Beyond Identity Cards to Distributed Identity

By Joe Andrieu <joe@legendaryrequirements.com>

A topic paper for the Rebooting Web of Trust IV Design Workshop, Paris, 2017

Abstract

Using a card-based metaphor to manage access to attributes through a public ledger misses perhaps the greatest opportunity for redefining digital identity. I propose a definition of distributed identity that is not only more self-sovereign than card-based approaches, it scales beyond web scale to allow every individual and IoT device to both create and consume identity. Discovering the best user interface idioms for managing distributed identity is a future exercise, but establishing the right conceptual foundation for identity opens new landscapes for innovation.

Metaphors

The prevalence of cards as a metaphor for controlling digital identity misses innovation that would truly revolutionize privacy and digital self-sovereignty. Information Cards from Microsoft and others[1]. Loyalty Cards from Digital Bazaar[2]. The e-Estonia electronic ID card from Estonia[3]. These efforts—technical and social advances worthy of note—are tied to a conceptual model of identity that unfortunately minimizes and dismisses the fundamental complexity of identity in society.

It's easy to choose "cards" as an interface paradigm for identity. They are concrete, simple, and well understood. Nearly everyone in the first world owns and uses multiple identity-related cards, often daily: drivers' licenses, insurance cards, credit cards, school ids, access cards. This metaphor has established itself in the canon of user-centric identity. Cards give users greater control over identity by letting individuals select which digital card to present to different online services. Unfortunately, the different efforts based on this paradigm have failed to make a dent in the problems of online identity.

One reason for these failures is the inevitable limitation of attempting to translate real-world mechanisms into digitally mediated interfaces. In his seminal work on user interface design, *About Face*, Alan Cooper put it this way:

> *It was widely believed that filling interfaces with visual representations of familiar objects from the real world would give users a pipeline to easy learning. As a result, designers created interfaces resembling offices filled with desks, file cabinets, telephones, and address books, or pads of paper, or a street with signs and buildings.*
>
> *[The] shift away from metaphor was long overdue, and for good reason: Strict adherence to metaphors ties interfaces unnecessarily tightly to the workings of the physical world. One of the most fantastic things about digital products is that the working model presented to users need not be bound by the limitations of physics or the inherent clumsiness of mechanical systems and 3D real-world objects mapped to 2D control.* [4]

[1] "Information Card". Wikipedia. https://en.wikipedia.org/wiki/Information_Card Accessed online April 13, 2017

[2] Digital Bazaar website. http://new.digitalbazaar.com/ Accessed online April 13, 2017

[3] e-Estonia.com, The Digital Society. Website https://e-estonia.com/ Accessed online April 13, 2017

[4] Cooper, Alan, et. al.; *About Face: The Essentials of Interaction Design;* 4th Edition, Wily, September 2014; ISBN: 978-1-118-76657-6

Much of the motivation for cards was, and is, increased user control over our identity. "User-centric identity" has been an active area of focused innovation for well over a decade. Exploring the latest iteration in that effort, this paper focuses on "self-sovereign" identity, which I define simply as using public ledger technology to provide robust, non-repudiable identity data with increased user control and privacy. The exact nature of how that is accomplished and what sorts of controls it gives individuals is an ongoing discussion.

The Functional Requirements of an Identity System

Let's break down the *functional* requirements for any identity system, digital or otherwise.

Identity is how we keep track of people and things.[5]

Identity is more than our name, our appearance, even our history. Identity is more than just an identifier; more than a collection of attributes. It is more than our profile or persona. Our identity is "who we are". It is how the world sees us *and* how we present ourselves to the world. In turn, other people's identity is how we see *them*—based in part on how *they* present themselves to the world.

Bigger than our digital footprint, our identity exists collectively in all the minds of everyone who recognizes us as "us". And we maintain, in our own minds, a small part of the collective identity of everyone we know. Any digital identity is *at best* an approximation of that vast subjective aggregate. The simplest digital identity can help organizations and computers provide advanced services to the right people, but even the most sophisticated digital shadows of identity can only approximate the complex and subtle understanding of self, others, and relationships that is identity.

When we realize that identity is how we keep track of people, we gain perspective on the process of identity. While our digital systems can never subsume the subtle depth of our full identities, they can enable the functional processes of identity and thereby give both people and systems effective tools for improving their notions of "who we are". Understanding these processes can also empower us to build systems that are more robust, resilient, and respectful of human dignity and freedom.

Self-Sovereign Identity

Identity is how we keep track of people. It is how we keep track of others *and* how others keep track of us. This functional definition lets us move beyond metaphors like identity cards to develop truly self-sovereign identity systems.

The motivation for self-sovereign identity is straightforward: it would be innately good if we, as individuals, have control over how other people keep track of us. We can't prevent identification outright—in fact, it would be a significant burden if we could—but we can, and arguably should, have greater control over how other people and organizations monitor and interact with us. In today's world of Big Data and the surveillance economy, the pendulum of control has swung too far to the right, with organizations driving the technical advances and investments to maximize their profit and power, with individuals and regulators far behind.

[5] For the sake of clarity, the rest of this paper work stick to "identity" as it relates to individuals.

Like all sovereignty, self-sovereign identity is a negotiated boundary of authority. It cannot give us control over how others recognize us or what they remember about us. It does not propose a miraculous technological power to force organizations to forget us. Even the EU's groundbreaking right to erasure only applies in specific situations[6] and depends upon the authority and mechanisms of the state for enforcement. What self-sovereign identity *can* give us is a more flexible tool, independent of traditional identity providers, for individuals and organizations to better manage the risks and benefits of identity. With luck, it can also stem the tide of the surveillance economy and its associated toxic data, restoring basic freedoms and building mutually respectful relationships between all parties.

To restore the authority, freedom, and dignity of individuals through self-sovereign identity systems, we need a clear understanding of the assets and processes of identity. Let's start with identity data.

Identity Data

There are two types of identifying information: "identifiers" and "attributes".

Identifiers are data specifically used to identify people across contexts: a name, an email address, a social security number, even the random, unique, anonymized key used by online ad services to track us as we visit different websites. Identifiers exist for the purposes of keeping track of people.

Attributes, in contrast, are statements, such as facts, observations, conclusions, or privileges, known or believed (true or false), *about* an individual (or group). Attributes represent a form of knowledge about people. They are used to provide advanced services. For example, customizing your movie listings based on your zip code. That zip code isn't used specifically to identify you as a unique individual, it's simply an attribute that enables the listing service to provide a customized experience.

The problem is that attributes can *also* be used to identify people and identifiers can be used to link previously isolated attributes. A few well-known data, referred to as "Personally Identifiable Information" or PII, are protected as special, but numerous incidents have shown that even unsuspecting attributes can be used to "re-identify"[7] and "de-anonymize"[8] individuals. So while some data may be seen in one context as unrelated to one's identity, in another, that same data could be the key factor in recognizing a particular individual. This basically makes PII a useless concept for distinguishing which data to treat as sensitive. It isn't that potential PII should be left unprotected, but rather that labeling a subset of data as PII leads to overconfidence in privacy protections, because of an incomplete model of identity.

Identity Processes

Identity is how we keep track of people.

[6] "The right to erasure (the right to be forgotten)" UK Information Commissioner's Office website. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/

[7] Barth-Jones, Daniel C., "The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now" (July 2012). Available at SSRN: https://ssrn.com/abstract=2076397 or http://dx.doi.org/10.2139/ssrn.2076397

[8] Barbara, Michael and Zeller, Tom, Jr. "A Face is Exposed for AOL Searcher No. 4417749" (August 9, 2006), *The New York Times*,. Accessed online April 8, 2017 at http://www.nytimes.com/2006/08/09/technology/09aol.html

Using identifiers and attributes, we accumulate knowledge about individuals and later apply that knowledge, bringing to bear data about them that are not observable in the immediate context. Others do the same in reverse, capturing knowledge about us and applying it to moderate how they relate to us.

Accumulate. Correlate. Apply.

These are the verbs of a functioning identity system.

- Accumulate data (from observation or acquisition from other sources).
- Correlate that data with one or more subjects.
- Apply that data in interactions related to or with those subjects.

This is what we do with identity.

As individuals, we accumulate data by watching and learning, correlating what we've seen and heard into a coherent picture—a notion, an idea, of "who somebody is". We then apply what we've learned—and inferred—to our dealings with others. Sometimes a deserved reputation enhances identity. Other times unfortunate stereotypes detract. These are the actions that constitute identity.

Similarly, organizations accumulate a history of interactions—and sometimes acquire outside data—which they correlate with customers, vendors, and employees. Then they apply the knowledge gained from those correlated histories to make better decisions about those parties and in turn provide more valuable services, where value is ultimately measured by shareholders.

Accumulate, correlate, and apply: these are the actions of an identity system.

The goal then of a self-sovereign identity system is to provide a framework where individuals manage the processes of identity: what data accumulates, how and when it is correlated, and who gets to apply it, AND do that with full appreciation of the innate symmetry of mutual sovereignty.

Distributed Identity

A distributed identity system is one that nobody controls and anybody can use. It is one in which anyone can say anything about anyone (with their permission) in a non-repudiable manner, and at the point of service, the subject[9] selectively discloses which data is shared with which recipients, for both correlation and enhanced services. The individual gets to say to service providers both "use this identifier for me" and "here's information about me". It is then up to the service provider to evaluate the authors and their claims before relying on them.

A self-sovereign distributed identity system requires that even querying or recording information about a subject requires authorization. It doesn't prevent private data storage outside the system, but it does depend on subject's permission to add records to the distributed record.

A distributed identity system provides a substrate for accumulating non-repudiable claims that the subject correlates on-demand when services need verifiable identity data. These claims are physically distributed for redundant access without reliance on interactions with specific services. For practical purposes, the claims themselves are encrypted so their distribution need not leak attributes.

[9] Or guardian

In a strongly distributed system, read/write access is open to anyone. In a managed distributed system, a governance framework may determine the rules by which approved participants access the system, with mechanisms for revoking that ability when those rules are broken. In any case, whoever is allowed to access the distributed system is free to do so without further permission, authorization, or interaction with the governing authority, and most importantly there is neither need nor means for recipients to interact with authors. All data store queries occur locally against a distributed data store and the distribution of that data is independent of the queries against it.

In the Joram 1.0.0 Engagement Model[10], we assumed a distributed data store as the foundation for an accretive identity context. Our hero, Joram, finds himself on the shores of Greece seeking asylum. As he interacts with agents of the Greek military, the UNHCR, Medicins Sans Frontiers, the French immigration authority, and others, an ongoing record of interactions accumulates, authored by those agents and dynamically correlated by Joram.

Although we didn't discuss the details, for Joram 1.0.0, we presumed a managed distributed identity system, with the UN setting the ground rules and authorizing agencies, and agencies in turn authorizing individuals for read/write access. The UN policed bad behavior, certified compliant software, and defined the mechanisms for social accountability by the actors in the system. Any of those agents, with Joram's authorization in the form of a QR code, PIN, and biometric, could retrieve and add records from what is essentially a semi-public ledger. All records shared by Joram were selectively disclosed using a standardized sharing ceremony on certified software and every app was warranted to use the data only for the intended purpose and to retain only that information required for the integrity of their service and legal compliance. This strawman architecture gave us a mental model for evaluating possible interactions without prejudice to the ultimate best solution. It also relied heavily on institutional and social accountability for preventing bad actors rather than on unproven technology to address every possible malicious act.

A distributed identity system does not preclude additional tracking, correlation, and application of data. It doesn't presume to demand, for example, that internal, unique keys in a vendor's database be a particular identifier. It doesn't outlaw use of data from strategic partners or other sources. It *does* enable attribute authors to establish themselves as credible sources of identity data *without* requiring them to run their own highly-available, secure attribute servers. It also enables attribute recipients to reduce internally stored and maintained toxic data. Finally, it should provide a foundation for vendors to dynamically access current attributes with full consent in compliance with GDPR and other privacy regulations.

Summary

In a distributed identity system, any approved author can record non-repudiable claims about anyone, with their permission. Any subject can selectively disclose specific claims to service providers they choose, with neither interaction with nor reliance on any authors or centralized services. Service providers evaluate, on their own terms, the claims of those authors to satisfy their unique requirements for identity assurance and service provision. This identity substrate provides a reliable context upon

[10] https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/final-documents/joram-engagement-model.pdf

which individuals can accumulate observations and assertions from any number of authors and, in turn, selectively and reliably disclose just the details that service providers need.

In contrast with identity cards—which typically present limited sets of attributes, bundled by author—a distributed identity system enables an essentially unlimited number of authors to record an unlimited set of identity data, all under individuals' control. A card-based interface to this distributed aggregate store would quickly become unwieldy with even just a dozen or so cards. Even digital wallets simply exacerbate the interface problem when people must chose card by card what to share with service providers.

What individuals need is an interactive aggregator that dynamically searches the individual's available identity data based on focused queries from the receiving service provider, allowing individuals to select precisely the data shared.

I don't yet know the right interface idiom—the right UI widget—to replace the metaphor of the identity card, but for a distributed identity system, something new is needed.