Proof-of-Concept Prototype for Agent-Based Digital Identity Architecture

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

kalmanctoth@gmail.com

Abstract

The proof-of-concept prototype described herein has been developed to assess the feasibility of operationalizing the "Agent-Based Digital Identity Architecture" [1] presented at PNSQC 2024. This architecture aims to reduce password dependency and impersonation risk due to shared, lost, hacked, or phished passwords. It compensates for the Internet's missing identity layer by progressively introducing identity agents working on behalf of owners to deploy cryptographically enabled digital identities. Identity agents binding owners to their devices maintain sovereign control over their authentication data, digital identities, identifying information, and other private data. They use standard methods and protocols to collaborate reliably. To facilitate technology-adoption, digital identities mimic the look and feel of physical credentials in one's wallet. Installed on smart phones, tablets and servers, *identity agents* create *digital identities* used to mutually authenticate owners, secure messages and transactions, protect private data, seal digital identities, notarize documents, proof identities, and delegate consent. This prototype demonstrates identity agents creating, exchanging and using digital identities to execute these processes. HTML, CSS, JavaScript, JSON, and node.js have been used to develop the software. React Native will likely be used for cross-platform development.

Biography

Kal Toth *has published numerous conference and journal papers, four published US patents, and one unpublished application in the field of digital identity. He has been developing a proof-of-concept prototype implementing essential functions and features of the agent-based digital identity architecture presented at PNSQC 2024. Kal provides technical expertise to law offices relating to copyright infringement and BitTorrent technology. He has held leadership positions with Hughes Aircraft of Canada, Datalink Systems Corp., CGI Group Inc., the Software Productivity Centre of B.C., and Intellitech Canada Ltd. (Ottawa). Kal has provided consulting services to Canadian federal departments including Defence, Communications, Transportation, Revenue and Taxation, the National Research Council, and the Communications Security Establishment. He developed, delivered and directed software engineering programs for the Oregon Master of Software Engineering (OMSE) and WestMost. He has held faculty positions at the Technical University of British Columbia, Oregon State University, Portland State University, and several western Canadian Universities. He is a past member of the PNSQC Board. Kal obtained his Ph.D. in computer systems and electrical engineering from Carleton University (Ottawa) and is a registered professional engineer with a software engineering designation in British Columbia.*

1. Purpose

The purpose of the proof-of-concept prototype described herein is to assess the feasibility of operationalizing the “Agent-Based Digital Identity Architecture” [1] presented at PNSQC 2024.

2. Problem Addressed

Today’s web exposes users and providers with countless security and privacy risks including phishing attacks, server-side breaches, software infections, and frustrating volumes of unsolicited information from unknown sources (e.g. spam, fake news). Since inception, the Internet protocol stack has not included an identity layer implementing proven protocols for mutually identifying and authenticating users and providers. Authors have written that the Web is composed of a patchwork of identity schemes that are not interoperable; do not identify users reliably; are incapable of preventing impersonation; and do not filter unwanted information. Password usage online is the bane of users maintaining countless passwords and service providers reprovisioning them. Passwords pose an impersonation risk when shared or lost. Hence password usage is unsustainable for both users and providers. There is a compelling need to reduce password usage, increase identity assurances, and thereby reduce impersonation risk.

The proposed agent-based digital identity architecture is a potential solution for these problems. Identity agents implementing common functions, protocols, and virtualized identities can be progressively introduced over the Web to authenticate owners, secure collaboration, and protect private information.

3. Synopsis of Agent-Based Digital Identity Architecture

Principal features and functions of the *Agent-Based Digital Identity Architecture* [1]:

- Device owners (Internet users and providers) have *identity agents* installed on their devices for creating, exchanging, and using *digital identities* for mutual authentication and collaboration.
- Identity agents use strong passwords and possibly biometrics to bind their owners locally to their digital identities, authentication data, and other private information.
- Identity agents give life to digital identities mimicking the look and feel of physical credentials in one’s wallet while cryptographically securing messages, transactions, and private data.
- Each digital identity created by the identity agent of an owner includes an identifier, attributes specified by the owner and encryption keys. Attributes are usually, but not necessarily identifying.
- When created, a digital identity has a *Sovereign Copy* (*Sov Copy*) controlled for the owner’s identity agent and a *Public Copy* (*Pub Copy*) transferred to identity agents of requesting owners.
- Each *Sovereign Copy* has three (3) private/public key-pairs generated by the identity agent: signing/verifying key-pair; decrypting/encrypting key-pair; and embossing/inspecting keypair.
- *Public Copies* inherit attributes and public keys of Sovereign Copies but not the private keys.
- Signing, verifying, decrypting, and encrypting keys secure messages, transactions, private data.
- Embossing/inspecting key-pairs are used to create and verify digital seals affixed to digital identities, documents, and tokens elevating identity assurances and preventing impersonation.
- *Sovereign and Public Copies* are attested and self-sealed by the identity agent when created.
- Identity agents regularly authenticate their owners to mitigate loss and take-over risks.
- Identity agents use Diffie-Hellman [13] key agreement when exchanging *Public Copies*.
- Identity agents use the public encrypting key of a *Public Copy when* invoking Diffie-Hellman.
- On receiving a *Public Copy*, the self-seal is verified using the inspecting key of the *Public Copy*.
- *Proof-of-possession and proof-of-custody* challenges elevate identity assurances.

Figure 1 depicts *Sovereign Copies* and *Public Copies* of digital identities that have been self-sealed and digitally sealed by other owners. This figure also depicts *Public Copies* that have been exchanged and cross-sealed by collaborating identity agents (see Section 5 Glossary of Terms for additional details).

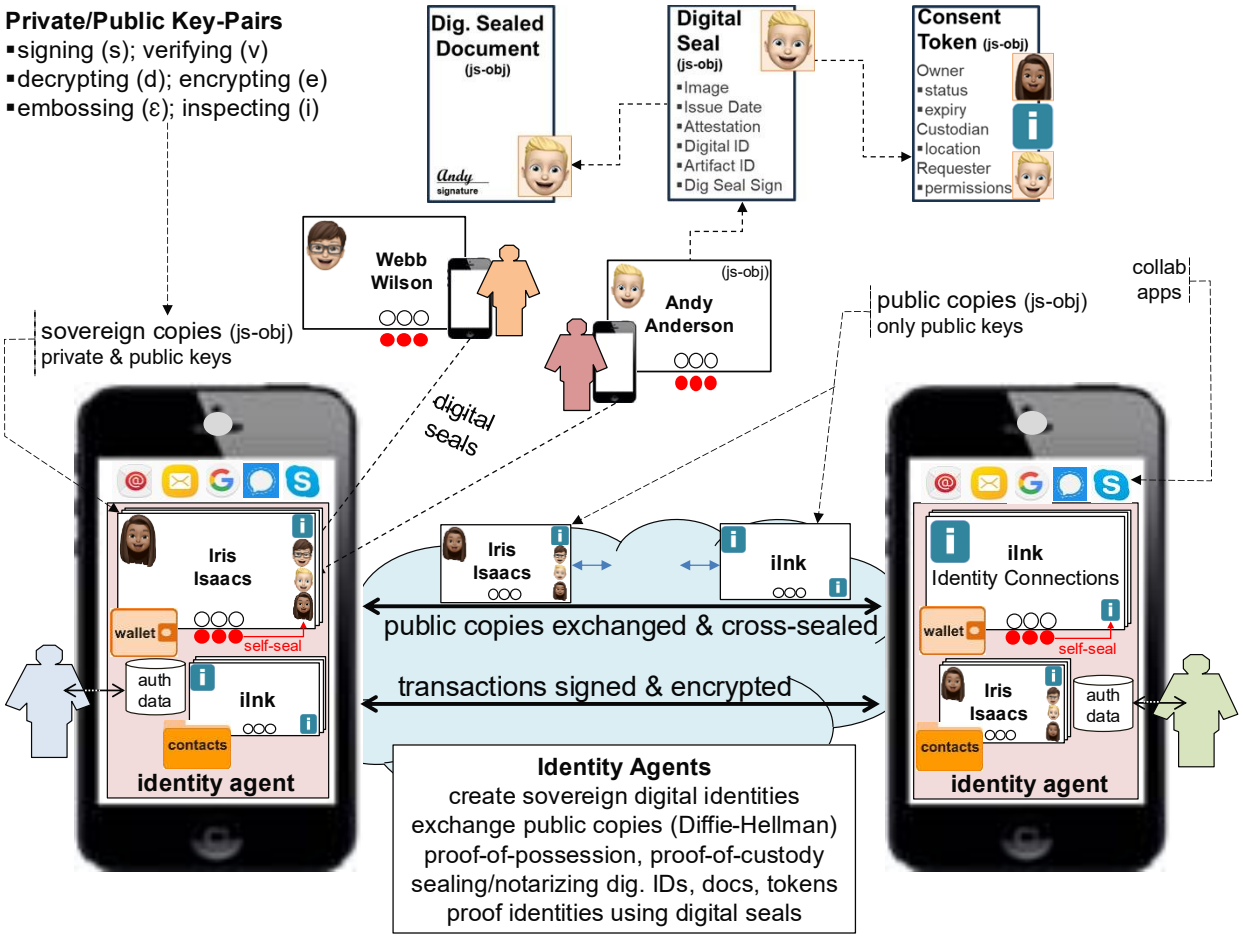

Figure 1. Agent-Based Digital Identity Architecture

4. The Proof-of-Concept Prototype

HTML, CSS, JavaScript, JSON, and node.js have been used to develop the code. Visual Studio, the Live Server extension, and Chrome DevTools have been used to edit, test and demonstrate the key features.

Digital identities, digital seals, sealed documents and sealed consent tokens have been coded as JavaScript Objects (denoted *js-obj* in Figure 1) and rendered using HTML/CSS Grid Layout.

Users and providers are depicted in separate Chrome tabs registering, signing in, and using *identity agents* as if installed on smart phones, tablet PCs or Web servers.

The prototype depicts digital identities, each specified by a unique key, image, attributes, and three private/public encryption key-pairs. Images and keys are visually and computationally bound to owners.

The prototype enables the depicted owners to specify up to six types of digital identities - *BizID, BnkID, CivID, GovID, MedID, WebID* - distinguished by border color. Custom digital identity templates specifying distinct attribute formats and backgrounds can be expected going forward.

Each *identity agent* of an owner encapsulates two JavaScript arrays called *wallet* and *contacts* used to store digital identities. Digital identity keys uniquely identifying each *Sovereign Copy* are stored in the *wallet* array while unique keys identifying *Public Copies* are stored in the *contacts* array.

5. Glossary of Terms [1]

Identity Agents. Identity agents create and deploy digital identities of the owner to ensure they are controlled by the owner, securely shared with collaborating owners, and correctly applied to identify the owner; prevent impersonation; secure messages, transactions and private data; digitally seal digital identities, documents, and consent tokens; identity-proof owners; and notarize documents. Identity agents are also responsible for backing up, recovering, importing and exporting digital identities across devices.

Specifying Digital Identities. Identity agents enable owners to specify identifying, pseudonymous, and anonymous attributes of digital identities generating three (3) private/public encryption key-pairs per digital identity: the signing/verifying and decrypting/encrypting keys secure messages and transactions; the embossing/inspecting keys are used to create and verify digital seals affixed to digital artifacts [2-5].

Sovereign Copies and Public Copies. Each digital identity created has both a *Sovereign Copy and a Public Copy.* The *Sovereign Copy* has three private/public key-pairs while the *Public Copy* holds only the three public encryption keys. A relying owners authenticates a presented *Public Copy* by using the public inspecting key of the *Public Copy* to verify the self-seal created and affixed to the *Public Copy* by the originating identity agent. Unsuccessful verifications likely represent attempts to impersonate.

Digital Seals and Attestations. A digital seal specifies an attestation bound to a digital artifact using the embossing key of a *Sovereign Copy* of the owner. The inspecting key of the *Public Copy* can be used by others to verify the digital seal by using the inspecting key to decrypt the *digital seal signature*. Hashing the concatenation of the owner's image, issue date, attestation, digital identity identifier, attributes, public keys, and artifact identifier yields a "*digest"*. The digital seal is valid if the *signature* and *digest* match.

Proof-of-Existence. Identity agents can choose to exchange *Public Copies* in-the-clear but this may enable denial-of-service risks. *Public Copies* are self-sealed when created, hashed, and both the hash and self-seal are deposited in a proof-of-existence repository. An identity agent receiving a *Public Copy* in-the-clear checks if the hash of the received copy and the affixed self-seal exist in the proof-of-existence repository. If they match it can be assumed the *Public Copy* was not modified during transfer.

Diffie-Hellman. [1] describes an adaptation of Diffie-Hellman [13] where identity agents exchange one-time passwords; use HTTPS to exchange public keys; and use Diffie-Hellman to combine the exchanged keys with the private keys they hold to create matching symmetric keys used to securely exchange their *Public Copies*. The alternative used herein is for the identity agents to exchange selected public keys and apply Diffie-Hellman to create a common symmetric key used to securely exchange *Public Copies.*

Delegating Consent. Consent tokens are attested and digitally sealed by stakeholders. Digital seals affixed by digital identity owners and custodians express their commitments to respect owner privacy and access permissions. Typically, requesters are granted read-only access to an owner's private data.

Elevating Identity Assurances (proving who you are).

Proof-of-Possession. An identity agent receiving a *Public Copy* detects impersonation by requiring the sending identity agent prove it holds the *Sovereign Copy*. The receiving agent sends a random value encrypted by the public inspecting key of the *Public Copy*; the sending agent decrypts the random value using the private embossing key. Impersonation is detected if the returned and sent values do not match.

Proof-of-Custody. An identity agent receiving a *Public Copy* issues a demand to the sending agent requiring the agent to authenticate the sending owner to confirm the sender controls digital identities it claims to hold.

Sealing and Notarizing Documents. The private embossing key of an owner's *Sovereign Copy* is used to generate a digital seal affixing an attestation of the owner to a document. If the owner affixing the digital seal is a qualified 3rd party (e.g. Notary Public), the document is said to be notarized.

Identity-Proofing. Having physical document(s) specifying identifying information, the identity agent of a requesting owner presents his digital identity and identifying information to a 3rd party owner qualified to conduct identity-proofing. The 3rd party owner validates his information and uses her identity agent and digital identity to create a digital seal affixing her attestation to his digital identity.

6. Owners Registering and Signing into Identity Agents

The prototype illustrates local password/PIN registration and sign-in to activate an owner's identity agent. Going forward devices can be expected to routinely include face, finger, voice, iris or other such biometric authenticators. Biometric authentication is not explored in any detail herein. Owners depicted by the prototype include users *andy, dawn, iris, karl, norm, tina, webb* and providers *ilnk*, *odmv*, *ubnk* and *well*.

The players first register with their identity agents each initializing the owner's digital *wallet* and *contacts. Sovereign Copies* are held in the wallet and *Public Copies* contacts. *Public Copies* include owner's and those obtained from other owners. Figure 2 shows Karl having registered his identity agent while Figure 3 shows owner Andy signing-in and thereby activating his identity agent.

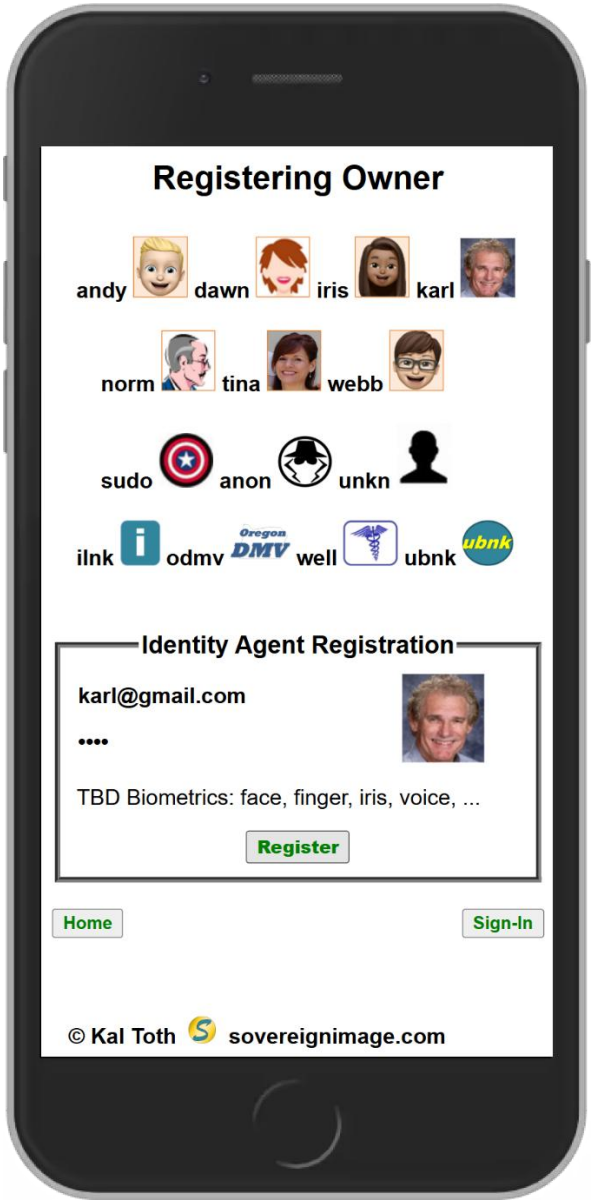

Figure 2. Owner Registering Identity Agent

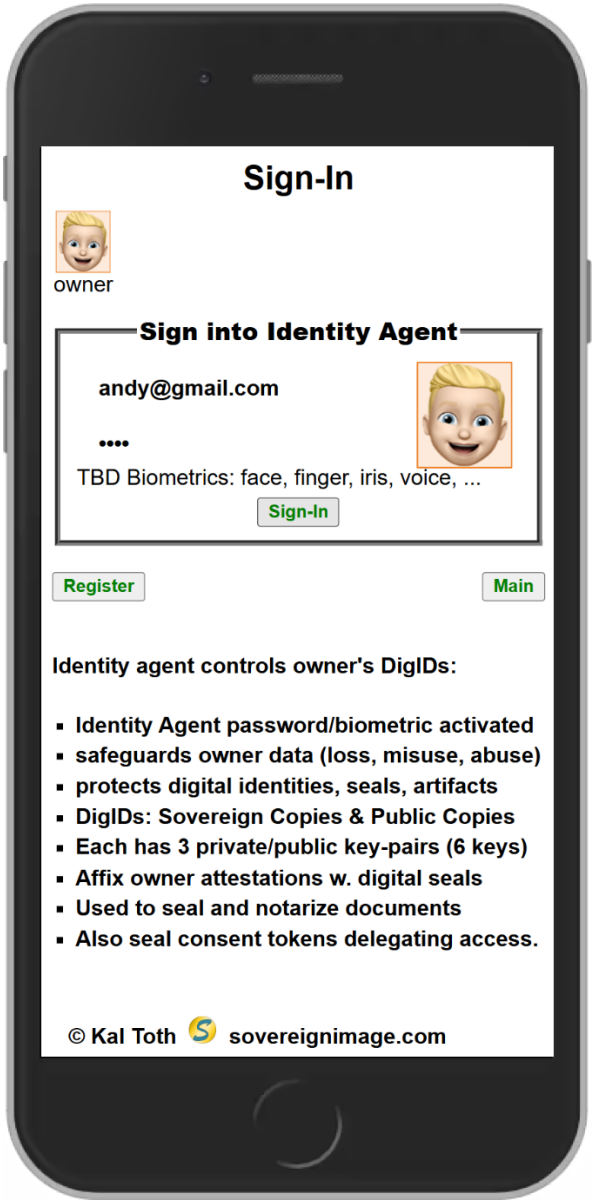

Figure 3. Signing in and Activating Identity Agent

7. Owners Creating and Displaying Digital Identities

Figure 4 shows owner Dawn having specified a digital identity (type: GovID). Her identity agent has generated three (3) private/public key-pairs for the *Sovereign Copy* and has used the embossing key to affix a self-seal represented by her (small) image. *Sovereign Copies* are kept in the identity agent's wallet. *Public Copies* are held in contacts and inherit self-seals affixed to the paired *Sovereign Copies*.

Figure 5 shows owner Webb using his identity agent to display the *Public Copy (Pub Copy)* of his MedID held in contacts. *Public Copies* have public keys only (no private keys). Figure 5 does not show the *Sovereign Copy (Sov Copy)* of his MedID which is held within his digital wallet.

A *Public Copy* is authenticated by using its public inspecting key to verify the affixed self-seal.

Figure 4. Creating a Sovereign Copy

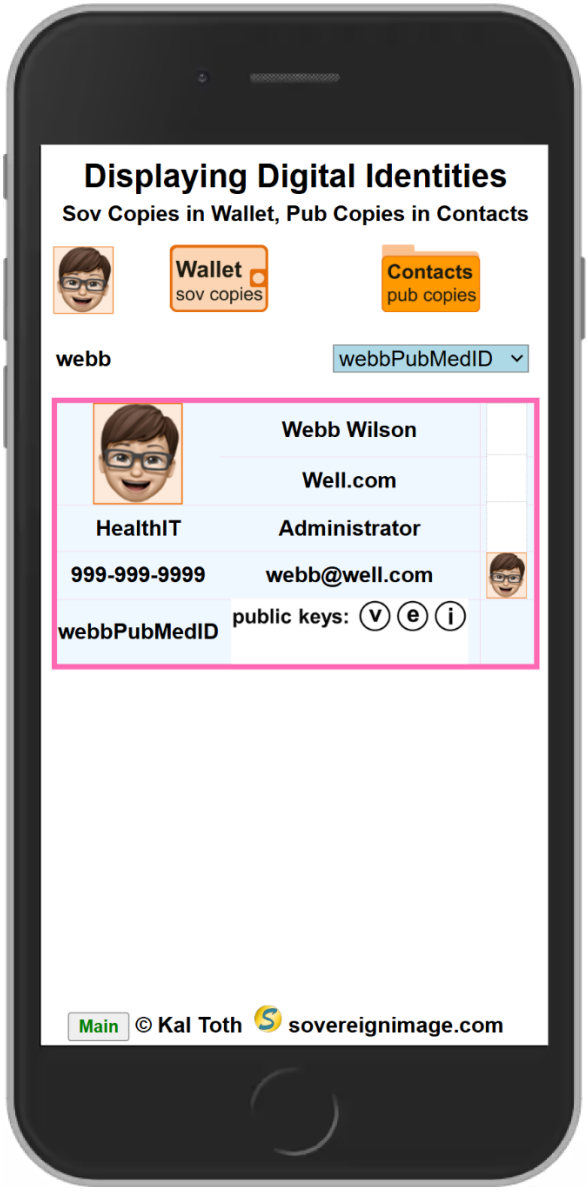

Figure 5. Displaying a Public Copy

8. Exchanging and Using Digital Identities for Messaging

Email, SMS, NFC and IP addresses can be used to securely exchange *Public Copies,* mutually authenticate, and secure person-to-person messaging. Since transferring in-the-clear exposes certain vulnerabilities, Diffie-Hellman is used to encrypt *Public Copies.* Figure 6 depicts Norm's and Dawn's identity agents using email and Diffie-Hellman when exchanging their *Public Copies*. Inspecting keys of exchanged *Public Copies* are used to verify the self-seals thereby mutually authenticating the owners.

Section 14 describes identity agents using IP addresses to exchange Public Copies.

Having exchanged Public Copies, identity agents can mutually authenticate owners by presenting and verifying affixed self-seals. Figure 7 depicts Norm's identity agent using his *Sovereign Copy* and Dawn's *Public Copy* to sign and encrypt messages to Dawn - received messages are decrypted and verified. Similarly, Dawn's identity agent uses her Sovereign Copy and Norm's *Public Copy* to secure messages.

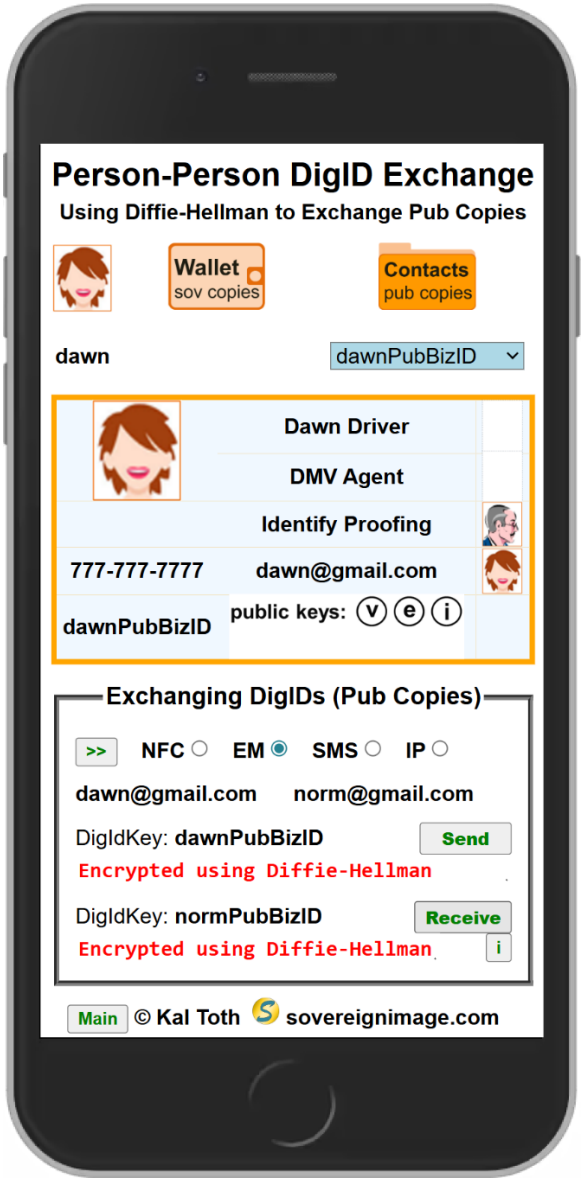

Figure 6. Owners Exchanging Public Copies

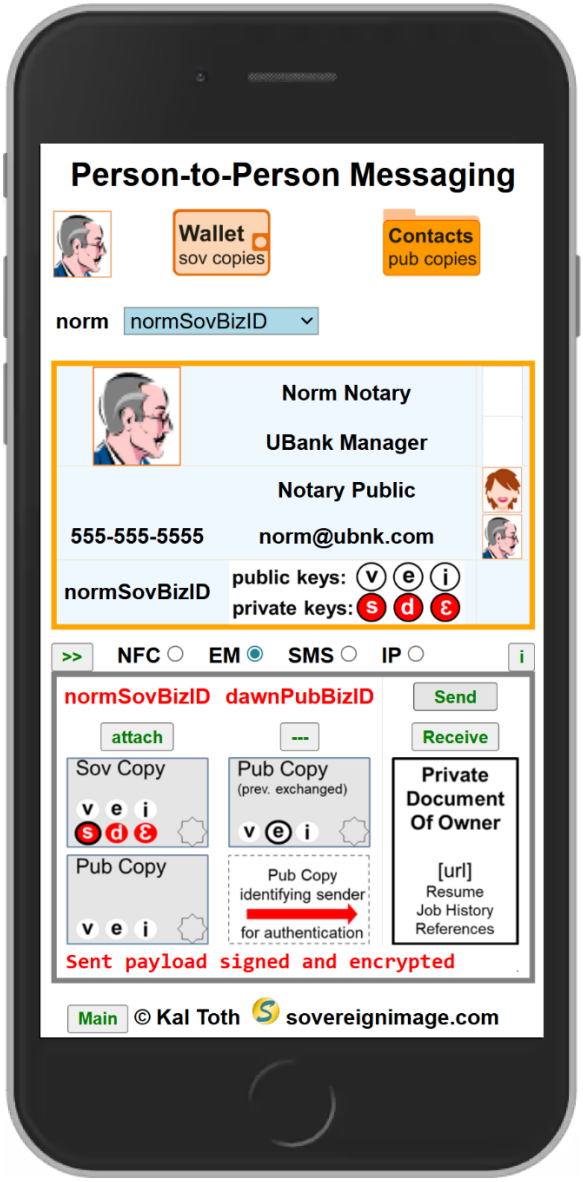

Figure 7. Digital Identities Securing Messages

9. Exchanging and Using Digital Identities to Transact Online

Digital identities have multiple encryption keys used for distinct cryptographic purposes [12]. Exchanging Public Copies of digital identities to mutually authenticate reduces remote access password dependency.

Consider Iris having a registered ***iInk*** account, user profile, and remote access password. Both Iris and provider ***iInk*** have installed identity agents. Iris' identity agent creates a self-sealed digital identity that matches her ***iInk*** user profile. She uses her password, and possibly a 2nd factor, to log into ***iInk*** *over* HTTPS. Iris presents the *Public Copy* of her digital identity to ***iInk*'s** identity agent which verifies the affixed self-seal and verifies that the *Public Copy* matches her online user profile. If successfully verified, Iris' and ***iInk's*** identity agents cross-seal and exchange their *Public Copies* (see Figure 8).

Figure 9 shows Iris and ***iInk*** presenting *Public Copies* to mutually authenticate. Presented Public Copies are matched to the previously exchanged copies and affixed self-seals and cross-seals verified. Proof-of-possession and proof-of-custody challenges can be conducted to elevate identity assurances.

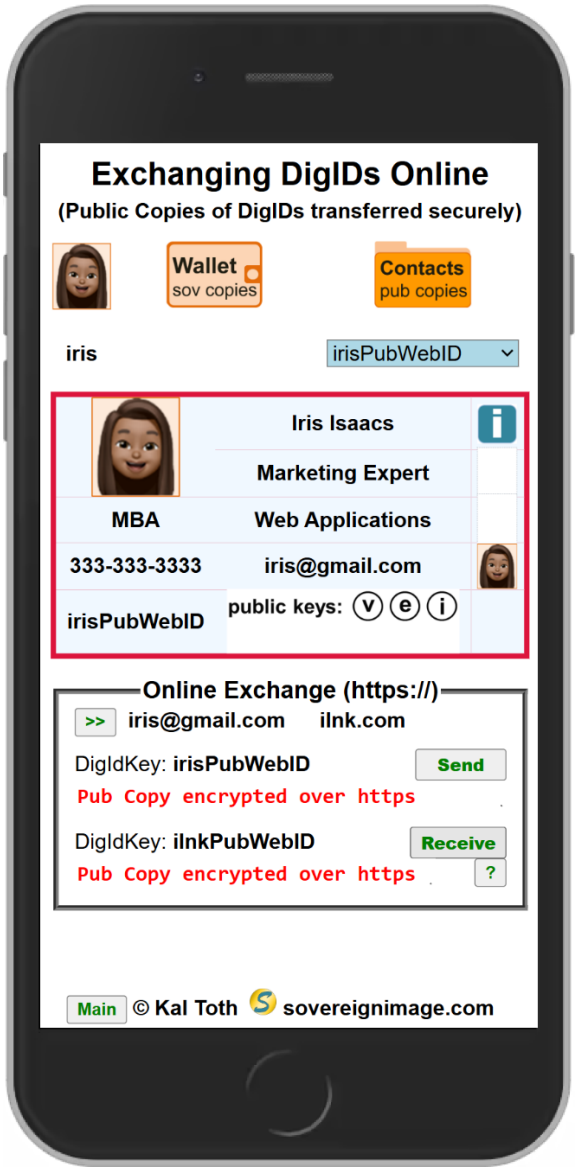

Figure 8. Exchanging Digital Identities Online

Figure 9. Online Transactions using Digital Identities

10. Digitally Sealing and Notarizing a Document

Owners can use digital identities to seal and notarize digital documents. Figures 10 and 11 illustrate Tina (Ubnk customer) and Norm (Ubnk notary public) using their identity agents to collaborate. Tina scans her identifying document; uses the embossing key of her digital identity to digitally seal it; and transfers her sealed document to Norm. Norm examines the document and Tina's affixed seal; uses the embossing key of his digital identity to affix his seal thereby notarizing it; and finally sends the document to Tina.

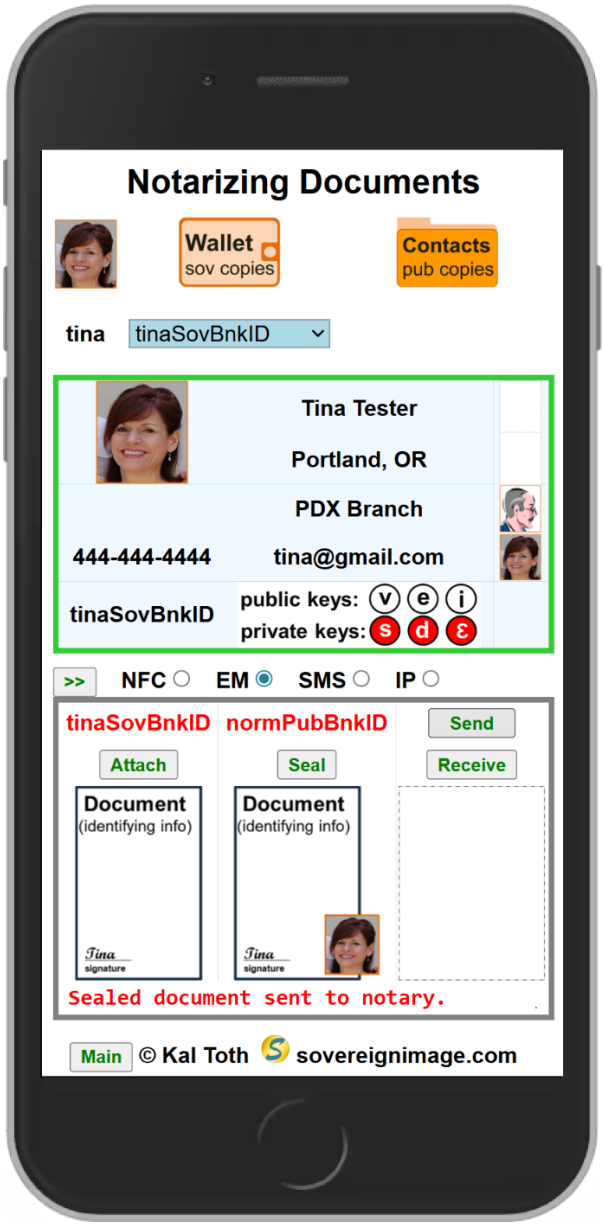

Figure 10. Tina Digitally Seals Document

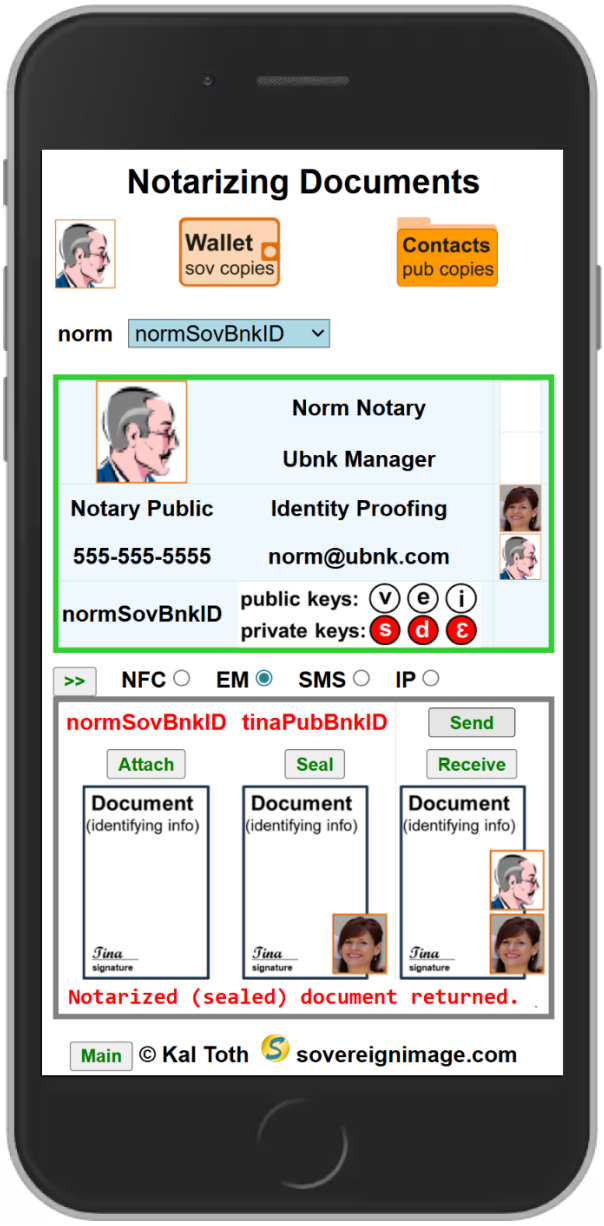

Figure 11. Notary Sealing/Notarizes Document

11. Using Identity-Proofing to Elevate Identity Assurances

Figure 12 depicts Tina using her identity agent to upload a digitally sealed driver's license renewal application and notarized identifying document to Oregon DMV. Tina's *Sovereign Copy* and the *Public*

Copy obtained from odmv.gov are used to secure the submission. Tina receives an acknowledgement that her documents, including her notarized identifying document, have been uploaded. Figure 13 depicts ODMV agent Dawn having downloaded Tina's documents from odmv.com and proofed her digital identity. Tina's application is in process. She will receive her sealed digital driver's license in due course.

Figure 12. Renewal Sealed, Documents Uploaded

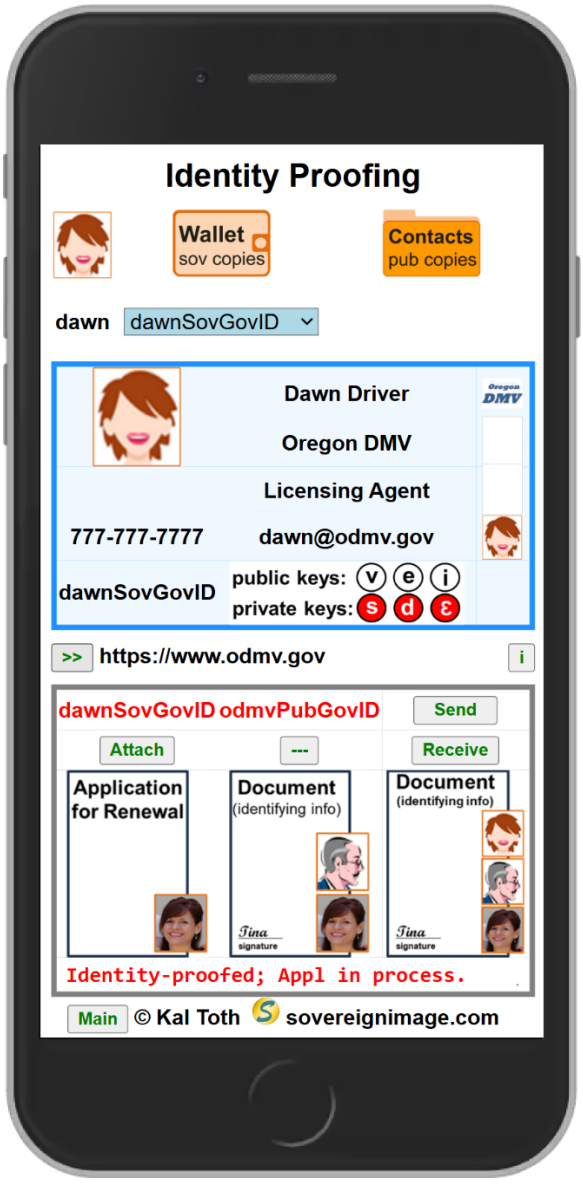

Figure 13. ODMV Agent Identity-Proofs Document

12. Delegating Consent to Access Private Data

In contrast to server-centric consent models, the agent-based identity architecture decentralizes control over consent to identity agent owners. Digital seals are used to cryptographically bind stakeholder commitments to consent tokens. Owners rely on consent tokens to reliably share specified private digital resources; requesters ask owners to delegate access to specified resources; and custodians hold and control access to resources according to permissions and expiry dates specified by owners. Figure 14 depicts a consent token with affixed digital seals of the owner, custodian, and requester controlling status, expiry, location and permissions over the token's lifetime. Consent tokens are archived for audit.

Figure 14. Private Data Consent Delegation

13. Limitations

The following requirements have been briefly explored but not thoroughly analyzed to date:

- Backup/recovery of digital identities.
- Backup/recovery of authentication data.
- Importing/exporting sovereign copies.
- Mapping digital identities to online profiles.

14. Elevating Assurances

Section 8 describes identity agents using asynchronous tools, Diffie-Hellman, and self-seal verification to securely exchange *Public Copies* of digital identities for their owners.

Proof-of-possession and proof-of-custody challenges are particularly useful when higher identity assurances levels are required. But it is not always practical to verify possession and custody over asynchronous channels.

This limitation can be overcome by transitioning from asynchronous to synchronous messaging:

Each collaborating identity agent captures the IP address used to transfer their *Public Copy* and actively listens on an available port number. They use the common symmetric key yielded by Diffie-Hellman to exchange IP addresses and port numbers (“sockets”) securely. Thereupon they use the symmetric key and sockets (IPs / ports) to establish a secure synchronous channel enabling them to execute proof-of-possession and proof-of-custody challenges to elevate identity assurances.

The symmetric key yielded by Diffie-Hellman can be used to safely exchange *Public Copies* before or after transitioning from asynchronous to synchronous collaboration. After proof-of-possession and proof-of custody challenges, self-seals of *Public Copies* should be verified.

15. Prototype Development

Prototype enhancement priorities include:

- Removing known deficiencies and bugs.
- Refining consent delegation demonstration.
- Implementing basic cryptographic features.
- Refining essential digital sealing features.
- Planning transition to React Native.

16. Areas for Further Study

- Using biometrics to activate identity agents.
- Integrating Near Field Communications.
- Ensuring identity agent reliability and trust.
- Applying Artificial Intelligence (AI) to enhance identity agent decision making.

17. Closing Remarks

Since inception, the Internet has been without an identity layer. This omission explains why today's Web is so dependent on password-based authentication and is so vulnerable to impersonation. Meanwhile, users and providers are frustrated using and provisioning countless passwords. These related problems can be resolved by deploying an architecture comprised of identity agents working to benefit their owners.

Commercial enterprises require extensive evidence of reliability, accuracy and trustworthiness before adopting a technology for critical online systems, payment processing, and back-office applications. Initially, social and professional networks could deploy identity agents and digital business cards to secure online and person-to-person transactions. Government agencies could progressively adopt identity agents and digital identities to achieve elevated identity assurances and transaction security for selected applications. And the financial industry could harness identity agents and digital identities to identity-proof customers and notarize documents.

References

[1] Kalman C. Toth, Agent-Based Digital Identity Architecture, PNSQC, October 14-16, 2024.

[2] Kalman C. Toth, *Electronic Identity 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,* unpublished.

[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.