A Technology-Free Definition of Self-Sovereign Identity

A topic paper by Joe Andrieu (joe@joeandrieu.com) for the third Rebooting Web of Trust DesignShop October 2016

Abstract

The desire for increased control over our identity has catapulted the idea of "self-sovereign identity" into the forefront of digital identity innovation, yet the term lacks a rigorous definition beyond specific technical implementations[1]. This paper explores what self-sovereign identity means independent of technology: what people need from independent identity capabilities. I want to understand how such a system enables both individuals whose identities are in play (subjects), as well as those who use those "identities" to correlate interactions across contexts (observers). I start with grounding individual sovereignty in the Enlightenment and identity in its core function of correlation, then propose core characteristics of a self-sovereign identity system. My eventual goal is to model the technology-independent requirements of a self-sovereign solution suitable for realizing UN Sustainable Development Goal 16.9: "Providing every last person on the planet with a legal identity by 2030."[2]

Background

Sovereign entities don't need to ask for permission. The Age of Enlightenment championed the sovereignty of the individual as the ultimate source of authority for shaping our world. Enlightenment philosophers replaced the state and the church with the individual as source of moral authority: free markets, free will, human rights, and equality before the law. These concepts dramatically reshaped our social, political, and economic worlds.

The "Digital Enlightenment" frames recent innovations as the technical realization of the values of Enlightenment thinkers. Modern tools like PCs, mobile phones, and the Internet, have dramatically increased the freedom of individuals to act on their own authority. The average individual today has much greater capability to act on their own initiative—without asking permission—than their peer of even a hundred years ago. There is a natural affinity between increased computational and communications capability and individual sovereignty and freedom. So how would sovereignty apply to identity?

Identity is how we keep track of things. From knowing your best friend's first name to formal birth certificates and passports, from the socially constructed identities of gender and race to the place names of cities on a map, all of these examples of demonstrate how identity correlates what we believe about something in one context and apply it in another. Identifying a subject *means* correlating the immediately topical entity with information from prior knowledge.

Most importantly, identity is something that emerges in the mind of an *observer* in relationship to the *subject*. It can be informed and shaped by the actions of the observed: wearing a sign or nametag, "Hi, I'm Joe" or dressing like a punk or a Goth or a businessman or house wife, but at its core, it is an innately

[1] No disrespect to Christopher Allen's opening to the conversation, *The Path to Self Sovereign Identity* - Christopher Allen 2016 http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html It gets a lot right, but leaves a few requirements out, e.g., recoverability and zero cost, and conflates "identities" and claims in an ambiguous manner. Chris clearly intended the paper would start the conversation; it has done a good job at that.
[2] "Sustainable Development Goal 16" Official UN website. Online. https://sustainabledevelopment.un.org/sdg16 retrieved October 12, 2016.

emergent and internal phenomenon. Identifiers and credentials help facilitate correlation, but the choice to accept a given identifier or credential—and hence recognize an asserted identity—remains entirely in the purview of the observer.

If identity is inherently a correlation in the mind of the observer, how can there exist *self-sovereign* identities? We can't control the minds of others, which means we can't control how others keep track of interesting subjects across contexts. Fundamentally, we can't directly control how others identify us. So how do we become self-sovereignty with respect to identity?

The answer is in the permission.

Self-sovereign identity means not having to ask permission to create, provide, or terminate the use of identifying information for correlation across contexts.

A self-sovereign identity system allows us to selectively present our own means of identification for correlating our interactions in formal and informal situations around the world, online and off.

It does not *control* how others identify us. The names and labels and history in other people's heads and databases are being our reach, but self-sovereign identity gives us the means to provide identity information on our own terms.

Ideally, identifiers and credentials from a self-sovereign system will become the lingua franca for intra- and inter-jurisdictional correlation of people across contexts. Such an accomplishment will mean that for a vast number of services, most people effectively control their identity.

Bad actors, inherent digital exhaust, and the needs of good actors who require correlation of greater scope (law enforcement, forensics, anti-terrorism units, military, etc.) will mean that, necessarily, there will be always be correlation by observers beyond any self-sovereign system. There will also always be the need for systems of governance and enforcement for minimizing and correcting abuses of such correlation. Technology can't fix everything, but it can dramatically improve the common experience.

A good self-sovereign identity system will allow individuals to directly influence how companies, governments, and others correlate our interactions across different services and locations *by default*. It won't fix all identity problems nor preclude alternative identity approaches, but it *will* put the individual in control of most uses of identity and give organizations a simpler, easier, more ethical way to use identity to improve how they provide services and products. When successful, it will not only enable individuals to exercise greater control over how companies and governments keep track of us, it will also illuminate those situations where self-sovereign identity is restricted, facilitating a conversation about when and where such limits are appropriate.

With that background, let us explore what would it mean for an identity to be self-sovereign.

Core Characteristics of Sovereign Identity

A self-sovereign identity means individuals don't need permission to take control of how others correlate us across contexts.

The individual is in control. The identity is accepted. The identity is free.

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.

Summary

Until we clearly demonstrate an understanding of the technology-independent requirements for both observers and subjects, it will be impossible to judge whether or not any given self-sovereign system fulfills the goal. There are a lot of great ideas floating around *and* a lot of misconceptions by practitioners, administrators, and end-users about what a self-sovereign identity would mean. In order to fund, co-develop, and eventually deploy a global self-sovereign solution to UN Sustainable Development Goal 16.9, it would be prudent to begin with an explicit requirements process *independent* of any specific technology.

In my lightning talk for this workshop, I will lay the groundwork for a requirements modeling process that starts with user needs, continues through lifecycle engagement, down to detailed interaction narratives to propose an end-to-end technology-free requirements model for self-sovereign identity.