MIS Quarterly Executive

Volume 21 | Issue 3 Article 6

September 2022

Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet

Mary Lacity

Erran Carmel

MIS Quarterly Executive

Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet

Self-sovereign identity (SSI) is a decentralized and automated approach for issuing, holding and verifying credentials. Its purpose is to address core weaknesses of the networked world: proving identity and verifying credentials. Many standards-making bodies, open-source working groups and organizations have been working on SSI and verifiable credentials for years. Now that production-ready solutions are becoming available, business and IT leaders, professionals and students need to start learning about SSI: What is unique about SSI? How can it be applied to deliver business value? Are there specific risks to mitigate? Is there anything idiosyncratic about managing an SSI project compared to other digital projects? Based on two years of research and active participation in SSI communities, we provide answers to these questions.[1]

Mary Lacity
University of Arkansas (U.S.)

Erran Carmel
American University (U.S.)

Introductory Comments

Gabriele (Gabe) Piccoli, *MIS Quarterly Executive* editor-in-chief, interviewed Mary Lacity and Erran Carmel about their SSI research program with the goal of consolidating what we know about SSI, learning lessons from early adopters and envisioning use cases that will deliver business value. He began by reminding Mary that she pioneered MISQE Insights so that *MIS Quarterly Executive* could publish timely insights that would normally not fit the mold of a full article. Self-sovereign identity (SSI) technology is a perfect example of an emerging topic that is certainly on the radar screen of *MIS Quarterly Executive* readers but, as yet, few scholars have generated considerable insights into this topic. Mary and Erran are two of these few and have been studying the very early stages of SSI.

Insights for IT Leaders

Gabe Piccoli: Let me begin by asking what is SSI and what intrigued you two about it?

Mary Lacity: First, a caveat. SSI is an unfortunate label because we—like many academics—view identity either as a psychological construct defined by an individual or as a social construct defined by an individual's social group. From that perspective, governments and organizations do not provide individuals with "identities." Instead, they provide individuals with "*credentials*," such as credentials of citizenship, licensing, credit, work history, skills,

1 This "MISQE Insights" is the edited transcript of an interview conducted by Gabriel Piccoli, MIS Quarterly Executive editor-in-chief, with the authors. The purpose of MISQE Insights is to distill the findings from academic research into actions that can be taken by IT practitioners.

DOI: 10.17705/2msqe.00068

vaccination status, etc. In our opinion, a better labeling of the SSI movement is "self-sovereign credentials"—or, more accurately, "self-sovereign *verifiable credentials*"—but alas, SSI is the entrenched term and we shall use that terminology.

So, what is self-sovereign identity? SSI is a movement spearheaded by global communities to decentralize and automate the issuing, holding and verifying of credentials made about subjects. It's part of the imperative to evolve the World Wide Web from centralized control by institutions to decentralized control by individuals. SSI empowers individuals to possess and control attestations made about them by authorized issuers—like a driver's license or a university diploma—and to provide a more secure and private version of the internet.

Like many interesting research projects, I stumbled upon it. In my role as director of the Blockchain Center of Excellence at the University of Arkansas, I hosted a workshop on decentralized identity and credentials in April 2020. One of our guest speakers was Drummond Reed, chief trust officer for Evernym—since acquired by Avast—a leading SSI company that has donated much of its software to the Hyperledger Foundation. Drummond, along with 26 companies, including some of our center's board member firms, established the Trust Over IP (ToIP) Foundation in May 2020. Our center was also a founding member. ToIP's mission is to provide a robust, common standard and complete architecture for internet-scale digital trust. Many open-source communities focus just on the technology, but I was attracted to this community because ToIP places equal emphasis on governance.

Around the same time, Erran called me to discuss his research project on digital health passports, a technology that emerged during COVID-19 and promised to help the world get back to work, travel, school and play. Digital health passports are a potential SSI use case because they are digital ecosystems for credentials—that is, ecosystems that include issuers, holders and verifiers. Erran will share how he became interested in SSI.

Erran Carmel: Many see a 2016 article by Christopher Allen[2] as the key to popularizing SSI. Like any tech that is norm-breaking, the evolution of SSI has many stories of dreamers, heretics and zealots. That was certainly the case with the related idea of zero knowledge proof (ZKP). My first impression of the ZKP field is that it attracts idealists whom, when I first spoke to one of them, seemed a bit like a cult that has become consumed by an esoteric idea. But then, once the vision sank in, I realized that like other grand concepts around distributed ledger, this one not only made sense but addresses one of the world's great challenges: identity in a networked world. Since then, I've interviewed leaders working on SSI and credentials in the U.S., Israel and Europe. I've also engaged with SSI leaders and working groups, including ToIP, the Good Health Pass Collaborative and the Covid Credentials Initiative. Mary and I started doing case studies of SSI solutions, including a study of the digital staff passport at the U.K.'s National Health Service and the New York State Excelsior digital heath pass.

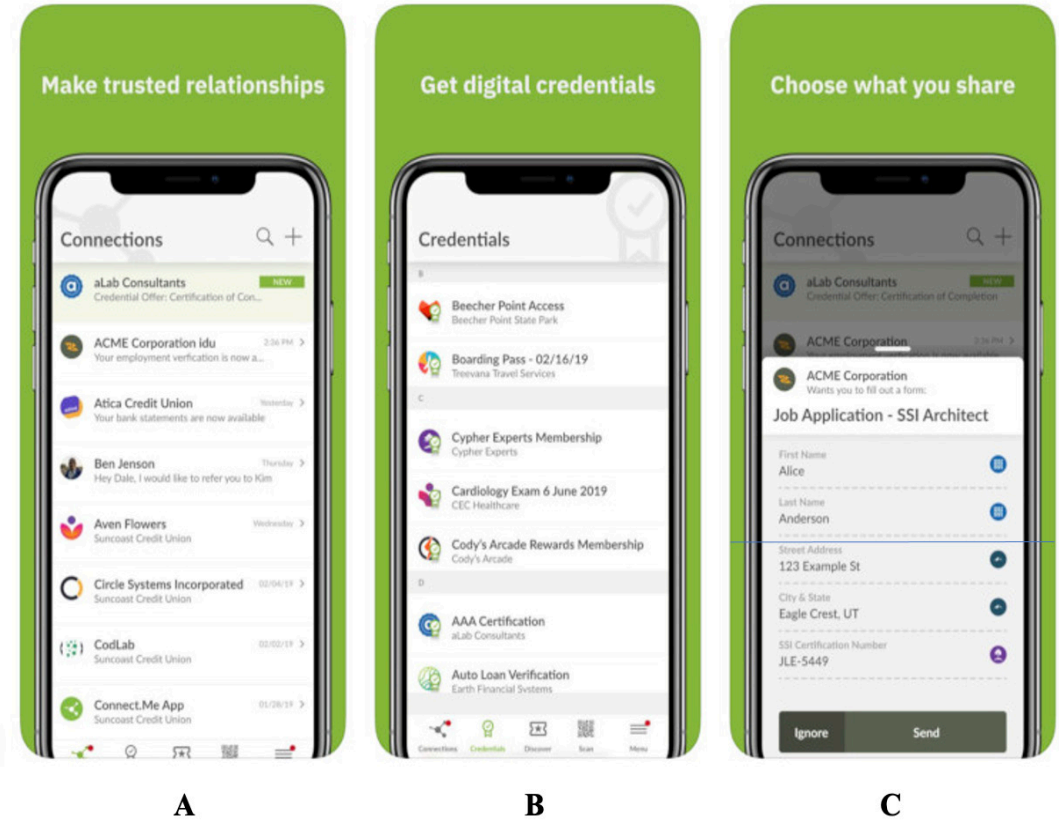
Gabe Piccoli: Yes, we in the information systems world would define identity differently, but the use of SSI does not surprise me since it is fairly standard in the computer science community. Solutions like Microsoft Active Directory or Okta's integrations are in fact called "identity and access management" solutions. So, defined in that way, surely "identity" is a key issue for CIOs and IT leaders.

Erran Carmel: Yes, it is, and that is why CIOs and IT leaders need to learn about SSI. SSI is quite different from Microsoft Active Directory. SSI will—at least partially—replace our outdated online identity systems that rely on centralized accounts and passwords by building decentralized peer-to-peer relationships that are private and secure. SSI will also replace—or live alongside—our centralized models for public key infrastructure (PKI) that verify digital signatures with cheap, fast and convenient decentralized PKIs. This means that the verification of credentials will be smoother.

Gabe Piccoli: How does SSI work?

2 Allen, C. *The Path to Self-Sovereign Identity*, CoinDesk blog post, available at https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/.

Figure 1: Example of an SSI Wallet (Connect.Me)



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

Mary Lacity: SSI makes use of decentralized identifiers (DIDs). In a document published in August 2021, the World Wide Web Consortium's (W3C's) Decentralized Identifier Working Group[3] proposed the following DID definition:

> *"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."*[4]

Each DID is controlled by a public-private key pair. The DID private key is stored in an SSI digital wallet (see Figure 1). DIDs are "under the hood" in that wallet users don't need to interact directly with them.

An SSI wallet generates a unique DID for each connection request from another SSI wallet. Each side's wallet stores a unique DID for the peer-to-peer relationship called a "connection." Each side has equal power over the relationship: both sides must agree they want to be connected, and

3 The World Wide Web Consortium (W3C) was founded in 1994 by Tim Berners-Lee, the 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.

4 *Decentralized Identifiers (DIDs)* v1.0, World Wide Web Consortium, August 2022, available at https://www.w3.org/TR/did-core/.

either side can terminate the connection at any time. One profound implication of SSI is that connections are no longer managed by log-on IDs and passwords. No trusted third party, central power or centralized database controls the relationship. It's important to understand that the connections only exist on edge devices.

The SSI wallet lives inside an ecosystem of issuers and verifiers, as I now explain. An SSI wallet can accept credentials from authorized issuers. An issuer signs a digital credential with its private key (stored in its wallet) and sends the credential directly to the holder's wallet. (The holder has the power to accept or reject loading the credential into the wallet). It's also important to understand that credentials are only stored on edge devices—there is no central database that stores credentials.

So, how can a verifier be confident that the credential is legitimate? Every credential in the SSI wallet has, under its hood, the issuer's machine-readable digital signatures. The issuer's DID public key is stored in a public trust registry, typically on a blockchain. Any ecosystem participant's wallet can verify that the issuer *and only the issuer* could have digitally signed the credential with their private key. This is the decentralized PKI part of the SSI model. The Sovrin Network—which is managed by the non-profit Sovrin Foundation—is an example of a live decentralized PKI. The Sovrin Foundation has authorized over 80 independent volunteers in six continents to operate the Sovrin Network's nodes.

Gabe Piccoli: Speaking of emerging identity and trust concepts, I have been hearing a lot about the zero trust security (ZTS) paradigm.[5] Is SSI related to it?

Erran Carmel: ZTS is indeed another hot area—this one in cybersecurity—that is gaining traction quite quickly. In the U.S., the federal government recently began mandating a transition to zero trust architecture (ZTA),[6] which requires authentication of every machine and every user regardless of its location or domain name. In the ZTS model, there is no sense of a safe perimeter where devices or users are trusted a priori. ZTA is about protecting organizational assets—especially data—by continuously verifying, all the time. To answer your question: no, ZTS was not designed with SSI in mind, but the ToIP community recognizes that SSI can support ZTA.[7]

Gabe Piccoli: We went deep into the acronym rabbit hole with DID, PKI, SSI, ZTS, so let's get back to the business questions: What is the problem that SSI is uniquely poised to solve?

Erran Carmel: Let's start with the pain points for one type of stakeholder in the ecosystem—the holders of credentials. We all hold credentials. For example, I hold proof of credentials issued to me by authorized parties inside my old-fashioned physical wallet. Among the more than 20 credentials in my wallet, I have a driver's license issued to me by the State of Virginia, a Visa credit card issued by Wells Fargo bank, a faculty ID card issued by American University, and my fraying COVID-19 vaccination card issued to me by a local hospital. These are my offline proofs of credentials. While they all exist in digital form somewhere, I have no control or direct access to them. I do have online relationships with some of the issuers, such as my bank and American University, but they control the online relationship via accounts and passwords. Even if I decide to end a relationship by "deleting" my account, all I have really accomplished is to deny myself access to the account. The organizations control the accounts and decide their fate. So, from my perspective as the holder of these credentials, I have very little "agency," meaning

5 For more information, see Raina, K. *Zero Trust Security Explained: Principles of the Zero Trust Model*, CrowdStrike, May 6, 2021, available at https://www.crowdstrike.com/cybersecurity-101/zero-trust-security.

6 *Office of Management and Budget Releases Federal Strategy to Move the U.S. Government towards a Zero Trust Architecture*, White House press release, January 26, 2022, available at https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/.

7 According to a ToIP blog post: "Zero Trust is based on the premise that 'that no actor, system, network, or service operating *outside or within* (emphasis added) the security perimeter is trusted.' In the same respect, SSI ascribes to the principle that identity is retained by the person (entity) and only shared based on pre-agreed terms of trust—a Trust Framework. ZTA requires that 'we must verify anything and everything attempting to establish access' while SSI prescribes selective disclosure and zero knowledge proofs that cryptographically confirm an identity without repeated disclosure of identity attributes for both authentication and authorization. ZTA and SSI then become 'both sides of the same coin,' protecting both the entity (which must trust the verifier in sharing their information) and the network (which must verify the entity to trust it with access)." The full post *"No, I Don't Trust You"—Implementing Zero-Trust Architecture in the World of Self-Sovereign Identity (SSI)*, ToIP, February 22, 2022, is available at https://trustoverip.org/blog/2022/02/22/no-i-dont-trust-you-implementing-zero-trust-architecture-in-the-world-of-self-sovereign-identity-ssi/.

I have little control over the credentials. That is one of the problems that SSI aims to solve for credential holders. An additional problem is the sheer number of accounts and passwords that each of us needs to manage. According to one study, the average U.S. internet user had 150 online accounts by 2017.[8]

Mary Lacity: The SSI vision is to empower every individual to possess and control digital proofs of credentials. Hence the term "self-sovereign"—i.e., the ability to exercise supreme authority of our credentials within a certain limited sphere. This will be achieved through an SSI digital wallet stored in an individual's smartphone. Moreover, we'll be able to decide how much data we need to share with verifiers—i.e., the individuals and organizations that need proof of our credentials.

Younger college-age readers will relate to the classic SSI example. When bartenders need proof that a patron is of legal drinking age, they ask to see the patron's driver's license. The bartender only needs to see the date of birth, but also sees the person's name and address. With an SSI wallet, patrons can prove they are over 21 years of age but keep their name and address hidden. This is called the SSI *data minimization principle*, which enhances individual privacy. And, finally, the SSI vision also addresses identity theft, which is a big problem. The FBI estimates that 1 in 15 people in the U.S. become victims each year.[9]

Gabe Piccoli: I see the value to holders, but where is the value for IT leaders in an SSI ecosystem?

Mary Lacity: Institutions—including governing authorities, issuers, and verifiers in a credentials ecosystem—incur high costs and face high cybersecurity threats from managing accounts and passwords. Every password reset costs, on average, $70.[10] Centralized identity models are honey pots that lure cyberthieves, and identity theft is costly to the companies that carry out financial transactions, such as Visa.

Erran Carmel: Let's bring in the notion of a trust diamond, which visually represents the roles involved in a credentials ecosystem. In the trust diamond shown in Figure 2, the governing authority sets rules in the ecosystem by specifying the types of credentials allowed/required in the ecosystem and specifies who is allowed to issue, hold and verify credentials. The governing authority publishes its governance framework, typically on a website. Consider my Visa payment card as an example. Visa Inc. is the governing authority of the Visa ecosystem and authorizes banks to issue Visa credit cards. In this ecosystem, banks are therefore the issuers of credentials. Authorized issuers include U.S. Bank, Barclays, Capital One and Chase. Individuals are the holders of the credentials. Verifiers are the people and institutions who need proof of individuals' credit, such as merchants, landlords and airlines.

At present, the digital elements of this ecosystem are highly centralized with root certification authorities (CAs) that are run as businesses and charge fees. While they are well protected, they are still vulnerable and some have indeed been compromised. IT leaders and chief information security officers (CISOs) are directly involved in the CA process. In contrast, as Mary explained above, SSI uses a decentralized PKI.

Gabe Piccoli: Let's dive deeper. I know you posted a white paper stemming from your research with the U.K.'s publicly funded National Health Service (NHS).[11] Walk us through the business case, adoption process and outcomes in this case.

Mary Lacity: We love this case study. If an organization the size of the NHS with over 1.1 million employees operating in one of the most highly regulated sectors can gain value from SSI, it stands to reason that other organizations can also benefit greatly.

The story begins in 2019. The NHS's 1,200 hospitals operate as independent units, each with its own records systems, including human resource (HR) systems. The NHS was suffering from a slow and expensive process

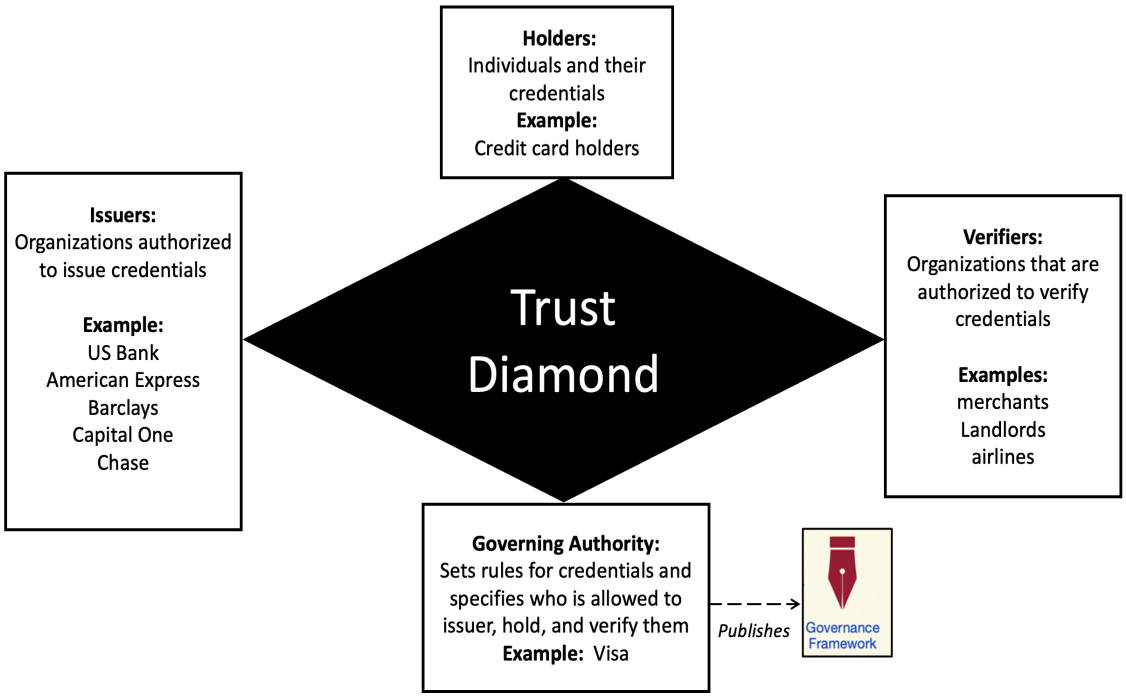
8 Caruthers, M. *World Password Day: How to Improve Your Passwords*, Dashlane Tech News, May 11, 2018, available at https://blog.dashlane.com/world-password-day/.

9 *Internet Crime Report 2020*, Federal Bureau of Investigation Internet Crime Complaint Center, 2020, available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

10 Douglas, A. *Are Password Resets Costing Your Company?* BioConnect, December 8, 2020, available at https://www.bioconnect.com/are-password-resets-costing-your-company/.

11 Lacity, M. and Carmel, E. *Implementing Self-Sovereign Identity (SSI) for a Digital Staff Passport at UK NHS*, Blockchain Center of Excellence, University of Arkansas Research Paper Series, January 27, 2022, available at https://blockchain.uark.edu/new-bcoe-white-paper-implementing-self-sovereign-identity-ssi-for-a-digital-staff-passport-at-uk-nhs/.

Figure 2: The Roles Involved in a Credentials Ecosystem Form a Trust Diamond



to transfer healthcare professionals from one hospital to another, a process managed by the individual hospitals' HR departments. Moving staff around the NHS was almost like hiring someone from the outside: staff needed to fill in multiple forms, prove their identity, credentials and prior employment—and nearly half were required to travel to complete the onboarding process in person. Moreover, staff often had to retake unnecessary training because they could not prove their prior training credentials. Onboarding also entailed security clearances and authorizations to access data required for the new position. The onboarding process before SSI took days to complete.

Erran Carmel: And the scope of the problem was huge. Each year, there are over 1 million staff transfers within the NHS. For just the doctors in training, the costs amounted to £22 million ($26 million)[12] in lost hours. The total cost attributed to lost hours across all employee categories was much higher. Those 1 million transferees were sitting in HR offices processing paperwork instead of caring for patients. The NHS wanted its doctors, nurses and other healthcare professionals transferred back to the front line as soon as possible.[13]

Adoption of SSI at the NHS also provided soft benefits. Staff now control their own digital credentials—i.e., they have more agency, meaning they are empowered at every step to accept, reject and share information via their SSI wallet. One of the key benefits is transparency: individuals know who has seen their information and for what purposes. Organizationally, there is now a single source of truth: one verifiable credential is issued and is interoperable. The result is less cheating, less suspicion and more efficiency.

Gabe Piccoli: When and how did the NHS's SSI adoption journey begin?

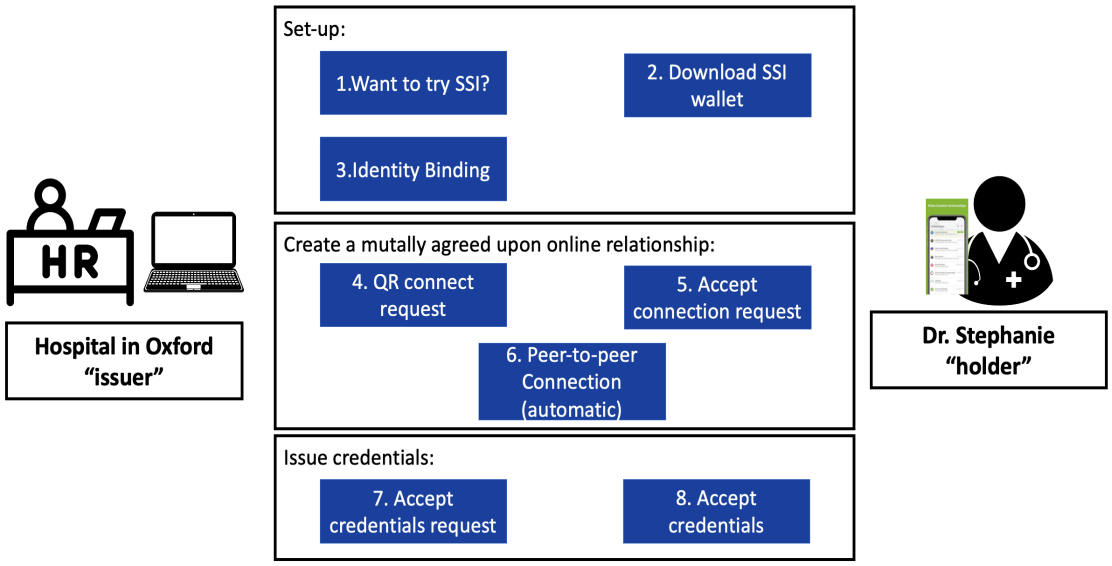
Mary Lacity: In 2019, the NHS established a minimal viable ecosystem (MVE) to build a pilot solution, which was initially called the "NHSX digital staff passport." The MVE involved NHSX,[14] NHS England, the General Medical Council (GMC), NHS trusts (e.g., Blackpool Teaching Hospitals;

12 Currency conversion rate as of July 2022.

13 Graham, P. *Enabling Staff Movement & Digital Staff Passports*, NYHDIF Conference presentation, November 11-12, 2021.

14 NHSX is a joint unit involving the U.K.'s Department of Health and Social Care, NHS England and NHS Improvement.

Figure 3: Outgoing Staff HR Transfer Process after SSI



NHS Foundation Trust) and technology providers including Accenture, IBM, Oracle, Microsoft, Evernym (now Avast) and Truu. The solution comprised many parts, including interfaces to hospitals' HR systems, but we'll focus on the SSI parts of the solution. Evernym and Truu built the digital wallet application and Microsoft provided the Azure-based cloud service. The 2019 NHSX pilot was ready just before COVID-19 hit.

Erran Carmel: The pandemic increased the urgency to onboard staff quickly, thereby accelerating the rollout. The NHS anticipated that staff mobility needs would escalate because of COVID-19, and that many new facilities like field hospitals with intensive-care beds and ventilators, would be erected.

Gabe Piccoli: Was there already a standard in 2019 when the NHS began this project?

Erran Carmel: Yes and no. Earlier, we mentioned W3C. The NHS adopted W3C's verifiable credential standard.[15] The NHS also used OpenID Connect standards for online identification.[16] However, SSI technology is still evolving, and some of the standards adopted by the NHS are provisional, such as the DID methods used.

Gabe Piccoli: Walk us through the staff transfer process after SSI.

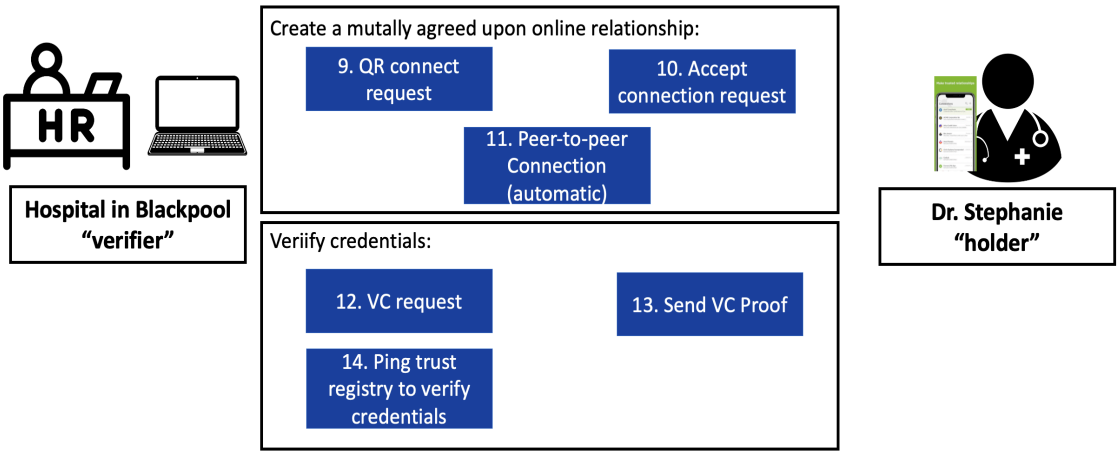
Mary Lacity: Let's use a scenario where Dr. Stephanie is being transferred from a hospital in Oxford to a hospital in Blackpool. In Figure 3, Dr. Stephanie's first stop is Oxford's HR department.

The HR employee thanks Dr. Stephanie for her service and asks her, "Before you move to Blackpool, 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?" The HR employee also explains the additional benefits, such as carrying all required credentials in one convenient place on her phone (with backup and recovery of her credentials provided in case her phone is lost or damaged) and controlling who sees her credentials. Dr. Stephanie agrees to try the new process. Oxford HR gets Dr. Stephanie to

15 W3C's verifiable credentials data model is available at https://www.w3.org/TR/vc-data-model/.

16 OpenID Connect allows verification of the identity of a user based on the authentication performed by an authorization server and provides access to the user's basic profile information. For more information, see *Welcome to OpenID Connect*, OpenID Foundation, 2022, available at https://openid.net/connect/.

Figure 4: Post-SSI Incoming HR Staff Transfer Process



download the Connect.Me SSI digital wallet app from Apple or Google. The next key step is "identity binding," which ensures that credentials are created for the correct employee. The HR person retrieves information from the employee database, including verification of Dr. Stephanie with a photo from the hospital's database.

Once the individual's identity is confirmed, the next steps establish a relationship between Oxford Hospital and Dr. Stephanie. HR sends Dr. Stephanie a QR code to request a peer-to-peer connection. 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. She accepts the invitation on her SSI wallet. When Dr. Stephanie scans the QR code, a unique and private peer-to-peer connection is established inside each side's SSI wallet. It's all automatic—no accounts or passwords are needed. The wallets keep track of the relationship and both sides have equal power to delete the relationship when they want.

Next, HR sends Dr. Stephanie a request to send all of her verifiable credentials to her SSI wallet. These credentials are extracted from the HR system and formatted for the SSI app. Dr. Stephanie must accept the invitation before her credentials are added to her SSI wallet.[17] She accepts the invitation and, voila, she has proof of citizenship, medical licenses, specialty licenses and criminal background checks all in one convenient place and under her control.

Gabe Piccoli: Got it; the peer-to-peer connection replaces the accounts and passwords, and credentials can be shared only after a relationship has been mutually agreed upon. What happens next?

Erran Carmel: Dr. Stephanie arrives at her new job and meets with HR at the Blackpool hospital (see Figure 4). Her credentials can be verified in just a few minutes. First, HR sends her a connect request. After Dr. Stephanie accepts the invitation on her phone, her SSI wallet now keeps track of two peer-to-peer relationships, one with her prior hospital in Oxford and one at her new place of employment in Blackpool. Next, HR asks Dr. Stephanie to prove her credentials. She opens her app and sends all her verified credentials to HR at the Blackpool hospital.

Gabe Piccoli: How can the HR person trust the credentials she sends? And more broadly, what's happening in the background of the process you described so far?

Mary Lacity: That's where the distributed public key infrastructure comes in. The verifier's app doesn't just accept Dr. Stephanie's credentials; first, the app pings a public distributed trust registry to retrieve the public key from the hospital in Oxford to verify that it—and only it—could have created Dr. Stephanie's

17 Unlike cryptocurrency wallets, where a sender can airdrop cryptocurrency into someone's digital wallet without the holder's permission, SSI wallet holders are in complete control of who they connect with and what data goes into their digital wallets.

credentials. Dr. Stephanie is now ready to start work at the new hospital.

Gabe Piccoli: Let's move to the business case. What about outcomes? Is the NHS case an early success?

Erran Carmel: So far, yes. NHSX is at a "production pilot stage," with 102 hospitals registered to use the system.[18] The initial adoption focused on temporary staff coming from the armed forces to fill staffing shortages during COVID-19. The first production pilot application used a "one size fits all" model.

The hard economic benefits appear promising, especially time savings: instead of spending days to onboard, the process takes a few minutes because much bureaucratic stuff can be reduced or eliminated. There is no need to request, respond to or repeat employment checks. There are also benefits for the NHS ecosystem because the agile and flexible movement of staff means that patients can be treated faster. Where NHS organizations are part of clinical networks, the passport enables the temporary movement of staff to work across several organizations to deliver either planned or emergency clinical care.[19] The NHS has not reported publicly on the project's return on investment. However, we know that the production pilot was not all that expensive.

The plan is to incrementally expand the scope of the NHS staff passport. A near-term phase is for different categories of staff movements, including junior doctors because they move frequently, then "bank" workers, who are freelance healthcare providers called upon to cover shifts or holidays.

Gabe Piccoli: Let's wrap up the NHS case with lessons learned from this project. Practitioners want to know whether there is anything idiosyncratic about managing an SSI project compared to other digital projects.

Mary Lacity: The lessons for managing an SSI project from the NHS were clear: there is nothing idiosyncratic about managing such a 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. Change management was demanding because the NHS moved quickly from paper-based processes to digital passports. Many people like to carry their own paper credentials and they need to see the benefits of digital versions. The NHS decided it was best to make adoption voluntary. An interesting piece of advice from one of the NHS project managers was, "don't use the b-word." By this, he meant don't talk about blockchains because users will think SSI is about cryptocurrencies and administrators will think it's all hype.[20] Erran and I took this lesson to heart. We have barely mentioned the b-word so far in this conversation. Erran and I also hope to study some of the other SSI early adopters to learn more.[21]

Gabe Piccoli: As a young technology, presumably there are plenty of risks with SSI.

Mary Lacity: Yes, SSI is a young tech concept so there are going to be risks. We see risks related to ecosystems, economic models and cybersecurity. There is a risk that SSI solutions will not grow into proper ecosystems for a long time. The NHS was successful, in part, because it oversees the national healthcare ecosystem. In many other ecosystems, such as educational credentials or vaccine credentials, there are thousands (or more) of ecosystem players who need to adopt SSI to achieve network effects.

Erran Carmel: The most promising catalyst may well be the interoperable European Digital Identity Wallet, which has many elements of SSI. However, SSI is a radical change and we

18 A list of participating hospitals is available at https://beta.staff-passports.nhs.uk/registered-organisations.

19 *Support the Temporary Movement of Staff for COVID-19 Response and the Recovery of Services*, available at https://beta.staffpassports.nhs.uk/.

20 Graham, P. *Digital Health Unplugged: Who Leads on NHS IT?* Digital Health Unplugged Podcast, Episode 35, available at https://www.digitalhealth.net/2021/02/digital-health-unplugged-who-leads-on-nhs-it/.

21 The NHS case was one of the first SSI cases. Another famous early case is the World Food Program in Jordan, which was set up for refugees from the Syrian civil war and used digital identities for stateless refugees to receive benefits and food. Initially, SSI was partially implemented but then, due to circumstances, was changed. Other well-known cases are the various instances of digital health passports that emerged in 2021 because of the COVID-19 pandemic. Several of these passes use SSI architectures to create COVID status credentials for vaccinations, tests and approved recovery. These passes include the New York State Excelsior pass, which was developed by IBM, and the International Air Transport Association (IATA) Travel Pass. A few other projects are in early implementation stages: Absa, one of the largest banks in South Africa, is working on a digital identity that will store key financial data and identity; the Canadian government's vision of a "Pan-Canadian Trust Framework" is based on SSI, and TruWest Credit Union (an American bank) completed an SSI pilot for identity.

have to be patient. In 2021, Gartner positioned *decentralized identity* (including SSI) at the peak of inflated expectations on its famous hype cycle.[22] This seems like a correct judgment. After all, SSI is an ecosystem play. Gartner anticipates that SSI will pull out of the "trough of disillusionment" between 2023 and 2026.

Mary Lacity: Another risk is economic: SSI does not yet have good economic models to support itself. For example, the Sovrin Network is quite inexpensive to use (it costs $10 to post a public key and zero dollars to read the ledger), and the Sovrin Foundation is subsidizing the costs and carrying a large debt.[23]

Cybersecurity is also a risk. SSI stores data at the edges, in digital wallets. We know from the cryptocurrency markets that most heists happen at the edges; Bitcoin and Ethereum's ledgers have never been breached, but millions have been stolen from digital wallets (and from poorly coded smart contracts).

The NHS protects private keys with a cloud agent that provides wallet backup and recovery. Social recovery "key sharding" is another approach to protecting private keys. 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. More backup and recovery methods are being developed, as protecting private keys is of paramount importance to the entire SSI model.

Erran Carmel: Another risk is "identity binding;" until we have a strong digital credential for individuals to bind to other credentials in the SSI wallets, the risk remains that the credential a person shares from their SSI wallet may belong to someone else. The NHS mitigated this risk with video or in-person interviews to make sure it was creating and sending credentials to the right person.

Gabe Piccoli: What are the other key recommendations you would provide to our readers? I know it is early in the SSI adoption story, but what else do you say to the CIOs you engage with?

Erran Carmel: My forecast is that the first SSI ecosystems to emerge will be in HR and employment, similar to the NHS case we described. The U.S. arm of Accenture listed the following credentials as part of the evolving "talent management" landscape: identity, driver's licenses, educational credentials, previous employment, criminal records, drug tests, credit scores, work skills, training and microcredentials, and health status. At the time of writing, I see that the urgency of digital health passports has lessened and the creation of the associated ecosystems has faced considerable pushback from citizens in multiple nations.

Mary Lacity: But perhaps the biggest future use cases will involve non-human holders of credentials that won't push back. The power of the SSI model is that anything that needs a credential is a potential SSI use case, including an animal, a physical thing, a digital thing or a logical thing. So, the SSI model is not just applicable to the credentials of people, which could lead to thousands of use cases in the longer run. Going back to the trust diamond shown in Figure 2, SSI could be used, for example, in food and drug supply chain ecosystems. Governing authorities (such as the U.S. government's Food and Drug Administration) could define the required credentials for food and drug safety, say for the quality of meat or for the expiration date of medicine, and authorize which parties are allowed to issue, hold and verify them. The verifiers in this scenario might include not only supply chain partners, auditors and inspectors, but also end consumers.

Gabe Piccoli: Thank you so much for sharing your insights with MIS Quarterly Executive. It was very valuable, and quite a bit to take in! Where should readers go to learn more?

Mary Lacity: We recommend what we call the "SSI Bible," a collection of pieces by over 51 SSI global leaders, edited by Alex Preukschat and Drummond Reed.[24] Evernym also has a plethora of learning videos for beginners.[25]

22 An image of this hype cycle, as of August 2021, can be found at https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/v2-hc-emerging-tech-2021.png.

23 In its April 2022 newsletter (available at https://us14.campaign-archive.com/?u=b2c2f50b93f0ad7684f55ccde&id=34bd91c991), the Sovrin Foundation made a plea to the community to help reduce its $2 million debt.

24 Preukschat, A. and Reed, D. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*, Manning Publications, 2021.

25 *Learn about Verifiable Credentials*, Evernym; this collection of over 40 hours of recorded content is available at https//www.evernym.com/webinars/.

Erran Carmel: We also encourage readers to get involved in one of the standards-making bodies, open-source working groups or organizations that are working on SSI.[26]

About the Authors

Mary Lacity

Dr. Mary C. Lacity is a Distinguished Professor and Director of the Blockchain Center of Excellence in the Sam M. Walton College of Business at The University of Arkansas. She was previously Curators' Distinguished Professor at the University of Missouri. She has held visiting positions at MIT, the London School of Economics, Washington University, and Oxford University. She is a Senior Editor for *MIS Quarterly Executive*, a Contributing Editor for *Journal of the British Blockchain Association*, member of the Global Standards Mapping Initiative (GSMI) of the Global Blockchain Business Alliance (GBBC), a fellow of the Association of Information Systems (AIS), a member of the Linux Foundation's Trust over IP (ToIP), and a Certified Outsourcing Professional. According to Google Scholar, her work has been cited over 22,000 times, with an h-index of 60.

Erran Carmel

Erran Carmel is a Professor of Information Technology at the Kogod School of Business at American University in Washington D.C. and former dean. He is known for his expertise on the globalization of technology work especially global outsourcing and is best known for his groundbreaking book Global Software Teams. He has taught many classes on diverse waves of emerging technologies including, most recently, on blockchain. As a futurist, he regularly teaches futures courses and publishes on various futures topics.

26 These organizations include the World Economic Forum, Internet Engineering Task Force (IEFT), Organization for the Advancement of Structured Information Standards (OASIS), World Wide Web Consortium, OpenID Foundation, ID2020, Decentralized Identity Foundation (DIF), MOBI, Hyperledger Indy, Hyperledger Aries, Trust Over IP, Good Health Pass Collaborative and Linux Foundation Public Health.