Self-Sovereign Identity
Personal Data Usage Licensing (SSI-PDUL) Model: Solution Concept

Version 0.27 REVIEW DRAFT

Michael Herman
Self-Sovereign Blockchain
Futurist, Architect, and Developer

Trusted Digital Web
Hyperonomy Digital Identity Lab
Parallelspace Corporation

Alberta, Canada

mwherman@parallelspace.net

The publication of this whitepaper coincides with recent discussions (January 2021) about how a user might assert permanent and absolute control over their personal digital identities: personal digital identifiers and any associated personal identity data.

TABLE OF CONTENTS

ABSTRACT

The purpose of this solution concept whitepaper is to provide the first complete description of the motivations, key concepts, problem statement, and solution approach for implementing the Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model, a functional component of the Self-Sovereign Identity Model (SSI Model).

This solution concept addresses the following user scenario:

> *How Alice User, an App User and Identity Owner, and Bob Developer, an App Developer and App Controller, might negotiate the use of Alice's personal digital identifiers and any associated personal identity data by Bob's app, based on Self-Sovereign Identity Model Usage Principles.*

The scope of the Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model is personal digital identifiers and any associated identity data presented by Alice to the App. It does not include the permissioning of data internal to the App (although the natural extension of the solution to internal data is an obvious one).

The intended audience for this whitepaper is a broad range of professionals interested in furthering the application and use of the SSI Model in software apps, agents, and services using an SSI Personal Data Usage Licensing (SSI-PDUL) Model approach. This includes software architects, application developers, and user experience (UX) specialists; as well as people involved in a broad range of standards efforts related to decentralized identity, verified credentials, and secure storage.

The work documented here was performed under the auspices of the Trusted Digital Web project in the Hyperonomy Digital Identity Lab of Parallelspace Corporation.

CONTEXT

The publication of this whitepaper coincides with recent discussions (January 2021) about how a user might assert permanent and absolute control over their personal digital identities: personal digital identifiers and any associated personal identity data.

Purpose

The purpose of this solution concept whitepaper is to provide the first complete description of the motivations, key concepts, problem statement, and solution approach for the SSI Personal Data Usage Licensing (SSI-PDUL) Model, a functional component of the SSI Model.

This solution concept addresses this user scenario:

How Alice User, an App User and Identity Owner, and Bob Developer, and App Developer and App Controller, might negotiate the use of Alice's personal digital identifiers and any associated personal identity data by Bob's app, based on Self-Sovereign Identity Model Usage Principles.

The scope of the Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model is personal digital identifiers and any associated identity data presented by Alice to the App. It does not include the permissioning of data internal to the App (although the natural extension of the solution to internal data is an obvious one).

Intended Audience

The intended audience for this whitepaper is a broad range of professionals interested in furthering the application and use of the SSI Model for software apps, agents, and services using an SSI Personal Data Usage Licensing (SSI-PDUL) Model approach. This includes software architects, application developers, and user experience (UX) specialists; as well as people involved in a broad range of standards efforts related to decentralized identity, verified credentials, and secure storage.

Motivation

The motivation for an SSI Personal Data Usage Licensing Model-based solution concept includes answering:

- What types of personal data are we trying to control the usage of?
- What are the different types of personal data?
- What user experience and software support is required to enable Alice to assert her self-sovereign rights over her personal digital identities and any associated personal identity data? …an SSI Model user scenario that is frequently raised but to which no known solution has been proposed
- What is Alice User's perspective of the problem? …that is, from the perspective of Alice, her personal digital identities and any associated personal identity data
- What is Bob Developer's perspective of the problem? …that is, from the perspective of Bob, the developer or publisher of an app, that can benefit from increased user-controlled access to Alice's personal data (and hopefully, increase the value Alice receives from Bob's app)

Sample user stories addressed by the SSI Personal Data Usage Licensing solution concept include:

- App X can refer to but cannot read and persist Alice's identity data to any external storage system (beyond where the original data currently resides) without Alice's expressed permission.
- App X cannot attach its own ancillary information to Alice's self-sovereign personal digital identifiers (e.g. DID or WebID) without Alice's expressed permission.
- App X can read Alice's identity data but cannot aggregate it (anonymously or not) to create its own new data without Alice's expressed permission.

Organization

The following sections of this whitepaper describe the SSI Personal Data Usage Licensing (SSI-PDUL) solution concept in increasing levels of detail.

The current section describes the Context including the purpose, intended audience, motivation, and key concepts.

The Problem Statement section more carefully describes the goal of the solution concept; the problems an eventual solution is intended to solve.

The Solution Approach section details the user scenarios, user stories, use cases, and the first attempt at a high-level solution vision.

The Proposed Solution section details an operational process model that is intended to be embedded in a software application or service committed to implementing the SSI Personal Data Usage Licensing Model.

The reader can choose to stop reading whenever they feel they have grasped the amount of detail that best fits their goals.

Key Concepts

What is a Self-Sovereign Identity Personal Data Usage Licensing solution concept?

The SSI Personal Data Usage Licensing (SSI-PDUL) solution concept is an initial software architecture and user experience solution for the SSI Personal Data Usage Licensing (SSI-PDUL) problem.

What is the Self-Sovereign Identity Personal Data Usage Licensing problem?

The SSI Personal Data Usage Licensing (SSI-PDUL) problem is the inability, in today's software apps, agents, and services industry, for a user, Alice, to have absolute control over her personal digital identities and any associated personal identity data that she chooses to exert permanent and absolute control over. At this time (January 2021), no known horizontal platform solution exists that addresses this problem.

What is Self-Sovereign Identity (SSI)?

Self-Sovereign Identity, as a standalone phrase (or acronym), is a very confusing, overloaded, ambiguous term whose use should be avoided in all situations[1]. In conversation, an article, or a standards document,

[1] The most recent example of SSI confusion is the *Principles of SSI* document published by the Sovrin Foundation (https://sovrin.org/principles-of-ssi/). The document makes no attempt to define SSI nor state what SSI is intended to be an acronym for. *Princples of SSI* has resulted in a lot of confudsion (https://hyperonomy.com/2018/12/18/definition-confuding/) in the decentralized identifer communities as different working groups try to apply the Principles in new domains without for descerning: a) precisely

it could mean any of the uncontracted terms in the following figure. The term Self-Sovereign Identity (or its acronym SSI) could refer to any or all of the uncontracted terms in the following figure – unless an author has taken care to be clear and precise with respect to every occurrence of the term and/or its acronym.

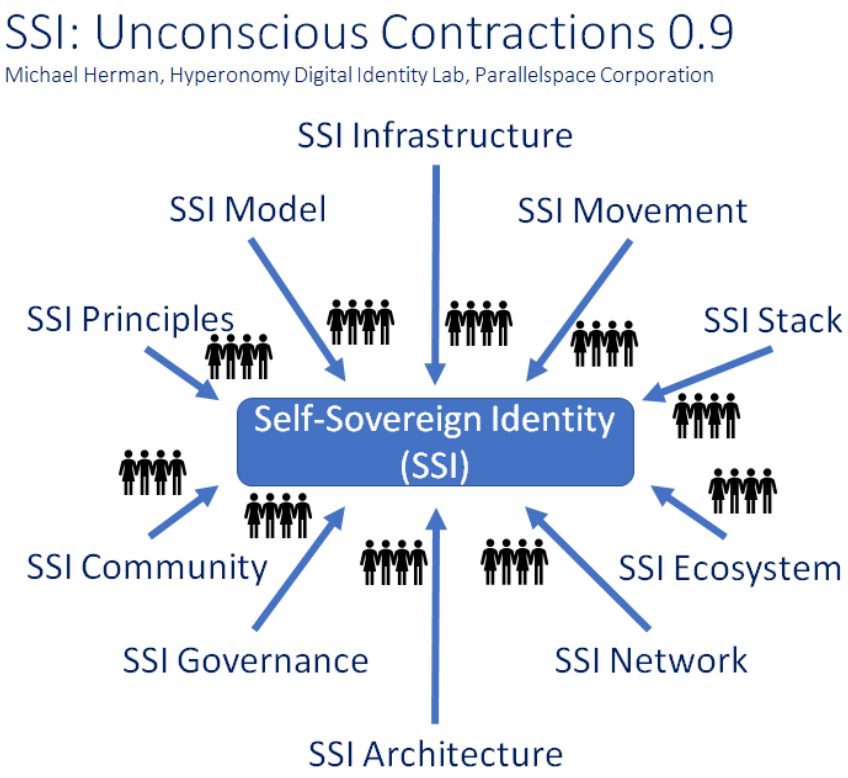


Figure 1. SSI: Unconscious Contractions

For the purposes of this document, the most commonly used and generically used term is the Self-Sovereign Identity Model (SSI Model) and it is always referred to as such. The second most commonly referred to related terms is the SSI Personal Data Usage Licensing (SSI-PDUL) Model.

What is the Self-Sovereign Identity Model (SSI Model)?

The Self-Sovereign Identity Model (SSI Model) is an identity system architecture based on the core principle that Identity Owners have the right to permanently exert control over the usage of one or more of their Personal Digital Identifiers and, independently, the usage of any associated Personal Identity Data.

---

which definition/application of SSI should be used and b) the types or categories of principles being represented in the document. Without first having a clear and precise definition for (a), successfully achieving (b) is almost impossible.

What is a Personal Data Usage Licensing Model (PDUL Model)?

A Personal Data Usage Licensing Model (PDUL Model) describes an approach for licensing the usage of personal data by an application or service. The model can include prototypical data structures and business processes designed to be implemented in software.

What is the Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model?

The Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model describes an approach for licensing the usage of Personal Data (Personal Digital Identifiers and any associated Personal Digital Identity Data) by an application or service based on SSI Model Principles.

Self-Sovereign Identity Model Landscape

The Self-Sovereign Identity Model Landscape is a visual reference model for most of the basic terminology in the SSI Model. These are the key terms needed to understand the SSI Model – as background for understanding the SSI Personal Data Usage Licensing (SSI-PDUL) Model solution concept described in the remainder of this whitepaper.

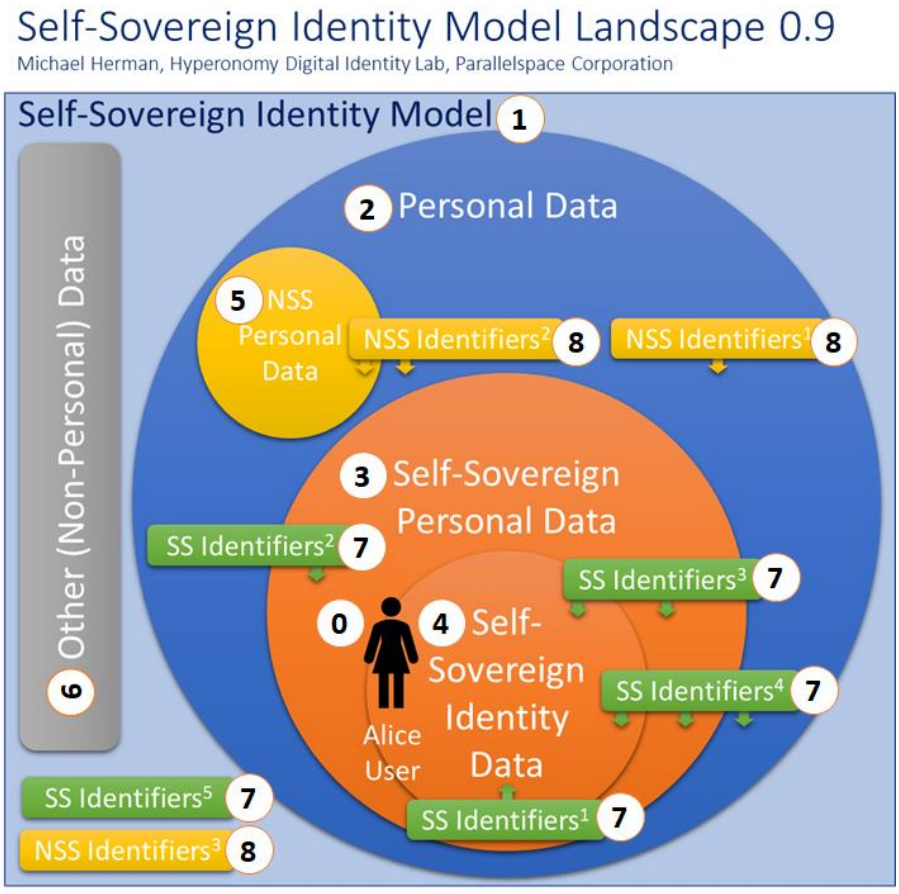


Figure 2. Self-Sovereign Identity Model Landscape

The following statements are used to further describe the SSI Model depicted in the above figure. More formal definitions for the SSI Model can be found in APPENDIX A – Self-Sovereign Identity Model Definitions on page 34.

0. **Alice User**: Alice User is both a Subject and a Data Controller. More importantly, Alice is the self-sovereign owner and controller over her Personal Digital Identifiers that she chooses to exert absolute assert control over in addition to any Personal Identity Data associated with these identifiers (i.e. Self-Sovereign Identifiers [7]) as well as her Self-Sovereign Personal Data [3] (which, in turn, includes her Self-Sovereign Identity [4])).
1. **Self-Sovereign Model (SSI Model)**: The SSI Model is an identity system architecture based on the core principle that Identity Owners have the right to permanently and absolutely control one or more of their Personal Digital Identifiers and, independently, with the usage of any associated Personal Identity Data.
2. **Personal Data**: Personal Data includes all data keyed, indexed, or otherwise associated with a Person (not an Organization nor a Non-Fungible Thing). Personal Data includes Self-Sovereign Personal Data [3], Non-Self-Sovereign Personal Data [5], Self-Sovereign Identity Data [4], and Self-Sovereign Identifiers [7].
3. **Self-Sovereign Personal Data**: Self-Sovereign Personal Data is a subset of Personal Data [2]. Self-Sovereign Personal Data includes all data keyed, indexed, or otherwise associated with a Person that they choose to assert absolute control over. Self-Sovereign Personal Data includes Self-Sovereign Identity Data [4], and Self-Sovereign Identifiers [7].
4. **Self-Sovereign Identity Data**: Self-Sovereign Identity Data is the subset of Self-Sovereign Personal Data that can be used to identify a person such as a name, photograph, fingerprint, etc. SS Identity Data can include:
   a) your identifying attributes (e.g. your names, DOB, hair color, eye color, height, SIN, driver's license number, driver's license photograph, passport photo, passport number, etc.), b) your relationships with other people and organizations (e.g. parents, the company you work for, the companies you've worked for in the past, the country you're a citizen of, the communities where you live, work, and play, the connections you have with friends, relatives, colleagues, etc.), and c) the agents who represent you or work on your behalf (e.g. your bank, credit card company, lawyer, real estate agent, smartphone apps, cloud services (e.g. email, PayPal, online banking), etc.)[2].
5. **Non-Self-Sovereign Personal Data (NSS Personal Data)**: NSS Personal Data is Personal Data associated with one of Alice's NSS Identifiers over which she doesn't or is otherwise unable to exert control.
6. **Other (Non-Personal) Data**: Other (Non-Personal) Data is data that is not associated with a Person. It may be data associated with an organization, non-fungible thing, physical phenomena, etc.
7. **Self-Sovereign Identifiers (SS Identifiers)**: An SS Identifier is a text string or other atomic data structure used to provide a base level of Identity for a Person (e.g. Alice) who chooses to absolute control over the identifier.
8. **Non-Self-Sovereign Identifier (NSS Identifiers)**: An NSS Identifier is a text string or other atomic data structure used to provide a base level of Identity for a Person (e.g. Alice) where that person chooses not to or is unable to have absolute control over the identifier.

[2] Daniel Hardman's SSIMeetup.com webcast: Identity and the quest for Self-Sovereign Identity (https://youtu.be/iqmY_h49vPs).

Self-Sovereign Identity Model Usage Principles

The Self-Sovereign Identity Model Usage Principles (SSI Model Usage Principles) are based on the *first of the three fundamental characteristics of Self-Sovereign Identities* – defined in the CONTROL section of APPENDIX G – Core Characteristics of Sovereign Identity [Identities] on page 58 by Joe Andrieu, October 2016. Quoting from the CONTROL section in APPENDIX G – Core Characteristics of Sovereign Identity [Identities], the SSI Model Usage Principles are:

1. Self-generatable and Independent

Individuals must be able to create identity information without asking for permission and be able to assert identity information from any authority. The resulting identity must have the same technical reliability as those provided by well-known, "official" sources. The observer, of course, is always free to decide whether or not a given piece of information is meritorious, but the information must be able to be verified as a non-repudiatable statement of correlation using exactly the same mechanisms regardless of source. Further, individuals must be able to present self-generated identity information without disclosing that the authority in the claim is the subject of the claim.

2. Opt-in

The affordance for asserting identity information starts with the individual. While an individual may present claims from known or accepted third party authorities, it is the individual who asserts that the claim applies to them. Self-sovereign identities begin with the will of the individual, with the intentional presentation of identity information.

3. Minimal Disclosure

Individuals should be able to use services with minimal identity information. Features that depend on enhanced correlation must be understood by the average user. Such features should be permissioned with the highest granularity, so functions independent of correlation work equally well alongside those dependent on it. It is not acceptable to deny services because of a refusal to provide unrelated information.

4. Non-participation

Individuals must be able to choose to not provide identity information for services where it isn't absolutely required. Any spontaneous identifiers necessary for a service to function, such as cookies or session ids, must use the same infrastructure for consent, persistence, transience, and disclosure as if provided by the individual.

5. Opt-out

Individuals should be able to opt-out of identifying records post-facto as a matter of course. People should be able to stop the use of a correlating identity information by request. Some transactions necessarily require long-term retention of identity information, such as financial transactions, purchases, and shipments. Actions that create permanent records should be clearly marked and communicated such that the retention is expected and understood by the average person. All other actions which leverage a self-sovereign identity should be de-correlated on-demand and said identifiers should no longer be used to correlate that individual across contexts.

Recoverable, the 6th principle in the CONTROL section of APPENDIX G – Core Characteristics of Sovereign Identity [Identities], is explicitly excluded from the SSI Model Usage Principles.

Self-Sovereign Identity Model Usage Principles Compliance Criteria

The following SSI Model Usage Principles compliance criteria or tests are abstracted directly from the above SSI Model Usage Principles.

1. Self-generatable and Independent Compliance Criteria

a. Ability [for individuals] to create identity information without asking for permission
b. Ability to assert identity information from any authority
c. Must have the same technical reliability as those provided by well-known, "official" sources
d. The observer is always free to decide whether or not a given piece of information is meritorious
e. Ability for [identity data] to be verified as a non-repudiatable statement of correlation using exactly the same mechanisms regardless of source
f. Ability to present self-generated identity information without disclosing that the authority in the claim is the subject of the claim

2. Opt-in Compliance Criteria

a. Affordance for asserting identity information starts with the individual.
b. Ability to present claims from known or accepted third party authorities
c. Ability to assert that the claim applies to them
d. Self-sovereign identities begin with the will of the individual, with the intentional presentation of identity information

3. Minimal Disclosure Compliance Criteria

a. Ability to use services with minimal identity information
b. Features that depend on enhanced correlation must be understood by the average user
c. Features should be permissioned with the highest granularity
d. Functions independent of correlation work equally well alongside those dependent on it
e. Not acceptable to deny services because of a refusal to provide unrelated information

4. Non-participation Compliance Criteria

a. Ability to choose to not provide identity information for services where it isn't absolutely required
b. Any spontaneous identifiers necessary for a service to function, such as cookies or session ids, must use the same infrastructure for consent, persistence, transience, and disclosure as if provided by the individual

5. Opt-out Compliance Criteria

a. Ability to opt-out of identifying records post-facto as a matter of course
b. Ability to stop the use of a correlating identity information by request
c. Actions that create permanent records [(long term retention of identity information)] should be clearly marked and communicated such that the retention is expected and understood by the average person
d. All other actions which leverage a self-sovereign identity should be de-correlated on-demand and no longer be used to correlate that individual across contexts

Additional Definitions

A comprehensive list of related definitions can be found in:

PROBLEM STATEMENT

"Each person's digital identity belongs to them. They control it."
[Joy Chik Corporate Vice President, Microsoft Identity
(https://www.microsoft.com/security/blog/2019/05/15/decentralized-identity-digital-privacy/)]

Overview

The problem to be solved by the Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model solution concept is defined by the following user scenario:

How Alice User, an App User and Identity Owner, and Bob Developer, an App Developer and App Controller, might negotiate the use of Alice's personal digital identifiers and any associated personal identity data by Bob's app, based on Self-Sovereign Identity Model Usage Principles.

Support for SSI Model Usage Principles

The Self-Sovereign Identity Personal Data Usage Licensing (SSI-PDUL) Model solution concept is focused on addressing the 5 SSI Model Usage Principles.

1. Self-generatable and Independent
2. Opt-in
3. Minimal Disclosure
4. Non-participation
5. Opt-out

These SSI Model Usage Principles are defined in an earlier section: Self-Sovereign Identity Model Usage Principles on page 11.

Sample Use Cases

Sample user stories include:

- App X can refer to but cannot read and persist Alice's identity data to any external storage system (beyond where the original data currently resides) without Alice's expressed permission.
- App X cannot attach its own ancillary information to Alice's self-sovereign personal digital identifiers (e.g. DID or WebID) without Alice's expressed permission.
- App X can read Alice's identity data but cannot aggregate it (anonymously or not) to create its own new data without Alice's expressed permission.

SOLUTION APPROACH

The solution approach begins with a discussion of the user scenario: user stories and use cases. Based on the user scenario, user stories, and use cases, a vision for the solution will be developed next.

User Scenario

How Alice User, an App User and Identity Owner, and Bob Developer, an App Developer and App Controller, might negotiate the use of Alice's personal digital identifiers and any associated personal identity data by Bob's app, based on Self-Sovereign Identity Model Usage Principles.

User Story

Alice User wants to use Bob Developer's App in a way in which she can completely control the use of her personal digital identifiers and any associated personal identity data. She wants and expects Bob's App to completely respect the SSI Model Usage Principles and the corresponding use of her personal digital identifiers and any associated personal identity data.

Alice's roles are as an App User and also as an Identity Owner; more specifically a Self-Sovereign Identity Owner who is exerting permanent and absolute ownership and control over her personal digital identities and any associated personal identity data.

Bob is the App Developer, App Publisher, and App Controller. To comply with the SSI Model Usage Principles, Bob has to implement a solution that supports/addresses SSI Model Usage Principles in his app. Bob has software architecture and design issues as well as user experience (UX) issues he needs to consider.

To support a range of identity data that Alice may permit Bob's App to access and use in a controlled manner, Bob has envisioned that his app will require a range of role definitions. Each role definition will have 2 aspects:

a. The subcollections of App functions that are enabled for each role.
b. The set of self-sovereign identifier and identity data claims that a user needs to present (assert) to enable each role.

Different sets of self-sovereign identifier and identity data claims will enable one or more levels of role definition(s) to be enabled in the App for Alice.

Depending on the self-sovereign identifier and identity data claims presented (asserted) by Alice, an automated negotiation process will select one of the role definitions supported by the app.

Use Cases

The use cases addressed by the SSI Personal Data Usage Licensing (SSI-PDUL) Model are divided into 2 categories:

- Self-Sovereign *Identifier* Generic Use Cases
- Self-Sovereign *Identity Data* Generic Use Cases

SS Identifier Generic Use Cases

The SS Identifier Use Cases include those SSI-PDUL use cases that specifically relate to the use and control of self-sovereign personal digital *identifiers*.

1. **Identifier Usage Claims**: Alice has the ability to control Alice's self-sovereign personal digital identifiers through the use of an identifier usage claims or licensing capability.
2. **Identifier Access**: App X cannot read or otherwise access Alice's self-sovereign personal digital identifiers without Alice's expressed permission.
3. **Identifier Persistence**: App X cannot read and persist Alice's self-sovereign personal digital identifiers to any external storage system, agent, or service (beyond where the original data currently resides) without Alice's expressed permission.
4. **Ancillary Data**: App X cannot attach its own ancillary data (or otherwise refer) to Alice's self-sovereign personal digital identifiers (e.g. DID or WebID) without Alice's expressed permission. When App X does receive permission from Alice to attached ancillary data to one of Alice's self-sovereign personal digital identifiers, App X will be designed to store only what is necessary (the minimum) for the app to support the set of functions dictated by the definition Alice's selected role definition for the app.
5. **Identifier Sharing**: App X cannot share any of Alice's self-sovereign personal digital identifiers (e.g. DID or WebID) with any third party without Alice's expressed permission.
6. **Identifier Removal**: App X must remove every and all *instances* of Alice's self-sovereign personal digital identifiers when requested by Alice.

SS Identity Data Generic Use Cases

The SS Identity Data Use Cases include those SSI-PDUL use cases that specifically relate to the use and control of *identity data* associated with one or more of a person's self-sovereign personal digital identifiers.

7. **Identifier Data Usage Claims**: Alice has the ability to control Alice's identity data that is associated with Alice's self-sovereign personal digital identifiers through the use of an identity data usage claims or licensing capability.
8. **Identity Data Access**: App X cannot read or otherwise access Alice's any personal identity data associated with any of her self-sovereign personal digital identifiers without Alice's expressed permission.
9. **Identity Data Persistence**: App X cannot read and persist Alice's any personal identity data associated with any of her self-sovereign personal digital identifiers to any external storage system (beyond where the original data currently resides) without Alice's expressed permission.
10. **Identity Data Aggregation**: App X can read Alice's identity data but cannot aggregate it statistically or otherwise (anonymously or not) to create its own new data without Alice's expressed permission. When App X does receive permission from Alice to aggregate the personal identity data associated with one of Alice's self-sovereign personal digital identifiers, App X will be designed to aggregate only what is necessary (the minimum) for the app to support the set of functions dictated by the definition Alice's selected role definition for the app.
11. **Identity Data Sharing**: App X cannot share any data associated with any of Alice's self-sovereign personal digital identifiers (e.g. DID or WebID) with any third party without Alice's expressed permission.

12. **Identity Data Removal**: App X must remove every and all *references* of Alice's self-sovereign personal digital identifiers when requested by Alice. App X will then need to remove any and all instances of Alice's personal identity data from its system that was referenced or otherwise indexed by the removed personal digital identifies. The instances of Alice's personal digital identifiers remain in App X unless removed by use case 6. Identifier Removal.

Use Case to SSI Model Usage Principles Cross-References

The above use cases are cross-referenced with the SSI Model Principles compliance criteria (from page 12) in the following 2 tables.

SS Identifier Generic Use Cases

The SS Identifier Use Cases Cross-References are described in the following table.

Table 1. SS Identifier Use Cases Cross-References

Use Case	1. Self-generatable & Independent	2. Opt-in	3. Minimal Disclosure	4. Non-participation	5. Opt-out
1. Identifier Usage Claims	●	●			
2. Identifier Access		●	●	●	●
3. Identifier Persistence		●	●	●	●
4. Identifier Ancillary Data			●	●	●
5. Identifier Sharing			●	●	●
6. Identifier Removal					●

SS Identity Generic Data Use Cases

The SS Identity Data Use Cases Cross-References are described in the following table.

Table 2. SS Identity Data Use Cases

Use Case	1. Self-generatable & Independent	2. Opt-in	3. Minimal Disclosure	4. Non-participation	5. Opt-out
7. Identity Data Usage Claims	●	●			
8. Identity Data Access		●	●	●	●
9. Identity Data Persistence		●	●	●	●
10. Identity Data Aggregation			●	●	●
11. Identity Data Sharing			●	●	●
12. Identity Data Removal					●

Alice's Compensation for the Use of Alice's Personal Identifier and Associated Identity Data

Let it be said that the topic of fair compensation for the use of a person's personal data is a favorite topic of the author[3]. That being said, fair compensation (financial or otherwise) for the use of personal data is not discussed in this whitepaper.

At the heart of the matter is a concern that, while people should be compensated for the use of their personal data for functions beyond the person's direct benefit, this becomes a *slippery slope* where people are financially induced (or otherwise compensated) to disclose more personal identifier or identity data that they would normally[4].

[3] *Are Canadian banks trafficking in the digital identities of millions of Canadians?* April 21, 2018. (https://www.linkedin.com/pulse/canadian-banks-trafficking-digital-identities-canadians-herman/)

[4] Similar to that way Americans are paid to *donate* blood in the United States.

Solution Vision

Basic Requirements

Any proposed solution to the Self-Sovereign Identity Personal Data Usage Licensing problem must be:

a. simple to understand and use, and
b. straight forward to implement in software.

The solution needs to be easy for Alice to understand and use as well as for Bob to understand and integrate into a new or, just as likely, existing app. Each party needs to be able to view the solution from each of their different and unique perspectives and, at the same time, have the solution *make sense* as a whole.

The common denominators for the proposed solution concept are:

- identifier and identity data usage claims (based on the W5 model described in this section)
- app role definitions

App Role Definitions

Application users are generally familiar with the concept of app role definitions within business applications and business processes. Closely related to this concept is the idea of different levels of product functionality being made available based on the "edition" of the product or service you purchase or subscribe to (e.g. Bronze, Silver, Gold, and Platinum service plans or product editions; for Free vs. Paid For subscriptions)[5].

In the current solution vision, Bob Developer is free to choose whatever role definitions make sense for his app. Ideally, the role definitions are somewhat hierarchical and correspond to different sets of functionalities enabled by Alice granting permissions to selected subsets of her personal identity data associated with, typically, a single personal digital identifier that Alice exerts control over. The choice of the selected role definition can depend on other factors too (such as the budget Alice has available to purchase and use a particular edition of the app).

Bob has envisioned that his app will need multiple successive levels of role definitions that are, in part, mapped to increased access to Alice's personal digital identifier and associated digital identity data:

1. New Member
2. Basic Member
3. Full Member
4. Premium Member

Identifier and Identity Data Usage Claims

Identifier and Identity Data Usage Claims are the mechanisms used by Alice to grant permissions for Bob's App to access her personal digital identity and any associated personal identity data as well as how the app can use it once it has assessed it. Some use case examples can be found in the section Use Cases on

[5] Don't get me started on the American healthcare marketplaces and their Bronze, Silver, Gold and Platinum healthcare plans. What a mess – especially for this Canadian who ended up moving back to Canada after a 7 month stay in Washington state.

page 15. These use cases represent a generic set that can be tailored to the needs of each specific app. Each app design should not unnecessarily try to wildly deviate from this initial set of generic use cases. It is expected that in the *fullness-of-time*, the SSI Personal Data Usage Licensing (SSI-PDUL) Model will coalesce around a fairly common set of Identifier and Identity Data Usage Claims (aka generic use cases).

Primary for convenience, Identifier and Identity Data Usage Claims, in turn, are packaged into named credentials called SSI Usage Licenses. The Credential format is chosen because of its popularity and common usage within the decentralized identity community, and, optional, to support verifiability (see the sections Verification on page 46 and Levels of Trust on page 47).

Identifier and Identity Data Usage Claims W5 Model

What is inside an Identifier or Identity Data Usage Claim?

What is the scope of what is needed to fully specify an Identifier or Identity Data Usage Claim?

As an initial answer to these two questions, the 5 W's are used to design an Identifier and Identity Data Usage Claim:

a. What
b. Where
c. Why
d. Who
e. When

While this approach is believed to be unique to the SSI Personal Data Usage Licensing (SSI-PDUL) Model solution, it was partly inspired by one of Daniel Hardman's SSIMeetup.com webcasts[6].

Table 3. Identifier and Identity Data Usage Claims W5 Model

Claim Dimension	Claim Description	Type
1. What	Which attributes	Container/Element/Attribute URI
2. Where	Which targets (relationships)	Identifier (e.g. DID, WebID)
3. Why	Which purposes/usage/actions	Enumeration (based on use cases)
4. Who	Which agents/intermediaries	Identifier (e.g. DID, WebID) mapped to Service Endpoint
5. When	Which time periods (initiation timestamp, expiration timestamp, retention periods, recurrence, etc.)	A Complex Time-based Structure

[6] Daniel Hardman's SSIMeetup.com webcast: Identity and the quest for Self-Sovereign Identity (https://youtu.be/iqmY_h49vPs?t=617).

PROPOSED SOLUTION

Introduction

From the process/task flow, user experience (UX), and data flow perspectives, the proposed SSI Personal Data Usage Licensing (SSI-PDUL) solution is depicted in the following figure.

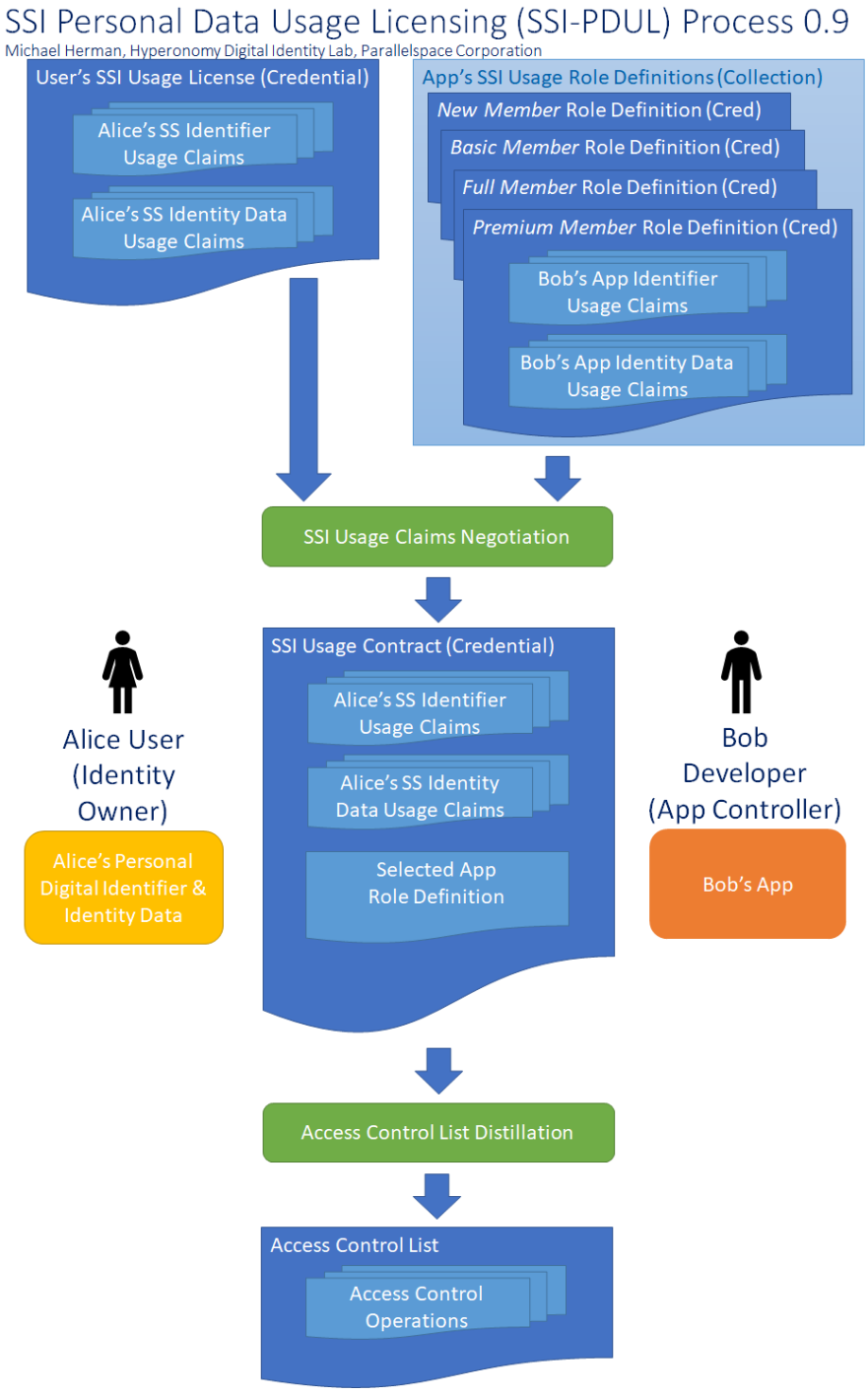


Figure 3. Proposed SSI Personal Data Usage Licensing (SSI-PDUL) Reference Process Model

Solution Concept

A detailed description of the overall SSI Personal Data Usage Licensing (SSI-PDUL) Reference Process Model is depicted below. Detailed explanations of the numbered elements follow the diagram.

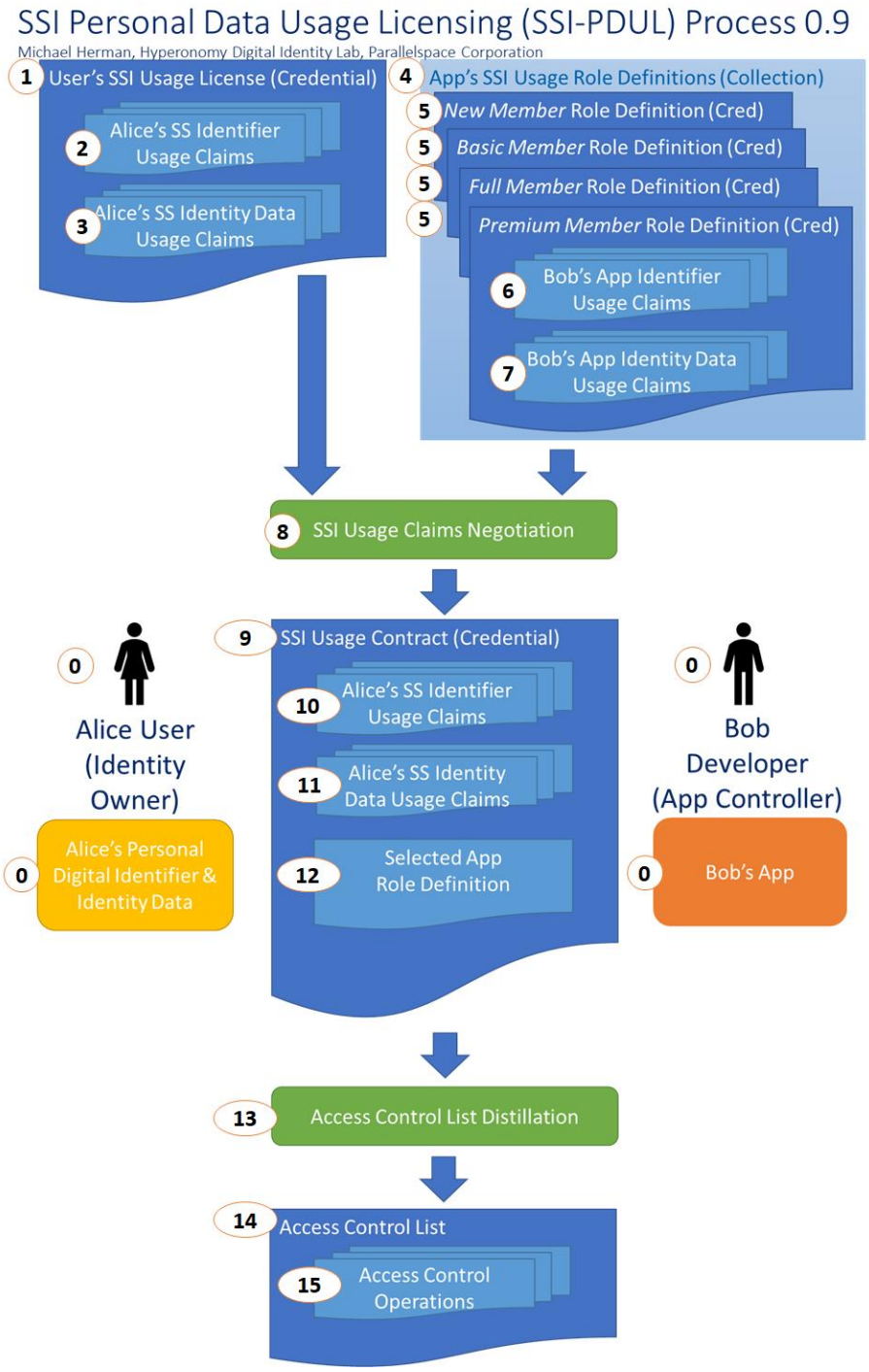


Figure 4. Annotated SSI Personal Data Usage Licensing (SSI-PDUL) Reference Process Model

The detailed explanation of the process depicted in the above figure can be found in the next section.

SSI Personal Data Usage Licensing (SSI-PDUL) Reference Process Model

Actors

0. **Actors**: Alice User wants to use Bob's App from Bob Developer, the App's Controller (developer and/or publisher). Alice also wants to assert her SSI usage rights (with respect to her Personal Public Identifier(s) and associated Personal Identity Data) in advance of using the App and in advance of agreeing to any of the Bob Developer's Terms of Service (ToS) for his App.

SSI Usage License

1. **Alice's SSI Usage License**: Alice starts to assert her SSI usage rights by creating a named SSI Usage License. The License is packaged as a credential containing 2 types of claims: Alice's SS Identifier Usage Claims [2] and Alice's SS Identity Data Usage Claims [3]. The SSI Usage License is specific to:
   a) one of Alice's particular Personal Digital Identifiers [0], and
   b) one of Bob's specific Apps [0].
   (Alice's SSI Usage Licenses may be reusable across multiple Apps and App Controllers TBD).
2. **Alice's SS Identifier Usage Claims**: An Identifier Usage Claim asserts a specific usage right against one of Alice's specific Personal Digital Identities [0]. For example, Bob's App cannot associate any App data with Alice's Personal Digital Identity (e.g. a DID or WebID).
3. **Alice's SS Identity Data Usage Claims**: An Identity Data Usage Claim s asserts specific usage right against one of Alice's all or part of the Identity Data associated with one of Alice's specific Personal Digital Identities [0]. For example, Bob's App cannot read, copy, and persist any of the Identity Data [0] associated with one of Alice's specific Personal Digital Identities [0].

SSI Usage Roles

4. **App's SSI Usage Role Definitions**: To facilitate and streamline the SSI Usage Claims Negotiation [8] process, Bob defines and creates a collection of SSI Usage Role Definitions [5] for his specific App.
5. **SSI Usage Role Definition**: Similar to Alice's SSI Usage License [1], each SSI Usage Role Definition is named and packaged as a Credential containing 2 types of Claims: App Identifier Usage Claims [6] and App Identity Data Usage Claims [7].
   Each role corresponds to a different set of Identifier and Identity Data usage rights (represented as individual claims). For example, the more limited the collection of usage rights claims is, the more restricted will be the App functional made available to Alice. How App roles are mapped into App functionality is entirely app and developer dependent as is how different roles map to different sets of Identifier and Identity Data usage rights claims.
6. **Bob's App Identifier Usage Claims**: Together with the Bob's App Identity Data Usage Claims [7], the App Identifier Usage Claims define which usage rights that need to be asserted by Alice's SSI Usage License [1] for one of Alice's particular Personal Digital Identifiers to be granted a particular SSI Usage Role [5] for Bob's App.
7. **Bob's App Identity Data Usage Claims**: Together with the Bob's App Identifier Data Usage Claims [6], the App Identity Usage Claims define which usage rights that need to be asserted by Alice's SSI Usage License [1] for one of Alice's particular Personal Digital Identifiers to be granted a particular SSI Usage Role [5] for Bob's App.

SSI Usage Claims Negotiation

8. **SSI Usage Claims Negotiation**: This is an automated (or at least semi-automated) process whereby Alice's SS Identifier Usage Claims [2] and Alice's SS Identity Data Usage Claims [3] from Alice's SSI Usage License [1] are used for selecting the matching App's SSI Usage Role Definitions [4,5]. The matching is performed using a "least common denominator" approach based on the respective collections of Alice's SS Identifier Usage Claims [2], Alice's SS Identity Data Usage Claims [3], Bob's App Identifier Usage Claims [6], and Bob's App Identity Data Usage Claims [7].

SSI Usage Contract

9. **SSI Usage Contract**: The output of the SSI Usage Claims Negotiation [8] process is an SSI Usage Contract. The SSI Usage Contract includes:
   a) the process inputs (Alice's SS Identifier Usage Claims [2] and Alice's SS Identity Data Usage Claims [3] from Alice's SSI Usage License [1]), and
   b) the primary process output: the Selected App Role Definition [12] from the App's SSI Usage Role Definitions [4,5] collection.
10. **Alice's SS Identifier Usage Claims**: Alice's SS Identifier Usage Claims [2] from Alice's SSI Usage License [1] that are used as an input to the SSI Usage Claims Negotiation [8] process.
11. **Alice's SS Identity Data Usage Claims**: Alice's SS Identity Data Usage Claims [3] from Alice's SSI Usage License [1] that are used as an input to the SSI Usage Claims Negotiation [8] process.
12. **Selected App Role Definition**: A Selected Role Definition is an SSI Usage Role Definition [5] selected from the App's SSI Usage Role Definitions [4,5] collection as an output of the SSI Usage Claims Negotiation [8] process.

NOTE: The following two sections are optional and only relevant when the target App's internal permissions model and logic don't have native support for the concepts introduced above; especially, lacks support for a per-user SSI Usage Contract [9]. An example is the Solid pod storage system and permissions model (https://solid.github.io/authorization-panel/wac-ucr/).

Access Control List Distillation

13. **Access Control List Distillation**: The Access Control List Distillation process and Access Control List [14] are optional but are included in the process for those apps that don't include native support for SSI Usage Contracts [9] in their internal data storage and permission model. The Access Control List Distillation process takes as an input an SSI Usage Contract [9] and distills it down into an Access Control List [14] using the technology and features available in the App's native data storage and permissions model (the process output).

Access Control List

14. **Access Control List**: The Access Control List corresponds to the access control list in an access control permissions model that controls access to data based on access controls like Write, Read, Update, Control, etc. An Access Control List is a collection of Access Control Operations [15].
15. **Access Control Operations**: Access Control Operations correspond to the most granular access control operations in an access control based permissions model (e.g. Write, Read, Update, Control, etc.).

WHERE DO WE GO FROM HERE?

[Strategists] need to 'think in time' linking an organization's past, present, and future in their thought processes. There are three components:

- *the predictive value of the past for the future;*
- *departures from the past which divert the organization from familiar patterns;*
- *the need for continuous comparison*

Jeanne Liedtaka in *The Business of Giving: The Theory and Practice of Philanthropy, Grantmaking and Social Investment* (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1)

Current Status

The current status of the SSI Personal Data Usage Licensing (SSI-PDUL) solution concept is as a process reference model as defined in this document. The next step towards adoption is to design and build a prototype app to actively demonstrate the concepts discussed in this whitepaper.

Technology Adoption Models

Careful consideration must be given to how a new solution as different and as important as the SSI Personal Data Usage Licensing (SSI-PDUL) Model is to the future of the Self-Sovereign Identity Ecosystem. Deployment and adoption are expected to be gradual and slow – full adoption taking place over several iterations and a significant amount of time.

A brief survey and discussion of a small number of technology adoption models taken from the article Technology Adoption Models: A Comprehensive Guide (https://hyperonomy.com/2019/10/16/technology-adoption-models/) is applicable. These include:

- 1. Crossing the Chasm: Technology Adoption Model
- 10. Technology Adoption Model illuminated by the Gartner Hype Cycle
- 19. Exponential Growth Model
- 20. Exponential Growth Model coupled with the Gartner Hype Cycle
- 2a. Social Evolution: Creation of a Nation State
- 2b. Social Evolution: Defining Principles

NOTE: To survey a comprehensive list of technology adoption models, check out the article Technology Adoption Models: A Comprehensive Guide (https://hyperonomy.com/2019/10/16/technology-adoption-models/).

Crossing the Chasm: Technology Adoption Model

Many people will be familiar with one of the original technology adoption models: The Technology Adoption Model. The Technology Adoption Model was originally described in the book *Crossing the Chasm, 3rd Edition: Marketing and Selling Disruptive Products to Mainstream Customers* (https://www.amazon.ca/Crossing-Chasm-3rd-Disruptive-Mainstream/dp/0062292986/ref=sr_1_1) and is depicted in the diagram below.

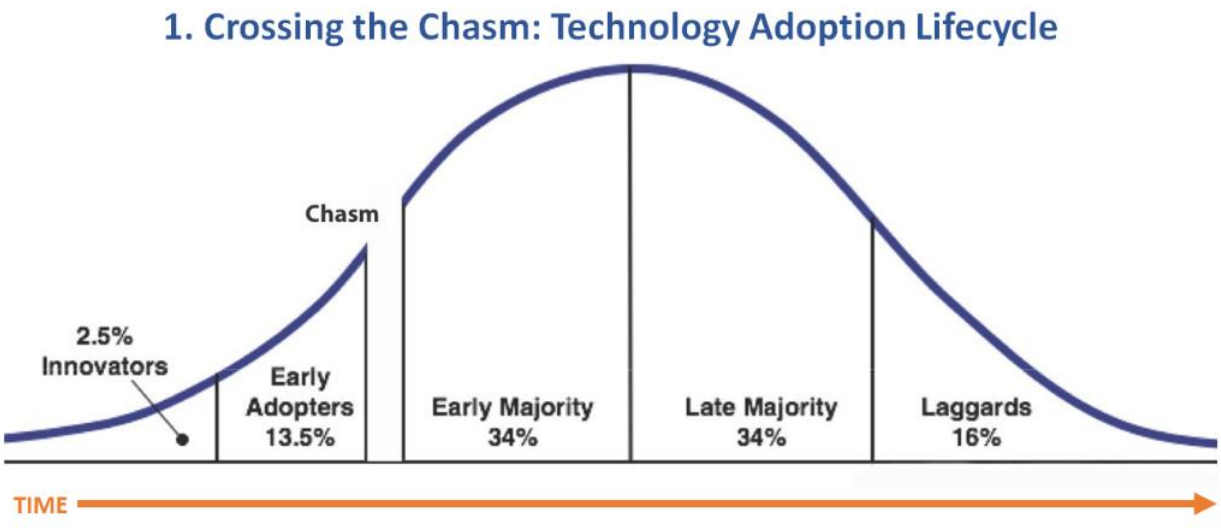


Figure 5. Model 1. Crossing the Chasm: Technology Adoption Lifecycle

While the Technology Adoption Lifecycle model depicted above is useful when explaining the need for a conservative, phased approach when introducing a new product or technology platform (in particular, a novel one), the model, while simplistic, does highlight where a project needs to start (at the left) and where most projects fail when they fail to only excite the Innovators and Early Adopters (at the Chasm).

A more interesting model results when the Technology Adoption Model is overlaid with the Gartner Hype Cycle. The Hyper Cycle serves as a first derivative acceleration/deceleration curve (from Calculus). It illustrates what's happening "behind the scenes" through the Peak of Inflated Expectations and Trough of Disillusionment phases of the Cycle.

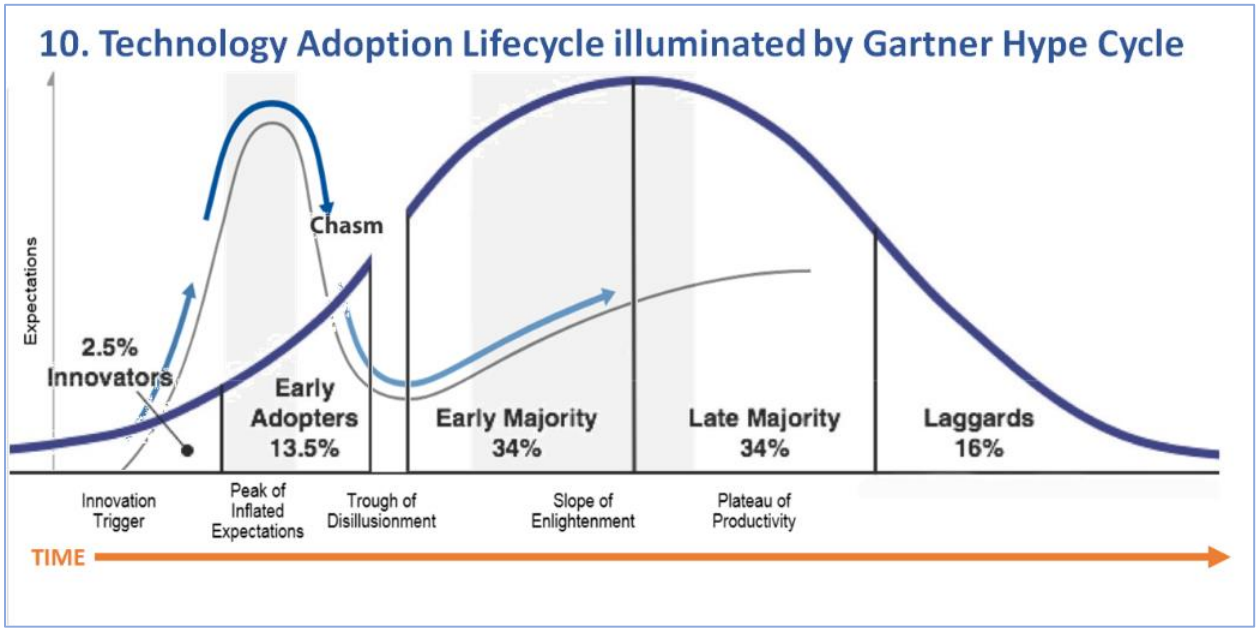


Figure 6. Model 10. Technology Adoption Lifecycle illuminated by the Gartner Hyper Cycle

Another fallacy is the adoption of new products and services often takes place at an exponential pace (exponential growth) as depicted in the diagram below taken from a recent industry report of digital wallets.

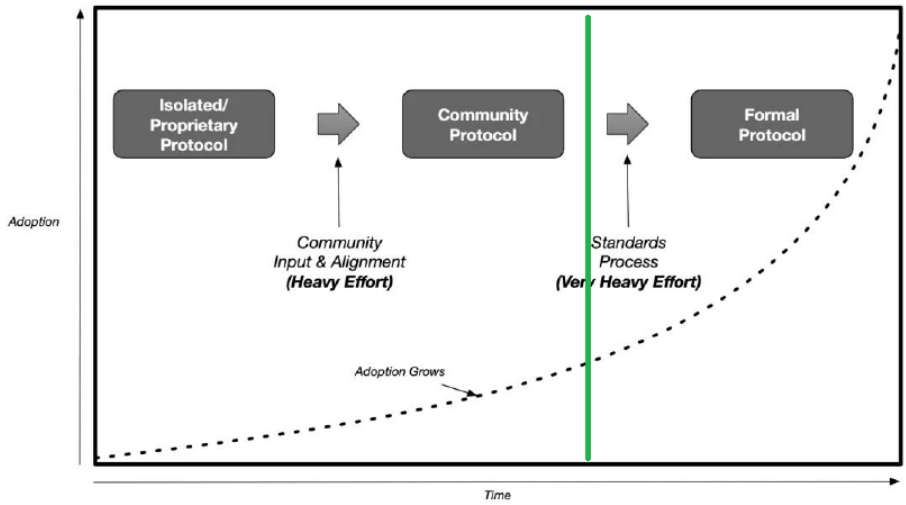


Figure 7. Model 19. Exponential Growth Model

Again, it's instructive to position an early-market exponential growth in the context of the Gartner Hype Cycle as shown below.

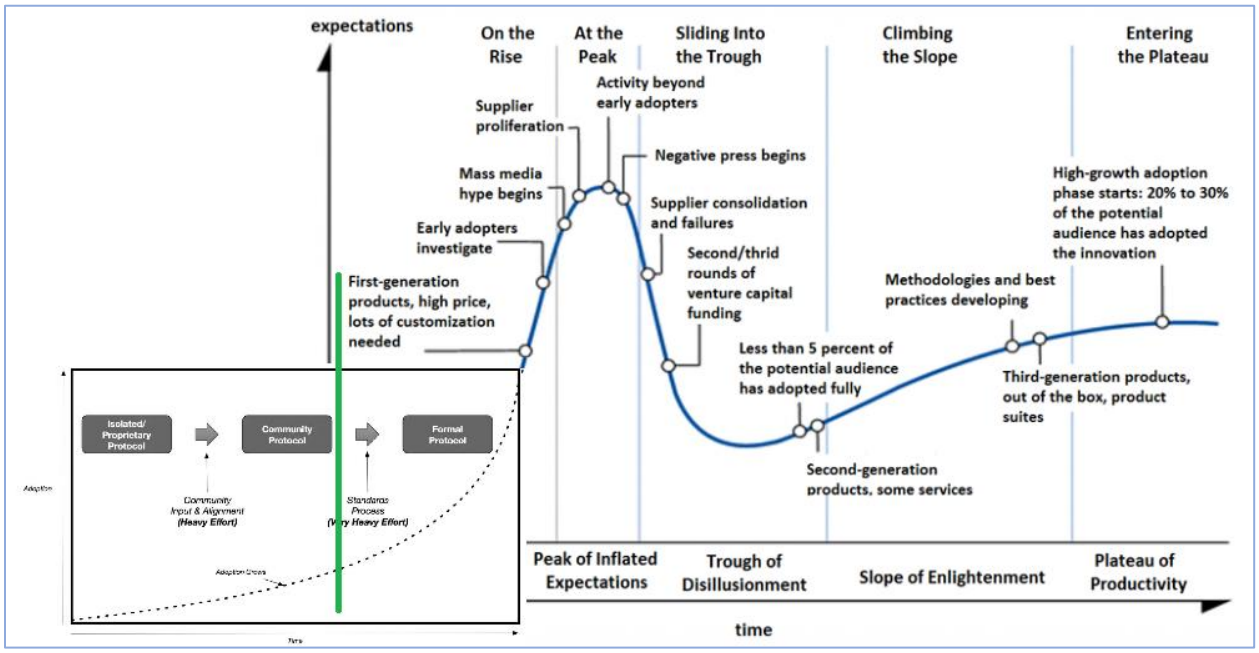


Figure 8. Model 20. Exponential Growth Model coupled with the Gartner Hype Cycle

Exponential growth by early market participants (i.e. unicorns) is often accompanied by a great deal of promotion (hype) until, again, the Peak of Inflated Expectations is reached, and the market caves in on itself. Eventually, if the technology is able to demonstrate ongoing promise and represents a true value differentiator relative to what is being used to solve a similar set of problems today, then the technology may be able to cross the Trough of Disillusionment and over to the lands of Enlightenment and Productivity.

Why does all this matter? More often than not, successful technology adoption more often reflects a social evolution as depicted in the following two models:

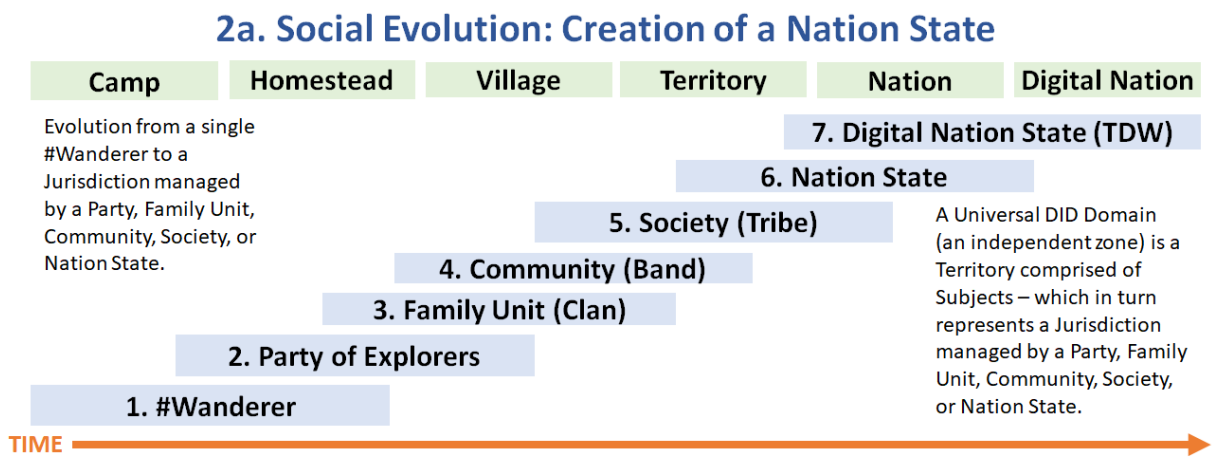


Figure 9. Model 2a. Social Evolution: Creation of a Nation State

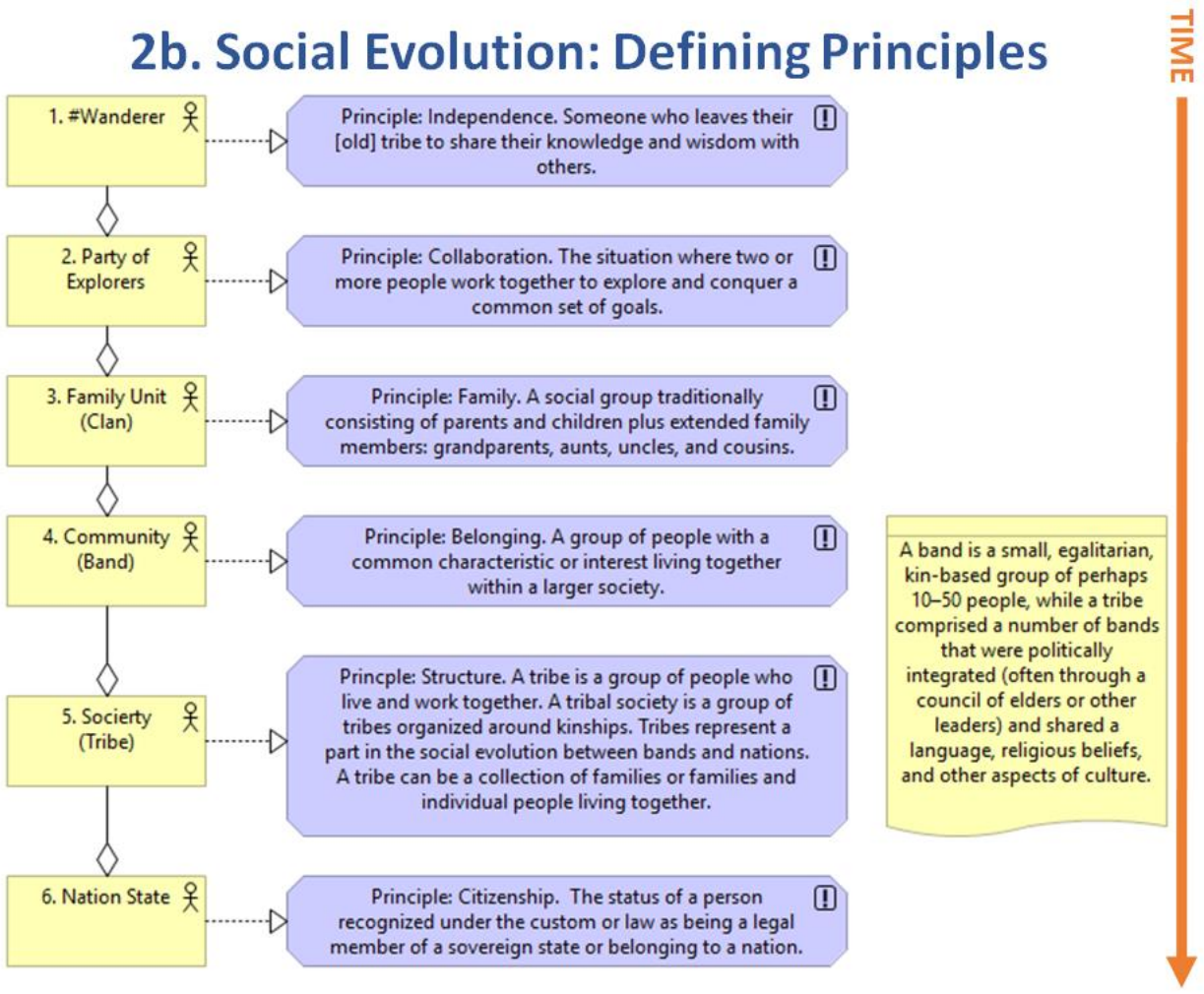


Figure 10. Model 2b. Social Evolution: Defining Principles

This is especially true for game-changing initiatives like the Self-Sovereign Identity Model and solutions like the SSI Personal Data Usage Licensing (SSI-PDUL) Model process reference model.

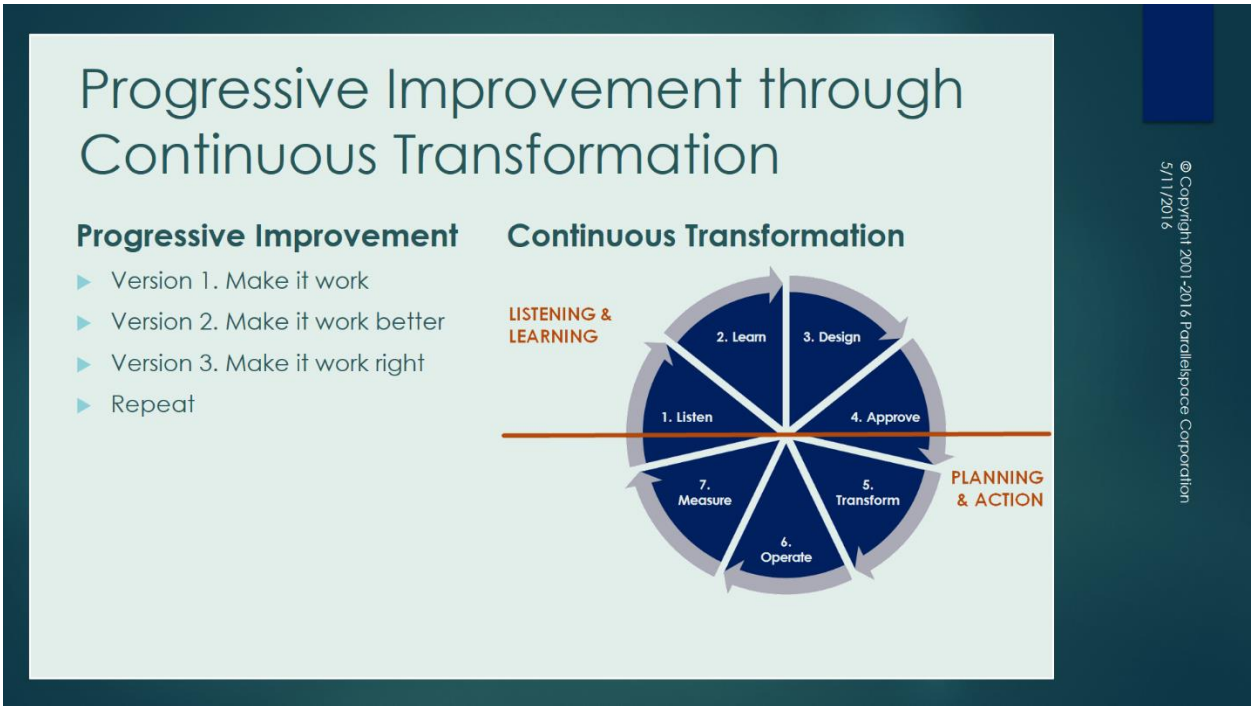
NEXT STEPS

Finally, strategic thinking is intelligently opportunistic. The organization whilst following a particular strategy should not lose sight of alternative strategies that may be more appropriate for a changing environment.

Jeanne Liedtaka in *The Business of Giving: The Theory and Practice of Philanthropy, Grantmaking and Social Investment* (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1)

Progressive Improvement through Continuous Transformation

How are we going to get there? The answer is progressive improvement through continuous transformation – as depicted below.



[How we think about how we work (https://hyperonomy.com/2016/05/09/how-do-we-think-about-how-we-work/)]

This whitepaper is the first attempt to describe the SSI Personal Data Usage Licensing (SSI-PDUL) Model in its entirety – both its motivations as well as a reasonable description of the complete, integrated solution. Full deployment will take several iterations and a significant amount of time – perhaps as long as the basic timeframe that it took the World Wide Web (running on top of the Internet) to develop into its current state.

A key advantage of the SSI Personal Data Usage Licensing (SSI-PDUL) Model is that it builds directly on top of existing Internet technologies, international standards (and specifications), and many open-source realizations of these technologies and standards.

CONCLUSIONS

If I have seen further, it is by standing on the shoulders of Giants.

[Issac Newton, 1675]

The above quotation is absolutely true when describing the gestation of the SSI Personal Data Usage Licensing solution concept. In addition, to quote a colleague[7],

Otherwise, I think it's a pretty unstudied problem.

This white paper as description a conceptual solution to the SSI Personal Data Usage Licensing (SSI-PDUL) Model problem. In addition, APPENDIX H – Android Runtime Permissions on page 60 has postulated an alternative approach based on the Android Runtime Permissions Workflow.

The next steps are to proceed with a prototype implementation of a proof-of-concept of all the features described in this document.

[7] Daniel Hardman, Private Communication, January 23, 2021.

APPENDICES

APPENDIX A – SELF-SOVEREIGN IDENTITY MODEL DEFINITIONS

NOTE: For consistency and continuity, the following definitions (except for those in Appendix A) are taken directly from the current version of the Trusted Digital Web whitepaper which can be found here: https://hyperonomy.com/2019/11/06/trusted-digital-web-whitepaper/.

Many of these definitions have been adapted from the Sovrin Glossary V3 (https://sovrin.org/library/glossary/).

Model Level Definitions

Self-Sovereign Identity Model (SSI Model)

An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Personal Digital Identifiers together with the usage of any associated Personal Identity Data.

Identifier Level Definitions

Self-Sovereign Identifier (SSI)

A Personal Digital Identifier that an Identity Owner has asserted the right to permanently control (along with the usage of the associated Personal Identity Data).

Non-Self-Sovereign Identifier (NSSI)

A Personal Digital Identifier that is not under the permanent control of the person associated with the Digital Identifier (i.e. a Facebook or LinkedIn login ID).

an Identity Owner has asserted the right to permanently control (along with the usage of the associated Personal Identity Data).

Personal Digital Identifier

A Digital Identifier for a person.

Identity Level Definitions

Identity Owner

The entity, usually a person or organization, who has ownership and control over a set of Personal Digital Identifiers and associated Personal Identity Data.

Self-Sovereign Identity

A Personal Digital Identifier and associated Personal Identity Data over which an Identity Owner exerts ownership and control.

Identity Data Level Definitions

Identity Data

The set of data associated with an Identity that permits identification of the underlying Entity. In the Self-Sovereign Identity Model, the sharing of Identity Data is under the control of the Identity Owner.

Self-Sovereign Identity Data

The Identity Data associated with a Self-Sovereign Identity.

Personal Data

All data associated with a Personal Digital Identifier – regardless of whether the data is owned and controlled by the Identity Owner identified by the Personal Digital Identifier.

Self-Sovereign Personal Data

Personal Data (including but possibly in addition to the Self-Sovereign Identity Data) associated with a Personal Digital Identifier over which the associated Identity Owner who has ownership and control.

APPENDIX B – TRUSTED DIGITAL WEB DEFINITIONS

NOTE: For consistency and continuity, the following definitions (except for those in Appendix A) are taken directly from the current version of the Trusted Digital Web whitepaper which can be found here: https://hyperonomy.com/2019/11/06/trusted-digital-web-whitepaper/.

Trust and Distrust

Trust

Definitions of trust typically refer to a situation characterized by the following aspects:

- *one party (trustor) is willing to rely on the actions of another party (trustee); the situation is directed to the future.*

In addition, the trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee. As a consequence, the trustor is uncertain about the outcome of the other's actions; they can only develop and evaluate expectations.

The uncertainty involves the risk of failure or harm to the trustor if the trustee will not behave as desired.

[Wikipedia: https://en.wikipedia.org/wiki/Trust_(social_science)]

Distrust

Noun

- *the feeling that someone or something cannot be relied upon.*
- *"his distrust of his mother's new suitor"*
- *synonyms: mistrust, suspicion, wariness, chariness, lack of trust, lack of confidence, lack of faith; skepticism, doubt, doubtfulness, dubiety, cynicism; misgivings, questioning, qualms; disbelief, unbelief, incredulity, incredulousness, discredit; informalleeriness*
- *"the general distrust of authority amongst drug users"*

Verb

- *doubt the honesty or reliability of; regard with suspicion.*
- *"like a skillful gambler, Dave distrusted a sure thing"*
- *synonyms: mistrust, be suspicious of, be wary/chary of, regard with suspicion, suspect, look askance at, have no confidence/faith in; be skeptical of, have doubts about, doubt, be unsure of/about, be unconvinced about, take with a pinch/grain of salt; have misgivings about, wonder about, question; disbelieve (in), not believe, discredit, discount, be incredulous of; informal, be leery of, smell a rat*
- *"for some reason Aunt Louise distrusted him"*

[Lexico.com: https://www.lexico.com/en/definition/distrust]

Trusted Digital Web

Trusted Digital Web (TDW)

The Trusted Digital Web (TDW) is a universal, trusted, frictionless, integrated, standards-based, general-purpose, end-to-end platform for global commerce, communication, and collaboration. The Trusted Digital Web is comprised of three (3) core software components: Trust-Based Applications (Trust-Based Apps or simply, TBAs), Universal DID (UDID) Data Service (UDIDService), and Trusted Digital Assistants (TDAs).

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Trusted Digital Web Project

The Trusted Digital Web Project is based on a set of open-source software projects and specifications (and their associated communities of people) that underpin the work involved in creating the Trusted Digital Web.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Trusted Digital Web Platform

The Trusted Digital Web Platform is the software platform on which the Trusted Digital Web is implemented. The Platform an extension and integration of the following open source projects.

- DnsServer (https://github.com/TechnitiumSoftware/DnsServer)
    - The DnsServer is extended to support additional DNS Resource Record types need to realize verifiable Universal Digital Identifiers and Digital Credentials
- TechnitiumLibrary (https://github.com/TechnitiumSoftware/TechnitiumLibrary)
    - Likewise, the TechnitiumLibrary is extended to support additional DNS Resource Record types need to realize verifiable Universal Digital Identifiers and Digital Credentials
- Maestro (https://github.com/monirith/maestro)
    - Maestro is extended to support the generation of Universal BPMN Byte Code that executes in the UDIDService Workflow Engine (which in turn is based on Maestro).
- StratisPlatform (https://github.com/stratisproject)
    - The StratisPlatform is the general-purpose, smart contract-enabled, blockchain platform used to support Universal Credential verification.
- SerentityData (https://github.com/mwherman2000/serentitydata)
    - SerentityData is a universal, dynamically configurable, byte-level data compaction technology used by decentralized applications (DApps) for more efficient storage of data on a blockchain.
- Camunda Modeler (https://camunda.com/products/modeler/)
    - BPMN standard-based workflow and business process open-source modeling tool
- Chromium (https://www.chromium.org/Home)
    - Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web. Chromium is used by Google Chrome and later releases of Microsoft Edge.
- CefSharp (http://cefsharp.github.io/)

- CefSharp is the easiest way to embed a full-featured standards-compliant web browser (Chromium) into your C# or VB.NET app.

The entire Trusted Digital Web Platform is released under the MIT open source license (for more details, see APPENDIX I – MIT License on page 62).

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Trusted Digital Web Components

Trust-Based Applications

A Trust-Based Application (Trust-Based App or simply, TBA) is a downloadable, plug-in app that is hosted by the Trusted Digital Assistant (TDA) and depends on the services of the TDA to perform:

- *Data notarization*
- *Credential storage and management using subsidiary ledgers*
- *Payments via decentralized currencies*
- *Identity via Universal Digital Identifiers*
- *Credential verification via pluggable verifying journal providers*
- *Agent-to-agent serverless network communications*
- *Workflow (business process) engine hosting*

[Michael Herman: https://www.linkedin.com/in/mwherman/]

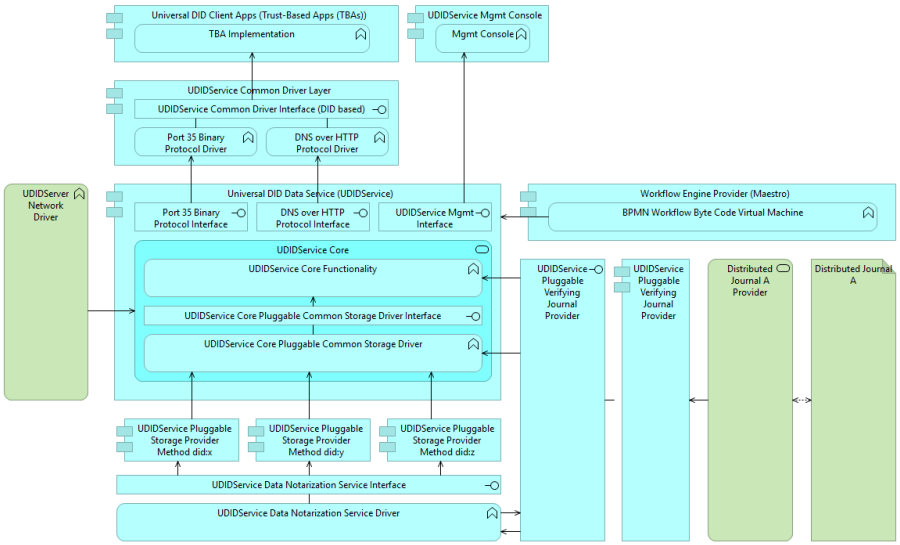
Universal DID (UDID) Data Service (UDIDService)

A Universal DID (UDID) Data Service (UDIDService) is a core service underlying the Trusted Digital Assistant (TDA) responsible for credential creation and management, certification, verification, agent-to-agent network communications, and workflow (business process) management.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Universal DID Data Service (UDIDService) Logical Architecture 0.9

Michael Herman
Self-Sovereign Blockchain Architect
Hyperonomy Digital Identity Lab
Parallelspace Corporation
October 11, 2019



Trusted Digital Assistants (TDAs)

A Trusted Digital Assistant (TDA), a core component of the Trusted Digital Web Platform, is the client application (app) the citizens use to access and use the Trusted Digital Web. The TDA is the application that hosts Trust-Based Applications (TBAs). The TDA provides the following services to TBAs hosted in the TDA:

- *Data notarization*
- *Credential storage and management using subsidiary ledgers*
- *Payments via decentralized currencies*
- *Identity via Universal Digital Identifiers*
- *Credential verification via pluggable verifying journal providers*
- *Agent-to-agent serverless network communications*
- *Workflow (business process) engine hosting*

[Michael Herman: https://www.linkedin.com/in/mwherman/]

APPENDIX C – IDENTIFIERS, IDENTITIES, CLAIMS AND CREDENTIALS DEFINITIONS

NOTE: For consistency and continuity, the following definitions (except for those in Appendix A) are taken directly from the current version of the Trusted Digital Web whitepaper which can be found here: https://hyperonomy.com/2019/11/06/trusted-digital-web-whitepaper/.

Subjects and Personas

Real (or Virtual) Subject

A Real (or Virtual) Subject is any unique and specific non-fungible object in the Physical or Digital Universe: a person, a place, a thing, an organization, digital visual or audio composition, business document, etc.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Persona

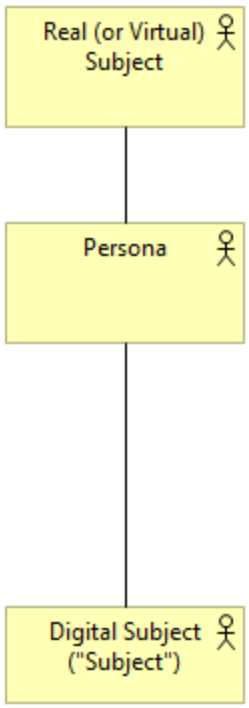
A persona (plural personae or personas), in the word's everyday usage, is a social role or a character played by an actor. The word is derived from Latin, where it originally referred to a theatrical mask.

[Wikipedia: https://en.wikipedia.org/wiki/Persona]

Digital Subject ("Subject")

A Digital Subject (aka Subject) is a unique digital representation of a Real Subject; more specifically, a particular Persona of a Real Subject.

[Michael Herman: https://www.linkedin.com/in/mwherman/]


Real (or Virtual) Subject
Persona
Digital Subject ("Subject")

Digital Identifiers

Digital Identifier (DID)

- See Universal Digital Identifier

Universal Digital Identifier (UDID aka "DID")

Short for Universal Digital Subject Identifier, a UDID (or "DID") is a character string representation whose value is unique and is used to address, index, search, and retrieve Claims about the associated Digital Subject (aka Subject). A Subject can have more than one UDID associated with it.

A DID starts with the character string `did:` *and is followed by 1 or more DID Method labels; followed by Method-define unique character string identifier. Examples:*

- `did:neonation:123-456-789`
- `did:usergroups:developers:abc12345678`

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Universal Digital Subject Identifier

- See Universal Digital Identifier

Decentralized Identifier

A Decentralized Identifier is a narrowly defined type of Digital Identifier that is verifiable using a blockchain-based immutable data store. See Trust Levels for Universal DIDs.

Digital Identities

Digital Identity

- See Universal Digital Identity

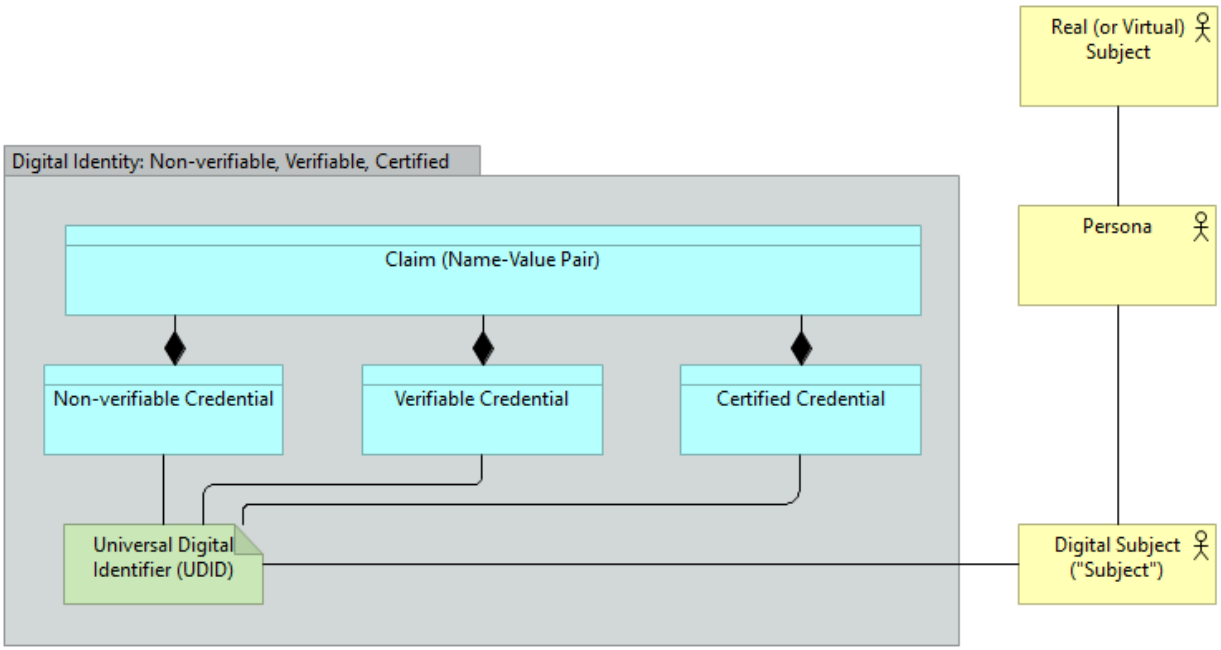
Universal Digital Identity

A Universal Digital Identity is a set of Claims made by one Digital Subject about itself or another Digital Subject [The Laws of Identity]. A Universal Digital Identity is associated with, or identified by, one or more Universal Digital Identifiers (UDIDs, or more simply, DIDs).

A minimal Universal Digital Identity contains a Claim (name-value attribute) named `id` whose value is the identifier associated with the credential. A Universal Digital Identity can have an unlimited number of Claims associated with it.

A Universal Digital Identity can be persisted as a Credential.

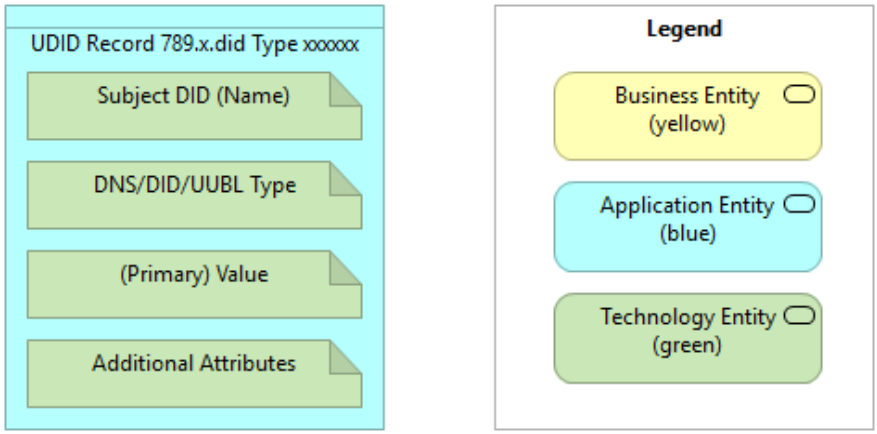
[Michael Herman: https://twitter.com/mwherman2000/status/1164540800526454786]



Claims, Profiles, and Credentials

Claim

A Claim is any data attached to, or associated with, a Digital Identity by way of a DID. A Claim is a name-value pair representing a datum associated with a DID. Preferably, claim data and the claims' relationships to a Digital Identity are represented (persisted) in a manner that is immutable, auditable, verifiable, historized, and permanent.



[Michael Herman: https://twitter.com/mwherman2000/status/1164540820092882944]

Credential

- See Universal Digital Credential

Universal Digital Credential (Credential)

A set of Claims is called a Universal Digital Credential (or more simply, a Credential) – of which there are 4 Trust Levels.

A minimal Credential is a Credential that contains a Claim (name-value attribute) named `id` whose value is the identifier associated with the credential. A Credential can have an unlimited number of Claims associated with it.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Profile

A collection of related Universal Digital Credentials is called a Profile. The collection of Credentials is related to a common Universal Digital Identifier.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

DID Credentials and DID Documents

DID Credential

A DID Credential is a specialization of a Universal Digital Credential (Credential). A minimal DID Credential is a Credential that contains a Claim (name-value attribute) named `id` that has a DID as a value and is associated with a Subject via the value of the `id` Claim. A DID Credential can have an unlimited number of Claims associated with it. The following is an example of a minimal DID Credential.

```
{
  “id”: “did:example:050B6A27-724E-44DC-892C-0378087C3A44”
}
```

The following is an example of another DID Credential.

```
{
  “id”:       “did:example:0853338A-5176-409D-8C0B-FEC3CD211E00”,
  “location”: “Calgary, Alberta”,
  “country”:  “Canada”
}
```

[Michael Herman: https://www.linkedin.com/in/mwherman/]

DID Document

A DID Document is a specialization of a DID Credential that contains specific Claims as defined in the draft `did-spec` specification (https://www.w3.org/TR/did-core/). The following is an example of a DID Document from the draft specification.

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",

  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],

  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": https://example.com/vc/
  }]
}
```

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Verification

Verifiable Digital Subject

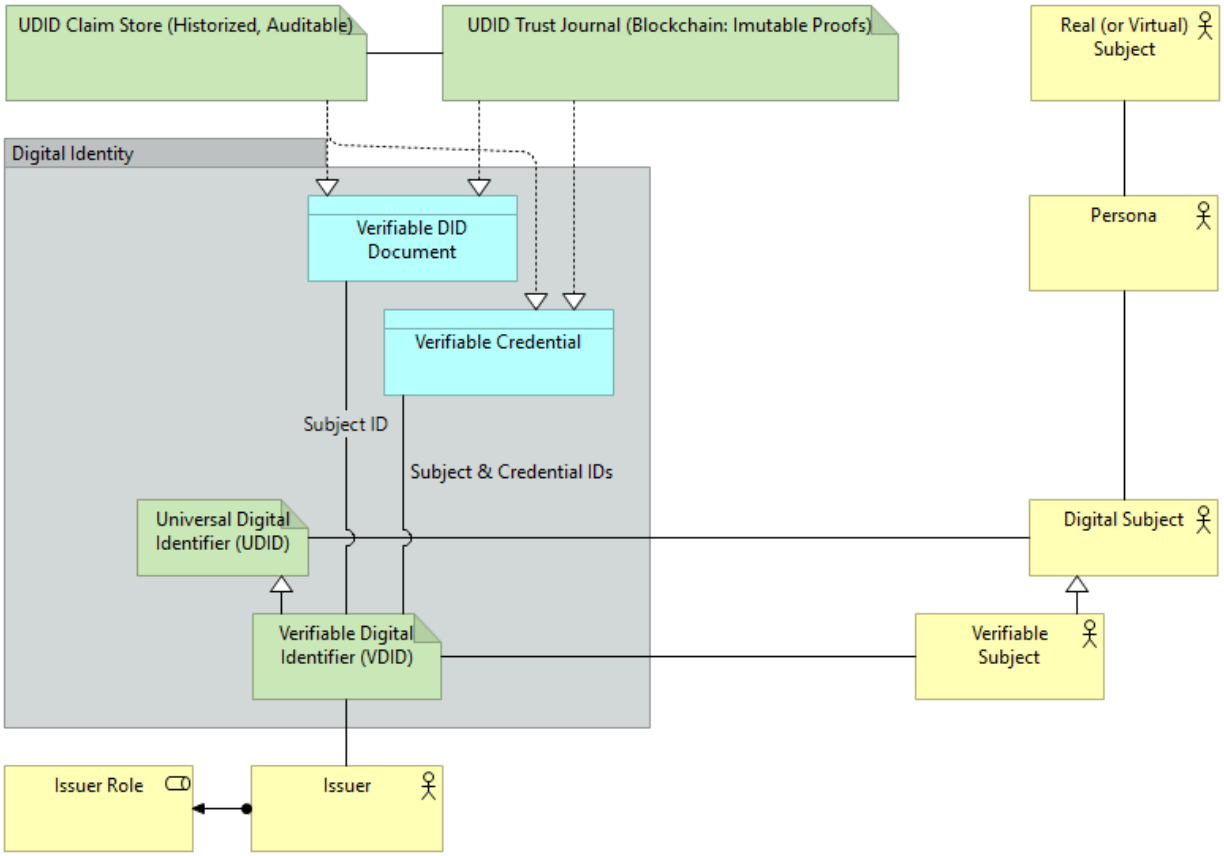
A Subject that is verifiable against a decentralized blockchain platform or other authority.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Verifiable Digital Credential

A Credential that is verifiable against a decentralized blockchain platform or other authority.

[Michael Herman: https://www.linkedin.com/in/mwherman/]



[Michael Herman: https://www.linkedin.com/in/mwherman/]

Levels of Trust

Trust Levels for Universal DIDs

Different Subjects (identified by their DIDs) can have different levels of trust in the Trusted Digital Web as defined by the following criteria:

Trust Level 0. Not Resolvable	*A Subject's DID (and by implication the associated Credentials and their Claims) is not verifiable. The Subject DID is not resolvable from the Data Registry.*
Trust Level 1. Resolvable	*A Subject's DID is resolvable from the Data Registry. There is at least one Claim associated with the DID for this Subject (even if the single Claim is the DID itself).*
Trust Level 2. Signed	*The Subject DID is resolvable and it has a validated DIDSUBSIG Claim associated with the DID in the Data Registry.*
Trust Level 3. Verifiable	*The Subject's DID is signed and the DID and DIDSUBSIG have been notarized; that is, they appear in the Data Notary and are valid and consistent with the corresponding data resolvable from the Data Registry.*

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Data Registry

A Data Registry is a data store (a service) that is used to store business data or references to business data (the latter being references to data stored in an external system such as a database or content management system). Digital signatures may also be stored in the Data Registry dependent on the DID Method's trust level. A Public Key can be stored in the Data Registry as a Credential Claim. Data in the Data Registry may be encrypted as determined by parameters associated with a particular DID Method. The attributes of a DID Method are represented as a Credential (a collection of Claims) in the Data Registry.

NOTE: A Credential is stored in a Data Registry as a collection of Claims.

NOTE: A Data Registry can be used to store data at any of the four (4) Trust Levels. Trust Level is a DID Method attribute (Credential Claim).

NOTE: A datum (Credential) stored in the Data Registry is retrieved by its Universal DID.

NOTE: In the Trusted Digital Web, a Data Registry is implemented using distributed Internet Domain Name Service (DNS) technologies.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Data Notary

A Data Notary (a service) is used to store copies of Digital Signatures and Verifiable Proofs for data stored in the Data Registry. A Data Notary supports (is required for) Trust Level 3. Verifiable for data stored in the Data Registry.

NOTE: A Data Notary is typically implemented using distributed journal (ledger) technologies.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Controllers

Controller

Every Subject (person, organization. And thing) has a Controller. A Controller is a role. There are two types of Controller roles: Self-Controllers and Thing Controllers.

Self-Controller

If a Subject can represent and act on its own behalf, the Subject has the Self Controller role.

Thing Controller

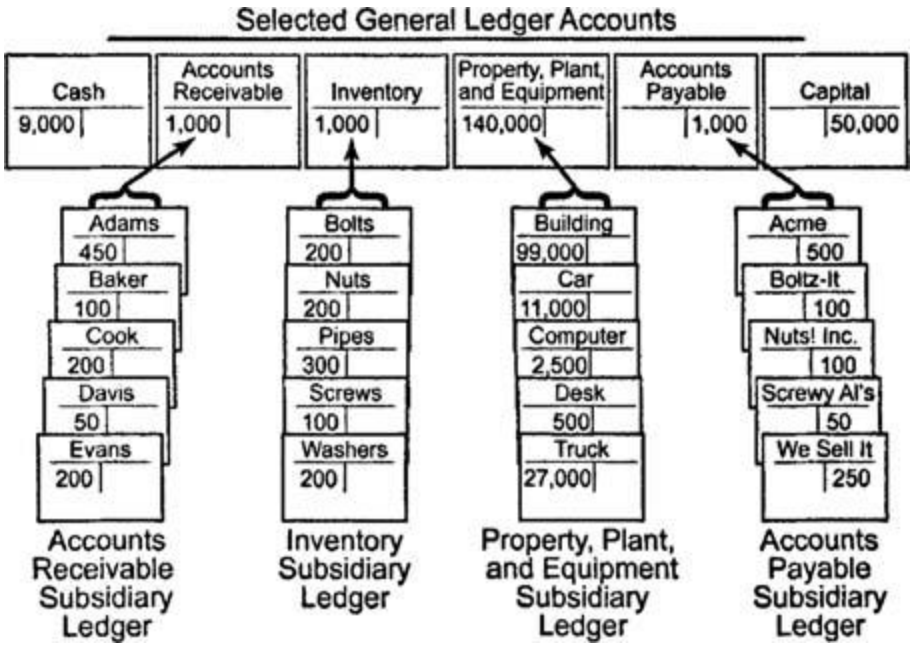
If a Subject is inanimate and cannot represent nor act on its own behalf, it requires one or more other Subjects to represent and act on its behalf. The latter is known as Thing Controller.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Accounting

Subsidiary Ledger

A subsidiary ledger is a group of similar accounts whose combined balances equal the balance in a specific general ledger account. The general ledger account that summarizes a subsidiary ledger's account balances is called a control account or master account. For example, an accounts receivable subsidiary ledger (customers' subsidiary ledger) includes a separate account for each customer who makes credit purchases. The combined balance of every account in this subsidiary ledger equals the balance of accounts receivable in the general ledger.



Subsidiary Ledgers (https://www.cliffsnotes.com/study-guides/accounting/accounting-principles-i/subsidiary-ledgers-and-special-journals/subsidiary-ledgers).

Workflow Actions and Business Processes

References to the term "Workflow Actions (Business Processes)" appear throughout this whitepaper. Each term has a separate, specific definition.

Workflow Action

In the context of the Trusted Digital Web, a Workflow Action is a simple network of interconnected work tasks that, when initiated, run to completion without blocking for user input or an external event. Workflows will generally be used to implement functionality internal to a Trusted Digital Assistant (but not exclusively).

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Business Process

In the context of the Trusted Digital Web, a Business Process is generally considered to be a more complex network of interconnected work tasks and may block waiting for input from a user, an external service, or some other event. A Business Process is used to support an external (real world) business process.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Both workflows and business processes are defined in the same way, are managed in the same way, and are executed in the same way - inside the Trusted Digital Assistant.

APPENDIX D – ADDITIONAL DEFINITIONS

NOTE: For consistency and continuity, the following definitions (except for those in Appendix A) are taken directly from the current version of the Trusted Digital Web whitepaper which can be found here: https://hyperonomy.com/2019/11/06/trusted-digital-web-whitepaper/.

Non-Fungible Things

Non-Fungible (1)

Fungibility is the ability of a good or asset to be interchanged for another good or asset of like kind. Like goods and assets that are not interchangeable, such as owned cars and houses, are non-fungible.

[Investopedia.com: *https://www.investopedia.com/terms/f/fungibility.asp*]

Non-Fungible (2)

Two goods or assets that may be technically different but may be considered to have the same usage value in a particular scenario may be considered highly exchangeable (aka fungible) goods or assets. They might not be considered non-fungible goods or assets.

For example, two slices of medium-toasted bread are technically different but from a usage perspective will often be considered highly exchangeable or fungible. On the other hand, a pair of digital photos, one taken of each slice of the two pieces of toast, are more likely to be considered definitive non-fungible assets based on the majority of use cases involving photos.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Digital Slavery

Traffic

- *(verb)*
- *to carry on traffic, trade, or commercial dealings.*
- *to trade or deal in a specific commodity or service, often of an illegal nature (usually followed by in).*
- *to traffic in opium.*

[Dictionary.com: https://www.dictionary.com/browse/traffic]

Slavery

Slavery is any system in which principles of property law are applied to people, allowing individuals to own, buy and sell other individuals, as a de jure form of property. A slave is unable to withdraw unilaterally from such an arrangement and works without remuneration.

[Wikipedia: https://en.wikipedia.org/wiki/Slavery]

Digital Slavery (1)

Digital slavery is any system in which principles of property law are applied to people (including their personal data and information), allowing individuals to own, buy and sell other individual's person or personal data or information, as a de jure form of property. A digital slave is unable to easily withdraw unilaterally from such an arrangement and hence is forced to provide benefits without remuneration. A digital enslaver is anyone who traffics in the personal data and information of others without providing remuneration or any form of compensation in return.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Digital Slavery (2)

The cross-industry business practice of #trafficking in and profiting from the #personal #data of individual #Canadians with #no compensation and #norenumeration (...vs. #financialslavery).

[Michael Herman: https://twitter.com/mwherman2000/status/1159170641691471873]

Digital Trust, Human Trust, and Cryptographic Trust

Digital Trust

Digital trust is the measure of consumer, partner, and employee confidence in an organization's ability to protect and secure data and the privacy of individuals. As data breaches become bigger and more common, digital trust can be a valuable commodity for companies that earn it, and it is starting to change the way management looks at security.

[CSOOnline.com: https://www.csoonline.com/article/3297037/what-is-digital-trust-how-csos-can-help-drive-business.html]

Human Trust

How we trust each other as individual human beings, participants in larger social orders, formal institutions, and governments. This type of human trust existed before the ecosystem we are trying to create and will always be a part of it. Without human trust, we have nothing.

Cryptographic Trust

What was once done by means of clay, parchment, and paper is now done by digital. The mechanisms of how we trust each other through digital means are largely due to cryptography to ensure confidentiality, integrity, and control. Without cryptography, we'd still be using paper (maybe clay and parchment, too).

[Medium.com: https://medium.com/@trbouma/self-sovereign-identity-making-the-ecosystem-real-2ea09b5ee33]

Reliable and Secure

Secure is a word that has many meanings and is not easily disambiguated in the context of trust. Similarly, reliable is not a word that is easily disambiguated.

Reliable

adjective

1. that may be relied on or trusted; dependable in achievement, accuracy, honesty, etc.:
    - reliable information.

Secure

adjective

1. free from or not exposed to danger or harm; safe.
2. dependable; firm; not liable to fail, yield, become displaced, etc., as a support or a fastening:
    - The building was secure, even in an earthquake.
3. affording safety, as a place:
    - He needed a secure hideout.
4. **in safe custody or keeping:**
    - **Here in the vault, the necklace was secure.**
5. **free from care; without anxiety:**
    - **emotionally secure.**
6. firmly established, as a relationship or reputation:
    - He earned a secure place among the baseball immortals.
7. sure; certain; assured:
    - secure of victory; secure in religious belief.
8. safe from penetration or interception by unauthorized persons:
    - secure radio communications between army units.
9. Archaic. overconfident.

verb (used with object)

10. to get hold or possession of; procure; obtain:

- to secure materials; to secure a high government position.

11. **to free from danger or harm; make safe:**
    - **Sandbags secured the town during the flood.**
12. to effect; make certain of; ensure:
    - The novel secured his reputation.
13. to make firm or fast, as by attaching:
    - to secure a rope.
14. Finance.
    - to assure payment of (a debt) by pledging property.
    - to assure (a creditor) of payment by the pledge or mortgaging of property.
15. **to lock or fasten against intruders:**
    - **to secure the doors.**
16. **to protect from attack by taking cover, by building fortifications, etc.:**
    - **The regiment secured its position.**
17. to capture (a person or animal):
    - No one is safe until the murderer is secured.
18. to tie up (a person), especially by binding the person's arms or hands; pinion.
19. **to guarantee the privacy or secrecy of:**
    - **to secure diplomatic phone conversations.**

verb (used without object)

20. to be or become safe; have or obtain security.
21. Nautical.
    - to cover openings and make movable objects fast:
        i. The crew was ordered to secure for sea.
    - to be excused from duty:
        i. to secure from general quarters.

[Dictionary.com: https://www.dictionary.com/browse/secure]

Trust Levels, Reputation, and Accuracy

Trust Levels

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behavior and applies only within a specific context at a given time.

That is, the firm belief is a dynamic value and spans over a set of values ranging from very trustworthy to very untrustworthy as illustrated in Table 1. The trust level (TL) is built on past experiences and is given for a specific context. For example, entity y might trust entity x to use its storage resources but not to execute programs using these resources.

The TL is specified for a given time frame because the TL today between two entities is not necessarily the same TL a year ago.

[University of Manitoba: ftp://ftp.cs.umanitoba.ca/pub/IPDPS03/DATA/W01_HCW_05.PDF]

Reputation

The reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time.

Seeking the reputation of a specific entity, entity x relies on information from a set of other entities referred to as recommenders' set (). A recommender is an entity that gives recommendations using its direct trust table (DTT) that includes trust values for entities with which the recommender had prior direct transactions. Recommenders might have different criteria for evaluating other entities. Hence, different recommenders might give different recommendations about an entity.

Therefore, Entity x associates an accuracy measure with each recommender in the recommender set. The information (i.e. the accuracy measure) on the set of entities that act as recommenders being used by x is kept in a recommender trust table (RTT). Entity x uses the accuracy measure to minimize the deviation between the information received from each recommender and the actual "trustworthiness" of y.

[University of Manitoba: ftp://ftp.cs.umanitoba.ca/pub/IPDPS03/DATA/W01_HCW_05.PDF]

Accuracy

A recommender is said to be accurate, if the deviation between the information received from it pertaining to the "trustworthiness" of a given entity in a specific context at a given time and the actual trustworthiness of within the same context and time is less than a precision threshold.

[University of Manitoba: ftp://ftp.cs.umanitoba.ca/pub/IPDPS03/DATA/W01_HCW_05.PDF]

APPENDIX E – STRATEGIC THINKING

The following is an excerpt from the book *The Business of Giving: The Theory and Practice of Philanthropy, Grantmaking and Social Investment* by Peter Grant (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1).

In the chapter *Can Philanthropy Learn from Business Models?* (on page 93), Grant describes Jeanne Liedtaka's point-of-view with respect to strategic thinking – succinctly in a single page. Here's is a list of those 5 points. They are extremely pertinent to the architecture, design, and social evolution technology model being used to create the Trust Digital Web.

NOTE: In the following quote from Grant, imagine replacing *organization* with the word *project*, the word *Internet*, or the Trusted Digital Web.

> *Firstly, strategic thinking is based on a systems perspective – a holistic view of an organization. The strategic thinker has a mental picture of the complete system of value creation in the organization and their own small role within the larger system.*
>
> *Secondly, strategic thinking is driven by the strategic intent of the organization providing focus and energy to the staff and the organization to achieve [its] goals.*
>
> *Thirdly, strategists need to 'think in time' linking an organization's past, present, and future in their thought processes. There are three components:*
>
> - *the predictive value of the past for the future;*
> - *departures from the past which divert the organization from familiar patterns;*
> - *the need for continuous comparison*
>
> *Fourthly, strategic thinking is 'hypothesis-driven' and the 'scientific method accommodates both creative and analytical thinking sequentially in its use of iterative cycles of hypothesis-generating and testing'.*
>
> *Finally, strategic thinking is intelligently opportunistic. The organization whilst following a particular strategy should not lose sight of alternative strategies that may be more appropriate for a changing environment.*

In hindsight, the Trusted Digital Web was conceived (and continues to grow and evolve) based on the above set of strategic thinking principles.

APPENDIX F – TRUSTED DIGITAL WEB COMMUNICATION PROTOCOLS

This appendix summarizes the protocols used in the Trusted Digital Web; more specifically, the protocols supported by:

- the Data Registry service (aka Universal DID Data Server), and
- the Trusted Digital Assistant client application.

NOTE: To learn more about the DNS protocol and to see examples of the DNS standard binary query/response messages, read APPENDIX A – on page 34.

Data Registry Service Protocols

DNS Query/Response Protocols

As a DnsServer-based open-source project (https://github.com/TechnitiumSoftware/DnsServer), the Trusted Digital Web Data Registry supports the DNS standard query/response protocol over the following transports and ports:

- TCP/IP port 53 (binary)
- UDP/IP port 53 (binary)
- DNS over TLS (DoT) over TCP/IP port 853
- DNS over HTTPS (DoH) over TCP/IP port 443

Data Registry Management API Protocols

For non-query management operations such as CRUD operations for DNS zones/DID methods, DNS records/DID claims, etc., the Data Registry supports a JavaScript-friendly Web API running over HTTP over TCP/IP port 80.

Trusted Digital Assistant Protocols

The protocols supported by the Trusted Digital Assistant client application include the common Internet browser transport protocols supported by the CefSharp (https://github.com/cefsharp/CefSharp) wrapper for the Chromium embeddable browser component (https://www.chromium.org/Home). Chromium is the Google open-source browser engine used by Google Chrome and several other browsers (https://en.wikipedia.org/wiki/Chromium_(web_browser)#Browsers_based_on_Chromium) – as well as the next version of Microsoft Edge (to be released in 2020). In addition, the Trusted Digital Assistant design leverages CefSharp's pluggable protocol handler capability for implementing custom URL syntax schemes. The Trusted Digital Assistant uses this capability to implement the `didttp:` scheme (DID Trusted Transport Protocol).

Common Internet Browser Protocols

The common Internet browser protocols supported by Chromium (and, in turn, the Trusted Digital Assistant) include:

- HTTP over TCP/IP
- HTTPS over TCP/IP

DID Trusted Transport Protocol (didttp:)

The DID Trusted Transport Protocol implements the didttp: URL scheme over the standard/default DNS binary query/response protocol running over TCP/IP port 53. That is, the Trusted Digital Assistant includes a pluggable protocol handler that maps the didttp: URL scheme into the appropriate DNS standard binary query, sends the query to the Data Registry over TCP/IP port 53, receives the DNS standard binary response, and then converts the response into a JSON for rendering in Chromium.

The didttp: URL scheme supports queries from a Trusted Digital Web Data Registry. The format of a didttp: URL is as follows:

`didttp://<dataregistryaddress>/did:<didmethod>[:<identifier>[#<fragment>]]`

where:

- `<dataregistryaddress>` is the conventional Internet domain name or IP address of the Data Registry. Most often, `<dataregistryaddress>` will most likely have a value of `localhost`.
- `<didmethod>` is a conventional DID Method string containing one (and possibly two or more labels). For example, `able` and `able:baker:charlie`.
- The optional `<identifier>` is any identifier compatible with the DID Method Specification for `<didmethod>`.
- The optional `<fragment>` is any string tag that is compatible with the DID Method Specification for `<didmethod>`. In the Data Registry, the `<fragment>` value is mapped to the value of the Tag claim in the Credential identified by the value of `did:<didmethod>[:<identifier>]`.

NOTE: The didttp: URL scheme is only processed with the Trusted Digital Assistant - where it is mapped directly into the DNS standard binary query protocol. At present, there is no need for didttp: URLs to be transmitted over the wire. This design may change in the future given a requirement to perform didttp: URL resolution in the Data Registry. However, the overarching requirement is for the Data Registry to remain 100% compatible with the current DNS IEFT specifications.

CLARIFICATION: The Universal DID Identifier component of the didttp: protocol scheme is the part that is sent to the Data Registry (as is) as part of a query. For example, for the following Trusted Digital Assistant URL, the following parts are used to constitute the DNS binary query:

URL: `didttp://localhost/did:foo:home#index.htm`

Query Parts: UDID `did:foo:home` and resource record type `ANY` is sent to the Data Registry located at DNS address `localhost`

CLARIFICATION: The Data Registry Address URI component `didttp://<dataregistryaddress>/` is expected to correspond to (be the value of) the Service Endpoint URL Claim in the DID Document for the specific DID Method `did:<didmethod>`.

Secure DID Trusted Transport Protocols (didttps:)

The Secure DID Trusted Transport Protocol (didttps:) implements the didttp: URL scheme over the standard/default DNS binary query/response protocol running over TLS port 853.

APPENDIX G – CORE CHARACTERISTICS OF SOVEREIGN IDENTITY [IDENTITIES]

Reference: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/characteristics-of-sovereign-identity.md

By: Joe Andrieu, October 2016

Control. Acceptance. Zero Cost.

These are the three fundamental characteristics of self-sovereign identity.

CONTROL

Self-sovereign identities are controlled by the individual:

Self-generatable and Independent: Individuals must be able to create identity information without asking for permission and be able to assert identity information from any authority. The resulting identity must have the same technical reliability as those provided by well-known, "official" sources. The observer, of course, is always free to decide whether or not a given piece of information is meritorious, but the information must be able to be verified as a non-repudiatable statement of correlation using exactly the same mechanisms regardless of source. Further, individuals must be able to present self-generated identity information without disclosing that the authority in the claim is the subject of the claim.

Opt-in: The affordance for asserting identity information starts with the individual. While an individual may present claims from known or accepted third party authorities, it is the individual who asserts that the claim applies to them. Self-sovereign identities begin with the will of the individual, with the intentional presentation of identity information.

Minimal Disclosure: Individuals should be able to use services with minimal identity information. Features that depend on enhanced correlation must be understood by the average user. Such features should be permissioned with the highest granularity, so functions independent of correlation work equally well alongside those dependent on it. It is not acceptable to deny services because of a refusal to provide unrelated information.

Non-participation: Individuals must be able to choose to not provide identity information for services where it isn't absolutely required. Any spontaneous identifiers necessary for a service to function, such as cookies or session ids, must use the same infrastructure for consent, persistence, transience, and disclosure as if provided by the individual.

Opt-out: Individuals should be able to opt-out of identifying records post-facto as a matter of course. People should be able to stop the use of a correlating identity information by request. Some transactions necessarily require long-term retention of identity information, such as financial transactions, purchases, and shipments. Actions that create permanent records should be clearly marked and communicated such that the retention is expected and understood by the average person. All other actions which leverage a self-sovereign identity should be de-correlated on-demand and said identifiers should no longer be used to correlate that individual across contexts.

Recoverable: Sovereign identities must be robust enough to be recovered even if hard drives are lost, wallets stolen, or birth certificates lost in a fire. Self-sovereign identities must provide a way for individuals to recover and reassert that existing identify information applies to them even in the face of complete loss of credentials. This may be challenging given current technical proposals, but the point of this paper is to explore the non-technical requirements of a self-sovereign identity. To fully address the needs of UN Sustainable Development Goal 16.9, identity assurance can't depend on pieces of paper, devices, or other artifacts that can be lost, stolen, destroyed, and falsified.

ACCEPTANCE

Self-sovereign identities are accepted wherever observers correlate individuals across contexts.

Standard: There is an open, public standard managed through a formal standards body, free to use by anyone without financial or intellectual encumbrance. Simple The core standard (schema, serialization, and protocols) must be atomically minimal, providing the barest data set, allowing complexity to emerge not from a complicated data model but from a multiplicity of information types, authorities, and observations.

Non-repudiatable: Individual claims should be cryptographically signed to assure non-repudiatable statements of correlation. Long term, public and semi-public ledgers should be used to record claims that become statistically impossible to falsify over time. Self-sovereign identities, at a minimum depend on cryptographic assurances, and most likely will be further enabled by non-repudiatable public ledgers.

Reliable: Access to self-sovereign identities must be at least as reliable as access to the Internet. It should not rely on any individual or group of centralized servers, connections, or access technologies. Substantially Equivalent Above all, self-sovereign identities must meet the needs of legacy identity observers at least as well as current solutions. If the core architecture is inherently less capable than existing approaches there is little hope of systemic adoption.

ZERO COST

Finally, any proposed standard for self-sovereign identity must be adoptable at absolutely minimal cost.

Not only must it be free of licensing encumbrances, it must be implementable with readily available, inexpensive, commodity hardware running common operating systems. If it can't be achieved using today's commodity products, then we must help manufacturers incorporate what we need.

In order to reach every last person on the planet—the explicit target of UN Sustainable Development Goal 16.9—self-sovereign identity must be realizable at massive scale with close to zero marginal cost.

The systems we use to make sense of the resulting identity transactions will provide more than enough consulting, software, and hardware revenue to finance the development of the core enabling technology. Just as the web browser was a zero cost entry into a vast economic and innovation engine of the world-wide web, so too must self-sovereign identity begin with the most cost-effective on-ramp that can be engineered.

APPENDIX H – Android Runtime Permissions Workflow

As an alternative to the SSI Personal Data Usage Licensing (SSI-PDUL) Model solution proposed in this whitepaper, it is possible to model a process and user experience (UX) style that mimics how Android prompts users for "just in time" app-specific permissions on a device (e.g. ability for an app to control the camera or access your contact list). The following diagram from the Android developer's website illustrates this workflow.

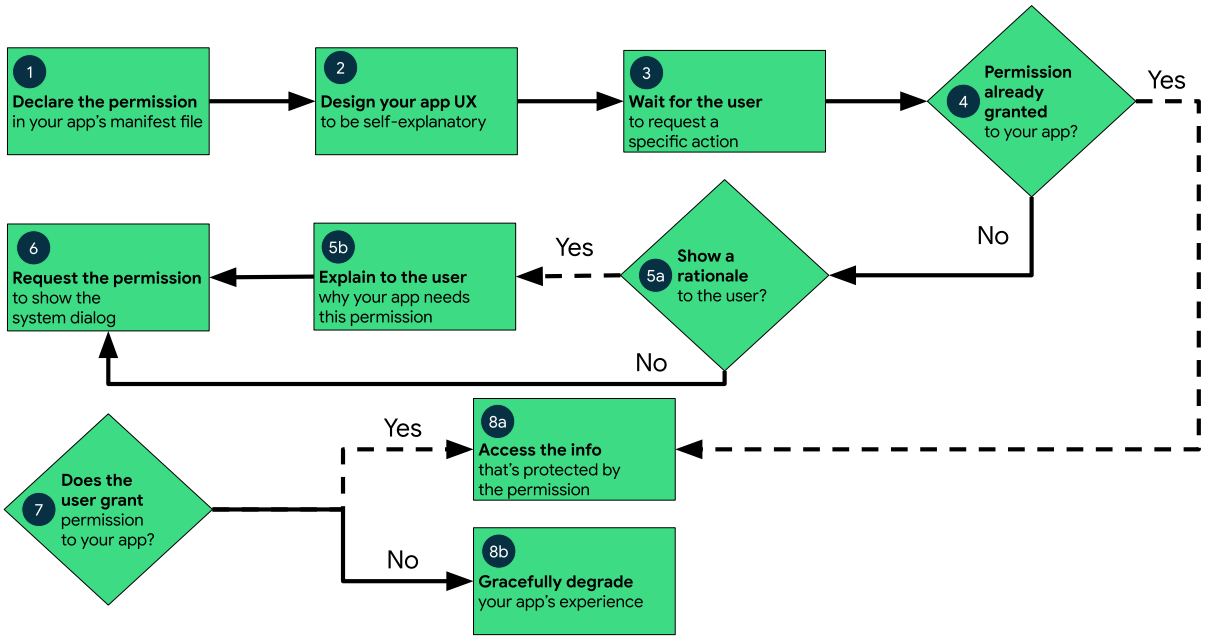


Figure 11. Android Runtime Permissions Process

A diagram that shows the workflow for declaring and requesting runtime permissions on Android. (https://developer.android.com/training/permissions/requesting#workflow_for_requesting_permissions)

A prototypical Android permissions dialog is illustrated in the following figure.

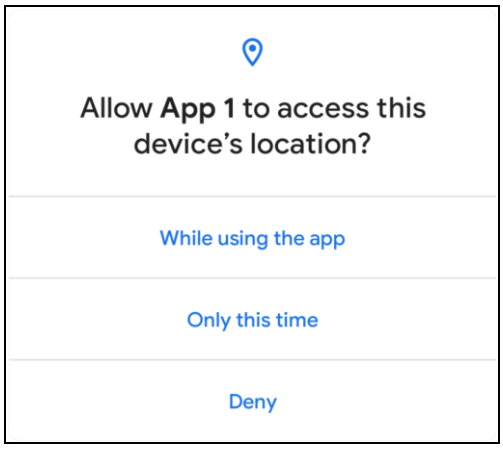


Figure 12. Prototypical Android permissions dialog

The following Java code snippet demonstrates the recommended Android process of checking for a permission, and requesting a permission from the user when necessary:

```
if (ContextCompat.checkSelfPermission(
        CONTEXT, Manifest.permission.REQUESTED_PERMISSION) ==
        PackageManager.PERMISSION_GRANTED) {
    // You can use the API that requires the permission.
    performAction(...);
} else if (shouldShowRequestPermissionRationale(...)) {
    // In an educational UI, explain to the user why your app requires this
    // permission for a specific feature to behave as expected. In this UI,
    // include a "cancel" or "no thanks" button that allows the user to
    // continue using your app without granting the permission.
    showInContextUI(...);
} else {
    // You can directly ask for the permission.
    // The registered ActivityResultCallback gets the result of this request.
    requestPermissionLauncher.launch(
            Manifest.permission.REQUESTED_PERMISSION);
}
```

Figure 13. Android process of checking for a permission

An alternate SSI Personal Data Usage Licensing (SSI-PDUL) Model solution could use a similar UX pattern when an app, for example, tries to access an item whose schema type the app has never accessed before (e.g. is it OK for App X to access First Name in a Contact credential?).

APPENDIX I – MIT LICENSE