Rao
Drummond Reed
Andre Kudra

Keywords: *Utility, Layer 1, Governance, VDR, DID, DID Document, Schema, Revocation Registry*

Acknowledgements

References

Links:

- <https://w3c.github.io/did-rubric/#background>
- <https://trustoverip.org/blog/2022/03/04/layer-1-utilities-an-underground-network-connecting-all-ssi-ecosystems/>
- <https://www.w3.org/TR/did-core/>
- <https://www.w3.org/TR/did-core/#methods>
- <https://wiki.trustoverip.org/display/HOME/List+of+Considerations+When+Choosing+a+Utility>

Executive Summary

This document provides a comprehensive framework on how to evaluate whether an existing **Layer 1 Public Utility (Utility)** will meet your needs as a consumer or considerations that should be made when looking to develop a Self-Sovereign Identity (“SSI”) ecosystem of your own. *The objective being to:*

- a. *Understand the differences in **Layer 1 Public Utilities**, on technical and practical levels;*
- b. *Expand on the work done on the [DID Rubric v1.0](#) by the World Wide Web Consortium (W3C);*
- c. *Design a **visual framework** for comparing Utilities.*

The framework described below is meant for organizations/ecosystems who want to operationalize the **Trust over IP stack** to choose the best possible **Utility** that is aligned to their needs. Note that in this document, we will primarily focus on blockchain-based Utilities. The document *may* also be extended to non-blockchain based Utilities, however, consideration should be given to the differences in core architecture, which may affect some points of comparison.

Table of Contents

Executive Summary	2
Table of Contents	2
Introduction	4
About the Trust over IP Foundation	4
Introduction to the Utility Foundry Working Group	4
What is a Public Utility?	5
Why use a Public Utility for SSI?	6
UFWG Registered Public Utilities	8
Evaluating a Public Utility	10
Broad differentiators, standards and questions	10
Public Utility Grading Criteria	11
Scoring system and simple graphic representation	12
Business Requirements	13
Notes and more subjective considerations:	13

Technical Requirements	14
Notes and more subjective considerations:	14
Legal Requirements	14
Notes and more subjective considerations:	15
Social Requirements	15
Notes and more subjective considerations:	16
Governance Requirements	16
Notes and more subjective considerations:	16
Overall framework and template	17
Glossary of Terms	17

Introduction

About the Trust over IP Foundation

The **Trust Over IP (ToIP) Foundation**, a project under the Linux Foundation that began in May 2020, is focused on defining governance procedures and globally accepted standards, protocols, and architecture to facilitate internet scale digital trust. Within ToIP, there are numerous working groups that aim to progress the mission of ToIP inclusive of defining specifications, making recommendations, delivering of guides, and production of white papers and glossaries to assist organizations in understanding decentralized identity and helping to bring it to life.

Introduction to the Utility Foundry Working Group

One of the core working groups of ToIP is the **Utility Foundry Working Group (UFWG)**. The UFWG aims to facilitate a community of best practices among governance authorities, implementers, operators, and service providers for **Trust over IP (ToIP) Layer One Public Utilities**. Utilities are described in the next section.

The UFWG strives to continually provide the most current guidance and specifications for the establishment and monitoring of new ToIP Layer One Utility projects as part of the ToIP technical stack, whether hosted at the Linux Foundation or external to it. Additional working group activities may include creation of a Request for Proposal (RFP)/Tender/Invitation to Bid (ITB) templates for organizations seeking to use Public Utilities, maintaining a list of ToIP-affiliated Foundry Utilities, identifying areas of collaboration and alignment between associated and/or disparate Utilities, and serving as a center of excellence for advancing the adoption of Utilities in decentralized identity.

Who will get value from the UFWG?

- Organizations/Ecosystems defined as families of applications and credentials designed to not only be technically interoperable, but share a common governance framework who want to evaluate an existing Utility using a framework to project the highest ROI and minimized risks.
- Organizations/Ecosystems interested in developing a new Utility to have a reference point to evaluate what is out there today and what market gap their Utility can fill.

Also, please do not hesitate to contact us if you have any questions or need any assistance at: utility-foundry-wg@lists.trustoverip.org

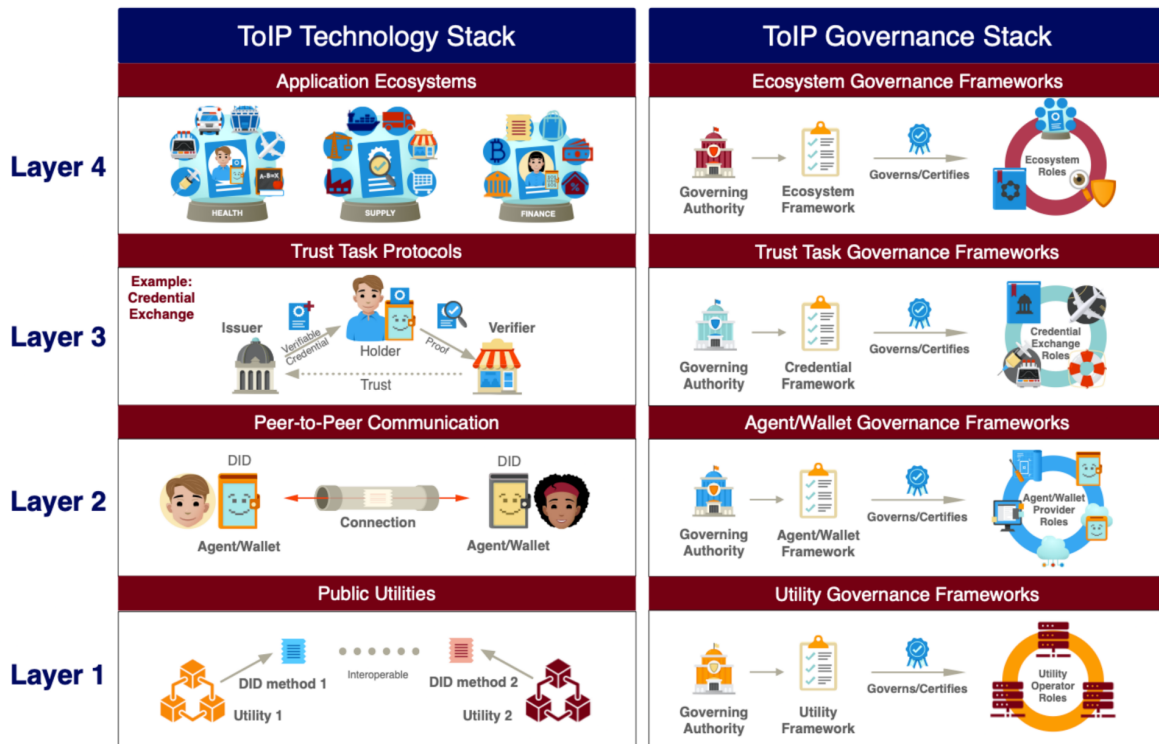
What is a Layer 1 Utility?

In an identity context, a **Layer 1 Utility (Utility)** refers to the infrastructure for a public identity verification service, sometimes known as a **Verifiable Data Registry (VDR)**. Utilities, though generally publicly accessible for read access, may have restricted write access as defined by the governance model of the Utility. However, there also exist fully permissionless Utilities without any read or write restrictions. Utilities may be operated by a single entity, a consortium of private sector entities, a decentralized autonomous organization (DAO), government entities, or a combination of these.

In the context of the ToIP, Utilities act as a base layer for the storage of Public (sometimes referred to as Anywise) **Decentralized Identifiers (DIDs)**. They may also store appropriate “**schemas**”, “**credential definitions**”, “**DID Documents**”, and “**Revocation Registries**”, depending on the type of Utility and its trust framework requirements.

The core purpose of every Utility is to offer a mechanism to achieve verifiable, cryptographic trust.

Through the use of **DIDs** and **Verifiable Credentials (VCs)**, third parties are able to verify the validity and authenticity of VCs through authenticating a DID on a Utility .



Utilities sit at Layer 1 of the Trust over IP stack, providing the core foundation and network governance for the layers built on top.

This is further explained in the Utility Foundry Working Group blog post: [Layer 1 Utilities: An Underground Network Connecting all SSI Ecosystems](#) and also in the [Trust over IP Metamodel Companion Guide](#).

Why use a Utility for SSI?

Summary

Like other service providers, Utilities are used for building decentralized trust for Self-Sovereign Identity (SSI) ecosystems. This document will focus primarily on blockchain-based utilities. These may be used alongside or as an alternative to more centralized utilities such as a secure web domain (did:web) or a verified github account (did:git). There are also other non-blockchain based utilities which are gaining popularity such as [KERI](#) or [Orb](#) which may fit into this framework, albeit more partially.

On a practical level, you may want to use a decentralized Utility for an identity use case for a few reasons:

- When there are **multiple parties in the ecosystem** which want to interact with each other in a trusted environment;

- When **interoperable and verifiable data** is required to be **shared between parties**;
- When there is value in **shared access**;
- When **agreement on business rules, governance, and standards** can be formed;
- When there is **value in understanding data provenance**;
- When you desire to support **user control, data sovereignty, and best practices around data consent**.

On a more technical level, Utilities may be used for various purposes, depending on the ecosystem and use case requirements:

- Anchoring **Decentralized Identifiers (DIDs)** for decentralized trust and authentication;
- Storing **identity primitives** such as “**schemas**” and possibly “**credential definitions**”, depending on the Utility;
- Storing Verifiable Credential **revocation registries**;
- Management of **cryptographic keys and DID Documents** through a **did method**;
- **Decentralized reputation management** to supplement the need for trust registries;
- **Decentralized governance** where users are able to democratically vote on changes to the network and stack above;
- Native **payments for Verifiable Credentials**, through a token, credit system or traditional payment rail.

Some key attributes of a decentralized network are listed below.

1. Provenance and Transparency

Anything written to a blockchain Utility is visible and transparent to the participants within the specific ecosystem. This could be DIDs, schemas, or even payment transactions.

2. Control

DID authentication, and public key management within DID Documents creates a model where trust and control is able to be demonstrated without reliance on a single database or centralized point of failure.

3. Security

Through anchoring trust using DIDs at the Utility layer, and keeping personal data off-chain in the form of Verifiable Credentials, there is less risk of large scale data breaches from ‘honeypots’ of data, where companies hold data on your behalf.

4. Exchange of data without intermediaries

Users all have permission to access the data without need for data to pass through a single central source. This is incredibly powerful as a tool to establish trust bilaterally between parties, empower data subjects to retain greater control of their data, and preserve privacy whilst doing so.

UFWG Registered Utilities

Below are some of the projects that have registered with the ToIP UFWG:

Utility	Description
Sovrin	The Sovrin Foundation is a nonprofit organization established to administer the Governance Framework governing the Sovrin Network, a decentralized global public network enabling SSI on the internet.
Bedrock	The Bedrock Consortium(this name will be changing) is a collection of international private sector companies that operate the Bedrock Business Utility (BBU), an independent self-governed legal entity.

Utility	Description
IDunion	The IDUnion consortium (formally known as SSI for Germany) is a public private partnership of companies and institutions, which implement and govern the IDUnion utility.
Indicio	Indicio, PBC was created to fill a need in the SSI community. Indicio's mission is to provide the professional services needed to build decentralized identity products.
cheqd	cheqd was built to create customizable commercial models for Verifiable Credentials and enable decentralized governance through a native token, \$CHEQ. Unlike most active utility projects, cheqd's network is public permissionless and is built on the Cosmos Software Development Kit (SDK).

There are also many Utility projects not yet engaged, but prominent in the decentralized identity community. These are some of the Utilities that the UFWG wants to engage in the coming months:

Utility	Description
KERI	Key Event Receipt Infrastructure (KERI) is the first truly fully decentralized identity system. It is ledger-less which means it doesn't need to use a ledger at all or ledger-portable which means that its identifiers are not locked to any given ledger and may switch as needed. In other words KERI identifiers are truly portable.
Velocity Network	Building an Internet of Careers, Velocity Network is a Layer 1 Network for exchanging and monetising trusted career

Utility	Description
	records using Verifiable Credentials and ledger-based signing keys.
Sidetree	Sidetree is a blockchain-agnostic layer 2 protocol that was designed to support a globally scalable, immutable append-only log with no central provider or authorities to be censorship and tamper resistant.
European Blockchain Services Infrastructure (EBSI)	The European Blockchain Services Infrastructure (EBSI) aims to become a “gold standard” digital infrastructure to support the launch and operation of EU-wide cross-border public services leveraged by blockchain technology.
Nym	Nym protects privacy at the network layer by encrypting and relaying your internet traffic through a multi-layered network called a mixnet. In each layer of the mixnet, mix nodes mix your internet traffic with that of other users, making communications private and hiding your metadata (IP address, who you talk to, when and where, and more).

The full directory of registered UFWG Utilities can be found [here](#).

This includes [instructions on how to add a new Utility to the directory](#).

Evaluating a Utility

This section will lay out the criteria for evaluating a Utility. It will also take inspiration and work from the [W3C DID Rubric v1.0](#), through the use of questions and evaluation criteria, in order not to duplicate work.

Broad differentiators, standards, and questions

Utilities for decentralized identity are not all built in the same way technically and may differentiate in various broad ways, in terms of their design and standards.

This section will lay out some of the more general points of differentiation to look out for, whereas, the following section will go into more specific detail on use-case-specific requirements. Since this section is looking more at the standard differentiators, the answers will be text based and will not employ the scoring model in the section below.

Differentiator	Explanation
Utility name	What is the public name of the Utility, blockchain or ledger?
DID Method	What DID method is used? Point to where it is registered on the DID Registry
Convenor	Which organization, person, or DAO is responsible for the Utility?
Base Protocol	What is the base protocol that the Utility is built upon (e.g. Hyperledger Indy, Ethereum etc.)?
Permissioned or Permissionless	Does the Utility have a permissioned or permissionless model?
Number of nodes	How many nodes, validators, or stewards (analogous) are there running on the network?
Schema storage	Where does the Utility store its Verifiable Credential schemas?
Credential Definitions	Does the Utility support Credential Definitions?
DID Document storage	Where does the Utility store its DID Documents?
Revocation registry supported	What type of Revocation method or registry is supported?
Credential type supported	What Credential flavors or types are

Differentiator	Explanation
	supported by the Utility?
Utility Software Development Kit (SDK)	What specific SDKs does the Utility support for utilizing its functionality?
Types of DID resolver supported	What implementations of a DID resolver does the Utility support?
Payments for DIDs supported	Does the Utility charge for Decentralized Identifier (DID) writes? <i><Please link to where the payment model is recorded></i>
Payments for VCs supported	Does the Utility have any functionality to support payments for Verifiable Credentials natively? <i><Please link to where the payment model is recorded></i>
Governance type	Does the Utility support a traditional or a decentralized governance model? <i><Please link to the Governance Framework></i>

A template for filling out the above may be found in the appendix of this document, and also on the [Utility Foundry Working Group Wiki here](#).

The UFWG suggests that for each Utility and application of a Utility, this template should be used to signpost the protocols and interoperability profile of the Utility. This transparency and detail in terms of a technical stack is important for the SSI ecosystem interoperating on a larger scale - and this entire conversation needs to be started from the Utility layer upwards.

Utility Grading Criteria

In creating business cases around technology, people often use a simple framework of *Business*, *Legal*, and *Technology* to support the business decision processes. A common mistake innovators should try to avoid is to start with **only** technology requirements, before considering the business and legal requirements. With decentralized architecture such as the ToIP Framework, it's critical to also take *Social* and *Governance* elements into consideration.

1. Business Requirements - How the Utility helps your business/clients/end customers from a business and economic perspective through its specific network design.

2. Legal Requirements - Any compliance requirements placed on an ecosystem or participants within the ecosystem that pertain to a range of laws such as financial regulations, tax obligations, and privacy regulations.
3. Technical Requirements - The range of technical issues that must be addressed to successfully complete a project using the Utility. These include but are not limited to interoperability, performance, reliability, and availability.
4. Social Requirements - It's important for the ecosystem to create value for the society and also be self-sustaining. Examples of social requirements can include transparency, inclusivity, diversity, and accessibility. Several researchers today use Environmental, Social, and Governance (ESG) metrics to analyze an organization's ethical impact and sustainability practices. This may also be an important factor in evaluating different types of Utility, based on factors such as carbon footprint or diversity in decision making.
5. Governance Requirements - The collection of governing processes required by the Utility to be successful and sustainable.

These may not be the only elements you want to use to evaluate your own project requirements, but we will focus on each of these elements below.

Scoring system and simple graphic representation

Unlike the [W3C DID Rubric v1.0](#), which goes into detailed specifics of each section of a Public Utility and DID method, using a A, B, C, D scoring system; the intention of this document is to create a more easily accessible, visual representation and template of how to compare Utilities.

For this reason the scoring system will be a more basic model:

Fully supported by the Utility	Partially supported by the Utility or on roadmap	Not supported by the Utility
-----------------------------------	--	---------------------------------

A template and visual representation to be filled out by parties who want to use this evaluation framework can be found on the ToIP Wiki here:

<https://wiki.trustoverip.org/display/HOME/List+of+Considerations+When+Choosing+a+Utility>

Business Requirements

This section is important to determine whether the Utility aligns with the commercial model of your company, whether it would be sustainable, and whether it provides easy and accessible software and documentation.

Further work from the UFWG may provide an additional companion guide to clearly explain each of the requirements below.

Does the Utility:

- Provide client software (or a Software Development Kit) to issue and consume Verifiable Credentials, with DIDs anchored on the Utility, for the purpose of developing SSI use cases?
- Utilize an Open Source license for its core network functionality and/or SDK?
- Have a transparent commercial costs model for DIDs anchored to the Utility?
- Support native payment flows for Verifiable Credentials?
- Remunerate Node Operators in any financial capacity?
- Have a financial or economic model for the sustainability of the Utility?
- Have examples of its use within a Proof of Concept (PoC)?
- Have examples of its use within a production environment?
- Provide a testnet or other testing environment?

Technical Requirements

This section will help you understand the technical specifics of each Utility, such as technical standards and capabilities, and considerations that you should make when approaching different Utilities you want to build on.

Does the Utility:

- Support Public DIDs, as defined in the [W3C DID core specification](#), anchored to the Utility for the purpose of Self-Sovereign Identity (SSI) use cases?
- Support W3C Verifiable Credentials, as defined in the Verifiable Credentials Data Model?

- Support AnonCreds V1?
- Support the storage of credential schemas on ledger?
- Support the storage of DID Documents on ledger?
- Support Verifiable Credential revocation?
- Provide privacy preserving Verifiable Credential revocation?
- Have a publicly accessible [DID Core compliant DID method](#)?
- Support multiple DID controllers in its DID method?
- Support Verification Method Relationships such as Authentication, Capacity Invocation and Assertion in its DID method?
- Support the retrieval of historic DID states, such as old/rotated Verification Methods?
- Have the capability to support multiple wallets and implementations on top of its core functionality?
- Provide clear technical documentation for setting up a node on its core Network?

Legal Requirements

This section should help assess whether each utility has done enough to stay compliant within the jurisdiction you want to build your SSI use case within.

Does the Utility:

- Support GDPR and other relevant data protection regulations by design (i.e. no personal data or personally identifiable information is written to the Utility)?
- Have a public crisis and contingency policy, in case the Utility enters a period of downtime or failure?
- Have a defined legal organization, responsible for the actions of the network?
- Utilize a Decentralized Autonomous Organization (DAO) to underpin its corporate structure?

Social Requirements

This section addresses social requirements, such as whether the Utility is environmentally sustainable, whether it is accessible and easy to understand, and whether it has a proactive and engaging community.

Does the Utility:

- Publicize educational content on how to create/resolve DIDs on the Utility?
- Formally support Trust over IP, as a registered Utility?
- Have a core team which actively engages in the SSI community on a weekly basis?
- Support and/or partner with SSI vendors?
- Engage in initiatives to offset its carbon footprint and/or reduce its environmental footprint?

Governance Requirements

Finally, this section will help you understand why governance is important and where traditional and decentralized governance differentiate.

Does the Utility:

- Support open, public participation in governance decisions?
- Have a public, transparent governance framework?
- Allow the community to influence the product roadmap?
- Have an active strategy to achieve a state of sufficient decentralization or censorship resistance?
- Have an enforcement policy for counteracting bad behavior on the Network?
- Have a forum for Utility-specific discussion for the users and participants?
- A governance voting structure, either based on an elected Board or through a more distributed/decentralized voting structure?

Overall framework and template

The idea behind this overall framework is to give organizations and individuals the tools they need to compare and contrast different Utilities in order to assess which are best fit for purpose for their own project.

These criteria should also be considered and evaluated for any party wanting to create their own Utility for the purpose of decentralized identity.

A template for comparing Utilities against each other can be found in the ToIP Wiki document below.

<https://wiki.trustoverip.org/display/HOME/List+of+Considerations+When+Choosing+a+Utility>

Glossary of Terms

Trust Over IP is in the process of creating a Terms Glossary. When the ToIP Terms Glossary is complete this document will be amended to have a link to it.

Appendix

Broad differentiators and technical standards supported by the Layer One Utility.

Differentiator	Explanation	Answer
Utility name	What is the public name of the Utility, blockchain or ledger?	<i><Please write all answers in this column, and delete this text></i>
DID Method	What DID method is used? Point to where it is registered on the DID Registry	
Convenor	Which organization, person, or DAO is responsible for the Utility?	
Base Protocol	What is the base protocol that the Utility is built upon (e.g. Hyperledger Indy, Ethereum etc.)?	
Permissioned or Permissionless	Does the Utility have a permissioned or permissionless model?	
Number of nodes	How many nodes, validators, or stewards (analogous) are there running on the network?	
Schema storage	Where does the Utility store its Verifiable Credential schemas?	
Credential Definitions	Does the Utility support Credential Definitions?	
DID Document storage	Where does the Utility store its DID Documents?	
Revocation registry supported	What type of Revocation method or registry is supported?	
Credential type supported	What Credential flavors or types are supported by the Utility?	
Utility Software Development Kit (SDK)	What specific SDKs does the Utility support for utilizing its functionality?	

Differentiator	Explanation	Answer
Types of DID resolver supported	What implementations of a DID resolver does the Utility support?	
Cross-ledger DID support	Does the Utility support or make any efforts to enable DIDs to be cross-utility compatible?	
Payments for DIDs supported	Does the Utility charge for Decentralized Identifier (DID) writes? If so, how much does it charge?	
Payments for VCs supported	Does the Utility have any functionality to support payments for Verifiable Credentials natively?	
Governance type	Does the Utility support a traditional or a decentralized governance model?	