Agent-Based Digital Identity Architecture

Kalman C. Toth Ph.D. P.Eng.

kalmanctoth@gmail.com

Abstract

At PNSQC 2015 [1] I highlighted the weaknesses of digital identity schemes and suggested how to overcome them. Many identity systems have been proposed since then, each yielding marginal benefits. The Internet remains far too dependent on server-centric password-based identity solutions.

This paper describes an identity architecture powered by collaborating software-based agents and so-called *self-sovereign digital identities*. The architecture decentralizes control over identity from web services to individuals with *identity agents* installed on their personal devices. The agents manage *digital identities* and private data on behalf of their owners to prove who they are, reduce dependency on passwords, securely interoperate, protect their identifying information, and delegate access to their private data. To facilitate ease-of-use and technology adoption, identity agents virtualize digital identities mimicking physical credentials in one's wallet. Digital identities specify private/public key-pairs for digitally signing, encrypting, and sealing digital identities, consent tokens, private files and other digital artifacts. Identity agents exploit *identity-proofing*, *digital sealing*, and *attestation* to elevate authentication and identity assurances associated with digital identities. A reference model for identity agent implementation is presented. Various aspects of the identity architecture are published in US patents [2-5], an unpublished patent application [6], conference proceedings, and technical journals [15-19].

Biography

Kal Toth *has published several conference and journal papers plus four US patents in the field of digital identity. He is refining a proof-of-concept prototype implementing features of the identity architecture described herein and provides technical expertise to law offices relating to BitTorrent and copyright infringement. He has worked for Hughes Aircraft, Datalink Systems Corp., CGI Group Inc., the Software Productivity Centre (BC), and Intellitech Canada (Ottawa), and he has provided consulting services to various organizations including the Canadian Communications Security Establishment. He was Executive Director of the Oregon Master of Software Engineering (OMSE) program and associate professor at Portland State University delivering software engineering courses to working professionals in Oregon. He obtained his Ph.D. in computer systems and electrical engineering from Carleton University and is a registered professional engineer with a software engineering designation in British Columbia.*

1. Synopsis

An agent-based digital identity architecture is presented where digital identities mimic physical credentials in one's wallet. Identity agents create and manage digital identities on behalf of their owners to identify and authenticate them; sign and encrypt transactions, messages and personal information; conduct identity-proofing; and delegate consent. The architecture promises to significantly reduce online password dependency and the volume of identifying information collected and retained by web service providers.

2. The Problem

Today's Internet is a patchwork of identity solutions - identity was not designed-in from inception. It does not have an protocol layer for identifying users. A small number of large providers control an enormous volume of private data globally. The Internet has a vexing problem with identity, privacy and security evidenced by far too many large-scale breaches - Capital One, Sony, JP Morgan, Equifax, and Facebook to name a few. Root causes include the insatiable need to collect private information for business and political purposes combined with unsustainable methods currently used to specify and manage identity. A huge inconvenience for users and service providers, the Internet remains excessively dependent on passwords. Biometrics, geo-location, and behavioral schemes have improved the situation marginally.

3. Addressing the Problem

Kim Cameron [7] first said the web is a patchwork of identity schemes. Various writers have advocated moving away from server-centric identity provisioning to decentralized schemes. Sir Timothy Berners-Lee, expressing [8] serious concerns about the Facebook breach disclosing the private data of millions of users, resolved to take back power from the big Internet players and give users control over their identifying data. Allen [9] proposed *self-sovereign digital identities* where users control their identities. The World Wide Web Consortium (W3C) [10] developed an identity model specifying cryptographically secure, privacy respecting, machine verifiable *credentials*. W3C's decentralized identifier (DID) model [11] includes registries, identity providers, and certificate authorities specifying cryptographic material.

4. How the Identity Architecture Addresses the Problem

Depicted in Figure 1, the digital identity architecture relies on collaborating *identity agents* installed on user devices (PCs) and web servers. The central purpose of an identity agent is to create, maintain, protect and deploy the owner's digital identities [2]. An identity agent uses device authenticators (face, voice, fingerprint, iris, etc.) to enroll and match authentication data of the owner. Digital identities specify attributes of the owner and have three public/private encryption key-pairs used for designated purposes. *Digital seals* cryptographically affix owner *attestations*, roles, permissions and commitments to digital identities, *consent tokens*, documents, and other digital artifacts.

Identity agents represent the integrative glue giving life to digital identities. When an owner first uses her identity agent, it enrolls her identifying data which is subsequently used to authenticate her. This binds the owner to her digital identities, consent tokens, private data, and other artifacts. Identity agents enable owners to use a proof-of existence identity registry to validate digital identities, use a digital identity exchange service to reliably transfer identities, secure transactions among owners, conduct online identity-proofing, secure their private, reliably delegate consent, and notarize digital documents.

5. Identity Agent User Interface

Figure 2 depicts the user interface of an *identity agent* installed on an owner's device including: collaborating applications using the identity agent; the owner leveraging authenticators to control the identity agent; documents used to proof the owner's identity; digital identities in the owner's digital wallet specifying private/public key-pairs and digital seals; and consent tokens, private data, and event logs.

The owner's contact list holds digital identities of other parties specifying public keys only. Figure 2 also depicts the identity agent collaborating with other owners and service providers on behalf of the owner.

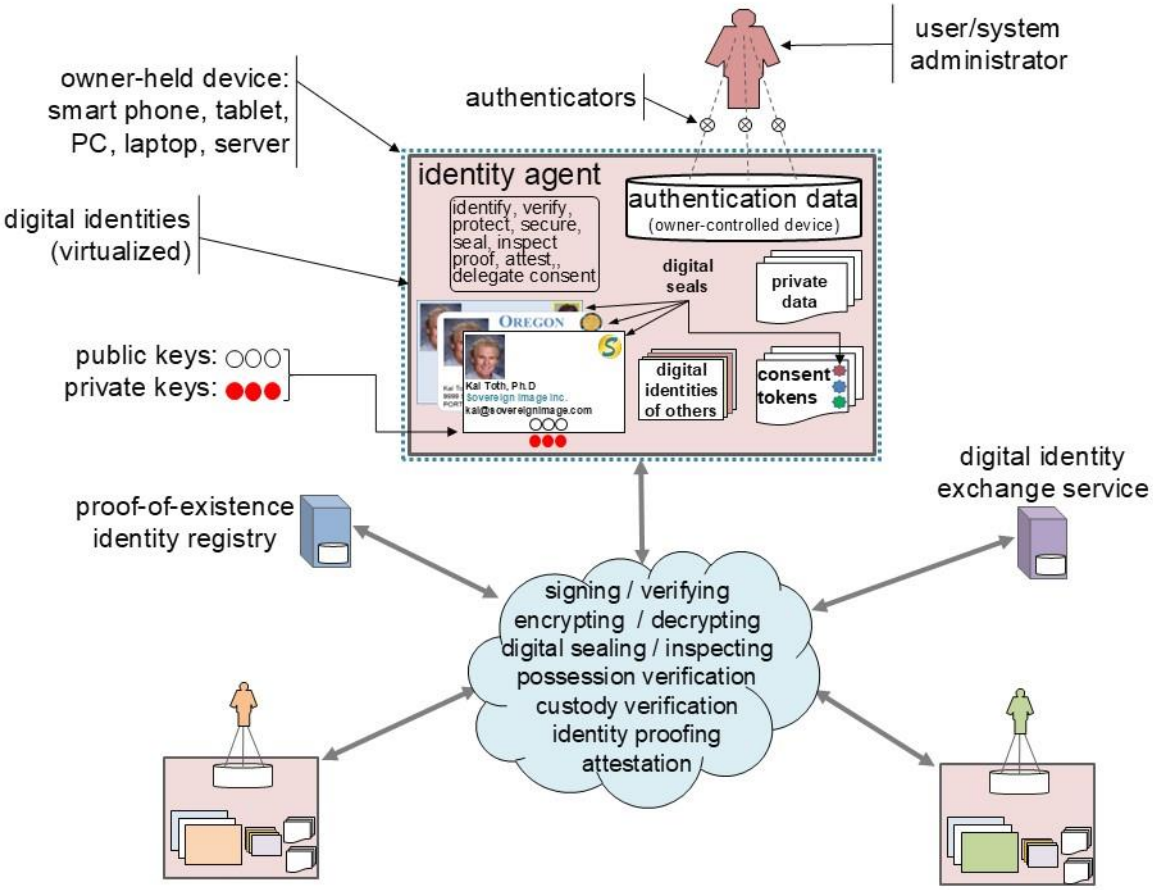

Figure 1. Agent-Based Digital Identity Architecture

6. Virtualized Digital Identities Mimic Physical Identities

The digital identities depicted in Figure 2 are virtualized to mimic physical credentials in one's wallet. This will facilitate ease-of-use and technology adoption. A *digital identity* specifies at least a unique identifier, issue and expiry dates, category or type, and attributes relevant to the category. Attributes may include legal names, informal names, and pseudonyms. Distinguishing features may include photo(s), endorsements, restrictions, and other identifying information. Digital identities are allocated *private/public key-pairs* by the owner's identity agent when they are created. Each digital identity of an owner specifies a *sealing image* used by the owner's identity agent to render *digital seals* affixed to digital artifacts.

7. Identifying, Pseudo-Anonymous and Anonymous Identity

Digital identities created by an owner's identity agent may specify different types (categories) of digital identities (a.k.a. credentials) using a common format, for example: digital driver's licenses, health cards, business cards, and credit cards. *Pseudo-anonymous* credentials specify nicknames, pseudo names and various attributes shared among various collaborators, possibly in confidence. *Anonymous* credentials provide no identifying information and are used for incognito browsing and web posting.

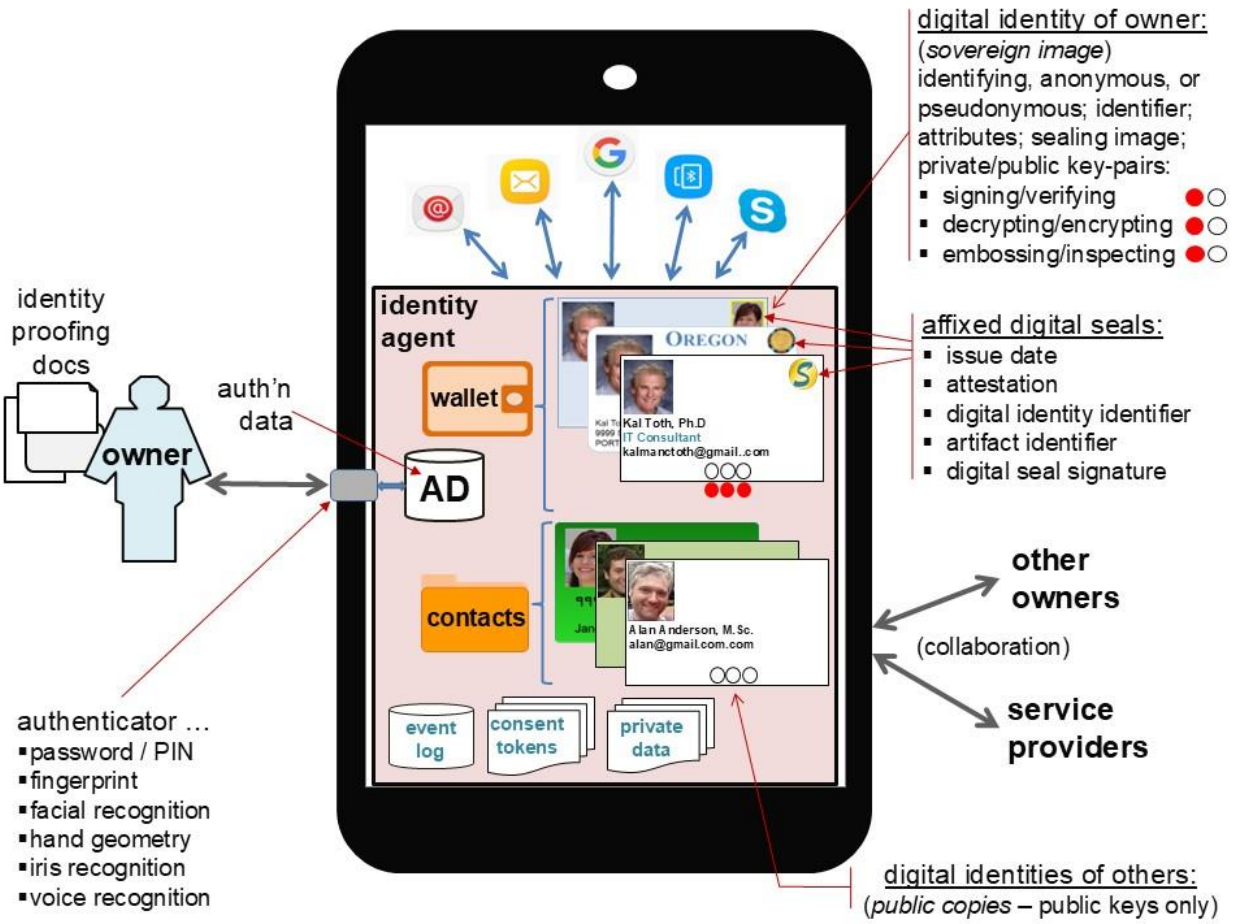

Figure 2. Identity Agent User Interface View

8. Digital Identities Specify Private/Public Key-Pairs

To increase resistance to attack, Asokan [12] recommended designating multiple cryptographic key-pairs for distinct purposes. Depicted in Figure 2, the identity agent has created three digital identities for the owner including three private/public key-pairs [2]:

- a signing/verifying key-pair for message integrity and message/transaction authentication.
- a decrypting/encrypting key-pair for securing transactions, documents, and messages.
- an embossing/inspecting key-pair for creating and verifying digital seals affixed to digital artifacts.

Collectively, identifiers, attributes, images, and private/public key-pairs of a digital identity are known as the *sovereign image* of a digital identity. The public copy of a digital identity specifies only the public keys (the private keys are excluded). The owner's identity agent ensures that the private keys are vaulted in a secure location and are not revealed to other parties. Public copies of digital identities cannot be used to impersonate the owner given they do not bear (hold) the private keys.

9. Virtual Identity Layer

Collaborating identity agents establish a virtual identity layer for the Internet. Figure 3 illustrates two identity agents exposing their user interfaces to the owner as well as to collaborative applications. The rely on the Internet's transport layer protocol (TCP/IP) to interoperate. The figure depicts authenticator(s)

and authentication data binding identity agent owners to their digital identities in their digital wallets and public copies of digital identities of others in their digital list of contacts. Also depicted are the proof-of-existence identity registry and the digital identity exchange service.

Collaborative applications authorized by the owner, such as email, messaging, conferencing, and data sharing, can exploit the owner's identity agent by way of an application programming interface (API) to obtain public copies of digital identities, securely collaborate, secure identifying and private information, delegate consent, and notarize (attest and digitally seal) documents.

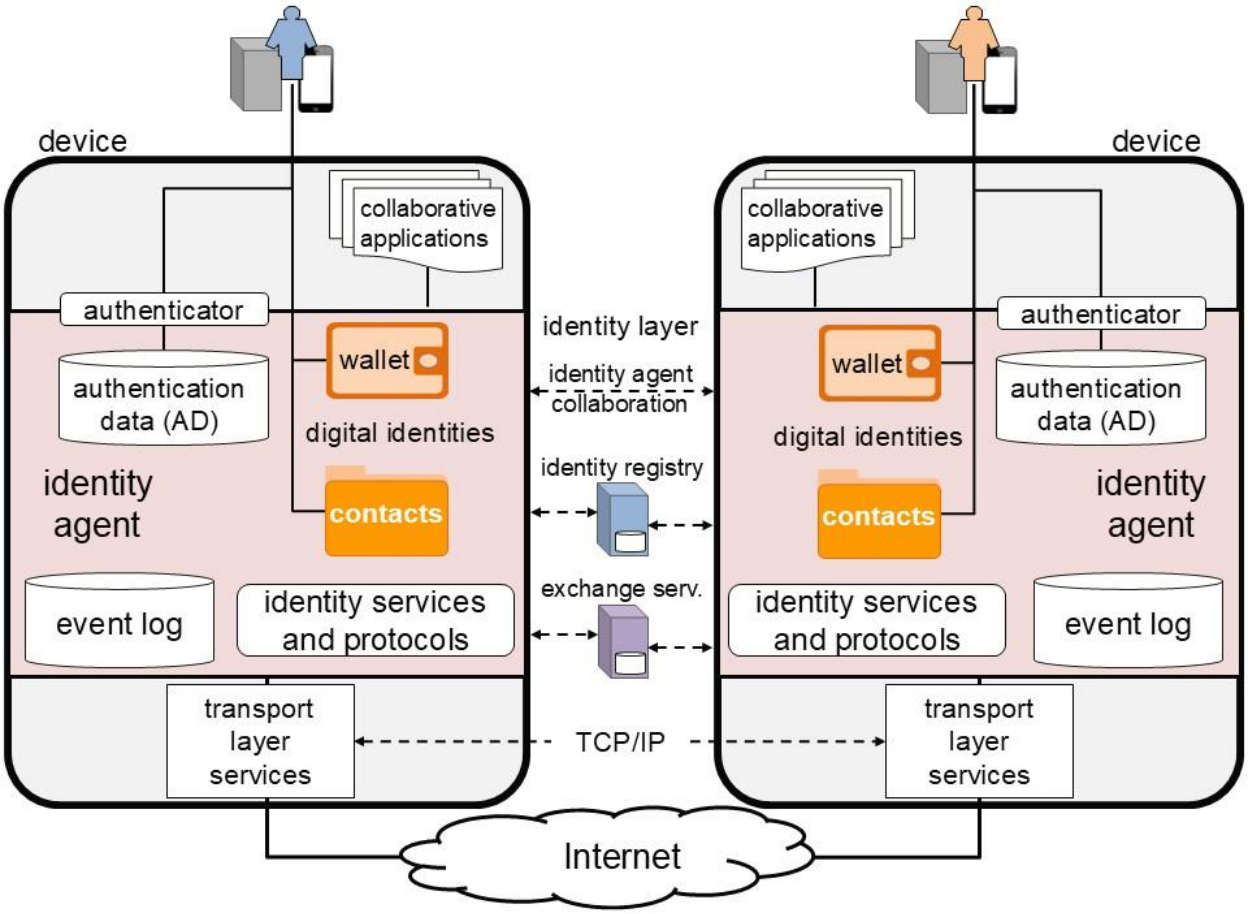

Figure 3. Identity Agents Establish a Virtual Identity Layer

10. Digital Seals, Attestation and Self-Sealing

Digital seals are analogous to physical seals affixed by notaries to physical documents. Owners can use their identity agents to create digital seals affixing attestations (declarations, commitments, permissions) to digital identities, consent tokens, contracts, documents, and other digital artifacts [3].

An identity agent uses a digital identity of the owner to issue (create) a digital seal affixing an attestation of the owner to an artifact (e.g. "proofed"). The issue date, attestation, digital identity (identifier, attributes, public keys) and the artifact identifier are concatenated and hashed yielding a digest; the digest is encrypted using the embossing key of the owner's digital identity to create a "digital seal signature"; and the sealing image of the owner's digital identity is combined with the issue date, attestation, digital identity identifier and digital seal signature rendering a digital seal affixed to the digital artifact. Using the embossing key to bind the fields and public keys of the digital identity to itself is called "*self-sealing*".

Relying parties can open and verify digital seals. Opening a seal reveals the issue date, attestation, digital identity identifier, artifact identifier and digital seal signature. The inspecting key of the digital identity is used to decrypt the digital seal signature yielding a result. Concatenating and hashing the issue date, attestation, digital identity (identifier, attributes, and public keys) and artifact identifier yields a digest. The digital seal is successfully verified if the result and digest match. The digital identity owner cannot repudiate having created the digital seal and attestation.

11. Signing and Verifying Messages and Transactions

Consider Alice and Bob having used their identity agents to create and self-seal digital identities and exchanged public copies of their self-sealed digital identities over a reliable channel. Figure 4 shows Alice and Bob using their digital identities and exchanged public copies to sign and verify messages.

First, Bob uses the private signing key of his digital identity to digitally sign and send a message to Alice who uses the public verifying key of Bob's public copy held by her to verify the signature thereby proving Bob originated the message. Similarly, Alice uses the private signing key of her digital identity to digitally sign and send a message to Bob who uses the public verifying key of Alice's public copy to verify the signature proving Alice originated the message.

Self-sealed digital identities can be verified using the inspection key of the received public copy.

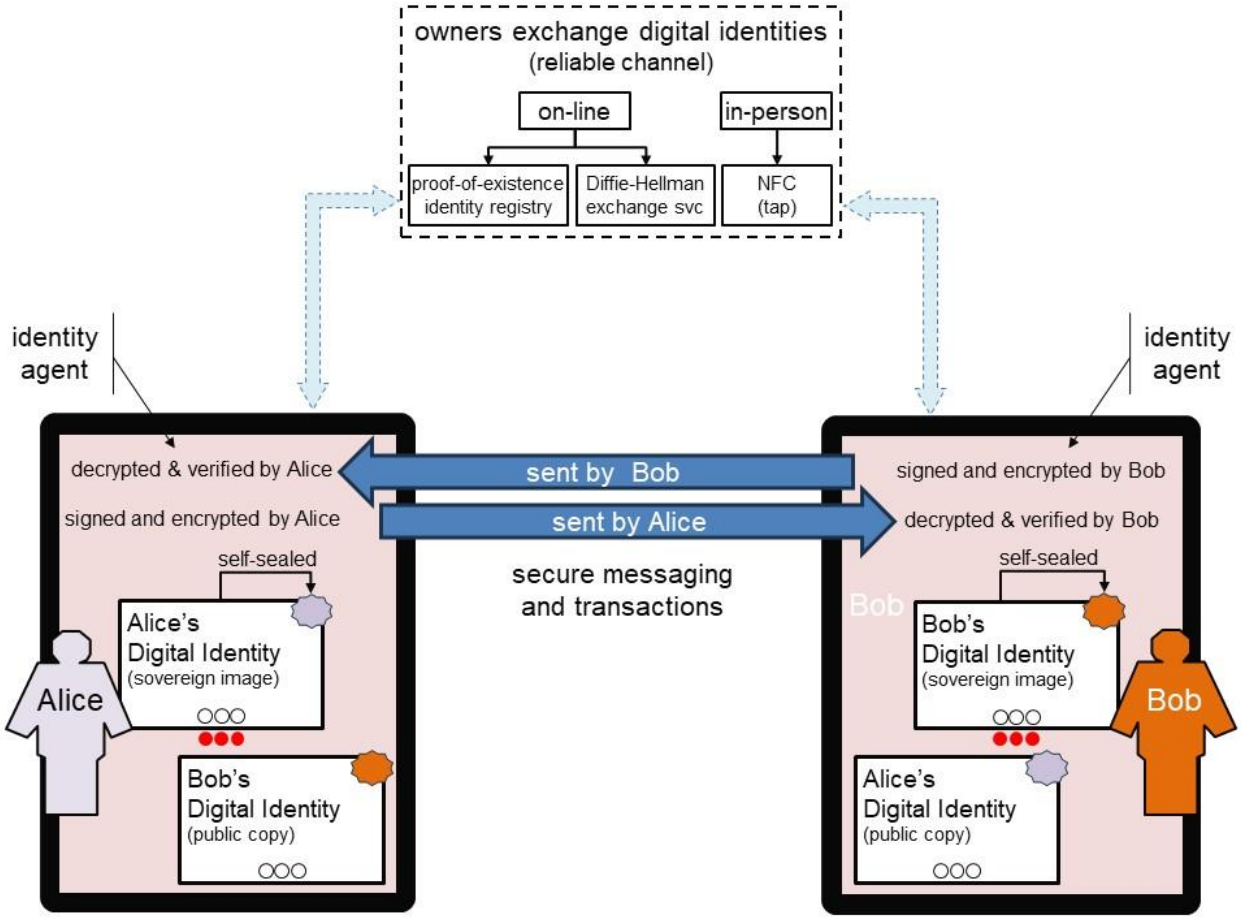

Figure 4. Securing Messages and Transactions using Self-Sealed Digital Identities

12. Encrypting and Decrypting Messages and Transactions

Once a first owner's identity agent has provided a public copy of her digital identity to a second owner, and the second owner's identity agent has provided a public copy of his digital identity, they can [also] encrypt and decrypt exchanged messages and transactions.

Figure 4 illustrates Bob and Alice having exchanged self-sealed public copies of their digital identities over a reliable channel. Bob uses the public encrypting key of Alice's public copy to encrypt and send a message to Alice. Then Alice uses the private decrypting key of her digital identity to decrypt the message enabling her to read the message. Similarly, Alice uses the public encrypting key of Bob's public copy to encrypt and send a message to Bob. And Bob uses the private decrypting key of his digital identity to decrypt the message enabling him to read the message. Thereafter, Alice and Bob can collaborate securely using email, messaging and other collaborative applications.

13. Proof-of-Possession and Proof-of-Custody Challenges

Having exchanged digital identities, identity agents can challenge each other to verify the corresponding identity agent holds a given digital identity and the identity agent's owner is authenticated and present [2]:

1. Proof-of-possession uses the encryption key of the public copy of a digital identity to encrypt and send a random value to an identity agent which decrypts and returns the value to prove possession.
2. Proof-of-custody involves an identity agent sending a demand to another identity agent to authenticate the owner and acknowledge that the owner is present (i.e. controls her device).

14. Exchanging Digital Identities

In the business world, people unknown to each other routinely exchange business cards face-to-face. In the online world, an equivalent mechanism for reliably exchanging digital identities is needed.

Transferring such identities in the clear over a wide-area network is a high-risk proposition given they may specify private and identifying information. Exchanging digital identities in-person between devices using cables, thumb drives, or QR codes are lower-risk options but may not always be practical. Exchanging digital identities in-person (device-to-device) using Near Field Communications (NFC) may be an effective solution but does not address the challenge of exchanging digital identities online.

15. Proof-of-Existence Identity Registry

Proof-of-existence enables relying parties to verify the integrity of digital identities received from others (i.e. confirm digital identities were not modified or corrupted in transit). When identity agents create digital identities for owners, they are self-sealed, hashed, and deposited in a proof-of-existence identity registry. The identity agent of a relying party receiving a public copy of a digital identity can verify if it exists in the registry. Since only hashes of digital identities are deposited, attributes of registered digital identities are not disclosed if the registry is hacked or otherwise breached.

Figure 5 depicts a proof-of-existence identity registry. When Alice's identity agent creates or updates her digital identity, it is self-sealed. When registering, her identity agent uses the inspecting key to verify the integrity of the self-seal, hashes her digital identity, and deposits the hash and self-seal into the registry. When relying party Bob receives a public copy of a digital identity apparently owned by Alice, his identity agent computes the hash of the received public copy and uses it to retrieve a record from the registry containing a hash and self-seal. Bob's identity agent verifies if the computed hash matches the hash retrieved from the registry. If they match, his identity agent extracts the digital seal signature from the self-seal and uses the inspecting key of the received public copy to decrypt the digital seal signature yielding a digest. If the digest and computed hash match, Bob is assured the received public copy is Alice's.

When Alice receives a public copy of Bob's digital identity, her identity agent hashes the public copy; uses the computed hash to retrieve a hash and self-seal; verifies the computed hash matches the retrieved hash; and uses the inspection key of the public copy to decrypt the digital seal signature of the self-seal yielding a digest. If the digest and computed hash match, Alice is assured the public copy is Bob's.

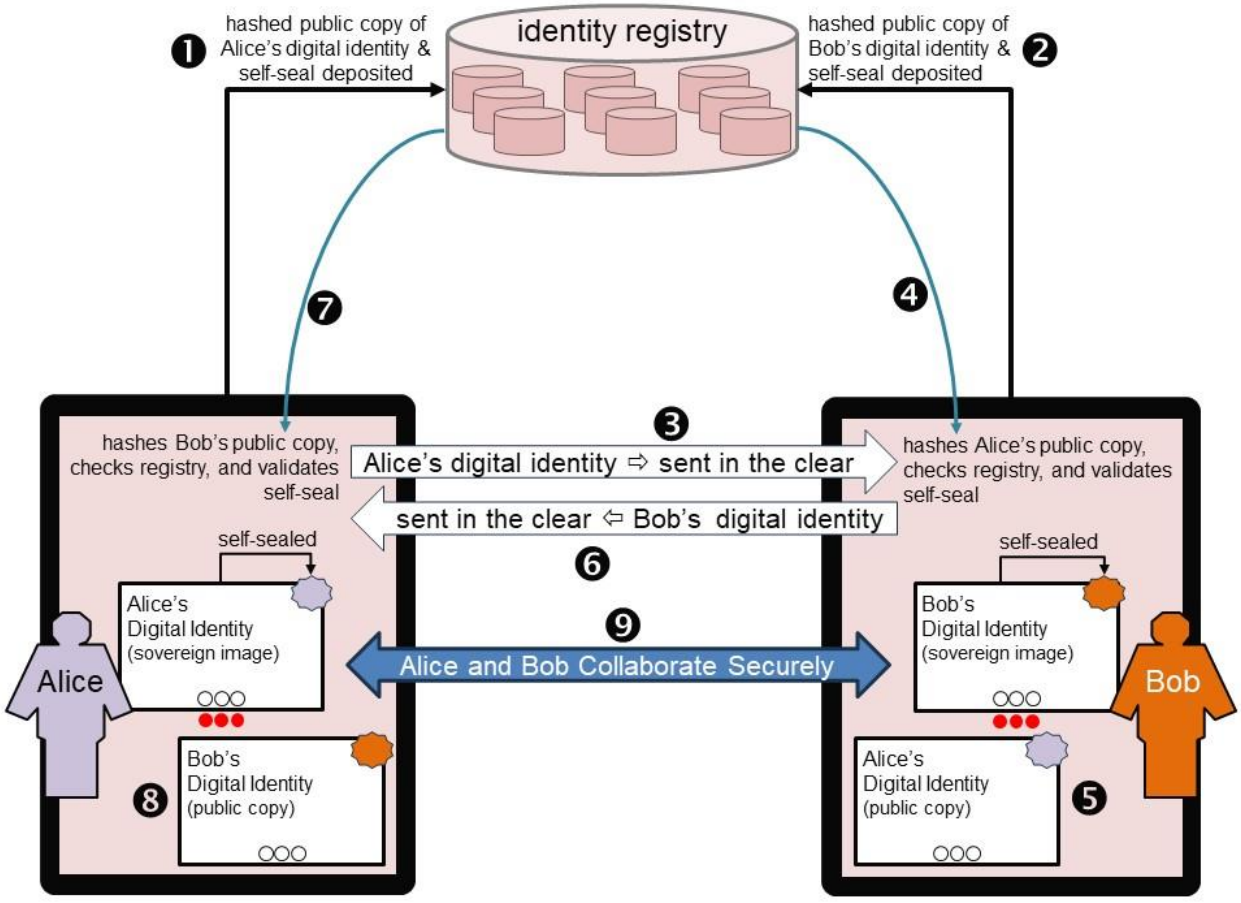

Figure 5. Proof-of-Existence Identity Registry for Exchanging Digital Identities

16. Digital Identity Exchange Service using Diffie-Hellman

Figure 6 depicts an adaptation of the Diffie-Hellman key exchange method [1] [5]. This method relies on one-time passwords, passphrases, or PINs ("OTPs") and the Diffie-Hellman key agreement method [13]. Owners 1 and 2 have digital identities they want to exchange. They use their identity agents to create OTP1 and OTP2, exchanging them over a reliable channel. Owner 1's identity agent uses the hash of OTP1 to store the public encryption key of her digital identity into the exchange service's repository, and owner 2's identity agent uses the hash of OTP2 to store the public encryption key of his digital identity into the repository. The hash of OTP2 is then used to retrieve owner 2's public key, and the hash of OTP1 is used to retrieve owner 1's public key. And the Diffie-Hellman method is used by their identity agents to combine owner 1's private key with the retrieved public key of owner 2 creating a symmetric encryption key; and combine owner 2's private key with the public key of owner 1 to create the same symmetric key. The symmetric key is then used by both owners to securely exchange their digital identities.

[1] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

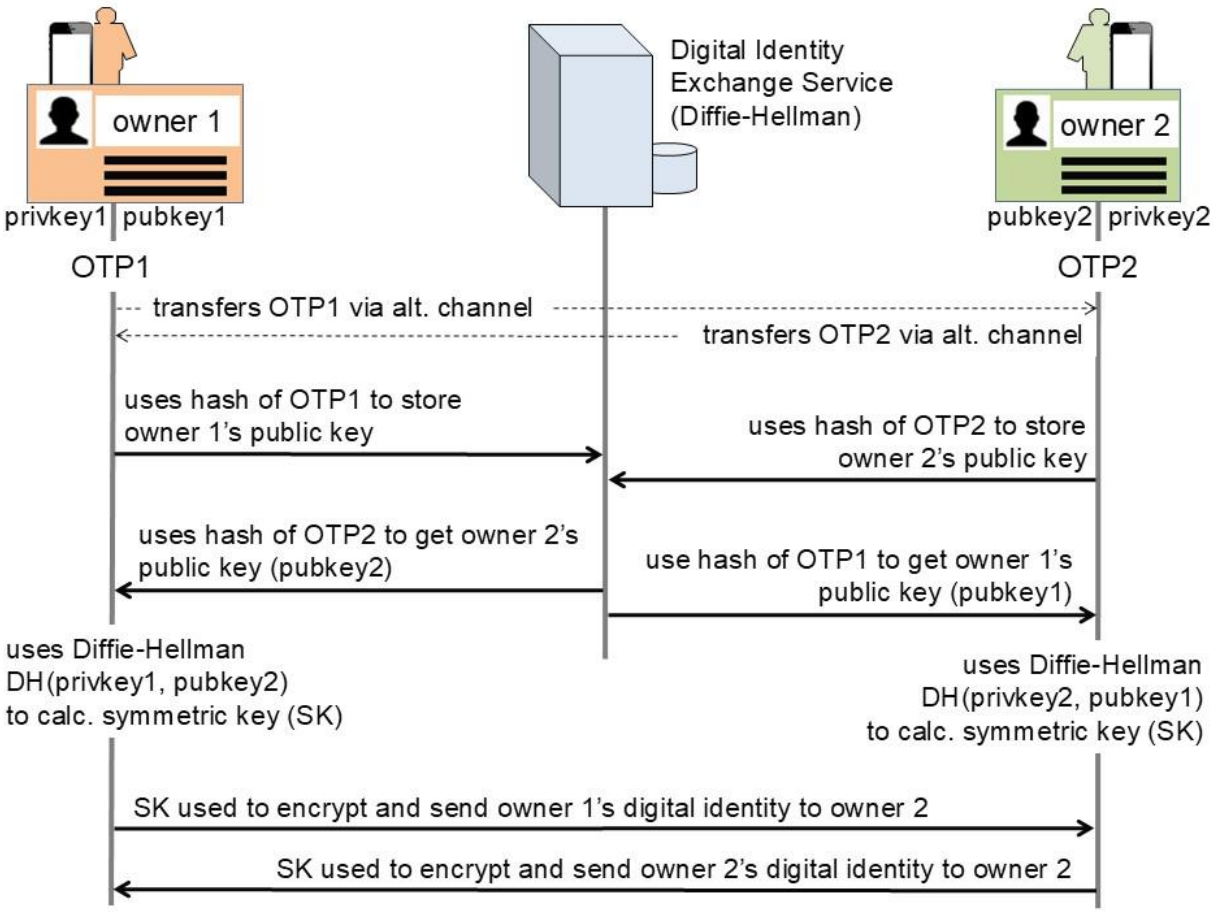

Figure 6. Adapted Diffie-Hellman Method for Exchanging Digital Idwentities

17. Identity Proofing and Attestation using Digital Seals

In the physical world, banks, passport offices and departments of motor vehicles (DMVs) proof identities of customers/civilians to elevate identity assurances associated with issued credentials. Proofing involves the requester providing identifying information and the proofer (issuer) verifying the information. In a similar manner, identity agents use digital identities and digital seals to identity-proof ("proof") [6] the digital identities of other owners. Having reliably exchanged public copies of their digital identities (Figures 5 and 6) Alice sends a secured request to Bob to identity-proof her digital identity. Her request may be accompanied by personally identifying document(s). Bob inspects Alice's self-sealed digital identity and identifying documents and conducts a background check. If satisfied, Bob's identity agent uses the embossing key of his digital identity to create a digital seal affixing his attestation to Alice's digital identity, and securely returns the digital seal, attestation, and identity-proofed digital identity to Alice.

18. Transitioning from Passwords to Digital Identities

An identity agent owner can transition from using her password to log into a web service to using a digital identity to reliably identify herself to the web service (see [6]). She has previously specified her online user profile with the web service and has a current identifier and password enabling access to the web service. A necessary precondition is for the web service to have an installed identity agent configured and managed by an authorized system administrator. Routine web administrator operations are automated. The owner creates a self-sealed digital identity matching the identifying information held by the web

service in her user profile. She logs into her account using her password and presents a public copy of her digital identity and self-seal to the identity agent of the web service. The web service uses the inspection key of the owner's digital identity to verify the self-sealed digital identity. If successfully verified, the identity agent of the web service verifies that the identifying information in the provided digital identity matches her user profile. If so, the web service's identity agent attests and digitally seals her digital identity and sends the attesting digital seal and a public copy of the service's digital identity to her identity agent. Thereafter she can use her digital identity instead of her password to authenticate (log in).

19. Delegating Consent to Access Private Data

In contrast to server-centric consent models, the identity architecture decentralizes control to owners. Identity agents use digital identities of owners to create digital seals that cryptographically bind stakeholders, commitments and permissions to consent tokens (see [5] and [19]). Stakeholders include owners sharing their resources, custodians holding the resources on behalf of owners, and requesters asking owners to delegate access to the resources. More specifically, identity agents use the digital identities of stakeholders to create digital seals that affix their commitments to consent tokens: requesters specify access and permissions they need; owners clear and grant access and permissions to resources; and custodians approve and control access to the private resources of owners. Digitally sealed consent tokens ensure that requesters and custodians reliably control access to owner resources.

20. NIST Identity Assurance and Authentication Levels

The National Institute of Science and Technology (NIST) has developed a model and guidance pertaining to identity authentication and identity assurance levels [14]. Figure 7 presents an adaptation of NIST's model leveraging methods and structures described in this paper including identity agents, digital identities, self-sealing, proof-of-existence identity registry, and adapted Diffie-Hellman exchange.

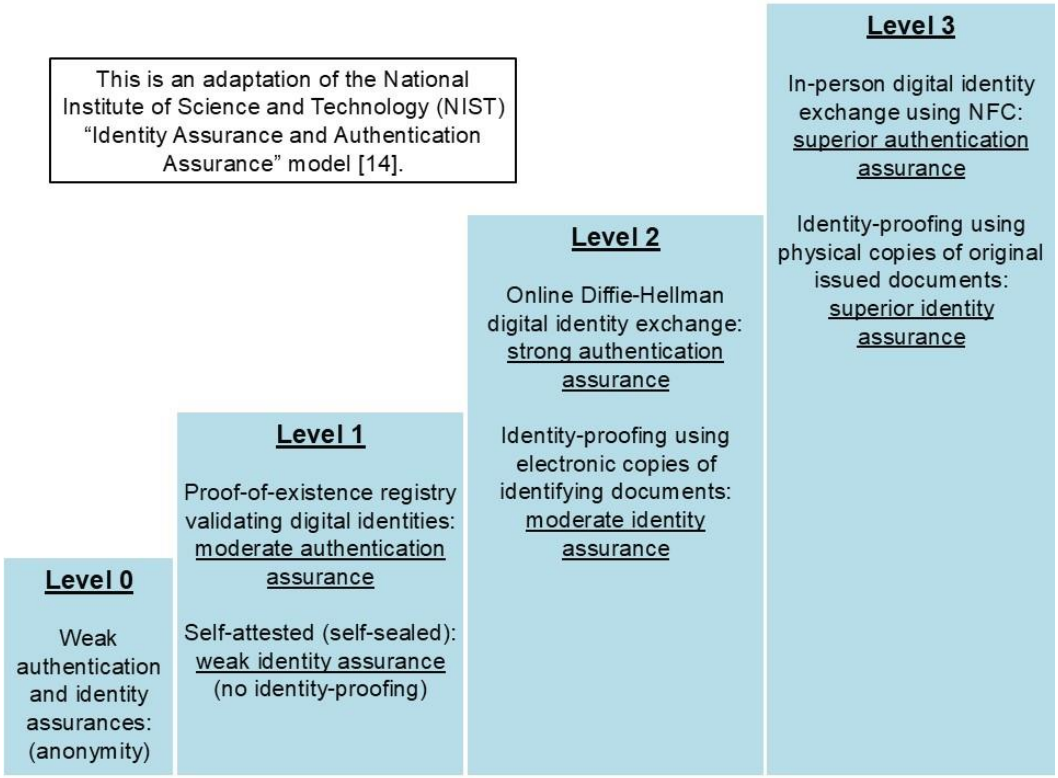

Figure 7. Identity Assurance and Authentication Assurance Levels

21. Identity Agent Reference Model

Figure 8 depicts the identity agent reference model to be developed into a technical specification. It relates the principal structures and interfaces of the architecture including: a common data structure for specifying digital identities (type/category, various attributes, private/public key pairs, sealing image); digital seals and requisite data fields; principal utilities, and external interfaces. The figure also depicts a removable non-volatile memory for vaulting the owner's authentication data and private keys.

Principal functions also depicted: Near Field Communications (tap) technology for in-person exchange of digital identities; a proof-of-existence identity registry; and adapted Diffie-Hellman method for exchanging digital identities online. The accompanying process diagram illustrates creating self-sealed digital identities; exchanging digital identities by three principal methods; using digital identities to collaborate securely; identity-proofing and using digital seals to affix attestations to digital identities; and using digital seals to affix identities and attestations to consent tokens, documents, and other digital artifacts.

This reference-model will be expanded into a specification for designing, defining and implementing the identity architecture including methods, modules, interfaces, and protocols. The architecture will be modularized to facilitate reliable development, testing and integration of the runtime system. Software engineering best practices to be applied include progressive software inspections and design reviews; multi-level repeatability and reproducibility testing; and independent software quality assurance.

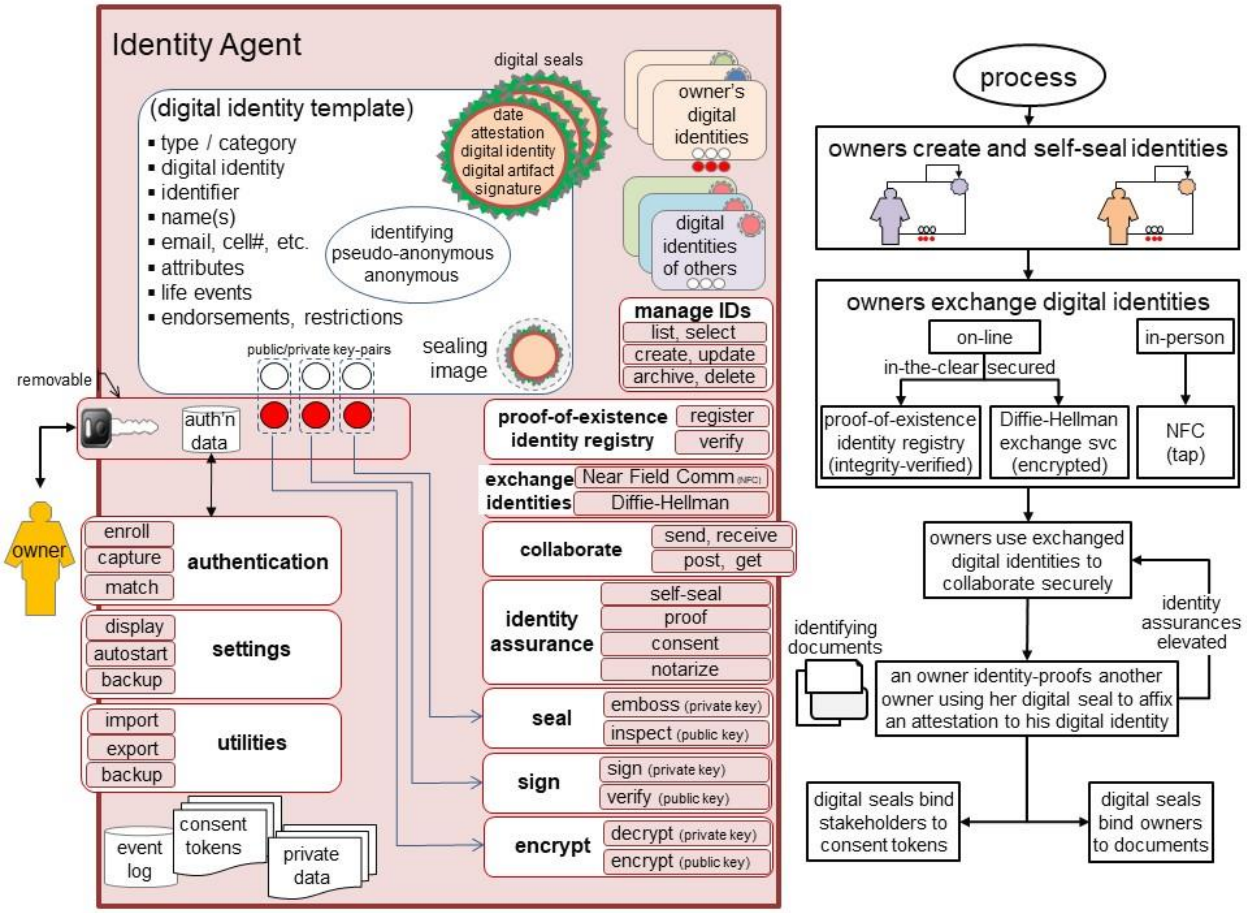

Figure 8. Identity Agent Reference Model

22. Closing Remarks

The identity architecture elevates identity assurances, security, privacy, and consent delegation for identity agent owners while reducing password dependency. The volume of personal information web providers must safeguard is substantially reduced. Decentralizing personal information increases the attack surface for hackers thereby significantly limiting how much personal data can be harvested.

23. Suggested Areas for Further Study

Applying formal software engineering methods and trusted execution environments to isolate identity agents from malware; adapting W3C's verifiable credentials data model to support virtualized digital identities; exploiting artificial intelligence and machine learning to enhance identity agent cognition.

References

[1] Kalman C. Toth, *Brewing Next Generation Identity*, PNSQC, October, 2015

[2] Kalman C. Toth, *Electronic Identity* [digital identities] *and Credentialing System*, USPTO 5/9/2017.

[3] Kalman C. Toth, *Methods for Using Digital Seals for Non-Repudiation of Attestations*, USPTO 2/20/2018. Digital seals cryptographically affix attestations to digital identities and other artifacts.

[4] Kalman C. Toth, *Systems and Methods for Registering and Acquiring E-Credentials using Proof-of-Existence and Digital Seals*, USPTO 11/13/2018.

[5] Kalman C. Toth, *Architecture & Methods for Self-Sovereign Digital Identity*, USPTO 8/25/2020. Covers proof-of-possession, proof-of-custody, delegated consent, and adapted Diffie-Hellman.

[6] Kalman C. Toth, *Methods for Identity-Proofing, Attestation and Replacing Passwords with Digital Identities,* not published.

[7] Kim Cameron, *The Laws of Identity*, May 2005, http://myinstantid.com/laws.pdf.

[8] Katrina Brooker, *Tim Berners-Lee tells us his radical new plan …, FastCompany*, Sept. 29, 2018.

[9] Christopher Allen, *The Path to Self-Sovereign Identity*, April 27, 2016, http://coindesk.com.

[10] World Wide Web Consortium (W3C), *Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web*, W3C Recommendation 19 November 2019.

[11] World Wide Web Consortium (W3C), *Decentralized Identifiers (DIDs) v1.0: Core Data Model and Syntaxes*, WC3 Working Draft 09 December 2019.

[12] N. Asokan, et. Al., *On the Usefulness of Proof of Possession*, *2nd Annual PKI Workshop*, Apr 2003.

[13] E. Rescorla, *Diffie-Hellman Key Agreement Method*, RTFM Inc., June 1999.

[14] NIST Special Pub. 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing*, Jan. 2017.

[15] Kalman C. Toth, Alan Anderson-Priddy, *Architecture for Self-Sovereign Digital Identity*, Computer Applications for Industry and Engineering (CAINE), New Orleans, LA, Oct. 8-10, 2018.

[16] Kalman C. Toth, Alan Anderson-Priddy, *Self-Sovereign Digital Identity: A Paradigm Shift for Identity*, IEEE Security and Privacy, Vol. 17, No. 3, May/June 2019, pp.17-27.

[17] Kalman C. Toth, Alan Anderson-Priddy, *Privacy by Design using Agents and Sovereign Identities*, Information Security and Privacy Protection Conference (IFIP-SEC), Lisbon, Portugal, June 2019.

[18] Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, *Privacy by Design Architecture Composed of Identity Agents Decentralizing Control over Digital Identity*, Open Identity Summit 2020, May 2020.

[19] Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, *Privacy by Design Identity Architecture using Agents and Digital Identities*, Annual Privacy Forum 2020, Lisbon, Portugal, Springer, October 2020.