Timothy Ruff Follow
CEO, co-founder of Evernym, co-inventor of Sovrin.
Apr 24 · 10 min read

The Three Models of Digital Identity Relationships

How self-sovereign identity is different, and why it's better.

Why SSI

As a relative "noob" in the identity world—five years and counting—it may seem presumptuous for me to attempt to distill all the types of digital identity relationships into just three models. But it needs doing.

Why? Because there's a new kid on the identity block—"self-sovereign" identity (SSI)—that purports to "re-imagine the identity data model," and apart from the December 2017 Gartner report, *Blockchain: Evolving Decentralized Identity Design*, where this assertion appears, I haven't seen any consensus on what it is nor *simple* illustrations or diagrams of how it works. The only piece I've found about how SSI stacks up against existing identity models is a solitary (but excellent) blog post written two years ago.

Plus, we need clarity to help distinguish the SSI contenders from the pretenders, as multiple companies now claim that their identity

offerings are self-sovereign, when by the literal definition of the term, they are far from it.

Most importantly, I believe we need to understand SSI because, unlike most overhyped new technologies, this one literally *will* change everything.

SSI represents a major breakthrough, the impact of which will extend far beyond what people typically think identity means; it will revolutionize digital relationships and interactions between people, organizations, and things. SSI is powerful yet elegant, bold yet familiar, and through it we can finally break free from the paradox of having to sacrifice security for user experience (or vice versa): we can have both, and at levels vastly improved over the status quo. Wonderfully, SSI also has life-altering potential for at-risk populations around the globe.

From the aforementioned Gartner report:

"The same way that people start physical life by having a birth certificate, people should start digital life with a self-sovereign identity."

But there's a long road between that world and where we are now, and the journey starts with better understanding how SSI differs from existing identity relationship models. So let's get started.

• • •

Understanding SSI

SSI is a concept some find difficult to understand at first, but offline it actually goes back a ways. The identity your parents gave you became self-sovereign—under your full ownership and control—when you gained legal independence. You likely still use this identity in different contexts as you deal with others in society, where you are often recognized as soon as you are seen or heard.

Now imagine having to use a different identity with each person you interact with, and every time you meet them they act as if they don't know you at first, because they literally cannot see you or hear your voice. So they ask you for "shared secrets"—key words, numbers, or

phrases that only you should know—with the presumption that if you know these secrets, you must be who you claim to be.

Sound risky and unfriendly? It is. But that is how things work online (and over the phone), and, unfortunately, we've become accustomed to it; there simply hasn't been a way for us to be easily recognized by those with whom we already have a relationship.

SSI promises exactly that, but the concept still confuses people…

- Why does it matter that people, organizations, and things can have self-sovereign identities?
- What does that even mean?
- And what big things can SSI do that current identity models cannot?

To answer these questions, let's look at two established digital identity relationship models and contrast them with SSI.

Please note: I've written this from the perspective of SSI's impact on organizations, even though the term "self-sovereign" usually refers to individuals. After all, it is the organizations we interact with—businesses, governments, nonprofits—that have the power to take SSI mainstream, or even make it the new status quo. Surprisingly, they also have the most to gain.

. . .

Model #1: Siloed / Traditional

How it Works

Traditional, “siloed” identity is the simplest of the three models: an organization issues to you (or allows you to create) a digital credential that you can use to access its service.

Trust between you and the organization is typically established through the use of shared secrets, usually in the form of a username and a password, but sometimes extending to other “secrets” such as your birthday, mother’s maiden name, PINs, and so on. Sometimes shared secrets are augmented with additional factors such as physical tokens or biometrics.

At least some of your personal data, whether shared by you or obtained from other sources, is typically stored within the organization’s data “silo,” a scenario that repeats for every organization, app, or website you log into. As a result, this model requires you to create and manage separate credentials for each relationship.

This is the oldest digital identity relationship model and by far the most commonly used today.

Pros

The primary advantage of this model is that it is widely established, well understood and straightforward to use.

It helps the organization manage compliance, liability, and other risks by “keeping subjects close,” keeping data in-house, and directly controlling all the actors and workflows, which reduces risk when compared to relying on a third-party identity provider (Model #2 below).

More advanced, FIDO-compliant implementations of siloed identity can eliminate the need for passwords by registering specific devices, which can then be used with a biometric or PIN.

Siloed identity also enables pairwise (unique) credentials for each relationship, which enhances both security and privacy as long as usernames and passwords are not reused.

Cons

From Gartner:

"Organizations require these digital identities before they can offer their services or allow any access to their resources. It is common for people to lose track of their siloed digital identities or not even have the ability to control their identity profile in many of these organizations. ***Both people and organizations increasingly feel the pain, and learn that this model is neither scalable nor sustainable as the use of digital services become more pervasive****." (emphasis added)*

As the Equifax and other hacks clearly show, the breach of an organization using siloed identity can be catastrophic, exposing the personal data of millions.

The siloed identity model has the worst customer experience of the three identity models. It forces you to maintain dozens or even hundreds of credentials—one for each app, service, or relationship—resulting in forgotten passwords and, worse, reused passwords, which lead to further security lapses. It also requires organizations to treat customers like strangers at the beginning of each interaction.

The siloed approach to authentication is one-way (open to phishing) rather than mutual, session-based rather than persistent, and doesn't work well for the Internet of Things because it was designed for people.

With siloed identity, each organization must become somewhat of an identity and security expert, which can be a challenge for churches, local governments, schools, credit bureaus, and, frankly, most organizations. The result: over $4 trillion in annual fraud-related costs worldwide.

. . .

Model #2: Third-Party IDP

How it Works

The IDP relationship model adds a third-party company or consortium to act as an "identity provider" (IDP)[1] between you and the organization or service you're trying to access. The IDP issues the digital credential, providing a single sign-on experience with the IDP which can then be seamlessly used elsewhere, reducing the number of separate credentials you need to maintain.

It works like this: you log in to the IDP, which then "federates" your login to the service you're trying to access using protocols such as OAuth, SAML, or OpenID Connect. Trust between you and the IDP is maintained in the same manner as in siloed identity—typically through shared secrets—and may be fortified with additional factors to provide a higher level of assurance to the organization. Identity data is centralized in the IDP.

A common example of the IDP model is "social login" on the Web using your Facebook, Google, Twitter, or other social ID to access a third-party service. With social login, one of these tech giants serves as your IDP, but this option is acceptable only in lower-trust environments such as e-commerce, and not in high-trust environments such as banking.

Pros

In lower-trust environments, IDP-powered social login enables users to access many applications with a single credential, simplifying authentication, reducing usernames and passwords, and improving customers' experiences. In high-trust environments the IDP model has the potential to do the same—if it can garner more widespread adoption.

Cons

The primary downside of the IDP model concerns high-trust applications, because a third party is inserted into the middle of every interaction, saying "Trust me."

The ceding of control and transfer of liability required in this three-way trust model is quite thorny. This is why, despite years of ongoing government efforts in the U.S. (NSTIC) and the U.K. (Gov.UK Verify), this model has not achieved significant adoption for high-trust, cross-

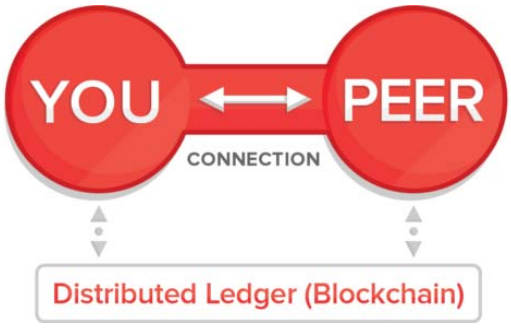
context applications, such as using a bank credential at more than one bank.[2]

This model often forces users to create a new relationship with a potentially unfamiliar IDP, separate from and in addition to the organization with which they're trying to interact. The IDP becomes a large trove of personal information, storing credentials and other data for all its clients' employees and customers. The IDP also determines the limitations of data structures and schema and must maintain direct connections with all network participants, inhibiting flexibility and scalability. And as we've seen in the recent Facebook scandal over Cambridge Analytica, it is the IDP that sets the policies and goes about enforcing them (or not).

As with the siloed approach, authentication in the IDP model is one-way rather than mutual (doesn't prevent phishing), session-based rather than persistent, and sequential rather than parallel; and it doesn't work well for authenticating organizations or things (needed for Internet of Things applications).

. . .

Model #3: Self-Sovereign / Peer-to-Peer



How it Works

Self-sovereign identity is a two-party relationship model, with no third party coming between you and the organization, now considered your "peer."

SSI Wallet and Verifiable Credentials

SSI begins with a digital "wallet" that contains digital credentials. This wallet is similar to a physical wallet in which you carry credentials issued to you by others, such as a passport, bank account authorization, or graduation certificate, except these are digitally signed verifiable credentials that can cryptographically prove four things to any verifier:

1. Who (or what) is the issuer;
2. To whom (or what) it was issued;
3. Whether it has been altered since it was issued;
4. Whether it has been revoked by the issuer.[3]

You can also carry self-signed credentials in your wallet, such as your preferences, opinions, legally binding consent, or other attestations you've made about anything.

Verifiable credentials can be issued and digitally signed by any person, organization, or thing and used anywhere they are trusted. SSI is as strong as the credentials it contains, strong enough for even high-trust industries such as finance, healthcare, and government. Organizations can choose to trust only credentials they have issued, credentials issued by others, or some combination, according to their security and compliance needs.

Out-of-Band Connection

To exchange digital credentials securely and privately, one peer—any person, organization, or thing—can establish a direct, encrypted connection with another peer. This connection can remain persistent (as opposed to session-based) at the option of each peer. Trust is mutually established when peers use this connection to exchange credentials and verify the digital signatures on received credentials using a distributed ledger.[4] [5] You control what you share with others, whether an entire credential, part of a credential (called "claims"), or zero-knowledge proofs (ZKP) derived from a credential (explained below).

Real Self-Sovereignty

You are literally the sovereign owner of your SSI wallet and the credentials inside: No one can "turn the lights out" or take them away

from you without your consent. As in the real world, issuers can revoke credentials they've issued, but you'll still possess them and they can continue to be useful, just as an expired driver's license can be used to prove your age. With verifiable credentials, however, a new recipient will know when you present it whether or not it has been revoked, without needing to contact the issuer.

SSI is becoming standardized and interoperable, and it is portable, with no vendor lock-in. Real SSI is not dependent on any particular company or other entity, as apps and agencies are modular and replaceable. Switching from one service provider or agency to another does not result in losing one's credentials, relationships, or history.

Pros

Contrary to popular belief, we don't have to wait for SSI to be ubiquitous before gaining a large chunk of its benefits. As we're learning from most of our clients and the use cases they have brought to us, we can begin benefiting right now, with "Single-Source" SSI.

"Single-Source" SSI

Two common (and contradictory) misperceptions about SSI are:

1. It only involves self-asserted claims;
2. It only involves third-party claims.

What many critics miss is SSI's powerful ability to operate between those extremes, for relationships between just two parties, where the only credentials an organization will accept *are those it issued in the first place.*

This is precisely how most identity interactions work today: you can only use your bank login at the bank, your student ID at the school, your Costco credential at Costco. Surprisingly, most of the benefits of SSI still apply to these, the most common identity relationships:

- **Stronger authentication:** Because shared secrets can be replaced with cryptographically secure, digitally signed credentials, you can exchange far stronger credentials, and more of them.

- **Great user experience:** Because authentication can occur out of band, you can open an app and already be signed in, or call your bank's customer service without answering silly questions about your birthday, mother's maiden name, SSN, and other personal info.
- **Phishing prevention:** Because authentication is mutual, when you get a suspicious call or message from someone, you can know for sure who it is, because *you can authenticate your bank as strongly as they can authenticate you.*
- **Private communication channel:** Because the out-of-band connection between SSI peers is private and secure—no intermediaries, encrypted end to end—it can be used for communication of any kind: text, voice, video, data sharing, and more. (Great for millennials, who hate email.)
- **Better relationships:** Because authentication happens passively behind the scenes, customers can be recognized and no longer treated as strangers at the beginning of each interaction, enabling a rich customization of each and every touchpoint.
- **Same liability model:** Because a bank, for example, can choose to accept only digitally signed credentials it has issued, SSI is no different than siloed identity from a liability perspective, meaning financial institutions and companies in other high-trust industries can utilize SSI without legal or compliance concerns.

Of course, once you have credentials in a self-sovereign wallet they're yours to keep and use with anyone who trusts them, whether that's one verifier or many.

Multi-Source, Multi-Verifier SSI

As remarkable as it would be just to regain control of our identities within distinct relationships, the most exciting version of SSI goes much further. It envisions a world where any person, organization, or thing can issue any kind of credential to any other person, organization or thing ("multi-source"), which can then be shared with any *other* person, organization, or thing, and the authenticity of which can be immediately and easily verified ("multi-verifier").

The advantages of such a world cannot be easily overstated. With everyone having a wallet full of cryptographically verifiable credentials, *simply having someone's personal information would no longer be sufficient to impersonate them*, raising the bar quite high for account take-over, phishing, fake news, or most forms of fraud; even spam becomes much more difficult. Add on top the benefits of having authenticated, peer-to-peer connections with every person, organization, or thing with whom you have a relationship, literally forming a newly decentralized web, built on open-source protocols and with no tech giants needed as intermediaries. It would improve almost every digital interaction.

Obviously, there is a massive chicken-and-egg problem to overcome—an obstacle between our world and that one called "network effect." Network effect is your friend and accelerator as a new technology gains momentum, but your nemesis at the beginning: imagine having the world's only fax machine versus working in the only office without one. We got over that hump with important new technologies like the telephone, the fax machine, and most crucially the internet, and we'll get there with SSI. Based on the activity we at Evernym are seeing around the world, we'll get there more quickly with SSI than most believe, because our world is more connected than ever, and the pains SSI addresses—fraud, security, privacy, compliance, user experience—are reaching a crescendo.

Legal Identity, Pseudonymity, and Anonymity

SSI has the important ability to strongly prove legal identity when desired, or enable trustworthy pseudonymity or anonymity when preferred. SSI that uses zero-knowledge cryptography opens up an entirely new world of powerful, private interactions, including:

- Websites and other services can verify that patrons are of a legal age, without needing name, location, age, or even birthday;
- Individuals can prove that they are employees of a certain company, or citizens eligible to vote; that they have a certain credit score; that their anonymous tip or whistleblowing is credible, etc., all without revealing their names, addresses, or other personal data;

- Pharma companies can have direct, private connections with patients who have verifiable prescriptions for their medications, without knowing who or where those patients are;
- When privately selling a car or other property, owners can prove their legal ownership without revealing any personal details;
- Internet users can participate pseudonymously in gaming, social, or other online communities.

Other Benefits

SSI has many other benefits for people, organizations, and things. Some of the biggest are:

- SSI simplifies and strengthens **compliance** with GDPR, KYC, AML, HIPAA, COPPA, and other regulations by eliminating intermediaries and ensuring cryptographically provable verification and **consent**.
- SSI can prevent unwanted **correlation** by third parties, and even among colluding second parties, by incorporating pairwise identifiers, powerfully addressing this known **privacy** problem common to blockchain technologies;
- SSI provides participants in **witness protection programs** and **intelligence operations** with cryptographically strong credentials;
- SSI can work **offline** as well as online, creatively utilizing smart cards, QR codes, NFC, Bluetooth, and other technologies.

Each of these benefits deserves further discussion and consideration, which we'll provide in future posts and papers.

Cons

Several of the capabilities discussed above aren't necessarily exclusive to SSI. Verifiable credentials, zero-knowledge proofs, and even mutual authentication, for example, could theoretically be built into non-SSI solutions, though I have never seen or heard of any such solution. And while, as footnoted, not all SSI solutions include all of these capabilities, at least one SSI system—Sovrin—was designed from the ground up to include all of these capabilities natively.

SSI is new and different than the way things are currently done, and that alone creates friction. There are switching costs of several kinds, including: modifying internal systems to issue claims and credentials and verify the same; upgrading user interfaces to replace usernames and passwords with the exchange of claims and proofs;[6] slowly replacing email as a means of communication; and educating and training staff, customers, and others.

Then there's key management, potentially the Achilles heel of all blockchain technologies. With bitcoin, for example, if you lose your private keys you lose your money, period. There is no "forgot password" option. SSI solutions will need a crutch analogous to password recovery if they are to become widely adopted. SSI systems that use pairwise identifiers, such as Sovrin, will generate hundreds or even thousands of private keys for people and organizations to manage, magnifying the need for comprehensive key management.[7]

In Conclusion

"On the Internet, nobody knows you're a dog."

"On the internet, nobody knows you're a dog," the famous *New Yorker* cartoon says. Accurate identification and authentication is still the great unsolved problem of the internet; we still can't tell the good guys from the bad. If we could, we'd block the bad ones and let the good ones through. Our failure to do so is the primary reason why our global economy loses trillions of dollars annually to fraud-related costs.

Make no mistake: traditional siloed identity is the main culprit here.

The third-party IDP model had promise when it first arose, but seemingly intractable problems remain. Bottom line: the current identity models are broken and in crisis, and SSI represents a revolutionary step forward. And now that SSI is possible, I think its ubiquitous adoption is inevitable.

SSI is not a single breakthrough but many. Trustworthy, truly peer-to-peer relationships between people, organizations, and things will revolutionize digital interactions. Mutual cryptographic authentication could address the internet's authentication problem, making identity theft, phishing, and other fraud much tougher for crooks. The compliance and consent requirements of the most stringent privacy regulations can be not only met but exceeded, in both letter and spirit, while improving customer experience rather than sacrificing it. Privacy can—and I believe will—have a major comeback. And only in science-fiction movies have we seen the types of user experiences that SSI will make possible.

All in all, it's high time for a change. The siloed and IDP models have had their run, and proven they're not up to the task.

The time for self-sovereign identity has come.

(Thanks to Drummond Reed, Phil Windley, Steve Wilson, Doc Searls, Brad Tumy, Andy Tobin, John Callahan, Sam Curren, James Monaghan, and Elizabeth Renieris for their editing and thought contributions to this article. Special thanks to Identity Woman (Kaliya Young) for her help distilling these three categories from significantly more complex models of identity.)

Founded in 2013, Evernym develops software solutions that leverage distributed ledger technology to provide every individual, organization and connected device with secure and irrevocable identity. Learn more about Evernym and its self-sovereign identity solutions at evernym.com.

. . .

Footnotes:

[1] When an organization acts as its own IDP, as often occurs with large organizations, I consider that a two-party siloed model, and not a 3rd Party IDP model.
[2] *"The switching cost to federated [IDP] identity where RPs come to rely upon external identities is a very big deal; I am not aware of any precedent where it has been done without legislation, such as the BankID regimes of Norway and Sweden."* (Stephen Wilson, managing director, Lockstep Technologies)
[3] Not all SSI solutions support revocation.
[4] The ledger must not be owned or controlled by any single company or entity, otherwise its users would be subject to that controlling entity and would not, by definition, be self-sovereign.
[5] The validation of digital credentials against a public ledger can be performed by any person, organization, or thing at any time and from anywhere, with or without the assistance of third parties.
[6] SSI need not be "rip-and-replace," and can be gradually implemented alongside existing solutions.
[7] For over a year now, Evernym has been working under a contract with the U.S. Department of Homeland Security's Science and Technology division on a fundamental solution to key management called DKMS (Decentralized Key Management System), an emerging open standard for interoperable key management that includes key backup and recovery features designed for everyday internet users.