MTR190655

MITRE TECHNICAL REPORT

Usability, Privacy, and Security Converge in the Fourth Generation of Digital Identity

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: Case Number 19-3453 Distribution Unlimited.

McLean, VA

Author: Christian J. Buchanan

October 2019

Abstract

Historically, it has been impossible for information security to coexist with usability without the sacrifice of personal privacy. Leading internet companies, which must maintain high levels of usability, are now capitalizing on the vast collections of personal information that they originally collected due to this natural imbalance. Google, Facebook, Microsoft and others have deployed federated identity services that are becoming the de facto standard for digital identity on the Internet, but it is increasingly clear that ceding personal privacy to companies that monetize their influence over people's actions while providing "free" services may not be the best digital identity solution for individuals or society. In 2019, The MITRE Corporation joined a growing consortium of companies, organizations, and government entities to develop concepts and capabilities for Self-Sovereign Identity (SSI); a fourth generation of digital identity that seeks to provide a universally portable digital identity while greatly improving individual privacy and information security.

Table of Contents

This page intentionally left blank.

1 Introduction

Historically, it has been impossible for information security to coexist with usability without the sacrifice of personal privacy. Leading internet companies, which must maintain high levels of usability, are now capitalizing on the vast collections of personal information that they originally collected due to this natural imbalance. Google, Facebook, Microsoft and others have deployed federated identity services that are becoming the de facto standard for digital identity on the Internet, but it is increasingly clear that ceding personal privacy to companies that monetize their influence over people's actions while providing "free" services may not be the best digital identity solution for individuals or society. In 2019, The MITRE Corporation joined a growing consortium of companies, organizations, and government entities to develop concepts and capabilities for Self-Sovereign Identity (SSI); a fourth generation of digital identity that seeks to provide a universally portable digital identity while greatly improving individual privacy and information security.

2 The Previous Three Generations

Before digital identity became its own Information Technology (IT) discipline, the login and password were used to secure individual devices. When multiple users accessed the same computer, Access Control Lists (ACLs) were used to control each user's access to resources. Once computers were networked and began sharing resources, the ACLs necessitated the use of identity in networked systems and digital identity was born.[1]

In its first generation, digital identity was **centralized** around each platform[2], and each platform provided each user a platform-centric identity. Then, in the second generation, **federation** allowed platforms to collaborate and provide platform-centric identities that worked among the participating platforms. These first two generations of digital identity succeeded because they were invented by platforms for their own use.

As the problems with platform-centric identity became clearer, identity professionals began to search for a way to offer **user-centric** identity – the third generation of digital identity. User-centric identity attempted to free users from reliance on and exploitation by platforms. However, even though it was supported by the President of the United States in the 2011 *National Strategy for Trusted Identities in Cyberspace*, the effort lacked enough momentum to succeed.

User-centric identity envisioned a user-controlled identity that could be used universally. This idea, though prescient, was caught in a dilemma described by Microsoft's Architect of Identity, Kim Cameron, in his 2005 blog post entitled *The Laws of Identity*. To be universally used, a digital identity system would either need to be centralized under one authority or be implemented as a metasystem. Neither option was feasible in 2005.

[1] An alternative approach is the Object Capability Model (OCAP) which combines location and permissions; eliminating the need for authentication to an access control list (https://en.wikipedia.org/wiki/Object-capability_model).

[2] The word "platform" is defined here as a service or network for which administrative control belongs to a single entity.

Today, SSI incorporates all the lessons learned over the past three decades of identity innovation to create the fourth generation of digital identity. In doing so, SSI may finally provide an end-to-end identity solution for the internet. With SSI, platform security and usability are no longer mutually exclusive to personal privacy. Additionally, digital identities are universally portable, people have primacy over platforms, private encrypted peer-to-peer connections are commonplace, and platforms and organizations benefit from increased competition in all areas of the digital identity ecosystem.

The promises of SSI for privacy, security, and portability are immense. Digital identity portability as well as the end of passwords and the vulnerabilities that come with them would be a huge leap forward for platforms and users alike. The decentralization and distribution of identity systems will create new industries in credentialing, identity proofing, verification, and their respective reputations. But the incoming tide of privacy improvements will raise all boats, including those of criminal and terrorist networks.

2.1 The Contemporary Sacrifice of Privacy, Security, or Convenience

Contemporary platforms tend to minimize friction for the user to improve users' experience. Users are more satisfied when they are not subjected to a virtual "stop and frisk" every time they go to a website, and they do not want compulsory two-factor authentication. The contemporary method of handling this issue through the use of ubiquitous surveillance is being pioneered by industry. By collecting vast amounts of device attributes and user behavior, industry is changing the user authentication process from proving what the user knows (password) and what the user has (second factor) to what industry knows and how the user behaves. This continuously deepening understanding of people and their devices through the unblinking eye of artificial intelligence yields one form of frictionless security. But it does not change the inversely proportional relationship between security and privacy. It simply dismisses privacy as an objective.

"SSI is powerful yet elegant, bold yet familiar, and through it we can finally break free from the paradox of having to sacrifice security for user experience (or vice versa): we can have both, and at levels vastly improved over the status quo."[3] – Timothy Ruff

Although the death of privacy may seem inevitable to some, SSI provides an identity framework in which ubiquitous surveillance is only inevitable as long as people desire it for themselves. In the fourth generation of digital identity, it is possible to have both frictionless security and privacy. This fact is made possible by the decentralization of identity. In contemporary identity systems, users arrive to a platform unidentified and must prove their authenticity. Only then are they granted a credential that allows them access to their account. SSI moves the credential into the control of the user so that they arrive to the platform with their credential already in hand. SSI changes the process from authenticating the user (an interactive process) to verifying the credential (a computational process). From the user's perspective, they simply arrive to the platform already known. From the platform perspective, there is no need for surveillance because there is no need for authentication. Authentication is handled locally by the wallet.

[3] https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

2.2 Universal Portability

In the first three generations of digital identity, universal portability was a fantasy, an equally tantalizing and inaccessible destination that had existed in the minds of identity professionals since the first user created their second online account. Referring back to Kim Cameron's work, he and his cohort surmised that to be universally portable, a digital identity would have to be both "polycentric" and "polymorphic." In other words, the identity could not depend on a central authority, nor could it exist in a single form.

The technologies to change the form of identities have existed for many years and helped enable the second-generation federated identities. Until recently, however, it had remained a truism that the decentralization of an identity also decreased its trustworthiness. Federation was simply a better way of sharing the burden of authentication and risk. The advent of Distributed Ledger Technology has changed that by enabling fourth-generation digital identity to push the platform credentials to the user while also making any tampering with the credential evident on inspection. Now a user can present a credential and the platform can cryptographically verify both the subject and the issuer of the credential while also having high assurance that the credential has not been changed since it was issued.

2.3 Asking the Right Questions

Earlier it was stated that a universal digital identity must be able to change forms – it must be polymorphic. Polymorphism is a function of the digital wallet with which the user interacts on their device. Digital wallets, which are familiar to those with smartphones, enable users to present credentials and payment cards to electronic readers and optical scanners. In the future, SSI wallets will likely operate in a similar fashion by allowing users to select which credentials they want to use for which identity transactions. Platforms or persons with whom they interact will also be able to request certain types of credentials or possibly just specific information, which can be derived from one or more of the credentials in the digital wallet.

SSI wallets will, with user consent, answer specific questions about the subject without revealing more than is required. For example, the wallet could repurpose the date field on a digital birth certificate to prove the subject is old enough to enter into an online agreement without revealing the actual age or birthday. The wallet will use cryptographic methods to ensure that the "morphed" credential can still be verified just like the original but preserves as much privacy as possible. Therefore, other persons, platforms, and devices can ask the right questions and get the security they require while preserving the maximum amount of privacy for the subject.

For example, someone buying alcohol in the United States may be required to show their state-issued photo identification to the cashier and then provide payment. The cashier is responsible to verify the identity before allowing the transaction. The cashier may be diligent in their biometric analysis and accurate when calculating the age of the consumer, but this process can be made still more accurate and less invasive by SSI. The vendor only needs to have two questions about the consumer answered in order to allow the transaction: "Is it legal for that person to buy that product at that time in that location?" and "Does that person have enough money to buy that product?" An SSI wallet could answer both questions at once without revealing any of the consumer's personal information.

Because the preceding transaction is interactive, the wallet can provide even more privacy by using progressive disclosure. In progressive disclosure, the questions and answers are asked in a privacy-preserving order. Using the previous example, the question of legality may be asked first. If the answer is “no,” it is not legal to buy the product, then there is no reason to ask whether the consumer has enough money. In this way, the consumer’s privacy is further preserved.

Another feature of SSI wallets will be the ability to select one or more attributes from a credential and then mix them with attributes from another credential to complete complex identity transactions in a single presentation.[4] For example, to receive a driving license in Virginia, one must submit at least one proof of identity and two proofs of residency.[5] If one has some combination of the required documents in their digital wallet, information from each document may be combined into a single presentation. This method simplifies the transaction, but far more important, a water bill presented as proof of residency is electronically signed by the water company, unlike the self-printed documents used today. Therefore, the efficacy of the driving license is increased, as are any subsequent identity transactions that rely on the driving license.

2.4 The Connecting Power of Peering

Fourth-generation identity systems like SSI push digital identity into the hands of the user. Each digital identity has a private component that is held by the subject in their digital wallet, and a public component that is written to a public ledger. These components are cryptographic keys, and together they are referred to as a keypair. When two people who have keypairs want to connect, they need only exchange their public keys in the form of a Universal Resource Locator. Once they know each other’s public keys, they can form an encrypted connection in which only the two of them can participate.

While it is possible, with great computational effort, to break the encryption on the connection, it is not practical to do this at scale. To do so, the interloper must have targeted the relationship and have the ability to intercept the peer-to-peer communication. The work of targeting is stymied by the fact that SSI connections may be pairwise pseudonymous – meaning that one connection cannot be correlated to another. Therefore, even if the interloper can see all connections, understanding the network of personal associations will take extraordinary effort.

3 The Fourth-Generation Identity Ecosystem

Users are not the only beneficiaries of fourth-generation systems. Platforms, other than those exploiting their patrons’ private information, also stand to have much better outcomes. When users arrive at the platform with their credentials in hand, platforms can focus on their relationship with their customers – like a boutique hotel greeting each customer by name when they enter the door without the need to abuse patron trust through reliance on ubiquitous

[4] https://www.w3.org/TR/vc-data-model/#presentations-0
[5] https://www.dmv.virginia.gov/apps/documentbuilder/date_type.aspx

technical surveillance. Platform providers benefit from economic incentive realignments, new identity markets, end-to-end security, and intrinsic regulatory compliance that all work together to reduce operating costs.

3.1 Economic Incentive Realignment

One aspect of SSI that is rarely talked about is the realignment of economic incentives in support of the identity ecosystem. In some implementations of SSI, it is possible for credential issuers, verifiers, and even users to get paid for each credential presentation. However, those parties relying on the credentials also get a choice of which issued credentials and what verification systems to use. This ability to choose will be supported by reputation systems that score issuers and verifiers based on their ability to provide the requisite security to their customers. SSI will provide not only the means for strong digital identities but also the economic incentives for strong digital identities.

Additionally, these economics support user privacy. Today, many systems resell user data to cover operational costs and for profit. However, if companies were expected to pay users for their identity information, many users would not find the value exchange worthwhile. In a 2019 article, Hanna Kozlowska[6] estimates the average Facebook user's data to be worth $7.50 per month. SSI users would therefore have to value their privacy at under $7.50 per month for Facebook to remain profitable. Facebook or a competitive product could lower their operating costs for behavioral prediction and manipulation[7] and simply provide users a privacy-protecting fee-for-service account.

For start-ups and smaller companies, the fee-for-service model levels the playing field, because profitability is not dependent on competing with data-capture giants like Google and Facebook. The realignment of incentives with respect to identity lowers the bar for scale and reduces uncertainty while offering users a clearer ability to determine value for themselves.

3.2 New Identity Markets

Fourth-generation identity creates new markets for digital identity. For example, identity proofing and identity verification services will likely become competitive markets. While identity proofing and verification can already be outsourced using federation, without universal portability the markets for these services lack the requisite competition to strongly incentivize the improvement of the identity ecosystem. For example, many airport travelers have already seen proofing and authentication services from CLEAR,[8] an offering for biometric authentication at some airport security checkpoints. Travelers can go through a quick proofing process with a government-issued photo ID, and CLEAR will enroll them into their biometric authentication system. Travelers may then receive expedited security screening wherever the CLEAR scanners are available. While this system increases security and enhances the user experience, the CLEAR system is still centralized. Centralization not only limits CLEAR's overall utility and profitability, but because users and airports are likely to commit to only one vendor, the CLEAR

[6] https://qz.com/1655610/how-can-you-measure-the-worth-of-your-data/

[7] https://www.forbes.com/sites/kashmirhill/2014/07/10/facebook-experiments-on-users/#72ebffc51c3d

[8] https://www.clearme.com

model is devoid of the direct competition that rapidly improves the overall strength of the identity ecosystem.

One company, Veridium ID, has already imagined a biometrically enabled SSI system that could meet the goals of CLEAR while remaining portable. In their paper, *The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity*,[9] Veridium describes a biometric protocol that allows the user to remain in control of their biometric templates and to use them just like any other credential. In the fourth-generation identity ecosystem, offerings from CLEAR and Veridium could provide trusted biometric enrollment any system could then use to biometrically verify that subject. Because both systems can be in direct competition for each transaction, the incentive for the companies is to provide better value to customers. In identity systems, this means higher levels of security for the airport and easier enrollment and portability for the users.

Biometric providers are only one example of competition in the fourth-generation ecosystem. Another possible example is cloud data stores for private information. In SSI these are referred to as Identity Hubs.[10] [11] The intent of the identity hub is to allow users to share files and records in a specific context for a specific time. For example, if a patient has both a pulmonologist and a cardiologist, the records from each doctor can be stored in the patient's identity hub and then shared with the other doctor with verifiable user consent. Additionally, the user can limit the time frame and context in which that data is shared. Does the pulmonologist need to see the cardiologist's determination of the patient's internal heart pressure? She must simply provide the properly formatted request to the patient, and the patient can then grant the pulmonologist one-time access to the record. The pulmonologist can reference the cardiologist's findings and signature in their own documentation and then push that back to the patient's identity hub. Because patients will be able to select their own identity hub providers, these providers will be in competition to increase the security, speed, and usability of their products.

Virtually every credential issued or verified may have a competitive market associated with it that works to continually strengthen identity systems globally. Because fourth-generation systems are decentralized metasystems like the internet itself, they enable internet-sized potential for innovation and technical advancement.

3.3 End-to-End Security

Every person, device, and thing in the fourth-generation identity ecosystem has at least one private key. Private keys enable encryption and data signing. As a result, every message and connection coming into an organization or platform using SSI has an identified source. Furthermore, SSI can make it clear to the receiver if the data has been altered in transit.[12] While these capabilities are not new, SSI makes them ubiquitous.

Because the security provided by SSI is end-to-end, organizations can worry less about man-in-the-middle and replay attacks. This advantage can already be seen in modern end-to-end

[9] https://arxiv.org/pdf/1711.07127.pdf

[10] https://didproject.azurewebsites.net/docs/hub-overview.html

[11] https://identity.foundation/working-groups/storage-compute.html

[12] https://w3c-dvcg.github.io/ld-signatures/

authentication systems like Fast Identity Online (FIDO).[13] SSI systems include all the advantages of today's centralized end-to-end identity systems but add the polycentric and polymorphic properties that make digital credentials universally portable. This portability, as discussed in the previous section, is the primary enabler of competition and progress. The progress of end-to-end security due to decentralization and portability benefits the entire identity ecosystem.

3.4 Intrinsic Regulatory Compliance

Fourth-generation identity systems like SSI can be inherently compliant with any reasonable privacy regulation. This is because SSI systems put the control over credentials into the hands of the user with a private key that enables data signing. Therefore, any data a user shares with the platforms may come with user-signed verifiable user consent. This not only makes compliance with privacy regulations easier but raises the bar for what may be regulated in the first place.

Today, platforms need to know not only who is accessing them, but what they are doing while they are there. As a result, mountains of metadata are compiled to help platforms understand their users as well as identify unusual behaviors. Platforms need this level of understanding about their users for their own security and for the security of their patrons, but in contemporary systems this creates an intractable problem. If the platform detects abuse and shuts down the user's account, the user's data and metadata are orphaned, along with the user's right to remove or have a copy of their data. This happens because their identity is provided by the platform and when the platform deletes the identity, there is no identity for that person to use in proving ownership of the orphaned data. In the SSI model, users control their credentials and can therefore have their access removed from a platform without losing their data rights. Furthermore, the regulations supporting these rights become more easily enforced when citizens can prove legal standing.

3.5 Reduced Operating Costs

SSI's economic incentive realignments, new identity markets, end-to-end security, and intrinsic regulatory compliance benefit platforms by reducing operating costs. Economic incentives are realigned to scale per capita and allow platforms to better understand their operating costs at both small and large scales. New identity markets allow platforms to outsource their identity operations completely and focus on their core business. Additionally, platforms can easily utilize multiple providers without the normal technology lock-in associated with contemporary identity systems. End-to-end security reduces technical risk for platforms and decreases the frequency and severity of identity-related attacks. Additionally, because of the outsourcing of identity services, relatively inexperienced developers can innovate rapidly while maintaining world-class identity processes. Finally, inherent regulatory compliance means platforms can be free of disruptions and fines from various world governments.

[13] https://fidoalliance.org/what-is-fido/

4 The Bad News

4.1 The Pressure to Deliver Is Mounting

Sovereign Security Identity may provide the most flexible, scalable, and secure identity system the world has ever known, but also it may not. The fledgling technologies and standards are not currently providing a fully coherent ecosystem, and by virtue of SSI's flexibility, there is no orthodox implementation. So far, the factions within the SSI movement have been held together by a common vision of what is possible and a seemingly indefatigable drive to make SSI a reality, but as revenue streams thin and the pressure to turn SSI profitable mounts, it is inevitable that someone will say, "This is good enough to sell." The question is, will that happen before or after SSI lives up to its potential?

This question is very important because SSI is a metasystem – meaning that it is a bunch of loosely coupled components with a few rules to govern their interoperation. If the first-to-market solution does not institute the underlying principles, then it will have created something *like* SSI, but **not** SSI. This is similar to AT&T's "5G Evolution" offering, which capitalizes on the term "5G" but is not 5G.[14] Without some form of accreditation standard for SSI, the term itself may be used to label any technology offering. The window for reasonable dialogue and philosophical debate regarding "proper implementations" of SSI is closing. Because the world has rarely seen a Silicon Valley technology fully formed before the battle for market share ensues, the definition of an orthodox implementation may be critical to SSI's success.

4.2 Coexistence with Other Identity Systems

Another potential problem for SSI is the adoption of SSI by platforms. Identity has become a source of free raw materials for many platforms. Conversion to SSI for these platforms, if it happens, is not likely to be as "privacy enhancing" as SSI intends to be because it would shut off their source of revenue. It would be unsurprising if platforms began to offer an "SSI Evolution" option to lure users away from orthodox implementations which represent an existential threat to the surveillance capitalist.[15] It is not as if there is a regulatory threat to counterbalance the unbounded ingestion, analysis, and resale of personal information. By confusing the public and regulators, surveillance capitalist platforms may be able to stave off such regulation indefinitely.

4.3 Retooling Security Systems

SSI enables peer-to-peer encrypted connections in a way that makes them uncorrelatable with other connections. Today, if someone uses a platform-enabled encrypted messenger like Facebook's WhatsApp,[16] he can securely communicate with other users through Facebook's platform. However, it is possible to detect his social network because he uses the same identifier for every conversation. When combined with the frequency and length of communication, it becomes possible to know which contacts are "closest" to him. By looking at how the other

[14] http://about.att.com/innovationblog/5g_evolution_record

[15] https://en.wikipedia.org/wiki/Surveillance_capitalism

[16] https://www.whatsapp.com

nodes overlap, it is possible to understand his circle of family and friends. In contrast, a messenger built on SSI could use a unique identifier for each conversation, which would break the social graph into individual relationship segments.

While there are still detectable signals and patterns in the data, anyone who is targeting people using these social connections will now have a much harder time separating the mother of three from the small-business owner or the wealthy entrepreneur from the starving artist. Without clear social connections or a platform from which to gather trillions of data points, the tools built over the last few decades to support cybersecurity and social network analysis may become far less useful as the signal in the noise attenuates.

4.4 **Global Reputation**

The concept of reputation systems exists in SSI to assess credential issuers and verifiers. However, there is nothing to prevent the establishment of reputation systems that report on individuals. Because SSI incentivizes lifelong digital identity, the institution of reputation systems regarding individuals could do more harm than good as over a person's life she is evaluated only on past mistakes and on not her ability to learn from the lessons those mistakes have afforded her.

Similar systems have been instituted in China[17] and have been problematic for its citizens. Chinese citizens may be banned from travel, excluded from school because of their parents' scores, and shamed into paying debts. These actions clearly favor the state and corporations by quantifying people's behavior and providing another metric with which to judge them, but reducing humans to a number has never benefited those enumerated.

4.5 **Enabling Criminal Networks**

SSI enables private, encrypted, peer-to-peer relationships and cryptographically verifiable credentials. For criminal and terrorist networks, this is helpful because a criminal can securely communicate and prove her affiliation and position in the criminal hierarchy. This becomes possible to do without revealing any personal information that might give her criminal cohort an informational advantage over her.

While credential issuance is complex, there is no reason to believe there will not be "an app for that" which makes issuance as easy as sending an email. It is easy to imagine a terrorist organization providing credentials to its members. A recruiter could offer a credential to a new recruit that accredits his allegiance to the organization. The recruit may then travel across boarders using the state-issued passport collocated in the same digital wallet with the terrorist organization's credential. The recruit can then complete his terrorist training and be accredited as trained. Then, this newly minted terrorist returns home, where he can be contacted directly via encrypted messages to link up with others and form an operational cell. The members of this cell could be further identified by an operational credential that allows them to authenticate each other as members of the cell and communicate securely.

[17] https://en.wikipedia.org/wiki/Social_Credit_System

5 Summary

MITRE is investigating SSI not only to determine the reality of its merits and drawbacks, but to understand if and how it should be implemented within MITRE's federal sponsors. Over the next year or more, MITRE will assess the maturity of SSI technologies, standards, and concepts firsthand through implementation and contribution with the hope that SSI lives up to its ideologies. When it does, it will make the online world a safer world.