SSI: A Roadmap for Adoption

> A Journey from huh? to DUH!

Moses Ma (FutureLab), Claire Rumore (FutureLab), Dan Gisolfi (IBM), Wes Kussmaul (Reliable Identities, Inc), Dan Greening (Senex Rex)

Abstract

This document proposes an industry group to develop the Self-Sovereign Identity (SSI) market. It lists key stakeholders who would actively promote SSI adoption, if they were well-informed. Its first project will be an SSI application market roadmap, to show the technical prerequisites, market enablers, risks, revenues, and costs of different SSI applications on a reasonable timeline. A roadmap will help SSI leaders, standards bodies, developers, academics, media, and investors focus on important work, and accelerate the SSI market. We illustrate industry marketing by summarizing our market strengths, weaknesses, opportunities, and threats (SWOT analysis), and show how this simple analysis exposes important marketing goals. Further projects will include go-to-market materials for developers, market explainers, frequently asked questions, market glossaries, and market research.

We wrote this paper to find more people who value a healthy SSI market. By working with us, you will grow the overall SSI market, meet the major SSI market participants, and advance your own ambitions. Please join us!

1 Self-Sovereign Identity Group Charter

This section describes the mission, stakeholders, goals, and initial organizational structure of the proposed Self-Sovereign Identity Group.

Mission

We improve social stability, economic productivity, and individual freedom by promoting broad use of self-sovereign identity.

Stakeholders

Our market development efforts will target these stakeholders, who can form a minimal viable community to drive adoption.

Role	Benefit
Technical leaders	Focus innovation on market enabling technology
Standards participants	Develop standards that promote high usage
Media	Develop more compelling, meaningful, and accurate stories
Developers	Create applications and services for rapid adoption
Businesses, Governments, Non-profits	Develop early customers and adoption
Venture capitalists	Make better decisions to reduce risk and increase IRR
Academics	Target hot research opportunities

Membership

Members in this organization must contribute to content development and distribution, stakeholder engagement and recruiting. In return, members' companies (or the individual if they are independent) will be highlighted on our web site and promotional materials. Individual members will learn an enormous amount about the SSI market, ICO funding strategies, identity stakeholders, standards organizations, and marketing. Members will meet many industry luminaries and through them gain career opportunities. Finally, to the extent possible we want members to have autonomy, by providing measurable goals and allowing them to achieve those goals as they see fit (within reason).

We expect the organization to ultimately self-organize to maximize market expansion. Initially, a single **Product Owner** may prioritize work, and a **Scrum Master** may be assigned to facilitate communication and work, manage the workflow and seek timely results.

These focus areas will likely dominate our activities.

- **Content**: Create informational content (presentation, videos, etc) suitable for stakeholders
- **Portal**: Create and maintain the organization's website
- **Communications**: Propagate SSI messaging to passive stakeholders
- **Stakeholder Engagement**: Engage key standards and open source workgroups in a two-way dialog
- **Management**: Recruit members, prioritize value, facilitate effort

Contact Moses Ma or Dan Greening to become a member.

Goals

- Get ourselves organized
  - **(DONE)** Agree on mission (see above)
  - **(DONE)** Setup tools (i.e. Trello)
  - **(DONE)** Establish web site (see Self Sovereign ID
  - **(in progress)** Complete the final draft of this
  - **(not doing until bigger)** Discuss project management
    - Schedule cadence (scrum) call
    - Review and refine tribe structure
  - Establish site login tiers (public, developer, marketer, press) and tracking to measure reach and engagement
- Create and promulgate a realistic technology and market roadmap
- Recruit initial foundational partners as adoption catalysts
  - Identify minimum viable ecosystem (DID network, wallet, browser integration, blog integration?)
    - Build Drupal plugin for *SuperSignOn*, a decentralized authentication system based on DID-Auth
    - Allow developers and others to *SuperSignOn* to our (Drupal) site
  - Recruit and help influential leaders (i.e: Reid Hoffman, Fred Wilson, etc) to speak favorably about SSI
    - Access to subject matter experts
    - Sample Presentations
    - Speakers bureau
  - Recruit/produce minimum viable ecosystem participants
    - willing networks, wallets, feasible browser plugins, feasible blog plugins
    - key communication technologies from Slack, Telegram, RocketChat, Wikipedia to support DIDs
    - Recruit developer support services, such as GitHub, CircleCI, BitBucket, to support DIDs
- Produce *Go To Market Resources* to support developers by year end 2018
  - **(in progress)** Glossary of market relevant terms
  - **(in progress)** Develop FAQs that debunk myths and promote adoption
  - Consolidate technical primers (tutorials) into a single getting started kit
  - Develop a Communications Kit
    - Simplify and articulate the concepts and benefits of SSI for the masses
    - Provide a cohesive narrative about SSI and its goals for the Media
    - Offer common baseline talking points for SSI developers

    - Explain wallets and DID distribution
        - Who are the wallet makers
        - How wallets will be interoperable and secure
    - High impact videos and other demo recordings (i.e.: RWOT)
- Best practices for businesses and government to create SSI strategy
    - Best practices for businesses to create a SSI strategy
    - Offer domain-specific descriptions and demonstrations (drivers licenses, voting, site login, insurance, business registration, etc
    - Presentations
    - Videos

Assets

This document was developed at RWOT6 (Rebooting Web of Trust, Spring 2018) group. Document source is HERE

An organizational web site has been created at selfsovereign.id.

An initial glossary is here SSI Glossary

Group work is prioritized and tracked at Trello.

Members communicate through Slack.

Contributors

Some people have contributed substantially so far. They are

Person	Company	Contribution
Dan Gisolfi	IBM	Content
Moses Ma	Futurelab	Content, Management
Darrell Duane	Crypto UBI	Portal
Wes Kussmaul	Reliable Identities	Content
Dan Greening	Senex Rex	Content

Possible volunteers

People who have expressed interest in the organization include:

Person	Company	Possible Role
Vishal Gupta	Diro Foundation	Portal (Design)
Chandran Gaurav	Diro Foundation	Portal (Design)
Kate Sills		Communications
Kaliya Young		Communications
Remy Lyon		Communications

People who have been invited are:

Person	Company	Possible Role
Alex Preukschat (Invited)	Globatalent	GTM Development
Sean Bohan (Invited)	Evernym	Stakeholder Engagement
David Crocker (Invited)	Brandenburg InternetWorking	Stakeholder Engagement
Nathan George (Invited)	Sovrin	Stakeholder Engagement

2 Existing Market

Motivation (SWOT)

This section describes the state of the SSI industry, as of 7 April 2018. We can gain a broad understanding of the maturity and vulnerability of our industry by listing strengths, weaknesses, opportunities and threats (SWOT analysis).

Strengths

- SSI networks provide affordability, scalability, reliability, trustability, privacy, security, and portability superior to traditional centralized and siloed identity networks;
- For decades, identity leaders have avoided partisanship and collaborated on identity fundamentals and standards;
- Our community has largely completed the SSI technical infrastructure to support SSI applications; and
- There are several operational and competing SSI distributed identity networks and wallets in beta.

Weaknesses

Our own complacency could derail or delay SSI adoption.

- Self-sovereign identity concepts can be confusing, especially when we lead with technology and not societal benefits
- We do not discuss deployment schedules for SSI networks and APIs, so many application developers refrain from investing effort;
- We do not broadly discuss expected costs for DIDs and SSI services, which creates financial risk for startups;
- We provide no SSI reference applications and libraries, from which developers could produce compelling applications;
- We don't list SSI network and wallet vendors, and so application developers worry that they will be locked in;
- Our narrow focus on technical and philosophical exploration is distracting us, and delaying the societal and individual benefits of SSI.
- Our individual non-specific identity concerns—such as whether biometric data might enable despotic states to track our movements—distract us from solving clear and present dangers, such as putting development work toward eliminating non-state-originated financial, identity, and privacy theft (which will actually help us better understand and address the challenges of despotic states);

Opportunities

Society is turning a corner in demanding better identity solutions:

1. Fear of identity hacks and theft are now pervasive,
2. Privately-maintained identity systems have exposed businesses and governments to hacking, leaks, and lawsuits,
3. Foreign enemies have destabilized nations through election and infrastructure hacking,
4. Malware-borne DDS attacks have damaged individual companies and degraded the internet, and
5. Social media and advertisers have enabled private data misuse (sometimes unintentionally).

Inexpensive SSI-based solutions can resolve each of these problems. If we direct some of our attention to expanding the SSI market, we can likely gain rapid traction.

Threats

Despite the many advantages of SSI, competitive threats could derail or significantly delay SSI adoption.

- Key customers could adopt inferior non-SSI alternatives;
- A poor identity decision by a customer will take years and cash to correct, due to high switching costs for identity;
- The low-agility of government agencies compounds the effect: their bad decisions could affect everyone for decades. If government agencies don't participate in distributed identity networks—for licenses, passports and national identity—it will degrade citizen security, financial tracability, and information verifiability for a long time;
- Standards bodies could produce standards incompatible with SSI. A specific concern is the mDL (mobile drivers license) standard being developed by the ISO/IEC JTC 1/SC 17/SG 1 working group;

False assumptions about SSI are rife:

- Some believe blockchain solutions store personally identifiable information (PII) on the distributed ledger.
- Some believe that participation in SSI networks is involuntary,
- Some believe that a decentralized ID could "*never be turned off or blocked*" due to the immutability of the distributed ledgers.
- Some believe it will be impossible to prevent anyone from publishing anything they want about you, without the standard societal repercussions (libel, etc.), and that ledger immutability negative reviews become part of an indelible permanent record.
- Few people know the privacy benefits of *Selective Disclosure* (or the Principle of Minimum Disclosure), and how SSI supports it.

Most of these threats can be disarmed by informing key influencers.

Industry Organizations

As far as we know, other non-profits focus on engineering, interoperability, specific networks, or specific application domains, but not general distributed identity market development. They include:

Rebooting Web of Trust (RWOT)

Rebooting Web of Trust is a group that meets twice yearly to develop position papers and kick off more significant efforts. It seeks to create the next generation of decentralized web-of-trust based identity systems. Each event generates roughly 5 technical white papers on topics decided by the group that will have the greatest impact on the future. RBOT may also use hackathons to implement those ideas.

This document is a "technical white paper" written at RWOT6 (Spring 2018).

Internet Identity Workshop (IIW)

Internet Identity Workshop is a group that meets twice yearly to share and refine ideas about identity and forge working relationships. It is organized as an unconference using Open Space Technology. It is highly effective, and that effectiveness is largely due to its insistence on note-taking and collaboration.

World Wide Web Consortium (W3C)

World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web. Two working groups are particularly relevant to self-sovereign identity.

Verified Claims Working Group (VC) seeks to make expressing and exchanging credentials that have been verified by a third party easier and more secure on the Web.

Credentials Community Group (CCG) explores the creation, storage, presentation, verification, and user control of credentials. The group drafts and incubates Internet specifications for further standardization and prototyping and testing reference implementations. CCG was the original source of material for the official Verified Claims Working Group.

Distributed Identity Foundation (DIF)

Distributed Identity Foundation (DIF) is an engineering-focused, non-profit organization composed of individuals and companies who are collaboratively developing an interoperable set of decentralized identity protocols, specs, and reference implementations that run across chains and service providers. Its goal is user-enablement via the creation of a ubiquitous decentralized identity ecosystem that benefits every person and company worldwide.

Sovrin Foundation (Sovrin)

Sovrin Foundation (Sovrin) is a non-profit organization that manages a permissioned blockchain identity network. Because the network is permissioned, participants must agree to maintain identity security and privacy (otherwise a collection of members could subvert the network). Authoritative network participants must sign the Sovrin Trust Framework, which gives them permission to operate a node. The Sovrin Foundation is a spinoff of the company Evernym.

The Sovrin Foundation has produced a substantial body of market-relevant material, but it is targeted toward one specific network. Other competing networks include Veres One (with its own network) and uPort (based on the Ethereum contract network).

Information Trust Exchange Governing Association (ITEGA)

Information Trust Exchange Governing Association provides Internet stakeholders a forum to convene, develop and implement governing protocols and business rules for protecting and balancing trust, privacy, identity and information commerce. It seeks to balance privacy, personalization, and payment to improve journalism and publishing. One of its first projects is to deploy a proof-of-concept for a first-party-user-data exchange that would be privacy-by-design.

Industry Goals

Here are the goals these other organizations have articulated:

- One million public (public or pseudonymous) DIDs issued by March 2019
- Formalized plans by year-end 2018 for foundational SSI specifications
    - W3C DID
    - W3C VC
    - Oasis DKMS
- Public release of a handful of reference applications that can help jumpstart developer applications

3 Summary

The distributed identity market is at a crossroads:

- market forces are demanding secure, privacy-respecting solutions to identity
- DID infrastructure is in beta or better
- whether we have a minimum viable ecosystem is debatable
- our market communications, so far, have been weak

This paper argues for the formation of an unbiased team to develop the Self-Sovereign Identity (SSI) market, across all participants. We will educate and support a variety of stakeholders to promote SSI. We will provide infrastructure and application developers unbiased information and tools to support their go-to-market efforts.

We seek your help.

Appendix A: WOWs to Consider

(Incorporate into roadmap or organization Backlog)

Another requirement for success is to create a design process that would lead to a sustainable flow of compelling technologies that provide a “wow” factor, that can form a pipeline of compelling functionality to fortify the value proposition for decentralized identity. An initial set of projects and ideas for “wow prototypes” include:

1. **Industry Demos**: Develop a number of vertical industry references. For example:
    - FinTech: A demo of the CULedger CUID Trust Framework that uses the Hyperledger Indy framework.
    - Travel and Transportation: A Dapps that implements one or more concepts outlined in the World Economic Forum’s Known Traveler Report.
2. **Community Badges Toolkit**: Produce a Starter Kit for any small or large community to begin to issue verifiable credentials in the form of OpenBadges. Such a toolkit would be a perfect *Getting Started* toolkit for a Go-to-Market (GTM) package of resources.

    > NOTE: The final paper submitted by the Open Badges are Verifiable Credentials RWOT Workgroup is suppose to produce a working prototype that can be used to seed this toolkit.

3. **Other Interesting Concepts**: There are a number of other potential reference applications that could be interesting to develop and deploy.
    - *SuperSignOn*, a decentralized authentication system based on the DID-Auth specification.
    - *GitHub Authentication* using Verifiable Credentials.
    - *ICO-LegalAssist* which would use Verifiable Claims as a basis for attestations by attorneys in ICOs.
    - *IDESG’s IDEF assessment* tool for receiving badges

Appendix B: Frequently Asked Questions

(Start of a section for the web site)

Naysayers illustrate the urgency for this effort. A poor communication plan gives rise to myths that need to be discredited. Here are a few examples of myths already circulating in the media and amongst analysts:

Do blockchain SSI solutions store personally identifiable information (PII)?

No. Commercial blockchain identity systems do not store personally identifiable information (PII) on blockchains, because it is unnecessary, expensive, and limits portability. Your DID entry on the blockchain may point to data, if there is any, stored elsewhere physically, typically in encrypted form. The SSI standards discourage storing personal data on blockchains, and the industry has established several principles against it.

Can I prevent someone from correlating my information from different sites to find out more about me?

Yes. Once you create a "public DID," you create "pseudonymous DIDs" whenever you establish a new online relationship (such as a new login). Pseudonymous DIDs cannot be correlated by others to your public DID without your involvement (and rarely need to be). See decentralized identifier (DID) and internet standard Universally Unique Identifiers (UUIDs).

Can I revoke an SSI distributed ID?

Yes. A decentralized ID is turned off by invalidated the data that the DID points to.

Can someone publish something permanently about me on an SSI blockchain?

No. Blockchains are "immutable," meaning data published there are never erased. However, the only things published on SSI blockchains are DIDs, encryption keys (not *decryption keys*), and pointers to outside data (which can be erased or changed). The DID specification states that the user/owner explicitly controls and administers the publishing of their decentralized IDs (this is actually the meaning of the phrase "self-sovereign ID." The proposed Verifiable Credentials specification states plainly that SSI credentials are revocable, expirable, and that an SSI network must enforce the data policies of both the issuer and holder. Existing SSI networks require an ID holder to approve before sharing an ID. This means that a competitor, who would not be trusted to make a claim about your business, could not append a negative claim about your business without your explicit approval. This is because both the issuer and holder both have the ability to revoke any claim.

When I use a DID with a provider, is my personal information exchanged?

If the DID is a new pseudonymous DID (easy to create from your public DID), the answer is "No." Furthermore, the SSI industry encourages applications to uses something called "Zero Knowledge Proofs" to limit the amount of information shared. For example, when you assure a bartender that you can legally drink, you typically show a drivers license and reveal your birthdate. With most SSI networks, an identity supplier that knows your birthdate can reveal your legal drinking status without sharing your birthdate.

How does SSI protect my privacy?

The SSI industry promotes the use of pseudonymoius IDs and encourages *Selective Disclosure* (or the Principle of Minimum Disclosure) to keep your personal data secure and private. Those practices also improve compliance with privacy regulations like HIPAA (Health Insurance Portability and Accountability Act) in the US and GDPR (Global Data Protection Regulation) in the EU. With SSI networks, users control their personally identifiable data and data privacy at levels they've never experienced before.