Self-Sovereign Digital Identity

A Paradigm Shift for Identity

Kalman C. Toth | NexGenID
Alan Anderson-Priddy | Portland State University

Self-sovereignty is a paradigm shift for digital identity that promises important benefits but lacks a definitional consensus. Herein, we validate nine properties of self-sovereignty proposed by credible sources, propose five new properties, and apply the features of our architecture for digital identity to reason about and validate these properties.

There is an alarming crisis of identity on the web.[1] The information repositories of Fortune 500 companies, like J.P. Morgan, Sony, Target, Home Depot, and Equifax, have suffered breaches that have enabled identity theft and fraud on a global scale. And the Internet fails to distinguish hackers from law-abiding consumers and fake news from truthful journalism.

The 2017 Equifax breach exposed the private and personally identifying information of more than 140 million American consumers.[2] More recently, publicity surrounding the Facebook/Cambridge Analytica scandal revealed that the private records of more than 87 million Facebook users were improperly disclosed—allegedly, users were microtargeted with political ads. U.S. Congress and Parliament in the United Kingdom have held hearings concerning consumer privacy, voting, and elections. Europe hopes the new General Data Protection Regulation will mitigate their serious concerns.

Consider the root causes. Over the last 25 years, advertising-based business models, lack of consumer awareness, and weak privacy legislation have enabled web service providers to capture massive amounts of private information. At the same time, service providers have collected enormous volumes of personally identifying information to sustain their centralized password-based logon schemes. Coincidentally, populous China and India have constructed huge centralized national identity systems capturing the personally identifying information of their citizenry, including their biometric data. Given the epidemic of large-scale server-side breaches, user frustration managing passwords, and growing concern about privacy and surveillance, it is not surprising that server-centric solutions have rapidly fallen out of favor.

Single sign-on and federated identity access and management systems along with tools helping users manage passwords have not been able to cope with the proliferation of passwords or contain the privacy, security, identity theft, and impersonation risks associated with passwords.

User-centric approaches for handling identity have gained favor lately. The OpenID series of protocol standards enables users to acquire identity tokens and delegate permissions for accessing online resources, giving users a measure of control. However, user authentication is centralized, password based, and wholly dependent on identity providers.

In recent years, it has been suggested that a user-centric identity model would solve the so-called identity crisis, enabling individuals to better manage and control their privacy. Under this model, everyone would have a digital persona describing who they are, and

Digital Object Identifier 10.1109/MSEC.2018.2888782
Date of publication: 14 May 2019

Privacy by Design: Toward Intelligent Software Agents

Ann Cavoukian | Ryerson University

Corporations and web service providers are collecting massive volumes of personally identifying and private information, including purchases, locations visited, employment records, tax returns, health records, and social profiles. Although they have invested heavily in costly mechanisms for detecting tampering, fraud, and data breaches, such protections do not appear to be coping. New regulations like the European Union's General Data Protection Regulation have been introduced to address privacy protection in the face of this data deluge and to enforce a new proactive approach called *privacy by design* and *privacy as the default*. But what more can be done?

What if people had their own intelligent software assistants, or what we call *smart data*,[S1] to protect their information assets? Such personal software agents would protect their private records stored in web repositories and enable users to effectively manage what information they choose to disclose and with whom they wish to share it. Solutions would be architected to deliver privacy by design: establishing privacy as the default setting; reducing the risks of human error; and securing transactions end to end, with full lifecycle protection. Much less private information would need to be collected; personal freedoms would be increased; risks to individuals from privacy infractions would be mitigated; and from a business perspective, costs for corporations, governments, and individuals would be greatly reduced.

Kalman C. Toth and Alan Anderson-Priddy describe in this article an identity architecture where a type of software agent tightly binds digital identities to their owners to enhance privacy and strengthen security. This thought leadership demonstrates that we are moving in the right direction and supports giving back control over one's personal information to the individuals to whom it relates—personal control, the true meaning of privacy!

Ann Cavoukian is the three-term Information and Privacy Commissioner of Ontario, Canada. She is widely respected for her critical contributions to the European Union's General Data Protection Regulation in her creation of privacy by design. She is presently the Distinguished Expert-in-Residence, leading the Privacy by Design Centre of Excellence at Ryerson University, Toronto, Canada, and she is the past executive director of the Privacy and Big Data Institute at Ryerson University.

Reference

S1. H. Jones, "Accelerating the future of privacy through SmartData agents," *Forbes*, Nov. 3, 2018. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2018/11/03/accelerating-the-future-of-privacy-through-smartdata-agents/#2acd2be63d79

they would use a common identity protocol to collaborate with each other. This thinking launched the idea of self-sovereignty, where digital identities are tightly controlled by their owners.

Expanding on this thinking, we believe digital identities should be intuitive and easy to use. Additionally, they should be virtualized to look and behave like identities used in the real world. This approach would help achieve user buy-in and facilitate adoption.

Properties of Digital Identity

Although account/password logon schemes are simple to use, they are vulnerable to loss, theft, cracking, and hacking, and they do not relate very well to how we handle identities in the physical world. Consider that account numbers and email addresses do not necessarily characterize their owners—nor do credit card numbers or social security numbers. On their own, they may not specify any meaningful identifying information about the holder and could be obfuscating. Typically, such identifiers point to fragments of private information of the user stored somewhere in the cloud, where they are vulnerable to breaches by unscrupulous parties.

Kim Cameron[3] defines digital identity to be "a set of claims made by one digital subject (e.g., a user) about itself or about another digital subject." He adds that claims are asserted truths of a subject (also called *attributes*) and that a subject may be a person or a thing. His definition implies that a subject can have multiple digital identities, each specifying claims of the subject; that claims of a first subject can be attested by another subject; and that claims can specify permissions granted by one subject to another. Cameron explains that a subject should only disclose information for intended purpose(s), and relying parties

should only use information provided to them with owner consent.

Cameron also asserts that a system handling digital identities should be able to reliably deliver identifying information of one subject to another subject while detecting deception, i.e., thwart man-in-the middle, phishing, pharming, and other impersonation attacks.

Established in April 2017, the W3C Verifiable Claims Working Group (VCWG)[4] launched a project to develop a machine-readable identity data model enabling collaboration among owners, issuers, and verifiers. Project goals include automating the provisioning of claims and credentials that can be deployed across a range of industries. Identity credentials are to be composed of sets of claims, where claims are signed and cryptographically verified. To the best of our knowledge, other identity-related issues, including application programming interfaces (APIs), exchanging digital identities, and identity protocols, have not yet been addressed. It can be safely said that the working group is progressively formalizing Cameron's perspectives.

Cameron's work combined with that of the W3C VCWG implies that digital identities should be specified in the form of one or more claims conforming to a common identity data model enabling consent, disclosure, and reliable delivery of identifying information between subjects.

Properties of Self-Sovereign Digital Identity

Arguably, self-sovereign digital identity promises to solve the identity crisis.[5] Privacy legislation in the western world commonly requires service providers to safeguard and ensure that private information is used only for consented purposes. Giving citizens explicit sovereignty over their digital identities promises to enhance privacy for citizens. Plus, reducing reliance on passwords means that service providers will not need to collect as much private and personal information, thereby easing their responsibility and burden for safeguarding private data. Self-sovereignty also promises to provide identities to those who have lost or have been dispossessed of their identities. Such persons can acquire digital identities proofed and attested by credible parties even when they cannot be acquired from designated identity issuers.

Christopher Allen[6] states that self-sovereignty over identity is achieved when users are able to control their digital identities and when central authorities have no authority over them. Allen explains that a consensus definition and applicable rules for self-sovereignty have not yet been established. To provoke discussion, he offers 10 principles of self-sovereign identity, which we have abstracted with commentary in Table 1.

Recently, the Sovrin Foundation[7] announced a project to establish a public utility for self-sovereign identity serving the Internet. Sovrin plans to leverage the VCWG's standard for an identity data model and employ public blockchain technology to implement a decentralized registry system for the discovery of public keys. Such keys will be used to verify digital signatures attached to verifiable claims. Sovrin defines self-sovereign identity as a "lifetime portable digital identity that does not depend on any central authority and can never be taken away." Close examination reveals that Sovrin's definition relies on Allen's principles of control, access, persistence, and portability.

Given the lack of definitional consensus, we evaluated the work of Cameron, the VCWG, Allen, and Sovrin, with the aim being to identify essential properties for self-sovereignty where general agreement exists.

As duly noted in Table 1, we conclude that existence, transparency, and protection as described by Allen should be set aside because they require further discussion. However, we concur with the following properties of self-sovereignty:

- *Identity data model*: The VCWG is consistent with Cameron, thereby enabling control, access, persistence, portability, and interoperability.
- *Control, access, persistence, and portability*: Proposed by Allen, these properties are reinforced by the Sovrin Foundation's definition for self-sovereignty.
- *Consent and disclosure*: These properties are advocated by Cameron, reinforced by Allen, and widely accepted.
- *Interoperability*: Proposed by Allen, this is an essential property that enables collaboration using identities controlled by owners governed by an identity data model (e.g., VCWG's).
- *Secure identity transfer*: Proposed by Cameron, digital identities of owners must be securely transferred to prevent man-in-the-middle attacks.

Observe that these properties do not cover situations where owners lose control of their digital identities because of poor user interfaces, counterfeiting, weak identity verification, spoofed identities, or insecure channels. We believe the following additional properties cover these cases.

- *Usability*: Owners must be able to intuitively and reliably control, manage, and use their self-sovereign

digital identities as well as the digital identities of collaborating parties.

- *Counterfeit prevention*: It should not be feasible for malicious parties to create bogus digital identities by simply acquiring the self-sovereign digital identities of other owners.
- *Identity verification*: Relying parties should be able to verify that digital identities are controlled by their owners or were controlled by their owners when created.
- *Identity assurance*: Relying parties should receive objective evidence that presented digital identities truthfully characterize their owners, thereby preventing spoofing.
- *Secure transactions:* Once owners have securely exchanged their digital identities, it should not be possible for malicious parties to read or tamper with their transactions.

We next explain and validate the 14 properties of self-sovereignty identified in Table 2.

Self-Sovereign Digital Identity: Property Descriptions

Identity Data Model, Persistence, and Portability

A common identity data model is needed to support the specification of digital identities comprising self-sovereign claims. Such a model must enable control and access by owners and relying parties, persist digital identities in memory controlled by users and providers, and support portability for secure identity transfer.

Control, Access, Consent, and Disclosure

In the physical world, users keep and control their identities in their wallets and address books, using them to consistently identify themselves and collaborate with others. Similarly, owners in the digital world should be able to control and access their digital identities to

Table 1. Allen's principles for self-soveign identity.

Allen's 10 principles of self-sovereign identity	Our comments and perspectives
Existence: A self-sovereign identity makes public and accessible some limited aspects of an individual's identity.	This principle seems self-evident. Instead we propose verifying the existence of identities.
Control: Identity owners have ultimate control over their identities and claims whether self-specified or specified by others.	This is consistent with Cameron's definition, which we expand upon.
Access: Owners have access to read and update their own identities—there are no gatekeepers (i.e., central authorities).	Agreed. We support and expand upon this important property.
Transparency: Systems and algorithms managing identities must be free, open source, and independent of architecture.	Systems and algorithms may not always be free or open—requires further discussion.
Persistence: Identities must be long-lived and updatable, and the owner should be able to forget them when no longer needed.	Agreed. A data model structuring persistent identities and claims is needed.
Portability: Information and services about identity must be transportable and must not be held by a singular third party.	Agreed. Implies a common data model for identity controlled by owners is needed.
Interoperability: Identities should be widely usable crossing international boundaries to create global identities.	Agreed. Implies common programming interfaces and protocols are needed.
Consent: Owners must consent to the use of their identities and specified claims by other parties, whether interactive or not.	Agreed. Is consistent with Cameron's definition and those of others.
Minimalization (disclosure): Disclosure of private information involves the minimum amount necessary for the task at hand.	Agreed. Validates disclosure property of Cameron and that of other writers.
Protection: Freedoms and rights of the individual should be preserved over the needs of the network when there is a conflict.	An important and challenging policy issue that we have set aside for further study.

interact with other parties. And they should be able to give consent and disclose just enough private information to satisfy the needs of relying parties. Digital identities need to be strongly bound to their owners to counter loss and theft.

Interoperability

Owners and providers must be able to use their digital identities to reliably and securely interact with each other over the web. Effective interoperability ensures that users and providers can correspond by way of the identity data model's APIs using collaborative web services, such as email, text messaging, and conferencing. Interoperability across the Internet must necessarily leverage the web's transport layer protocols.

Usability

User interfaces are effective if they hide underlying complexity, such as cryptographic operations, biometric mechanisms, database access, and protocols. Ordinary users should not need to understand or know how to use such mechanisms. Usability[8] significantly increases if owners can intuitively control their digital identities and avoid making fatal mistakes. Effective control can be achieved by rendering digital identities that mimic physical identities and can be intuitively selected and managed following familiar workflows used in the physical world.

Counterfeit Prevention

The physical world uses special materials, watermarks, photographs, logos, and antitamper technologies to thwart the creation of bogus credentials. Similarly, it should be infeasible for malicious parties to create counterfeit digital identities. Reliable mechanisms are needed to ensure that owners remain in control of their digital identities while preventing tampering, social engineering, channel sniffing, and other attacks.

Identity Verification

Owners of self-sovereign digital identities must be able to use them to reliably prove who they are whether collaborating synchronously or asynchronously. When collaborating online (synchronously), each owner presents a self-sovereign digital identity to the other party to identify themselves. Both parties must be provided assurances that the received digital identity was not modified in transit and that the originating owner controls the received digital identity. When collaborators use an asynchronous service like email or a short messaging service (they are not concurrently online), they must be provided assurances that the corresponding party controlled the digital identity used to originate asynchronously received message(s) or transaction(s).

Identity Assurance

Relying parties must be provided assurances that digital identities truthfully characterize their owners rather than imposters. In the physical world, third-party identity proofing is used to provide such assurances. Similarly, a requesting digital identity owner should be able to submit her digital identity and personally identifying information to an issuer who proofs the requester and issues an attestation when successfully identity proofed. Binding the issuer's attestation and digital identity to the requester's digital identity provides remote identity assurances. Proofing can be in-person or online. In-person identity proofing normally achieves higher levels of identity assurance than online proofing because the issuer can ask probing questions and inspect physical credentials. When a requester and an issuer are well-known to each other, personally identifying information may not need to be communicated. Attestations by multiple trusted parties can mitigate the risks associated with a single root of trust and the possibility of collusion.

Secure Identity Transfer

Digital identities may specify publicly available information, such as names, cell numbers, and email addresses, as well as identifying information, such as social security, medical provider, and credit card numbers. Owners should be able to securely transfer their digital identities to other parties, especially when specifying sensitive data.

Secure Transactions

Once their digital identities have been securely transferred, owners should be able to use their digital identities to secure their transactions and maintain their privacy.

Table 2. Proposed essential properties for self-sovereignty.

Identity data model	Interoperability
Persistence	Usability
Portability	Counterfeit prevention
Control	Identity verification
Access	Identity assurance
Consent	Secure identity transfer
Disclosure	Secure transactions

Validating Properties of Self-Sovereignty

Our Architecture for Digital Identity (NexGenID)

We have applied the functions, features, and mechanisms of our identity architecture to validate the 14 properties of self-sovereignty identified in Table 2. Our reasoning about how each property can be satisfied is explained later. We acknowledge that our peers may challenge our design and thinking about the proposed properties and may discover other properties of self-sovereignty. We welcome constructive debate.

Our identity architecture[9] combines identity specification, user authentication, and third-party identity proofing and attestation to create digital identities that prove "who you are." Digital identities (also called *e-credentials* and *identity credentials*) are virtualized and safeguarded within the personal devices of owners having preinstalled software agents (apps) called *identity engines*.

Figure 1 illustrates owners controlling and using their digital identities to securely transfer their digital identities; present, register, and verify identities; proof, attest, and issue identities; and secure transactions. The functions and features of our architecture are detailed in issued and pending U.S. patents.

Identity Data Model, Persistence, and Portability: Enable Specification, Control, and Access

Our identity model enables owners to specify, control, and access their digital identities including identifiers, claims, attributes, and images. Our data model also supports affixing multiple owner attestations to digital identities and persisting digital identities within the personal devices of owners, thereby enabling portability of digital identities, backup, recovery, and escrow.

The VCWG identity data model defines how credentials are composed of claims (initially, VCWG addressed only claims). The congruency between our identity model and that of the VCWG validates our assertion that having a robust identity model is a foundational property for self-sovereignty. Our identity model enables an owner to present a public copy of one of her self-sovereign digital identities to prove who she is to another party.

Control, Access, Consent, and Disclosure: Digital Identities Strongly Controlled by Owners

Figure 2 depicts selected components of our identity architecture showing an owner, a personal device, an installed identity engine, and digital identities of the owner and collaborating parties. Owners use these components to

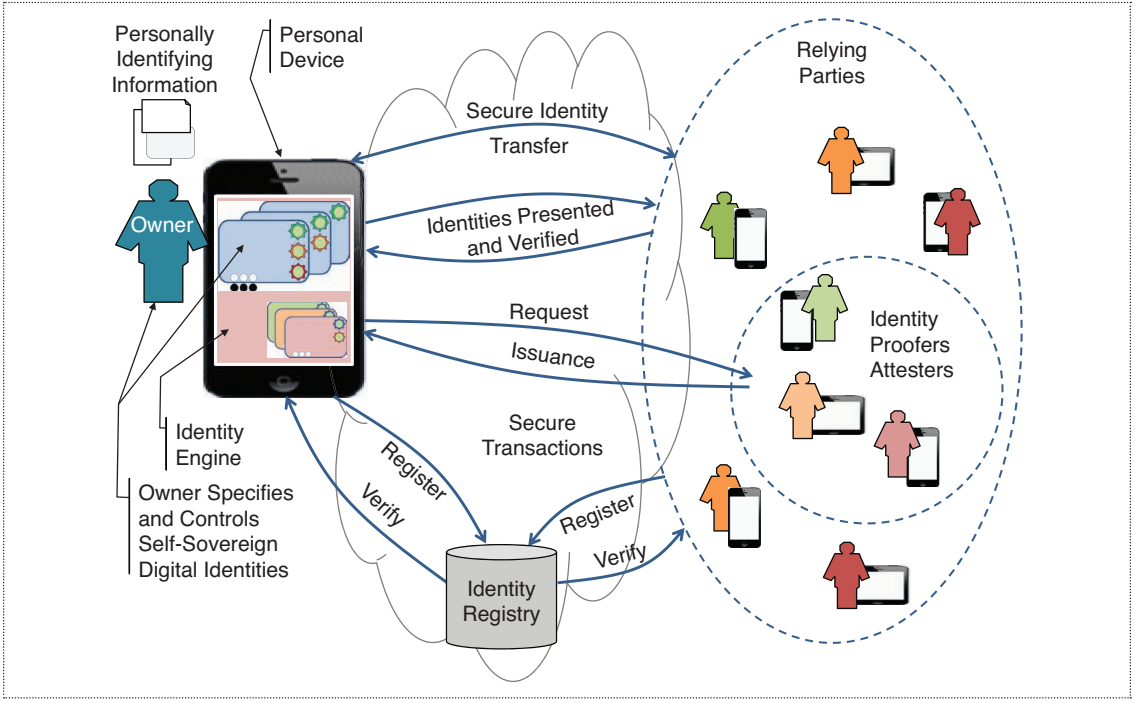

Figure 1. Owners can create and control their digital identities using personal devices to prove who they are, verify the identities of other parties, have their identities proofed and attested by way of in-person and online encounters, and use them to collaborate reliably and securely.

establish sovereignty over their digital identities by maintaining a sovereign image of each digital identity within the identity engine. Only owners can create and use their sovereign images. However, owners can send public copies of their digital identities to relying parties.

Figure 2 also depicts the identity engine encapsulating the owner's authentication data enrolled and used by the authentication mechanisms of the owner's personal device. The identity engine does not reveal authentication data outside its context other than to these mechanisms. Further, the identity engine is isolated from the logic of the device's authentication mechanisms. Given that the owner's sovereign images and authentication data are controlled by the owner's identity engine, these mechanisms strongly bind the digital identities to the owner.

Thus, our architecture validates the essential property of self-sovereignty that owners strongly control and have access to their digital identities. Owners are therefore able to control what private information is disclosed when selecting and presenting their digital identities.

Interoperability: Owners Use Digital Identities and Application Services to Collaborate

Our R&D was partially motivated by Cameron[3] who pointed out that the Internet is crucially missing an identity layer for reliably connecting collaborating parties. The benefits of implementing an identity layer between the Internet's application layer and the transport layer are many. Such a layer can support consistent interfaces for application services, thereby enhancing software maintainability; encapsulating critical identity-related logic, programming interfaces, and protocols; and streamlining access to Internet transport layer services. Figure 3 depicts our approach for achieving interoperability across applications and services employing personal devices, identity engines, and digital identities of owners. Complexity can be contained by encapsulating identity-related data and methods within identity engines collaborating on behalf of owners across the identity layer.

Creating such a standard will require considerable effort, consensus, and time. Our start-up approach will bootstrap our development by establishing a limited-scope project that deploys personal devices with identity engines across a constrained network context. A pilot project in a moderately sensitive sector will be a suitable target. For example, digital business cards (identities) may be deployed in partnership with a professional network to simplify access to their web-based affiliate services. Members could also use their digital business cards to securely collaborate with each other. This project would enable entering into other social networking, education, legal, government, and financial markets. Our architectural design demonstrates that the interoperability property can be satisfied.

Usability: Virtualized Digital Identities Mimic Identity Handling in the Physical World

To manage complexity for users and facilitate technology adoption, user interfaces should be visually easy to use, unambiguous, intuitive, familiar, efficient, and flexible.[8] They should also be rendered consistently across the full range of use cases to ensure they are long-lasting and can be adapted for evolving needs. Our architecture for digital identity leverages markups providing functionality that enables users to combine images and claims to create identities that can be virtualized. Figure 4 depicts such identities including one representing an anonymous blogger.

Owners can use their identity engines to mimic processes used in the physical world to acquire and issue identities. Each identity engine exposes a user interface that enables the owner to intuitively control her digital identities to prepare, proof, attest, and issue them (see Figure 5). Our architecture for digital identity therefore tackles the often-underestimated value of effective user interfaces and demonstrates that the usability property of self-sovereignty can be satisfied.

Counterfeit Prevention: Leverages Public/Private Key Cryptography

Our architecture adapts and combines features of public-key infrastructure, pretty good privacy, and a recommendation by Asokan[10] leveraging public/private key-pairs for distinct purposes. Our design strategy thwarts

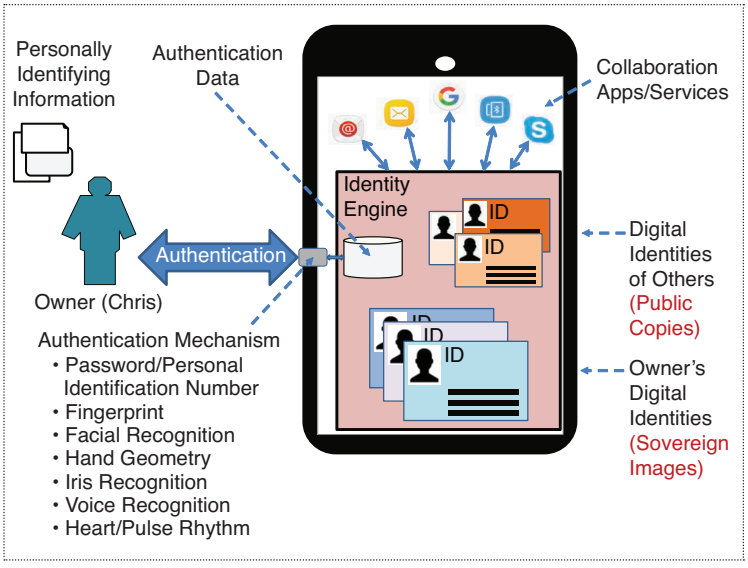

Figure 2. The owner has a personal identity device with an installed identity engine encapsulating her authentication data. The owner can select one of her digital identities, an identity of another party, and a collaboration service to interact securely with other parties.

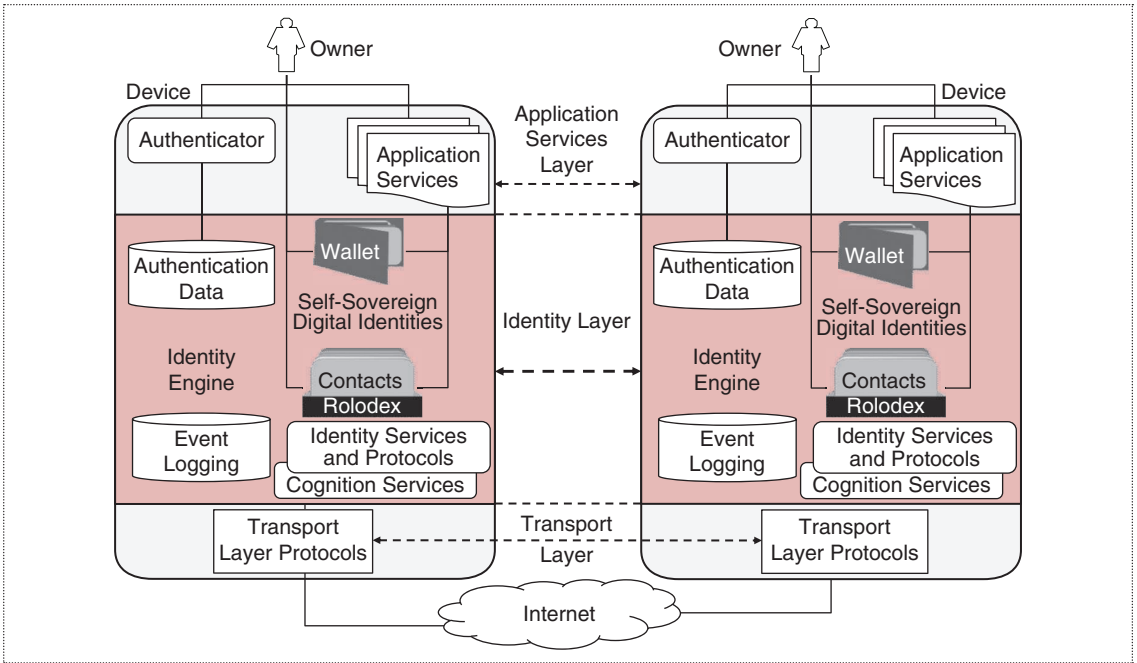

Figure 3. Identity engines expose a user interface; integrate with the device's authentication mechanisms, including biometrics; support application layer services; and leverage the transport layer to enable interoperability among identity engines across the identity layer.

counterfeiting and elevates resistance to cryptographic attack. When a digital identity is created, distinct public/private key-pairs for digital signing, encrypting, and digital sealing are bound by the owner's identity engine to the sovereign image of the digital identity, thereby protecting the private keys from tampering and inadvertent disclosure.

As illustrated in Figure 6, whenever a digital identity is presented to a relying party, the identity engine presents only the public copy of the digital identity, which includes only the public keys—the associated private keys are not revealed. It is infeasible to calculate a private encryption key (of adequate length) from the paired public encryption key. If a malicious party captures the public copy of a digital identity, it is prohibitive for that party to discover the distinct private keys from the presented public keys for the purpose of creating a counterfeit identity. However, a relying party can challenge an originator to prove possession (control) of the private keys. Our approach demonstrates that it is feasible to construct a design that prevents bogus copies (counterfeits) of digital identities from being created, thereby satisfying this property.

Figure 4. Examples of virtualized digital identities: (a) a business card, (b) a driver's license, (c) a bank card, and (d) an anonymous blogger.

Synchronous Identity Verification: Using Proof of Possession and Proof of Custody

When collaborating interactively (synchronously), our architecture for digital identity enables owners to play both originating and relying roles when presenting their digital identities. As illustrated in Figure 6, once an originating owner has presented her digital identity to a relying party, the identity engine of the relying party verifies the integrity of the presented digital identity and then obtains proof that the originating owner controls the presented digital identity.

To accomplish this, the relying party's identity engine executes a proof-of-possession challenge[10] using a selected public key of the presented digital identity. This

challenge can only be satisfied by the paired private key of the originator's sovereign image. Upon a successful challenge, the identity engine of the relying party can send a demand to the identity engine of the originator's personal device to locally authenticate the holder to obtain proof of custody by the owner. This strategy demonstrates that the identity verification property for self-sovereignty can be satisfied when collaborating synchronously.

Asynchronous Identity Verification: Using a Proof of Existence Identity Registry

Parties can collaborate asynchronously when using email, text messaging, and other such applications. To support asynchronous identity verification, our architecture includes a capability for registering digital identities in an identity registry that enables relying parties to verify the existence of digital identities.

We have combined our digital sealing method with a proof-of-existence method popularized by blockchain.[11,12] As depicted in Figure 5, owners can register digital identities in the identity registry when created, updated, and issued. Issuers can register digital identities once proofed and attested. The registering process hashes the digital identity, storing the hashed record into the registry. The registering party selects one of her digital identities to digitally seal the hashed record and link the digital seal to the hashed record stored in the registry. Digital seals linked to the hashed record of registered digital identities provide assurances that a hashed digital identity was controlled by the owner when registered. When a relying party has acquired a digital identity, he can verify the existence of the presented digital identity in the identity registry. If found in the registry, the attached digital seal can be verified to determine if the digital identity was registered by the owner or issuer(s), thereby proving it was controlled by the owner when registered.

The identity registry can be made publicly available because only hashes of digital identities are stored, making the registry immune to breaches. We plan to explore the potential use of blockchain technology to implement a decentralized proof-of-existence identity registry for verifying self-sovereign digital identities and their public keys. Our approach confirms that the identity verification property for self-sovereignty can be satisfied when collaborating asynchronously.

Identity Assurance: Using Proofing, Attestation, and Digital Seals

Third-party identity proofing and attestation is needed to provide assurances that a digital identity

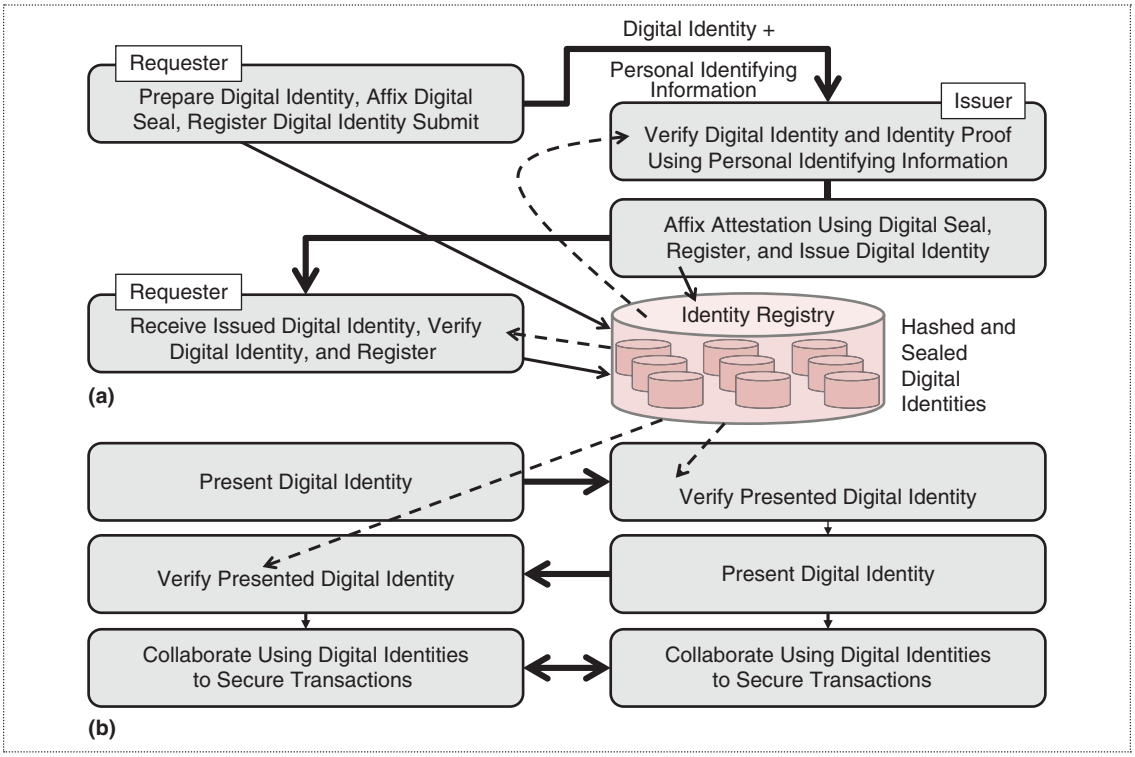

Figure 5. A requesting owner registers his/her digital identity before and after issuance. (a) The issuer registers the requester's digital identity once proofed and attested. (b) Later, when owners use their digital identities to collaborate synchronously or asynchronously, relying parties can use the identity registry to verify the existence of presented digital identities.

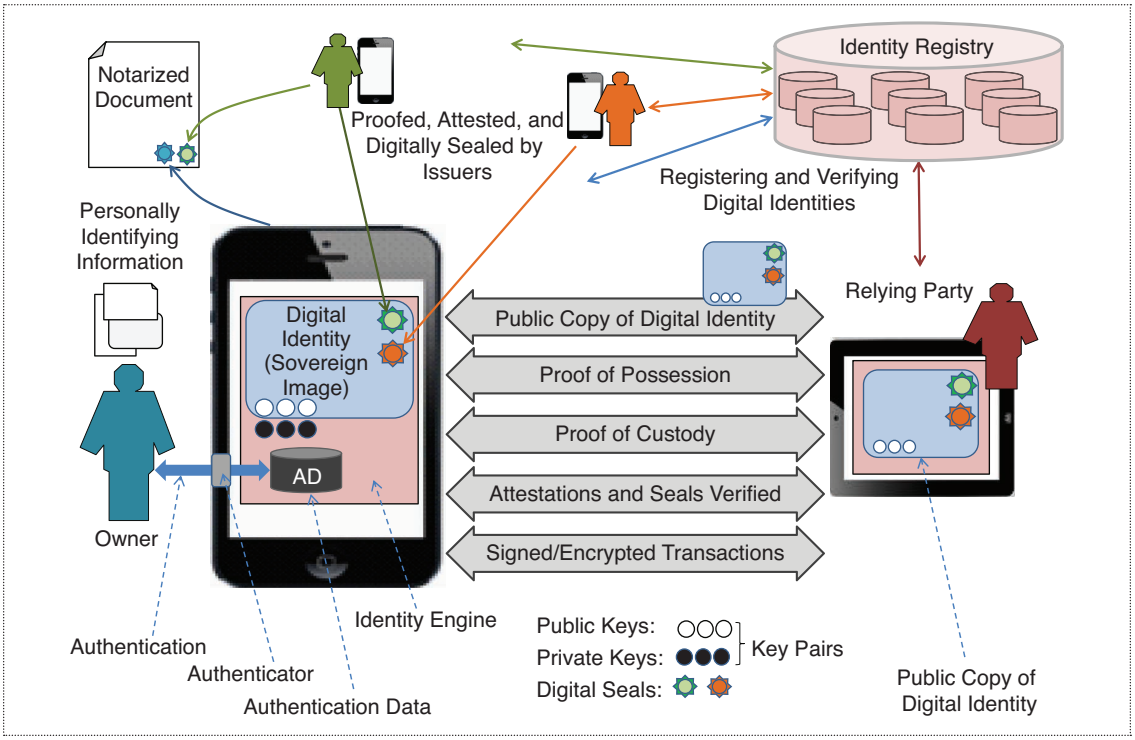

Figure 6. (a) Chris's digital identity has been proofed, attested, and digitally sealed by two issuers. (b) The relying party, receiving a public copy of her digital identity, uses it to verify that Chris possesses and has custody of her digital identity and then verifies attestations and seals of issuers.

characterizes the owner and not some imposter. Our architecture mimics how physical identities, such as driver's licenses and passports, are proofed and attested. Depicted in Figure 5, a requester can use his identity engine to present one of his digital identities and personally identifying information to another owner, the issuer. The issuer uses her identity engine and the provided identifying information to proof the claims of the requester's digital identity. If successfully proofed, the issuer specifies an appropriate attestation (e.g., "proofed") and selects a designated private key to create a digital seal that binds the attestation and issuer's digital identity to the requester's digital identity. This method achieves elevated nonrepudiation strength over a traditional digital signature.

Referring again to Figure 6, relying parties can use their identity engines to verify attestations by inspecting digital seals affixed to digital identities presented to them. Digital identities can also be attested and issued by multiple parties. And owners can meet in-person to issue digital seals and attestations over direct connections [e.g., near-field communications (NFC), Bluetooth, and Wi-Fi]. Our architecture for digital identity elevates identity assurances for owners so they can reliably use their self-sovereign digital identities to prove who they are.

Secure Identity Transfer: In-Person and Online Methods

Digital identities should be transferred securely to prevent phishing, pharming, impersonation, and other man-in-the-middle attacks. When digital identities do not specify sensitive information, collaborating parties can use their identity engines to transfer them by simply meeting in-person and transferring them directly using NFC, Wi-Fi, QR codes, USB cable, memory cards, and the like. Another simple strategy is to have their identity engines exchange digital identities in the clear using a messaging service. The identity registry can be used to confirm that they were not corrupted, retrying when errors are detected. One-time-passwords and elliptical curve cryptography can also be leveraged to exchange digital identities securely.

Secure Transactions: Using Public/Private Keys of Digital Identities

Once collaborators have exchanged their digital identities, their identity engines can use them to securely collaborate. The public/private encryption key-pairs associated with the digital identities of collaborators enable transactions to be bilaterally secured using the signing/verifying and encrypting/decrypting key-pairs. Attestations affixed

by digital seals to digital identities can be verified by both parties using the key-pair used to create and verify digital seals. Similarly, documents can be notarized by using these key-pairs to create and verify attestations affixed to documents (e.g., "this is a true copy") using digital seals. Our approach demonstrates that it is feasible to deploy digital identities such that they satisfy the secure transactions property of self-sovereignty.

Our perspectives and reasoning about digital identity have provided fresh insights and discovered new properties characterizing self-sovereign digital identity. We validated 14 properties of self-sovereignty by reasoning about the work of Cameron, the VCWG, Allen, and the Sovrin Foundation, and by applying the features of our architecture for self-sovereign digital identity.

Self-sovereign digital identity promises to solve the identity crisis. We believe that deploying self-sovereign identities will greatly reduce impersonation, fraud, and breaches. Transitioning from using passwords to using digital identities will simplify access for users and reduce the need for providers to gather large volumes of private information.

Furthermore, owners will be able to use the same digital identities across multiple sites and users; consumers will be able to reliably prove who they are without having to physically meet; and the public will be able to verify digital identities presented to them.

To enhance our understanding of self-sovereignty and improve our identity architecture, we plan to study the following:

- adapting recommendations emerging from the W3C VCWG
- incorporating user consent into our identity architecture
- automating policies for aligning provisioned identity assurances with transactional risks
- employing containerization technologies to protect against hacking and malware
- employing blockchain technology to decentralize our proof-of-existence registry. ■

References

1. J. Macnight, "Will the digital world solve the identity crisis?" TheBanker.com. Accessed on: Jan. 2, 2018. [Online]. Available: http://www.thebanker.com/Transactions-Technology/Will-the-digital-world-solve-the-identity-crisis
2. CBS This Morning, "Equifax data breach was 'entirely preventable,' congressional report finds," CBS News, Dec. 11, 2018. Accessed on: Feb. 26, 2019. [Online]. Available: https://www.cbsnews.com/news/equifax-data-breach-was-entirely-preventable-congressional-report-finds/
3. K. Cameron, "The Laws of Identity," May 2005. [Online]. Available: http://myinstantid.com/laws.pdf
4. World Wide Web Consortium (W3C), "Verifiable credentials data model 1.0: Expressing verifiable information on the web," Cambridge, MA. [Online]. Available: https://www.w3.org/TR/verifiable-claims-data-model/
5. N. Kshetri, "An opinion on the 'Report on Securing and Growing the Digital Economy,'" *IEEE Security Privacy*, vol. 15, no. 1, pp. 80–85, 2017.
6. C. Allen, "The path to self-sovereign identity." Accessed on: Apr. 27, 2016. [Online]. Available: http://www.coindesk.com
7. Sovrin Foundation, "Sovrin: A protocol and token for self-sovereign identity and decentralized trust," Salt Lake City, UT. Accessed on: Feb. 27, 2019. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf
8. D. Balfanz, G. Durfee, R. E. Grinter, and D. K. Smetters, "In search of usable security: Five lessons from the field," *IEEE Security Privacy*, vol. 2, no. 5, pp. 19–24, 2004.
9. K. C. Toth and A. Anderson-Priddy, "Architecture for self-sovereign digital identity," in *Proc. 31st Int. Conf. Computer Applications for Industry and Engineering (CAINE)*, New Orleans, LA, 2018.
10. N. Asokan, B. Niemi, and P. Laitinen, "On the usefulness of proof of possession," in *Proc. 2nd Annu. PKI Workshop*, Apr. 28–29, 2003, pp. 136–141.
11. PoEx Co., Ltd., "What is proof of existence?" Accessed on: Feb. 27, 2019. [Online]. Available: https://docs.proofofexistence.com/
12. K. Robles, "BlockchainMe, a tool for creating verifiable IDs on the blockchain," GitHub. Accessed on: Dec. 2, 2016. [Online]. Available: https://github.com/kiarafrobles/blockchainMe

Kalman C. Toth is a Professional Engineer registered in British Columbia, Canada, and is the founder and chief executive officer at NexGenID. His research interests include information security, software and quality engineering, e-commerce, and distributed database systems. Toth received a Ph.D. in electrical and computer systems engineering from Carleton University, Ottawa, Canada. Contact him at kal@nexgenid.com.

Alan Anderson-Priddy is with the Office of Information Technology at Portland State University. His research interests include software and systems consulting, technology research and development, enterprise software integration, and software prototype development. Anderson-Priddy received a master's degree in software engineering from Portland State University, Oregon. Contact him at alan@nexgenid.com.