UNIVERSITY OF ARKANSAS | Sam M. Walton College of Business
Blockchain Center of Excellence

Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK National Health Service (NHS)

By Mary Lacity and Erran Carmel

BCoE Whitepaper | 2022-01

Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK NHS

Mary Lacity
Walton Professor and director of the Blockchain Center of Excellence, University of Arkansas

Erran Carmel
Professor of Information Technology, American University

Abstract:

Self-sovereign identity (SSI) is an idea, a movement, and a decentralized approach for establishing trust online. Many standards-making bodies, open-source working groups, and organizations have been working on SSI and verifiable credentials for years. Although production-ready solutions remain in the developmental stage, business executives, professionals, and students need to start learning about what's ahead. Business practitioners want to know what is unique about SSI. Is there anything idiosyncratic about managing an SSI project compared to other digital projects? How can we apply SSI to deliver business value? We help to answer those questions by explaining SSI through a case study at UK National Health Service (NHS). NHS developed a digital staff passport to verify health professionals' qualifications and credentials so that healthcare staff could be moved around quickly during COVID-19. While SSI provides some unique capabilities, it does not require unique project-management practices. Like all digital projects, the aim was to build capabilities and design for interoperability to avoid vendor lock-in. Building on its early success, NHS intends to expand the application to enable its strategic people plan.

Keywords: Self-sovereign identity (SSI), verifiable credentials, Trust over IP, decentralized identifiers, National Health Service (NHS)

Introduction

Self-Sovereign Identity (SSI) is an idea, a movement, and a decentralized approach for verifying credentials in online relationships.[1] SSI aims to empower individuals to possess and control digital proofs of their credentials; thus, the term "self-sovereign."

Many standards-making bodies, open-source working groups, and organizations are working on SSI and verifiable credentials standards and protocols (see Appendix B). Overall, the communities agree on the principles of user control, decentralization, data privacy and security, availability for all, interoperability across platforms, data minimization so that holders share the minimum amount of information required for

[1] Firstly, we clarify the term "**identity.**" Scholars from the many disciplines, such as philosophy, ethics, psychology, and sociology, consider identity to be an inalienable human right, a psychological construct defined by self, and/or a social construct defined by one's social groups. From these perspectives, governments and organizations do not provide individuals with identities, but with credentials. A better labeling of the SSI movement, in our opinion, is "self-sovereign *credentials*" (or, to be more accurate, "self-sovereign *verifiable credentials"),* but alas, SSI is the entrenched term, and we shall proceed with that nomenclature.

verification, and transparency about data creation, collection, storage, and usage (Lacity and Carmel, 2022). As one specific example, the Trust over IP Foundation's 12 guiding principles are provided in Figure 1.

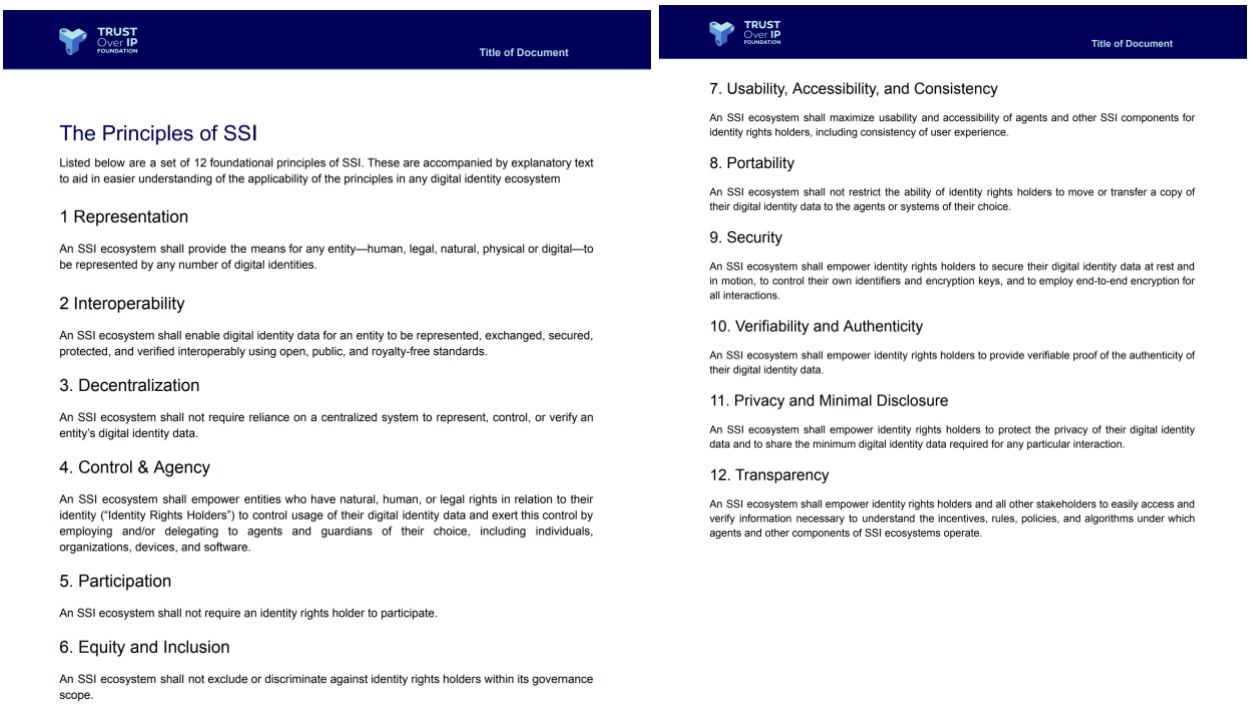


Figure 1: An example of SSI Principles by the Trust Over IP Foundation (2020)

Image credit: https://trustoverip.org/wp-content/uploads/2021/10/ToIP-Principles-of-SSI.pdf

SSI aims to provide a way for more people who lack identities to prove their residency, skills, and experiences. It offers a new way to prevent hackers from stealing credentials (i.e., identity theft). SSI replaces usernames and passwords with peer-to-peer relationships and provides verification of credentials within seconds (Preukschat and Reed, 2021).

The global SSI community has been working on SSI for years and the time is ripe for non-specialists to learn what's ahead. While many SSI resources exist to educate the market, we aim to educate business practitioners (managers and students). Business practitioners want to know what is the same, what is unique, and what is provocative about SSI compared to what they currently use. They want to know if there is anything idiosyncratic about managing an SSI project compared to other digital projects. They rightly ask how SSI might be applied to deliver business value (Lacity et al., 2021). We help to answer those questions by explaining SSI through an example of a first-generation application. The application is used by UK National Health Service (NHS) to verify healthcare staff's qualifications and credentials. The solution was a finalist for the prestigious *Health Service Journal* (HSJ) 2021 award for connecting services and information (HSJ, 2021).

SSI in action at NHS: The digital staff passport for healthcare professionals

In this case history based on interviews with the suppliers, NHS documents, and NHS presentations, we describe the overview of the staff movement problem at NHS, the vision for a digital staff passport solution, how the solution maps to the four roles of the trust diamond, the implementation journey, outcomes thus far, and future plans.

Overview of the staff movement problem

The year is 2019. The National Health Service (NHS), the government healthcare system in the United Kingdom (UK), is working with a number of stakeholders to solve the problem of processing staff transfers. More than 1,200 NHS hospitals employ more than 1.1 million people (NHS Digital, 2021). Every time staff members move from one hospital to another, all of their credentials must be re-verified because NHS hospital systems operate independently and manage their own human resources (HR). Staff must fill in multiple forms to prove their identity, credentials, and prior employment, and nearly half are required to travel to complete the onboarding process in person. Moreover, staff often retake training unnecessarily because they cannot prove their existing credentials. Onboarding also entails security clearances and authorizations to access data required for the new position, which often take days to complete.

Given that NHS frequently ranks among the five largest employers worldwide, the scale of the problem is huge (Alexander, 2012). NHS onboards or moves staff more than 1 million times per year. Junior doctors, for example, move an average of 10 times during training. More than 100,000 person-days are spent each year verifying junior doctors. The lost hours are worth about £22 million; more importantly, doctors are not caring for patients while waiting for their credentials to be verified (*The Independent*, 2021; NHS, 2021).

The vision: digital staff passports

In 2019, NHS developed a vision to "enable staff to more easily move from one NHS employer to another" (NHS, 2019). The solution would rely on a digital staff passport to share HR records, as well as statutory and mandatory records. Staff members would carry their credentials on their smartphones and control who might see them. The vision outlined the following ambitions:

- All staff would have access to a digital staff passport.
- All workforce (HR) systems would be interoperable.
- All staff would be able to easily and securely log into clinical/workforce systems.
- All staff would experience a more efficient and focused induction, recognizing previous training and experience.

NHS envisioned that, in the long term, a staff member's digital wallet would aggregate and hold multiple credentials. It foresaw a solution that is "future proof," based on open standards and open software for interoperability, thereby avoiding vendor lock-in. For example, NHS sought to avoid requiring staff to buy a specific phone or to rely exclusively on one vendor's digital wallet. For these reasons, NHS became

interested in SSI and adopted WC3's verifiable credential standard[2] for the digital representation of physical credentials and OpenID Connect standards for online identification.[3]

As an architecture model, SSI aims to automate the four relationships in the "trust diamond."

The Trust Diamond

The trust diamond comprises four roles involved with creating and verifying credentials: issuers, holders, verifiers, and governing authorities (see Figure 2).

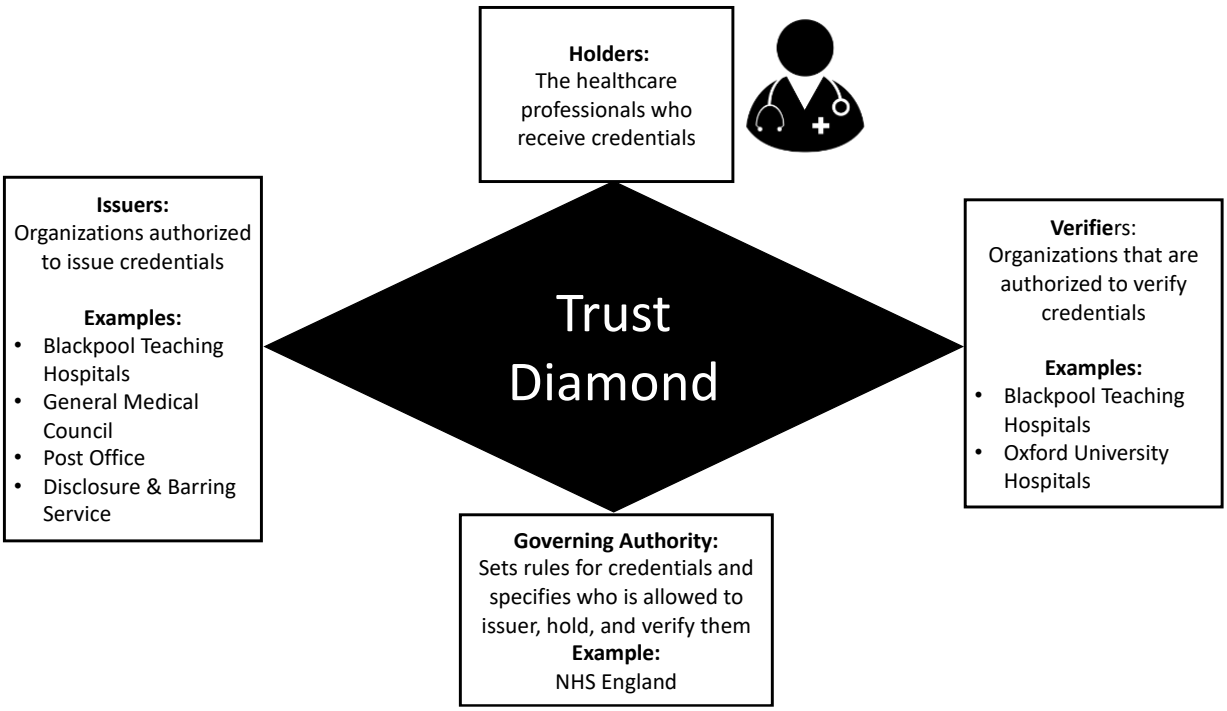


Figure 2: The trust diamond for the digital staff passport application

The **governing authorities** set rules in the ecosystem by specifying the types of credentials allowed/required in the ecosystem and by specifying who is allowed to issue, hold, and verify credentials. In our case study, NHS England is the primary governing authority. NHS requires various credentials for a doctor to work in its hospitals, such as a nationally recognized proof of identity (e.g., passport), a General Medical Council (GMC) professional registration license, specific medical certifications (e.g., advanced

[2] The W3C was founded in 1994 by Tim Berners-Lee, inventor of the World Wide Web. W3C oversees W3C/IETF standards for the Internet protocol suite; communities include the Decentralized Identifier Working Group and the Verifiable Credentials Working Group. The Verifiable Credentials Data Model is available at: https://www.w3.org/TR/vc-data-model/

[3] OpenID Connect allows verification of user identity based on the authentication performed by an Authorization Server, as well as to obtain the user's basic profile information in an interoperable. See: https://openid.net/connect/

life support, infectious disease), a Disclosure and Barring Service (DBS) criminal-background check, and prior employment credentials. The doctors (and other healthcare professionals) are the **holders** of the credentials. In Figure 2, Blackpool Teaching Hospitals, GMC, the Post Office, and DBS serve as **issuers** of credentials, but the hospitals become **verifiers** when a healthcare professional begins work at their facility. Again, each hospital needs to verify credentials before onboarding any new employee, even for staff who have worked at other NHS hospitals.

Development and implementation of the digital staff passport

NHS convened a minimal viable ecosystem (MVE) to build the pilot solution. The MVE comprised NHS England, NHSX[4], General Medical Council (GMC), NHS trusts (e.g., Blackpool Teaching Hospitals NHS Foundation Trust) and technology providers Accenture, IBM, Oracle, Microsoft, Evernym[5], and Truu (Evernym, 2021b). The technology providers worked on different parts of the pilot solution. For example, Evernym and Truu built the digital wallet, while Microsoft provides the Azure-based cloud service (Microsoft, 2021).

The MVE spent nine months documenting the before-and-after processes (Evernym, 2021b). The 2019 NHSX pilot was ready just before COVID-19 hit, but the pandemic increased the urgency to onboard staff, thereby accelerating the rollout. NHS anticipated that staff mobility needs would escalate because of COVID-19, and that many new facilities with intensive-care beds and ventilators would be erected.

The production version, referred to as the COVID-19 Digital Staff Passport[6] (DSP), commenced rollout in early summer 2020. The solution comprises many component parts, such as interfaces to HR systems, but in this paper, we focus on the edge technologies comprising the digital wallets and how they combine to automate the trust diamond.

The solution makes use of **decentralized identifiers (DIDs),** DID documents, and DID methods (Appendix A provides an overview of SSI concepts and technologies for interested readers). Concerning the DID method, the NHS solution uses the Sovrin Network, where authorized parties can verify digital credentials by querying the public **distributed ledger[7]** without needing a trusted third party. The nonprofit Sovrin Foundation manages the Sovrin Network, providing support for the network's open-source governance, operations, and community engagement. As of fall 2021, the Sovrin Foundation had authorized more than 80 independent volunteers across six continents to operate the Sovrin Network's nodes.[8]

To set up the application, NHS England, serving as the governing authority, made the first entry on the Sovrin Network to publicize its public key and the data schema it accepts as a verifiable credential. NHS used emails and meetings to inform HR directors within its network of the opportunity to adopt the digital

[4] The NHSX is a joint unit between the UK Department of Health and Social Care, NHS England, and NHS Improvement.
[5] Avast acquired Evernym in December 2021, but since our case history precedes that date, we use the name Evernym throughout.
[6] The COVID-19 Digital Staff Passport was named for *why* it was deployed, i.e., to quickly verify skills and credentials during the pandemic; it did not capture or track COVID-19 immunization status.
[7] Distributed ledger: a time-stamped, permanent record of all valid transactions that have occurred within a given digital network. Each node of the network has an identical copy; no node is in charge. A smart contract stores and executes rules agreed upon by trading partners on when and how to update the trust registry (Lacity, 2020).
[8] See https://sovrin.org/annual-reports/

staff passport. HR personnel sign up for training, watch videos, and attend live virtual support sessions. NHS also keeps an updated website for NHS employers[9] and staff (NHS Digital Staff Passport, 2021).[10]

Each hospital that joins posts its public key to the trust registry on the Sovrin Network. When a hospital is in the role of an *issuer* of a verifiable credential, the hospital's app uses the NHS England data schema to format the credential and signs the digital credential with the hospital's private key. When a hospital is in the role of *verifier* of a credential, its app looks up the public key on the Sovrin Network to make sure the credential was signed by an authorized issuer. Thus, the Sovrin Network serves as the **public key infrastructure (PKI)**[11] for the app. As of January 2022, 102 NHS hospitals had registered to use the system, which represented 43 percent of NHS England hospitals.[12]

On the *holder* side, only existing NHS staff members are eligible and adoption is voluntary at this point. For the initial launch, HR personnel were the primary communication channel to make staff aware of the new application. HR personnel encourage staff to use the app as part of the transfer process. Since HR is involved in all staff transfers, they have an opportunity to ask staff members, "Would you like to try a new digital onboarding process that takes only a few minutes, or do you prefer the old manual process which takes a couple of days?" HR also explains the additional benefits, such as carrying all required credentials in one convenient place on their phones, providing backup and recovery of their credentials in case their phone is lost or damaged, and controlling who sees their credentials (NHS Digital Staff Passport, 2021).

The simple process for staff to join entails downloading Evernym's Connect.Me SSI digital wallet app from Apple or Google. The first step is **identity binding**, which ensures that credentials are created for the correct employee. This initial step is performed by HR in person or on a video call. An HR staffer retrieves information from the employee database (which is why the app is only offered initially to existing staff), including a photo of the staff member, to perform identity binding. Once the staff member's identity is confirmed, HR sends a QR code to the staff member to request a peer-to-peer connection between the hospital and the staff member. The QR code includes the hospital's public key and connection invitation. (One can think of the QR code as a sort of public email address and email invite for this hospital.) When the staff member scans the QR code, a unique and private peer-to-peer connection is established inside each side's SSI wallet. Next, HR sends all of the staff member's verifiable credentials to the staff member's wallet, including a hash of their photo. Once again, the staff member must accept the credentials before they are added.[13] Staff can reject a credential if it is incorrect, and HR can reissue a correct one. As of fall 2021, NHS did not disclose the number of doctors and staff using the app, but many of the initial adopters were healthcare staff from the armed forces deployed to deal with COVID-19 (BBC, 2020).
NHS established a support center to assist passport adopters with any questions, concerns, or issues through its business services organization. The center provides three tiers of support. The most frequent issues are minor connection problems, such as a lack of cellphone service coverage in some areas of a hospital.

[9] See https://beta.staffpassports.nhs.uk/employers/
[10] See https://beta.staffpassports.nhs.uk/staff/
[11] A public key infrastructure (PKI) is the foundation for securing exchange of data within a network in which some of the parties cannot be trusted – which is always the case. The "public key" is like an email address that you may share broadly, and the "private key" is like a password that is kept secret.
[12] For a list of participating hospitals, see https://beta.staffpassports.nhs.uk/registered-organisations
[13] Unlike cryptocurrency wallets, where a sender can air drop cryptocurrency into someone's digital wallet without the holder's permission, holders are in complete control of who they connect with and what data goes into their SSI digital wallets.

Outcomes from the COVID-19 digital staff passport

As of November 2021, NHS summarized the positive experience to date, including the following benefits:

- **Staff control:** Staff control their own digital identity, employment checks, credentials, and core skills training.
- **Staff empowerment:** Staff are empowered at every step to accept, reject, and share information.
- **Transparency:** Staff know who has seen their information and for what purpose, ensuring their privacy and security.
- **Single sources of truth:** One verifiable credential is issued and is interoperable, reducing duplication.
- **Time savings:** Instead of spending days to onboard, the process takes only a few minutes.
- **Valid data:** Verifiers now have a machine-readable way to automatically verify holders' claims.
- **Better healthcare services:** Healthcare providers more quickly get to the core business of caring for patients.

Future plans for a strategic NHS digital staff passport

For the first production system, the application was a "one size fits all" model for the temporary movement of staff. Whereas the initial adoption focused on armed forces, junior doctors are being prioritized going forward because of the number of times they move (Department of Health & Social Care, 2020). Future releases also will cater to the needs of different categories of staff movements, including permanent moves and "bank" workers, which are freelance healthcare providers called upon to cover shifts or holidays (see Figure 3). The solution will also extend to using the digital staff passports to access systems like primary care systems, email, and NHS digital services.

For the first phase of the application, NHS hospitals operate on a property of **transitive trust**. If Hospital A has verified that a doctor has a GMC professional registration license, it issues the doctor a verifiable credential of that license. Other hospitals in the network can use that verification as proof that the doctor is licensed. In future releases, the ecosystem will expand to include the GMC, Post Office, DBS, immunization providers, and other issuers; however, adding more training credentials will require the integration of more than thirty training systems. NHS also plans to adopt multiple wallets to prevent vendor lock-in and to expand identity binding to include biometrics.

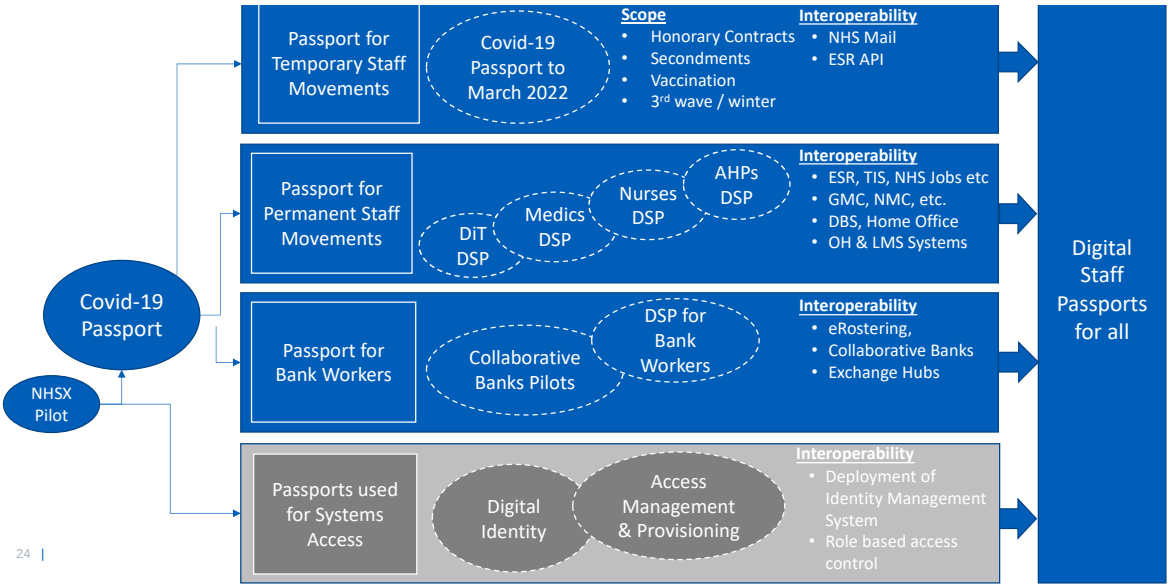


Figure 3: Roadmap for the digital staff passport
Source: NHS presentation at Identity Week (2021)

Lessons learned

Business practitioners want to know SSI's unique features, whether there is anything idiosyncratic about managing an SSI project compared to other digital projects, and if SSI can deliver business value. The first generation of the NHS digital staff passport helps to answer these questions.

SSI's unique capabilities

SSI's decentralized architecture is different from traditional centralized systems. First, the connections of the ecosystem players (issuers, holders, and verifiers) are peer to peer; each side has equal power over a relationship; both sides must agree they want to be connected; and either side can terminate the connection at any time. One profound implication of SSI is that ***connections are peer to peer and are no longer managed by log-on IDs and passwords!*** No trusted third party, central power, or centralized database controls the relationship.

At NHS, connection requests use QR codes to perform "challenge-response" verification, such as issuing and proving credentials using OpenID Connect standards.[14] Holders decide whether to accept connection requests, whether to allow their digital credentials to be loaded in their wallets, and what and with whom to share their credentials.

[14] https://openid.net/connect/

Second, ***SSI uses a decentralized public key infrastructure (PKI),*** which also does not rely on trusted third parties. More than 100 decentralized PKI networks are under development.[15] In the NHS example, the trust registry is operated by Sovrin Network, an open-source network to manage identities (see Figure 4).

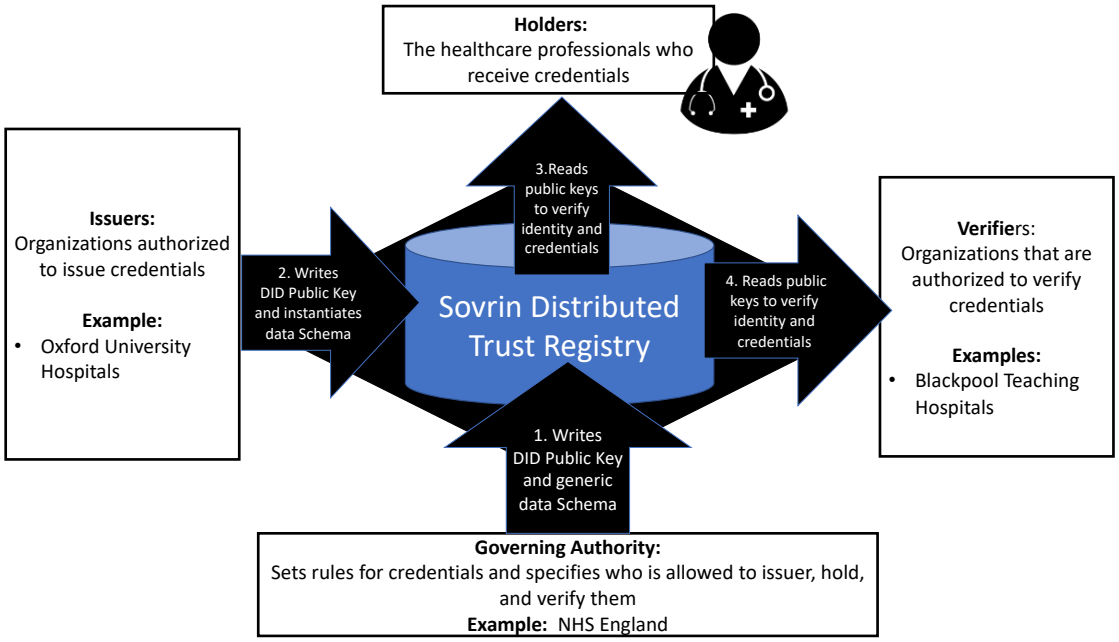


Figure 4: Sovrin Network's trust registry: NHS Example

Very little information is written to a public trust registry. The governing authority and each issuer write ONE TIME to post their public keys and VC formats (data schema) on the network. All credentials are created and stored at the edges; verifiable credentials are NOT stored on the public trust registry, which enhances privacy and scalability.

The private key for the decentralized identifier, called a DID[16], is stored on the SSI digital wallet (or in a cloud agent). For the governing authorities and issuers, the public key for the decentralized identifier is stored on Sovrin Network's distributed ledger. This way, any participant can query the Sovrin Network to verify a digital signature—i.e., that only the owner of the private key could have issued the credential.[17]

[15] The W3C keeps a list of methods under development. See https://www.w3.org/TR/did-spec-registries/

[16] According to the W3C (2020), "DIDs are designed to enable individuals and organizations to generate their own identifiers using systems they trust. These new identifiers enable entities to prove control over them by authenticating cryptographic proofs, such as digital signatures. Since the generation and assertion of decentralized identifiers is entity-controlled, each entity can have as many DIDs as necessary to maintain their desired separation of identities, personas, and interactions."

[17] For example, to look up the public keys for participating NHS hospitals, one may look at a Sovrin Network Explorer for schema name NHS-X COVID-19 EO: https://indyscan.io/txs/SOVRIN_MAINNET/domain?page=1&pageSize=50&filterTxNames=[]&sortFromRecent=true&search=C19EOJobRole

It's important to note what is NOT stored on a public ledger. **Holders do not need to post public keys to the ledger.** Peer connections are not stored on the ledger, but are managed on edge devices. Issuers do not post verifiable credentials to the ledger, as these, too, are held locally. SSI is thus a very lightweight use of distributed ledger/blockchain technologies because the only things stored on the ledger are public keys for issuers, governing authorities, and possibly verifiers.

As far as the costs, the Sovrin Network only charges a one-time fee of $10 to register a public key and $25 to post a data schema for the format of credentials. Posting to the network only happens once, and then an unlimited number of credentials can be generated on the edges and verified with the public key on the trust registry. Reading the network to verify a signature is free and happens in seconds. This is how SSI scales. Andrew Tobin, managing director EMEA for Evernym, said: "SSI has a huge scale advantage because all of the transactions happen at the edge. When an issuer issues a credential, it is not writing anything to any ledger; it all happens peer to peer. This is what makes the whole protocol really elegant: the setup is done once and then you can create a billion credentials without ever having to write to a ledger."

Managing an SSI project

One of the NHS project managers—Phil Graham, digital program director at Blackpool Teaching Hospitals—spoke at a November 2021 event about this project. According to him, there hadn't been anything idiosyncratic about managing the SSI project compared to other digital projects. The usual digital project management issues were present: stakeholder buy-in, information governance, change management, working with suppliers, mitigating risks, and testing the technology (Graham, 2021a).

Graham noted that in terms of stakeholder buy-in, nontechnical people do not need to understand the underlying architecture, but rather what it enables. He explained that with users, "We don't need to use the b-word (blockchain)." The main part of communications is to emphasize enabling staff movement and credentials. Stakeholders do need to understand that their data is safe, which is why significant effort was devoted to information governance. Governance specifies where data will be stored and who is authorized to read or process it. Change management was also demanding because NHS was moving quickly from paper-based frameworks to digital passports. Many people like to carry their own paper credentials and need to see the benefits of digital versions, i.e., the relative advantage. NHS decided it was best to make adoption voluntary (Graham, 2021a). Overall, the trialability, compatibility, observability, and simplicity of the digital staff passport solution are well-established attributes of any innovation designed to spur adoption (see Figure 5).

Innovation Attribute	Description	Effect on Adoption Rate
Relative Advantage	"The degree to which an innovation is perceived as better than an idea it supersedes." The innovation may be better economically, functionally, or socially.	
Trialability	"The degree to which an innovation may be experimented with on a limited basis." Trialability reduces uncertainty.	
Compatibility	"The degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters."	
Observability	"The degree to which the results of an innovation are visible to others."	
Complexity	"The degree to which an innovation is perceived as difficult to understand and use." The more complex the solution, the slower it will be adopted.	

Figure 5. Five attributes of innovations
Source: Adapted from Rogers (2006)

As far as the IT staff, distributed ledgers and blockchains are more widely known and accepted now than a few years ago. The IT staff vetted the technology. NHS' Graham said, "We've been trying to break the technology. As a mathematician by training, I am looking to prove something by exception. If it doesn't work for one, it won't work for all. So far, we cannot break it." (Graham, 2021a)

Based on the NHS case, the overall advice to executives is to ***build capability, not product.*** Designs should be "future-proofed" by adopting open standards and open software to avoid vendor lock-in.

The business value of SSI

No matter how intriguing the innovation, ***organizations will only adopt SSI if the business benefits exceed the costs and risks.*** We've already covered some of the benefits of the NHS digital staff passport. The specific benefits for NHS hospitals are:

- **Reduced administrative activity:** e.g., eliminates the need for honorary contracts[18], secondment agreements, or letters of access/authority
- **Eliminates the need to request or respond to employment check data requests** when releasing or receiving staff temporarily
- **Eliminates the need to repeat employment checks**
- **Speeds up onboarding process** for HR teams and staff
- **Delivers rapid, safe, and secure staff movement** to respond to clinical need
- **Lowers costs and improves patient care** by releasing and receiving skilled staff quickly

[18] An honorary contract holder is someone who is not directly employed and paid by NHS—i.e., a person working through a third party (https://www.ouh.nhs.uk/working-for-us/sectors/honorary-contracts/)

- **Increases flexibility:** Where organizations are part of a clinical network, the passport enables network staff to move and work across a number of organizations to deliver either planned or emergency clinical care.[19]

The business will incur costs to build internal SSI capabilities, develop or buy SSI applications, operate the application, and manage change, including educating employees, customers, or other target users. NHS has not reported publicly on the project's return on investment (ROI). What is known is that the pilot project and COVID-19 version were not expensive. The technology providers charged nominal fees because they were learning alongside NHS.

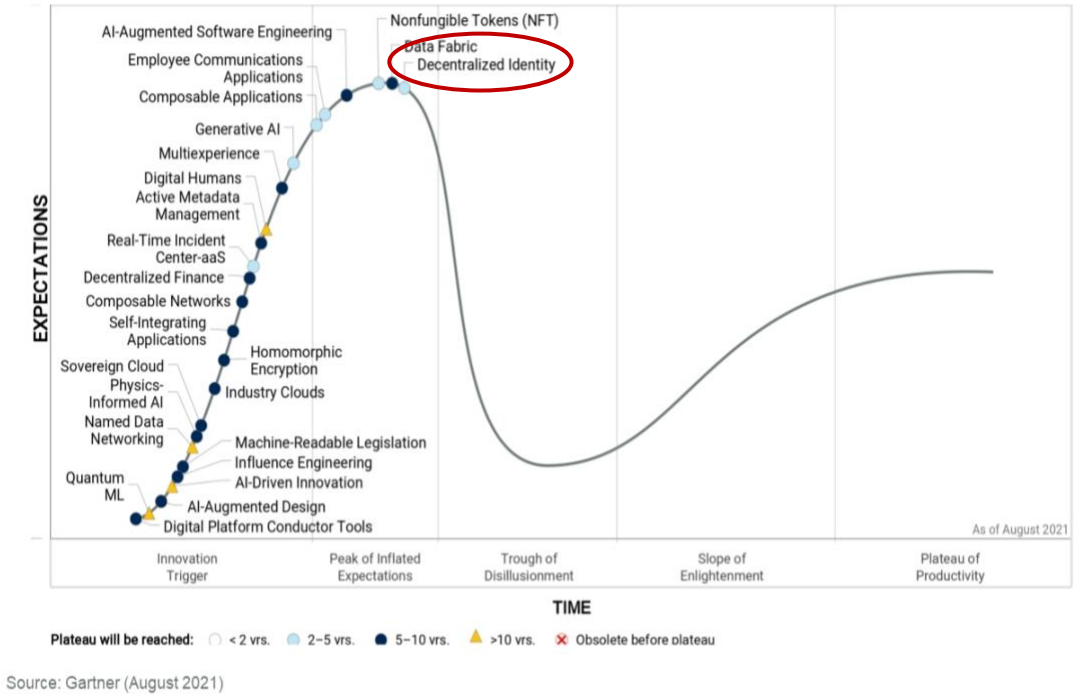
Businesses will face additional risks, such as relying on shared governance models for public trust registries. For example, businesses can sue trusted third parties, but not a dispersed community of node operators. At this stage, we do not have details about the costs and risks of early adoptions to illuminate the full picture of a typical business case. We intend to study more early production systems to answer what SSI means more fully for business.

How mature is SSI technology today?

As far as <u>when</u> SSI might be widely adopted, we are still in the early days. The W3C standard for verifiable credentials 1.0 was passed in 2019, and the standard for DIDs, as of fall 2021, had not been ratified. As of August 2021, Gartner placed "decentralized identity" at the top of the "peak of inflated expectations" (see Figure 6). During this phase, a few early successes garner attention, such as the NHS Digital Staff Passport. Senior executives start to take notice and tend to view the technology as a silver bullet—i.e., something that promises to instantly solve a long-standing problem. Many organizations start testing the technology, but some will enter the trough of disillusionment phase when instant success is not achieved. It's hard work to get value from a new innovation. As time passes, organizations build capabilities, upgraded versions of the technology are released, the market producers consolidate, and organizational consumers learn how to gain value from the innovations (Lacity, 2020b). Gartner anticipates this will happen between 2023 and 2026.

We make two points about the hype cycle depicted in Figure 6. First, it is useful for discussing overall global trends, but industries and specific organizations within industries adopt technologies at different rates. Besides NHS, other organizations have already developed applications for travel, healthcare, food supply chains, and business licenses (e.g., the IATA Travel Pass; the Canadian government's business licenses; TruWest Credit Union; and Farmer Connect). Second, the pace of adoption is not deterministic; individuals and organizations do not just sit around and wait for the future, but actively create it. This is why we encourage business professionals and students to start learning about SSI now. Appendix B explains how to get involved in communities working on decentralized identity and verifiable credentials.

[19] https://beta.staffpassports.nhs.uk/



Source: Gartner (August 2021)

Figure 6: Maturity of Decentralized Identity as of August 2021

Image credit: https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/v2-hc-emerging-tech-2021.png

Appendix A: SSI concepts and technologies

The *vision* for SSI is relatively simple, but understanding how SSI works requires exposure to new concepts and technologies. The SSI space is laden with new vocabulary, such as "decentralized identifiers," "DID documents," "trust registries," "DID methods," and "verifiable credentials." In this appendix, we explain the terminology.

Decentralized Identifiers

A decentralized identity model needs decentralized identifiers. In our NHS example, each hospital controls its own unique identifiers so that members of the ecosystem can recognize each other online. Multiple decentralized identifiers per holder are used to enhance privacy. For example, a healthcare professional's wallet creates a new decentralized identifier for each relationship she has with a hospital.

While many decentralized identifiers have been considered, SSI standards are coalescing around one called **Decentralized Identifiers (DIDs)**. According to the W3C (2020), "DIDs are designed to enable individuals and organizations to generate their own identifiers using systems they trust. These new identifiers enable entities to prove control over them by authenticating cryptographic proofs such as digital signatures. Since the generation and assertion of decentralized identifiers are entity-controlled, each entity can have as many DIDs as necessary to maintain their desired separation of identities, personas, and interactions." This last point is vital; unlike a Social Security number that leaves a digital trail everywhere it is used, a new DID will be generated for each connection. We anticipate that everyone will have thousands of DIDs to enhance their privacy. But unlike accounts and passwords, we will not have to create or remember them, as those are functions of SSI wallets. Well-designed SSI wallets will also include backup and recovery features, so that in theory, we'll never have to worry about losing our digital wallets (Preukschat and Reed, 2021).

A W3C standard DID has three data fields (see Figure 7). The first is always the three letters "did," just as the first data field for websites is "www." The DID method is the second data field, which indicates the method for creating, reading, updating, and deleting (CRUD) a DID. The third field is a completely unique number that is controlled by private-public key pairs, much like Bitcoin addresses. Only the holder of the private key can control CRUD functions.

Figure 7: Decentralized Identifier (DID) Format

Image credit: From https://www.w3.org/TR/did-core/

The power of the SSI model is that anything that needs a credential can have a DID, including a person, a group, an organization, an animal, a physical thing, a digital thing, or a logical thing (Trust Over IP, 2021).

DID document

The DID itself is just a large number, so it's not very useful on its own. However, every DID is matched to its single and unique **DID document**. It's the same concept as resolving a unique web address to a unique IP address. (For example, the webpage www.blockchain.uark.edu resolves to the IP address of the server where the University of Arkansas hosts the Blockchain Center of Excellence's web page.)

Although the term "document" suggests something that humans can read, the DID document is, in fact, machine-readable code. It's designed to be consumed by a specific SSI application, like the NHS example. A DID document contains metadata about the subject. Figure 8 shows a very simple DID document that contains the DID number so that the application can find the DID document and a public key the application can use for verification. In reality, DID documents could contain many other data elements.

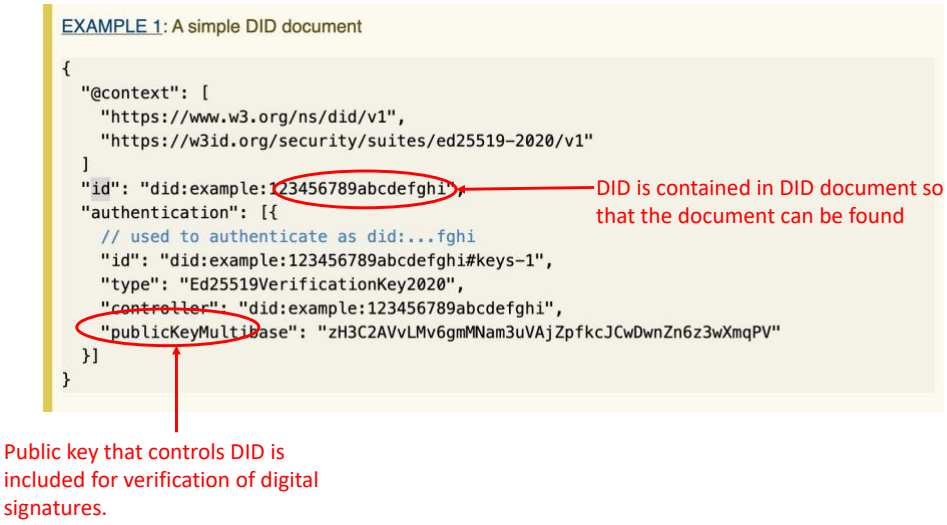


Figure 8: A simple DID Document
Image credit: Adapted from https://www.w3.org/TR/did-core/

How does an application find the document? Most public keys are stored on a public trust registry.

Trust registries and DID methods

Before explaining SSI trust registries and DID methods, it's useful to review how pre-SSI registries work. The Internet's domain names (e.g., blockchain.uark.edu), IP addresses (e.g., 172.16.254.1), and public keys used for encryption and verification are managed by trusted third parties, including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Assigned Numbers Authority (IANA), and certificate providers like IdenTrust, Digicert, and GoDaddy. In contrast, decentralized identifiers do not

rely on any centralized organization. Instead, the public key infrastructure is provided by public **trust registries** that are managed by incentivized communities. But which trust registry? The second data field in the DID, namely the **DID method**, indicates where and how DIDs and DID documents can be retrieved. To refine our definition from above, the DID method indicates the method for creating, reading, updating, and deleting (CRUD) a DID and a DID document.

In the NHS digital staff passport example, the trust registry is managed by the Sovrin Network. The Sovrin Network's DID method is called "did.sov" (see Figure 9). The private key for the DID is stored locally on the SSI digital wallet (or in a cloud agent). The public key for the DID number is stored on the Sovrin Network's distributed ledger. This way, any participant can query the Sovrin Network to verify a digital signature that only the owner of the private key could have issued.

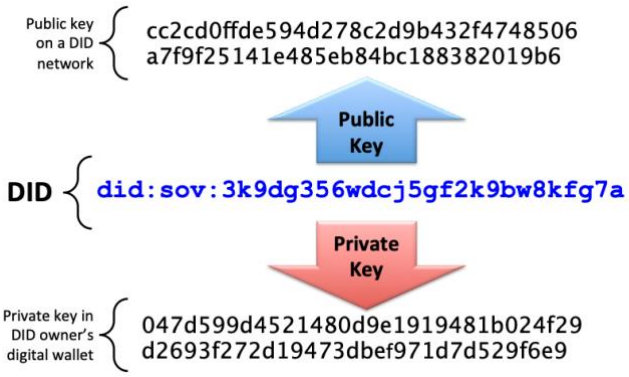


Figure 9: An example of a DID that uses the Sovrin Network ("sov")
Image credit: Preukschat and Reed, 2021

The Sovrin Network setup is quite simple. Returning to the NHS example, NHS England, serving as the governing authority, made the first entry on the Sovrin Network. It posted the public key of its unique DID to the trust registry on that network. Anyone can look up the DID document associated with NHS England's public key. In addition, NHS England posted its generic verifiable credentials schema, which specifies the data elements to be contained in a credential.

Next, a hospital registers by posting its public key and a signed version of the data schema to the Sovrin Network. NHS England maintains a registry of all legitimate hospital public DIDs. When any staff member gets a request to connect to a hospital, the wallet pings the Sovrin Network to make sure it's a legitimate hospital. When any verifier receives a proof of credential from a staff member, the system pings the Sovrin Network to make sure the issuer is authorized and that it used its private key to sign the credential.

Besides the Sovrin Network's DID method, W3C tracks more than one hundred DID methods under development.[20] Many DID methods use distributed ledgers as the trust registry. Some DID methods use public blockchains like Bitcoin and Ethereum, while others use private blockchains like Hyperledger Indy and Corda. Some DID methods do not rely on blockchains at all, but on a trusted community, such as

[20] W3C's list of DID methods: https://www.w3.org/TR/did-spec-registries/

Github. The diversity of methods demonstrates the widespread interest and commitment to DIDs. However, we anticipate that the market will coalesce around a few DID methods.

Now that we have defined the major attributes of DIDs, we can appreciate their four properties (Evernym, 2019):

1. **Persistence.** Unlike log-on IDs, email addresses, or URLs, no one else has the power to revoke someone's DID. Once an individual, organization, or other entity creates a DID (via an SSI app), the owner or custodian may continue to use it permanently or delete it as per their choice.

2. **Resolvable.** Again, just as a URL resolves to one and only one IP Address, a DID resolves exclusively to one DID document, meaning one can find meta data associated with the DID.

3. **Cryptographically verifiable.** A DID is cryptographically verifiable; whoever controls the private key is considered to be the legitimate owner of the DID. Verifiers can look up the issuer's public key to verify that only the issuer could have created the DID document.

4. **Decentralized.** A DID is decentralized; no trusted third-party registration authority is required. With SSI, a centralized public key infrastructure (PKI) is replaced with a decentralized PKI, as indicated by the DID method.

Drummond Reed, chief trust officer for Evernym (now Avast), said: "The reason there is so much excitement about DIDs is that there's never been an identifier in history that does all four of those things." (Evernym, 2019)

However, there is one type of method that posts NOTHING on a trust registry; it is used for peer-to-peer connections.

Peer DID

A peer DID is managed locally; no public keys are stored on a trust registry because they are not needed. Peer-to-peer connections are like establishing a dial tone on a telephone.

W3C posted the peer DID method, specified as "did.peer." Peer DIDs create the conditions for people to have full control over their side of digital relationships. According to W3C, peer DIDs offer these advantages (https://identity.foundation/peer-did-method-spec/index.html):

- Peer DIDs have no transaction costs, making them essentially free to create, store, and maintain.
- Peer DIDs scale and perform entirely as a function of participants, not with any central system's capacity.
- Because peer DIDs do not exist in any central system, there is no trove to protect.
- The connections are private, known only to the parties in the relationship.

- Because peer DIDs are not beholden to any particular blockchain, they have minimal political or technical baggage.

Again, Peer DIDs have this profound implication: online relationships are no longer managed by log-on IDs and passwords!

Verifiable credentials

DIDs are just the identifiers. They are important because they enable verifiable credentials. We have defined the term "credential" as an attestation made by an issuer about a holder. The term "verifiable credential" is a special type of credential that is machine-verifiable. More formally, W3C defines a **verifiable credential** as "a tamper-evident credential that has authorship that can be cryptographically verified." A verifiable credential contains meta data, claims made by an issuer about the subject, and proof that the issuer generated the credential (see Figure 10). DIDs are embedded in the VC to identify the subject, to uniquely identify the credential, and to verify the issuer's signature.

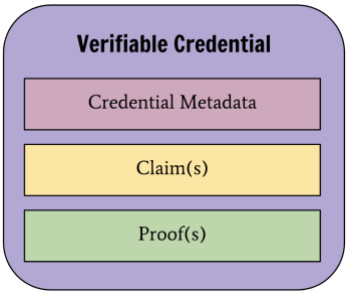


Figure 10: Parts of a verifiable credential
Image credit: https://www.w3.org/TR/vc-data-model/

A university issuing an alumni credential provides a basic example of a verifiable credential (see Figure 11). In this example, we'll call the alumna Mary. Mary provided her alma mater one of her DIDs via her SSI wallet when the university asked to connect with her. The university created the alumni credential for Mary, and it has the power to revoke her status in the future. (For example, if she fails to pay a parking ticket while attending a tennis match on campus.) Thus, the university controls the contents of the credential, but Mary controls which verifiers are allowed to read her credential (if the SSI application follows SSI principles).

We note that the example is overly simplistic. Many verifiable credentials have multiple attributes, and each attribute must be signed by the issuer so that the holder can selectively display proofs to verifiers. Moreover, community standards are evolving around the notion of enhancing privacy even further by using **zero-knowledge proofs**.[21]

[21] **Zero-knowledge proof:** Invented by Shafi Goldwasser, Charles Rackoff, and Silvio Micali in 1985, zero-knowledge proofs are a method for one party to verify possession of a piece of information to other parties without revealing the information.

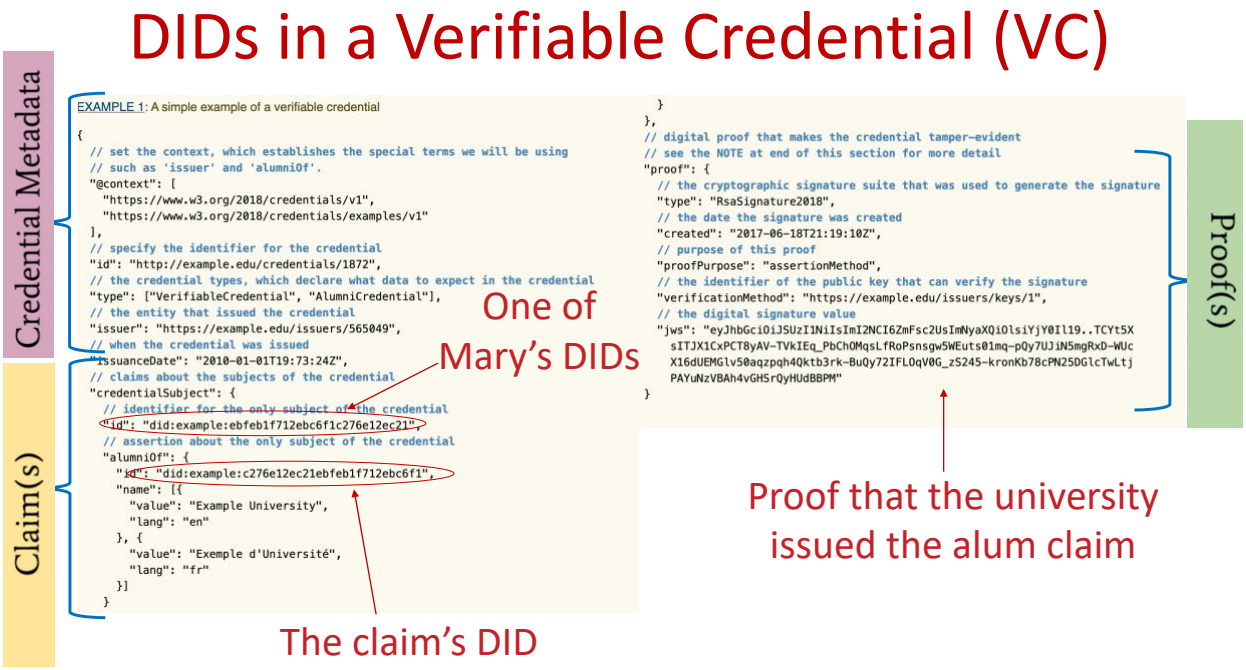


Figure 11: Parts of a verifiable credential for alumni status
Image credit: Adapted from https://www.w3.org/TR/vc-data-model/

So far, this section has described what's happening *inside* an SSI application. The average user, however, will interface with SSI applications using a friendly SSI wallet.

SSI wallets

Holders likely will use digital wallets to interface with SSI applications. Digital wallets are software applications that provide several functions, such as managing peer-to-peer connections, storing verifiable credentials created by authorized issuers, and sharing the credentials with verifiers. Digital wallets may be noncustodial (held by the holder) or custodial (managed by someone else, like a parent for a child). Figure 12 shows some user screens for Evernym's SSI wallet, called Connect.me.

Since SSI wallets contain the private keys that control DIDs and VCs, it is imperative that users select commercial-grade SSI wallets that feature automatic encrypted backup and recovery. Recovery keys should be encrypted and stored in a safe place, such as in an offline cold-storage device or possibly with a cloud agent. Social recovery key sharding is another approach. A user instructs the SSI wallet to divvy up the recovery keys among people the user trusts, and pieces of the key are stored in those people's wallets. At least *n* out of *m* shards are needed to reconstruct the recovery key (Preukschat and Reed, 2021). More backup and recovery methods are being developed, as protecting the private keys are paramount to the entire SSI model.

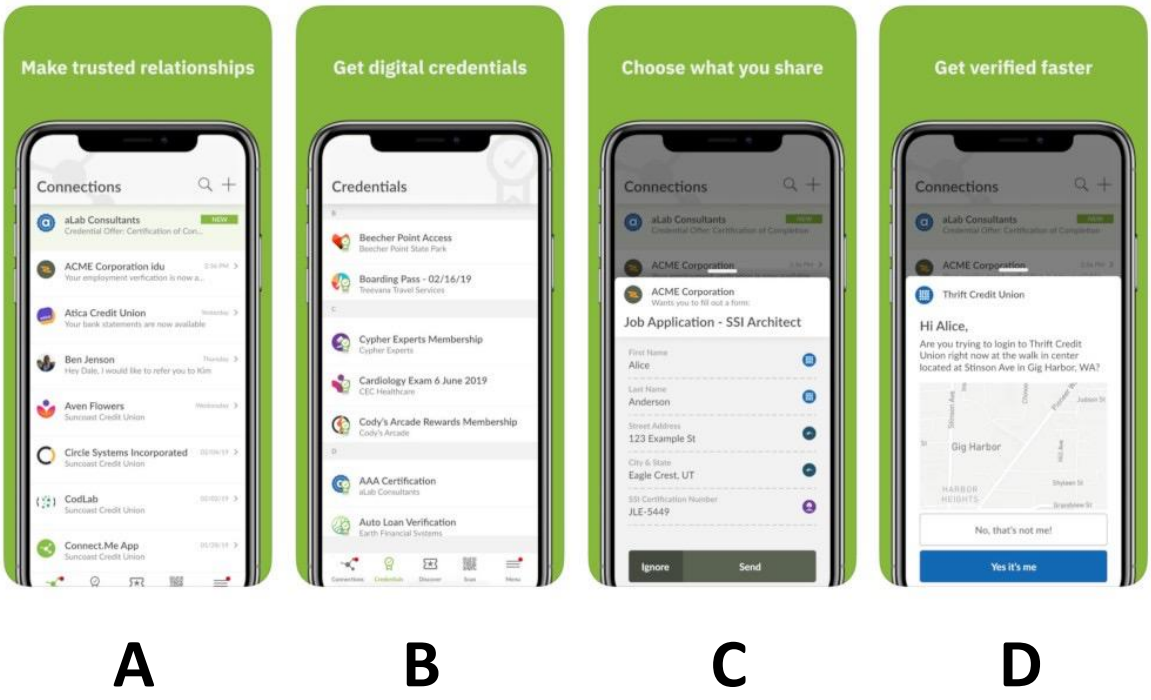


Figure 12: Evernym's SSI Wallet

A: Peer-to-peer connections with issuers and validators
B. Issuers provide credentials in a format that is machine verifiable
C. When a verifier requests a proof of credentials, the holder decides what to share
D. Additional safety features based on GPS location

There are many more enabling SSI concepts and technologies that have not been discussed in this overview. We have not discussed agents, multiparty keys, multiparty credentials, controllers, zero-knowledge proofs, or detailed privacy or security considerations. To learn about the full SSI technology stack, Preukschat and Reed (2021) is a recommended source.

Appendix B. Communities working on decentralized identity and verifiable credentials

Many standards-making bodies, open-source working groups, and organizations are working on self-sovereign identity (SSI) and verifiable credentials standards and protocols (see Table 1). These SSI communities convene around common interests pertaining to human rights, technical standards, or application-specific standards like digital health passes.

Many of the groups listed in Table 1 share ideas, cross-reference each other's work, or work together to aid in standards development. For example, the Trust Over IP Foundation and DIF are involved in W3C's specifications for W3C Decentralized Identifiers (for DIDs) 1.0, W3C DID Specification Registries (for DID methods), W3C DID Method Rubric 1.0 (for market evaluation of DID methods), and the W3C Implementation Guide.

We also acknowledge several individual SSI pioneers. Devon Lofretto coined the sister term Sovereign Source Authority (SAA) in a 2012 blog post. Lofretto argued that identity is a human right; governments should not administer a person's identity. He wrote, "Declaring a national sovereign structure for identity at birth inherently denies a basic human right to the individual; the right to self-declare participatory structure and authority."[22] Christopher Allen (2016), author of "The path to Self-Sovereign Identity;" Kim Cameron (2002), author of "The laws of identity;" Kaliya Young (2020), author of "The domains of identity;" Phil Windley (2005), author of "Digital Identity;" and Alex Preukschat and Drummond Reed, authors of "Self-sovereign identity, decentralized digital identity and verifiable credentials" (Preukschat and Reed, 2021) are recommended sources.

Table 1: Communities working on decentralized identity and verifiable credentials

Community	Founded	Key players	Community Focus
World Economic Forum https://www.weforum.org/	1971	Founded by professor Klaus Schwab; also the convenor of Davos.	Curates a platform called Good Digital Identity at: https://www.weforum.org/projects/digital-identity Convenes meetings and reports on digital identities. Key reports are listed in the references.
Internet Engineering Task Force (IEFT) https://www.ietf.org/	1986	Housed by The Internet Society (nonprofit).	Works on Internet standards like TCP/IP.
Organization for the Advancement of Structured Information Standards (OASIS) https://www.oasis-open.org/	1993	Provides infrastructure for open-source projects.	Advances projects for cybersecurity, blockchain, IoT, emergency management, cloud computing, and legal data exchange.
W3C https://www.w3.org/	1994	Founded and led by led by Tim Berners-Lee, inventor of the World Wide Web.	Oversees W3C/IETF standards for the Internet protocol suite; communities include the Decentralized Identifier

[22] https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

			Working Group and the Verifiable Credentials Working Group.
OpenID Foundation https://openid.net/	2007	Nonprofit chaired by Nat Sakimura; corporate members such as Cisco Systems, Google, Microsoft, Oracle, Verizon.	Promotes, protects, and enables the OpenID technologies and community. OpenID standard authenticates users using a TTP service rather than relying on a webmaster. Usage of OpenID is tracked. https://trends.builtwith.com/docinfo/OpenID
ID2020 https://id2020.org/	2016	Part of United Nations Sustainable Development Goal; key companies include Accenture, Microsoft, PwC, and Cisco Systems.	Advocates for digital identity for the one billion undocumented people worldwide.
Decentralized Identity Foundation (DIF) https://identity.foundation/	2017	Funded by government of British Columbia, Sovrin Foundation, Blockstack, Microsoft, and IBM.	Advances the interests of the decentralized identity community, including performing research and development to advance "precompetitive" technical foundations towards established interoperable, global standards.
MOBI https://dlt.mobi/	2018	MOBI is a nonprofit alliance of vehicle manufacturers, technical companies, and other members.	Creates standards in blockchain, distributed ledgers, and related technologies. > 100 members
Hyperledger Indy https://www.hyperledger.org/use/hyperledger-indy	2019	Managed by HyperLedger Foundation by Linux Foundation.	Develops distributed ledger standards and protocols focused on verifiable credentials for DLT; Indy resolver; Indy nodes; Plenum BFT; Sovrin Foundation donated the code built by Evernym; HyperLedger Foundation has hundreds of members.
Hyperledger Aries https://www.hyperledger.org/use/hyperledger-aries	2019	Managed by HyperLedger Foundation by Linux Foundation.	Develops distributed ledger standards and protocols focused on verifiable credentials for client-side components (wallets, agents) that interact with blockchains. Evernym donated the code.
Trust Over IP https://trustoverip.org/	2020	Managed by Linux Foundation; founded by 27 organizations, including the BCoE at the University of Arkansas.	Promotes standards for bringing together all of the efforts in decentralized identity and verifiable credentials in a dual, four-layer stack comprising technical and governance layers. Trust Over IP has 20+ steering members and hundreds of members/contributors.
Good Health Pass Collaborative https://www.goodhealthpass.org/	2021	Launched by ID2020	Promotes ethical and design principles for digital health passes, such as proving COVID-19 health status. Members number more than 125.

About the Blockchain Center of Excellence (BCoE)

The Blockchain Center of Excellence is housed in the Information Systems Department of the Sam M. Walton College of Business at the University of Arkansas. The BCoE was officially launched by Arkansas Gov. Asa Hutchinson on August 1, 2018. The center's vision is to make the Sam M. Walton College of Business a premier academic leader of research and education on blockchain-enabled technologies and digital ecosystems. The BCoE's case study series is one activity toward achieving that vision.

Acknowledgements:

Thank you to our SSI learning coaches Drummond Reed, Jim St. Clair, Andrew Tobin and Scott Perry.

Disclosures:

The BCoE is a founding member of the Trust Over IP Foundation.

Accenture, IBM and Microsoft, mentioned as suppliers in this case, are members of the BCoE's executive advisory board.

References

Allan, D. (2015). We all have too many online accounts – and can't remember the passwords, ITProPortal, retrieved July 10, 2021, from https://www.itproportal.com/2015/07/23/we-all-have-too-many-online-accounts-and-cant-remember-the-passwords/

Allen, C. (2016). The Path to Self-Sovereign Identity. Retrieved July 12, 2021, from http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Alexander, R. (March 20, 2012). Which is the world's biggest employer? BBC retrieved November 30, 2021, from https://www.bbc.com/news/magazine-17429786

Anderson, L., Holz, R., Ponomarev, A., Rimba, P., and Weber, I. (2016). New Kids on the Block: An Analysis of Modern Blockchains *CoRR*, abs/1606.06530. Retrieved March 20, 2018, from http://arxiv.org/abs/1606.06530

BBC (January 19, 2020). Covid-19: 400 military troops deployed to hospitals. Retrieved November 30, 2021, from https://www.bbc.com/news/uk-england-55726112

Cameron, K. (2005). *The Laws of Identity*. Retrieved July 12, 2021, from http://www.ict-21.ch/ICT.SATW.CH/IMG/Kim_Cameron_Law_of_Identity.pdf

Campbell-Kelly, M., & Garcia-Swartz, D. (2013). The history of the internet: The missing narratives. *Journal of Information Technology*, *28*(1), 18-33.

Department of Health & Social Care (November 24, 2020). Busting bureaucracy: empowering frontline staff by reducing excess bureaucracy in the health and care system in England. Retrieved November 30, 2021, from https://www.gov.uk/government/consultations/reducing-bureaucracy-in-the-health-and-social-care-system-call-for-evidence/outcome/busting-bureaucracy-empowering-frontline-staff-by-reducing-excess-bureaucracy-in-the-health-and-care-system-in-england

Carmel, E., and Lacity, M. (2021). Digital Health Passes: It's Not the Technology but the Ecosystem That Matters, Walton Insights. Retrieved July 11, 2021, from https://walton.uark.edu/insights/digital-health-passes.php

Evernym (April 2021a). "Credentials, COVID-19, & Digital Staff Passports: Lessons from the NHS Front Line. Retrieved January 19, 2022, from https://www.youtube.com/watch?v=iCL5bddCTtI

Evernym (November 2021b). Why The Web Needs Decentralized Identifiers (DIDs) — Even if Google, Apple, and Mozilla Object. Retrieved January 19, 2022, from https://www.youtube.com/watch?v=FGdQWuZC-oY

Graham, P. (2021a). Enabling Staff Movement & Digital Staff Passports, NYHDIF Conference presentation, November 11/12, 2021.

Graham, P. (2021b)., panelist, Digital Health Unplugged: Who leads on NHS IT?. Digital Health Unplugged Podcast, Episode 35, Retrieved January 19, 2022, from https://www.digitalhealth.net/2021/02/digital-health-unplugged-who-leads-on-nhs-it/

The Independent (August 4, 2021). NHS entrepreneurs are revolutionising staffing checks. Retrieved October 31, 2021, from https://www.independent.co.uk/news/business/business-reporter/nhs-entrepreneurs-revolutionise-staffing-checks-b1883780.html

Lacity, M. (2020b). *Blockchain Foundations for the Internet of Value*, Epic Books/University of Arkansas Press, Fayetteville Arkansas.

Lacity, M. and Carmel, E. (2022). Verifiable Credentials in the Token Economy, in Blockchains and the Token Economy: Studies in Theory and Practice (eds. Horst Treiblmaier and Mary Lacity), Palgrave, London, forthcoming.

Lacity, M., Willcocks, L., Gozman, D. (2021). Influencing Information Systems Practice: The Action Principles Approach Applied to Robotic Process and Cognitive Automation, *Journal of Information Technology*, 36(3), pp. 216-240.

Microsoft (March 15, 2021). The NHS rapidly meets clinical demands using verified credentials. Retrieved January 19, 2022, from https://customers.microsoft.com/en-us/story/1348169400682329017-nhs-foundation-trust-health-provider-m365

NHS (September 22, 2021). Enabling Staff Movement & Digital Staff Passports, Identity Week presentation.

NHS (2020/2021). We are the NHS: People Plan for 2020/2021. Retrieved December 2, 2021, from https://www.england.nhs.uk/wp-content/uploads/2020/07/We-Are-The-NHS-Action-For-All-Of-Us-FINAL-March-21.pdf

NHS Digital Staff Passport. Retrieved November 1, 2021, from https://www.nhsx.nhs.uk/information-governance/guidance/digital-staff-passport/ and https://beta.staffpassports.nhs.uk/

NHS Digital (February 25, 2021). NHS Workforce Statistics – November 2020. Retrieved November 30, 2021, from https://digital.nhs.uk/data-and-information/publications/statistical/nhs-workforce-statistics/november-2020#

Preukschat, A. and Reed, D. (2021). *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Manning Publications, Shelter Island.

Sovrin Foundation (2020). The Principles of SSI. Retrieved July 13, 2021, from https://docs.google.com/document/d/1GhcLeZEujX9h5gqrFNP-C1dMrS71EdCY4Uc1hGQbqI0/edit#heading=h.u4d08qmj8eyz

Trust Over IP Foundation (2020). Principles of SSI. Retrieved July 13, 2021, from https://trustoverip.org/wp-content/uploads/2021/10/ToIP-Principles-of-SSI.pdf

W3C (2019). Verifiable Credentials Implementation Guidelines 1.0. Retrieved July 11, 2021, from https://www.w3.org/TR/vc-imp-guide/

W3C (2020). Decentralized Identifiers (DIDs) v1.0. Retrieved July 12, 2021, from https://www.w3.org/TR/did-core/

Windley, P. (2005). *Digital Identity: Unmasking Identity Management Architecture*. O'Reilly Press, Cambridge.

World Economic Forum (2018). Identity in a Digital World: A new chapter in the social contract. Retrieved November 2, 2021, from https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

World Economic Forum (2020). A billion people have no legal identity – but a new app plans to change that. Retrieved October 31, 2021, from https://www.weforum.org/agenda/2020/11/legal-identity-id-app-aid-tech/

World Economic Forum (2020) Presidio Principles Foundational Values for a Decentralized Future. Retrieved July 13, 2021, from http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf

World Health Organization (2021). Smart Vaccination Certificate Working Group. Retrieved July 12, 2021, from https://www.who.int/groups/smart-vaccination-certificate-working-group

Young, K. (2020). *The domains of identity: A framework for understanding identity systems in contemporary society*. Anthem Press, London.

