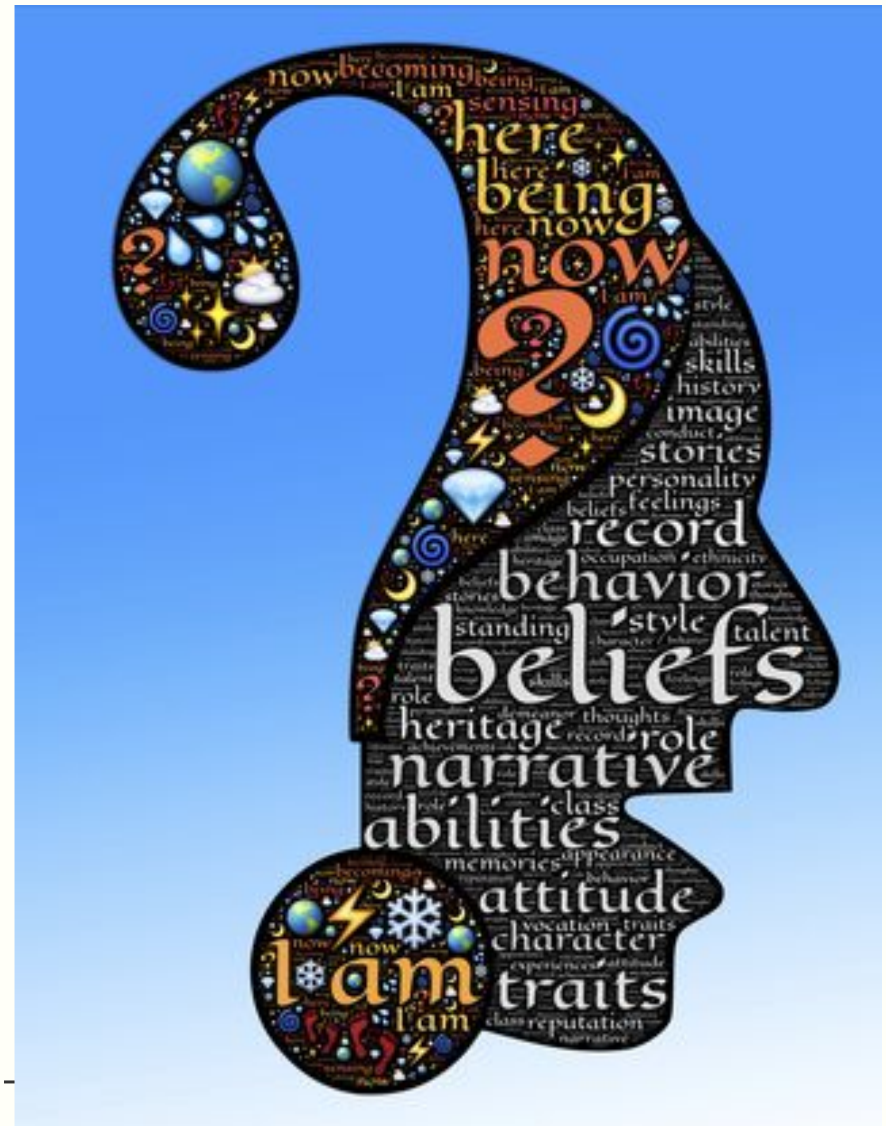
Life With Alacrity

A blog on social software, collaboration, trust, security, privacy, and internet tools by Christopher Allen.

The Path to Self-Sovereign Identity

April 25 2016 - 4200 Words
by Christopher Allen



Today I head out to a month-long series of events associated with identity: I'm starting with the 22st (!) Internet Identity Workshop next week; then I'm speaking at the blockchain conference Consensus about identity; next I am part of the team putting together the first ID2020 Summit on Digital Identity at the United Nations; and finally I'm hosting the second #RebootingWebOfTrust design workshop on decentralized identity.

At all of these events I want to share a vision for how we can enhance the ability of digital identity to enable trust while preserving individual privacy. This vision is what I call "Self-Sovereign Identity".

Why do we need this vision now? Governments and companies are sharing an unprecedented amount of information, cross-correlating everything from viewing habits to purchases, to where people are located during the day, to where they sleep at night, and with whom they associate. In addition, as the Third World enters the computer age, digital citizenship is providing Third World residents with greater access to human rights and to the global economy. When properly designed and implemented, self-sovereign identity can offer these benefits while also protecting individuals from the ever-increasing control of those in power, who may not have the best interests of the individual at heart.

But what exactly do I mean by "Self-Sovereign Identity"?

You Can't Spell Identity without an "I"

Identity is a uniquely human concept. It is that ineffable "I" of self-consciousness, something that is understood worldwide by every person living in every culture. As René Descartes said, *Cogito ergo sum* — **I think, therefore I am**.

However, modern society has muddled this concept of identity. Today, nations and corporations conflate driver's licenses, social security cards, and other state-issued credentials with identity; this is problematic because it suggests a person can lose his very identity if a state revokes his credentials or even if he just crosses state borders. **I think, but I am not.**

Identity in the digital world is even trickier. It suffers from the same problem of centralized control, but it's simultaneously very balkanized: identities are piecemeal, differing from one Internet domain to another.

As the digital world becomes increasingly important to the physical world, it also presents a new opportunity; it offers the possibility of redefining modern concepts of identity. It might allow us to place identity back under our control — once more reuniting identity with the ineffable "I".

In recent years, this redefinition of identity has begun to have a new name: *self-sovereign identity*. However, in order to understand this term, we need to review some history of identity technology:

The Evolution of Identity

The models for online identity have advanced through four broad stages since the advent of the Internet: centralized identity, federated identity, user-centric identity, and self-sovereign identity.

Phase One: Centralized Identity *(administrative control by a single authority or hierarchy)*

In the Internet's early days, *centralized authorities* became the issuers and authenticators of digital identity. Organizations like IANA (1988) determined the validity of IP addresses and ICANN (1998) arbitrated domain names. Then, beginning in 1995, certificate authorities (CAs) stepped up to help Internet commerce sites prove they were who they said they were.

Some of these organizations took a small step beyond centralization and created *hierarchies*. A root controller could annoint other organizations to each oversee their own heirarchy. However, the root still had the core power — they were just creating new, less powerful centralizations beneath them.

Unfortunately, granting control of digital identity to centralized authorities of the online world suffers from the same problems caused by the state authorities of the physical world: users are locked in to a single authority who can deny their identity or even confirm a false identity. Centralization innately gives power to the centralized entities, not to the users.

As the Internet grew, as power accumulated across hierarchies, a further problem was revealed: identities were increasingly balkanized. They multiplied as web sites did, forcing users to juggle dozens of identities on dozens of different sites — while having control over none of them.

To a large extent, identity on the Internet today is still centralized — or at best, hierarchical. Digital identities are owned by CAs, domain registrars, and individual sites, and then rented to users or revoked at any time. However, for the last two decades there's also been a growing push to return identities to the people, so that they actually could control them.

Interlude: Foreshadowing the Future

PGP (1991) offered one of the first hints toward what could become self-sovereign identity. It introduced the 'Web of Trust'[1], which established trust for a digital identity by allowing peers to act as introducers and validators of public keys[2]. Anyone could be validator in the PGP model. The result was a powerful example of decentralized trust management, but it focused on email addresses, which meant that it still depended on centralized hierarchies. For a variety of reasons, PGP never became broadly adopted.

Other early thoughts appeared in "Establishing Identity without Certification Authority" (1996), a paper by Carl Ellison that examined how digital identity was created[3]. He considered both authorities such as Certificate Authorities and peer-to-peer systems like PGP as options for defining digital identity. He then settled on a method for verifying online identity by exchanging shared secrets over a secure channel. This allowed users to control their own identity without depending on a managing authority.

Ellison was also at the heart of the SPKI/SDSI project (1999) [4] – [5]. Its goal was to build a simpler public infrastructure for identity certificates that could replace the complicated X.509 system. Although centralized authorities were considered as an option, they were not the only option.

It was a beginning, but an even more revolutionary reconception of identity in the 21st century would be required to truly bring self-sovereignty to the forefront.

Phase Two: Federated Identity *(administrative control by multiple, federated authorities)*

The next major advancement for digital identity occurred at the turn of the century when a variety of commercial organizations moved beyond hierarchy to debalkanize online identity in a new manner.

Microsoft's Passport (1999) initiative was one of the first. It imagined *federated identity*, which allowed users to utilize the same identity on multiple sites. However, it put Microsoft at the center of the federation, which made it almost as centralized as traditional authorities.

In response Sun Microsoft organized the Liberty Alliance (2001). They resisted the idea of centralized authority, instead creating a "true" federation, but the result was instaed an oligarchy: the power of centralized authority was now divided among several powerful entities.

Federation improved on the problem of balkanization: users could wander from site to site under the system. However, each individual site remained an authority.

Phase Three: User-Centric Identity *(individual **or** administrative control across multiple authorities without requiring a federation)*

The Augmented Social Network (2000) laid the groundwork for a new sort of digital identity in their proposal for the creation of a next-generation Internet. In an extensive white paper[6], they suggested building "persistent online identity" into the very architecture of the Internet. From the viewpoint of self-sovereign identity, their most important advance was "the assumption that every individual ought to have the right to control his or her own online identity". The ASN group felt that Passport and the Liberty Alliance could not meet these goals because the "business-based initiatives" put too much emphasis on the privatization of information and the modeling of users as consumers.

These ASN ideas would become the foundation of much that followed.

The Identity Commons (2001-Present) began to consolidate the new work on digital identity with a focus on decentralization. Their most important contribution may have been the creation, in association with the Identity Gang, of the Internet Identity Workshop (2005-Present) working group. For the last ten years, the IIW has advanced the idea of decentralized identity in a series of semi-yearly meetings.

The IIW community focused on a new term that countered the server-centric model of centralized authorities: *user-centric identity*. The term suggests that users are placed in the middle of the identity process. Initial discussions of the topic focused on creating a better user experience[7], which underlined the need to put users front and center in the quest for online identity. However the definition of a user-centric identity soon expanded to include the desire for a user to have more control over his identity and for trust to be decentralized[8].

The work of the IIW has supported many new methods for creating digital identity, including OpenID (2005), OpenID 2.0 (2006), OpenID Connect (2014), OAuth (2010), and FIDO (2013). As implemented, user-centric methodologies tend to focus on two elements: user consent and interoperability. By adopting them, a user can decide to share an identity from one service to another and thus debalkanize his digital self.

The user-centric identity communities had even more ambitious visions; they intended to give users complete control of their digital identities. Unfortunately, powerful institutions co-opted their efforts and kept them from fully realizing their goals. Much as with the Liberty Alliance, final ownership of user-centric identities today remain with the entities that register them.

OpenID offers an example. A user can theoretically register his own OpenID, which he can then use autonomously. However, this takes some technical know-how, so the casual Internet user is more likely to use an OpenID from one public web site as a login for another. If the user selects a site that is long-lived and trustworthy, he can gain many of the advantages of a self-sovereign identity — but it could be taken away at any time by the registering entity!

Facebook Connect (2008) appeared a few years after OpenID, leveraging lessons learned, and thus was several times more successful largely due to a better user interface[9]. Unfortunately, Facebook Connect veers even further from the original user-centric ideal of user control. To start with, there's no choice of provider; it's Facebook. Worse, Facebook has a history of arbitrarily closing accounts, as was seen in their recent real-name controversy[10]. As a result, people who access other sites with their "user-centric" Facebook Connect identity may be even more vulnerable than OpenID users to losing that identity in multiple places at one time.

It's central authorities all over again. Worse, it's like state-controlled authentication of identity, except with a self-elected "rogue" state.

In other words: being user-centric isn't enough.

Phase Four: Self-Sovereign Identity *(individual control across any number of*

authorities)

User-centric designs turned centralized identities into interoperable federated identities with centralized control, while also respecting some level of user consent about how to share an identity (and with whom). It was an important step toward true user control of identity, but just a step. To take the next step required user autonomy.

This is the heart of *self-sovereign identity*, a term that's coming into increased use in the '10s. Rather than just advocating that users be at the center of the identity process, self-sovereign identity requires that users be the rulers of their own identity.

One of the first references to identity sovereignty occurred in February 2012, when developer Moxie Marlinspike wrote about "Sovereign Source Authority"[11]. He said that individuals "have an established Right to an 'identity'", but that national registration destroys that sovereignty. Some ideas are in the air, so it's no surprise that almost simultaneously, in March 2012, Patrick Deegan began work on Open Mustard Seed, an open-source framework that gives users control of their digital identity and their data in decentralized systems[12]. It was one of several "personal cloud" initiatives that appeared around the same time.

Since then, the idea of self-sovereign identity has proliferated. Marlinspike has blogged how the term has evolved[13]. As a developer, he shows one way to address self-sovereign identity: as a *mathematical policy*, where cryptography is used to protect a user's autonomy and control. However, that's not the only model. Respect Network instead addresses self-sovereign identity as a *legal policy*; they define contractual rules and principles that members of their network agree to follow[14]. The Windhover Principles For Digital Identity, Trust and Data[15] and Everynym's Identity System Essentials[16] offer some additional perspectives on the rapid advent of self-sovereign identity since 2012.

In the last year, self-sovereign identity has also entered the sphere of *international policy*[17]. This has largely been driven by the refugee crisis that has beset Europe, which has resulted in many people lacking a recognized identity due to their flight from the state that issued their credentials. However, it's a long-standing international problem, as foreign workers have often been abused by the countries they work in due to the lack of state-issued credentials.

If self-sovereign identity was becoming relevant a few years ago, in light of current international crises its importance has skyrocketed.

The time to move toward self-sovereign identity is now.

A Definition of Self-Sovereign Identity

With all that said, what is self-sovereign identity exactly? The truth is that there's no consensus. As much as anything, this article is intended to begin a dialogue on that topic. However, I wish to offer a starting position.

Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale.

A self-sovereign identity must also allow ordinary users to make claims, which could include personally identifying information or facts about personal capability or group membership[18]. It can even contain information about the user that was asserted by other persons or groups.

In the creation of a self-sovereign identity, we must be careful to protect the individual. A self-sovereign identity must defend against financial and other losses, prevent human rights abuses by the powerful, and support the rights of the individual to be oneself and to freely associate[19].

However, there's a lot more to self-sovereign identity than just this brief summation. Any self-sovereign identity must also meet a series of guiding principles — and these principles actually provide a better, more comprehensive, definition of what self-sovereign identity is. A proposal for them follows:

Ten Principles of Self-Sovereign Identity

A number of different people have written about the principles of identity. Kim Cameron wrote one of the earliest "Laws of Identity"[20], while the aforementioned Respect Network policy[21] and W3C Verifiable Claims Task Force FAQ[22] offer additional perspectives on digital identity. This section draws on all of these ideas to create a group of principles specific to self-sovereign identity. As with the definition itself, consider these principles a departure point to provoke a discussion about what's truly important.

These principles attempt to ensure the user control that's at the heart of self-sovereign identity. However, they also recognize that identity can be a double-edged sword — usable for both beneficial and maleficent purposes. Thus, an identity system must balance transparency, fairness, and support of the commons with protection for the individual.

1. **Existence**. *Users must have an independent existence.* Any self-sovereign identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.

2. **Control**. *Users must control their identities.* Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This doesn't mean that a user controls all of the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.

3. **Access**. *Users must have access to their own data.* A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.

4. **Transparency**. *Systems and algorithms must be transparent.* The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.

5. **Persistence**. *Identities must be long-lived.* Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.

6. **Portability**. *Information and services about identity must be transportable.* Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear — and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity no matter what, and can also improve an identity's persistence over time.

7. **Interoperability**. *Identities should be as widely usable as possible.* Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.

8. **Consent**. *Users must agree to the use of their identity.* Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.

9. **Minimalization**. *Disclosure of claims must be minimized.* When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatibility is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.

10. **Protection**. *The rights of users must be protected.* When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.

I seek your assistance in taking these principles to the next level. I will be at the IIW conference this week, at other conferences this month, and in particular I will be meeting with other identity technologists on May 21st and 22nd in NYC after the ID 2020 Summit on Digital Identity. These principles will be placed into Github and we hope to collaborate with all those interested in refining them through the workshop, or through Github pull requests from the broader community. Come join us!

Conclusion

The idea of digital identity has been evolving for a few decades now, from centralized identities to federated identities to user-centric identities to self-sovereign identities. However, even today exactly what a self-sovereign identity is, and what rules it should recognize, aren't well-known.

This article seeks to begin a dialogue on that topic, by offering up a definition and a set of principles as a starting point for this new form of user-controlled and persistent identity of the 21st century.

Glossary

The following terms are relevant to this article. These are just a subset of the terms generally used to discuss digital identity, and have been minimized to avoid unnecessary complexity.

Authority. A trusted entity that is able to verify and authenticate identities. Clasically, this was a centralized (or later, federated) entity. Now, this can also be an open and transparent algorithm run in a decentralized manner.

Claim. A statement about an identity. This could be: a fact, such as a person's age; an opinion, such as a rating of their trustworthiness; or something in between, such as an assessment of a skill.

Credential. In the identity community this term overlaps with claims. Here it is used instead for the dictionary definition: "entitlement to privileges, or the like, usually in written form"[23]. In other words, credentials refer to the state-issued plastic and paper IDs that grant people access in the modern world. A credential generally incorporates one or more identifiers and numerous claims about a single entity, all authenticated with some sort of digital signature.

Identifier. A name or other label that uniquely identifies an identity. For simplicity's sake, this term has been avoided in this article (except in this glossary), but it's generally important to an understanding of digital identity.

Identity. A representation of an entity. It can include claims and identifiers. In this article, the focus is on *digital* identity.

Thanks To…

Thanks to various people who commented on early drafts of this article. Some of their suggestions were used word for word, some were adapted to the text, and everything was carefully considered. The most extensive revisions came from comments by Shannon Appelcline, Dave Crocker, Anil John, and Drummond Reed. Other commentators and contributors include: Doc Searls, Kaliya Young, Devon Loffreto, Greg Slepak, Alex Fowler, Fen Labalme, Justin Netwon, Markus Sabadello, Adam Back, Ryan Shea, Manu Sporney, and Peter Todd. I know much of the commentary didn't make it into this draft, but the discussion on this topic continues…

Image by John Hain licensed CC0 https://pixabay.com/en/identity-mask-disguise-mindset-510866/

The opinions in this article are my own, not my employer's nor necessarily the opinions of those that have offered commentary on it.

---

[1] Jon Callas, Phil Zimmerman. 2015. "The PGP Paradigm". #RebootingWebOfTrust Design Workshop. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/topics-and-advance-readings/PGP-Paradigm.pdf.↩

[2] Appelcline, Crocker, Farmer, Newton. 2015. "Rebranding the Web of Trust". #RebootingWebOfTrust Design Workshop. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/rebranding-web-of-trust.pdf↩

[3] Ellison, Carl. 1996. "Establishing Identity without Certification Authorities". 6th USENIX Security Symposium. http://irl.cs.ucla.edu/~yingdi/pub/papers/Ellison-OldFriend-USENIX-Security-1996.pdf.↩

[4] Ellison, C. 1999. "RFC 2692: SPKI Requirements". IETF. https://tools.ietf.org/html/rfc269↩

[5] Ellison, C., et. al. 1999. "RFC 2693: SPKI Certificate Theory". IETF. https://tools.ietf.org/html/rfc269↩

[6] Jordon, Ken, Jan Hauser, and Steven Foster. 2003. "The Augmented Social Network: Building Identity and Trust into the Next-Generation Internet". Networking: A Sustainable Future. http://asn.planetwork.net/asn-archive/AugmentedSocialNetwork.pdf↩

[7] Jøsang, Audun and Simon Pope. 2005. "User Centric Identity Management". AusCERT Conference 2005. http://folk.uio.no/josang/papers/JP2005-AusCERT.pdf↩

[8] Verifiable Claims Task Force. 2006. "[Editor Draft] Verifiable Claims Working Group Frequently Asked Questions". W3C Technology and Society Domain. http://w3c.github.io/webpayments-ig/VCTF/charter/faq.htm↩

[9] Gilbertson, Scott. 2011. "OpenID: The Web's Most Successful Failure". Webmonkey.

http://www.webmonkey.com/2011/01/openid-the-webs-most-successful-failure↩

[10] Hassine, Wafa Ben and Eva Galperine. “Changes to Facebook’s ‘Real Name’ Policy Still Don’t Fix the Problem”. EFF. https://www.eff.org/deeplinks/2015/12/changes-facebooks-real-names-policy-still-dont-fix-problem↩

[11] Marlinspike, Moxie. 2012. “What is ‘Sovereign Source Authority’?” The Moxie Tongue. http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html↩

[12] Open Mustard Seed. 2013. “Open Mustard Seed (OMS) Framework). ID3. https://idcubed.org/open-platform/platform/↩

[13] Marlinspike, Moxie. 2016. “Self-Sovereign Identity”. The Moxie Tongue. http://www.moxytongue.com/2016/02/self-sovereign-identity.html↩

[14] Respect Network. 2016. “The Respect Trust Network v2.1”. oixnet.org. http://oixnet.org/wp-content/uploads/2016/02/respect-trust-framework-v2-1.pdf↩

[15] Graydon, Carter. 2014. “Top Bitcoin Companies Propose the Windhover Principles – A New Digital Framework for Digital Identity, Trust and Open Data”. CCN. https://www.cryptocoinsnews.com/top-bitcoin-companies-propose-windhover-principles-new-digital-framework-digital-identity-trust-open-data/↩

[16] Smith, Samuel M. and Khovratovich, Dmitry. 2016. “Identity System Essentials”. Evernym. http://www.evernym.com/assets/doc/Identity-System-Essentials.pdf↩

[17] Dahan, Mariana and John Edge. 2015. “The World Citizen: Transforming Statelessness into Global Citizenship”. The World Bank. http://blogs.worldbank.org/ic4d/category/tags/self-sovereign-identity-systems↩

[18] Identity Commons. 2007. “Claim”. IDCommons Wiki. http://wiki.idcommons.net/Claim↩

[19] Christopher Allen. 2015. “The Four Kinds of Privacy”. Life With Alacrity blog. /2015/04/the-four-kinds-of-privacy.html↩

[20] Cameron, Kim. 2005. “The Laws of Identity”. https://msdn.microsoft.com/en-us/library/ms996456.aspx↩

[21] Respect Network. 2016. “The Respect Trust Network v2.1”. oixnet.org. http://oixnet.org/wp-content/uploads/2016/02/respect-trust-framework-v2-1.pdf↩

[22] Verifiable Claims Task Force. 2006. “[Editor Draft] Verifiable Claims Working Group Frequently Asked Questions”. W3C Technology and Society Domain. http://w3c.github.io/webpayments-ig/VCTF/charter/faq.html↩

[23] "Definition of Credential". Dictionary.com. http://www.dictionary.com/browse/credential?s=t↩

orginal layout

Life With Alacrity