Privacy by Design Identity Architecture

Verifiably Owner-Controlled Identity using Agents

IdentityNORTH 2020 Virtual Annual Summit
Toronto, Canada, June 17-18, 2020

Kalman C. Toth Ph.D. Ann Cavoukian Ph.D. Alan Anderson-Priddy, M.Sc.

This paper documents the narrator's script, author biographies and references for the video presented at the IdentityNORTH 2020 Virtual Annual Summit. Sections 1-9 below correspond to the nine segments of the video and the screen shots in the annex.

1 Introduction

Presented is a privacy by design identity architecture where digital identities are verifiably owner-controlled, intuitive, and identity-assured. Identity agents decentralize identity by deploying digital identities that enable users to prove who they are, protect their private data, and securely collaborate.

This presentation explores relevant risks, issues and opportunities across the identity landscape; describes the proposed system concept; explains how privacy by design principles have been applied; and highlights the architecture's distinguishing design elements and capabilities.

These papers provide additional details [see list of references below].

2 Boosting Solution Strength, Flattening the Curve

Over the past 20 years, single sign-on, federated identity, identity access management, second factor authentication, and biometrics have progressively strengthened identity solutions. Despite these innovations - breaches, identity theft, impersonation and fraud continue to escalate. Root causes include large-scale data collection; excessive dependency on remote access passwords; and burgeoning system complexity. Rapidly growing Internet usage is also widening the gap.

The proposed architecture boosts solution strength and flattens the risk curve by:

- satisfying the principles of privacy by design
- decentralizing identity to users, and
- deploying identities that are verifiably owner-controlled, intuitive & identity-assured.

Copyright 2020 Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy

3 Issues and Opportunities Across the Identity Landscape

Comprehensive validation of identity should cover all five dimensions of the identity landscape: what one knows, what one holds, what one is, what one asserts, and what others assert. Existing solutions don't address identity comprehensively. Consider the issues and opportunities.

- "What one knows" depicts technologies requiring users to specify their online profiles and passwords. Users are frustrated juggling countless profiles and passwords. *They need much more convenience and less friction maintaining their private data and proving who they are.*
- "What one holds" depicts messaging applications running on individuals' smart phones and tablet PCs. Such personal devices can be lost and stolen. *Built-in biometrics and cryptographics should be exploited to mitigate the risk of owners losing control of their devices.*
- "What one is" depicts authenticators typically using biometrics to bind their owners. Such single-purpose devices do not solve the problem of updating online user profiles. *General purpose devices having biometrics, such as smart phones, could be engineered to specify owner-controlled identities.*
- "What one asserts" depicts the W3C's emerging models for decentralizing identity using machine-readable credentials. Neither ease-of-use nor verifiable control are addressed. *These models, biometrics and encryption can be combined to create intuitive identities controlled by their owners.*
- "What others assert" depicts banking and governmental systems. Chip-and-PIN smart cards attesting that the holder was identity-proofed and qualified, elevate identity assurances in the physical world. *So, too, it should be possible to proof and elevate identity assurances for owners in the digital world.*

A holistic approach for identity is needed. Biometrics and encryption can be used to bind users to their digital identities and verify that they control them. Virtualizing identities would help users intuitively, easily and reliably manage their private and identifying data. Identity-proofing and attestation would elevate identity assurances associated with their digital identities.

4 Leveling the Playing Field

The 2018 Facebook-Cambridge Analytica scandal revealed that an enormous volume of collected private data had been misused by political operatives. Later that year, 87 million private records of Facebook users were breached. Sir Timothy Berners-Lee subsequently declared that power over identity and privacy must be taken back from the big Internet players and returned to users.

Copyright 2020 Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy

The proposed architecture levels the playing field for users by applying the principles of privacy by design; decentralizing identity; and deploying digital identities that are verifiably owner-controlled:

- Privacy by design minimizes private data collection. Users control the disclosure of private data; they can reliably delegate consent to access their private data for express purposes; their private data and transactions are protected; and privacy is the system's default setting.
- Decentralizing identity shifts responsibility over identity from providers to users by deploying credentials and identifiers that can be specified by users and are portable. Decentralizing identity disperses the attack surface and reduces breach risk and service provider liability.
- Owner-controlled identity binds users to their digital identities and enables relying parties to verify that presented digital identities are controlled by their owners. Users can intuitively manage their digital identities, thereby reducing the risk of unintended disclosure. To elevate identity assurances, users can be identity-proofed and have their digital identities attested by other owners.

5 System Concept: Verifiable Owner-Controlled Identity

This figure depicts the building blocks enabling verifiable owner-controlled identity.

- Ordinary users, system administrators and service providers have identity agents installed on their Internet devices, for example, on their smart phones, tablet PCs, laptops, and/or servers.
- Each identity agent reliably controls identity, privacy and security on behalf of its owner. Identity agents enable their owners to prove who they are, control disclosure of private data, secure private data, messages and transactions, proof and attest identities, and delegate consent.
- Identity agents encapsulate authentication data, such as the owner's biometric minutia, to tightly bind the owner to her device, digital identities, private data, consent tokens, and other artifacts.
- Identity agents use a digital identity model to virtualize identifying credentials for the owner, as well as notarizing seals that can be cryptographically affixed to digital identities. Each digital identity is allocated multiple public/private key-pairs for signing, encrypting and digital sealing purposes.
- Identity agents can securely exchange digital identities online or by direct device-to-device transfer. Once exchanged, their keys can be used to secure messages, transactions and other artifacts.
- When receiving a digital identity, the owner's identity agent verifies that it was registered in a proof-of-existence registry; that the originating identity agent has possession of the digital identity that was received; and that the originating owner has custody of her device.

Copyright 2020 Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy

- Ordinary users and designated parties can use their identity agents to elevate identity assurances by proofing, attesting and digitally sealing a requester's identity. Multiple parties can seal an identity. Because digital seals cryptographically bind identities to attestations, they cannot be denied.
- When delegating consent, the resource owner, resource custodian and the requesting owner create digital seals affixing commitments to consent tokens that they cannot repudiate. Risks are reduced when stakeholders use digital identities having elevated identity assurances.

6 Privacy by Design Process

The principles of privacy by design were applied to discover and validate the privacy requirements and design elements of the identity architecture.

The top-level privacy requirements and system design specifications were broken down, mapped to each other, and partitioned into four views - the User Interface Design View; the Interoperability Design View; the Verification Design View; and the Delegated Consent Design View.

7 Design Views

The design views are detailed in our Annual Privacy Forum paper.

- The User Interface Design View specifies how identity agents and digital identities are controlled by the owner and protected; how identities are virtualized; and how disclosure is controlled.
- The Interoperability Design View specifies how identity agents interoperate; how they interface with messaging applications; and how they exchange identities on behalf of their owners.
- The Diffie-Hellman method has been adapted to securely exchange identities.
- The Verification Design View specifies how identity agents verify that presented identities are controlled by their owners, and how identities are proofed, attested, sealed and verified.
- The Delegated Consent Design View specifies how stakeholder commitments are affixed to consent tokens; how access to private data is controlled; and how critical events are logged and monitored.

8 Capabilities and User Empowerment

Identity agents will empower users and stimulate technology adoption because they deploy digital identities that increase usability; enable owners to reliably disclose private data and delegate consent; secure transactions and messages; and prevent impersonation.

- By virtualizing identities and notarizing seals, and holding their digital identities tightly, identity agents offer their owners a much more intuitive, easy-to-use experience than

Copyright 2020 Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy

passwords. They overcome user frustration maintaining online profiles, and friction provisioning passwords.

- Identity agents help owners securely and conveniently exchange their digital identities both online, and in-person with other identity agent owners.
- By encapsulating authentication data, identity agents ensure that their owners tightly control their own devices, identities, private keys, consent tokens, PINs, passwords and other private data.
- They prevent impersonation by verifying that presented identities have been registered, and that collaborating owners control their identities, and their devices.
- Both ordinary users and designated parties can use their identity agents to elevate identity assurances for other parties by proofing, attesting and digitally sealing their identities.
- When receiving an identity and delegating consent, users and service providers can leverage their identity agents to assess whether provided identity assurances are acceptable.

9 Closing Remarks

In summary, identity agents prevent impersonation and reduce risks for their owners by deploying digital identities they control, can be verified by other owners, are intuitive and easy to use, and can be identity-assured by ordinary users as well as designated owners.

We welcome your comments, questions and requests. Thank you for listening!

Patents

Three patents and one patent pending cover electronic identity and credentialing, digital sealing, proof-of-existence registry, secure identity exchange, identity verification, and delegated consent.

Bibliography

Katrina Brooker, “Tim Berners-Lee tells us his radical new plan to upend the World Wide Web,” *FastCompany*, Sept. 29, 2018.

Fast Identity Online (FIDO) specification: www.fidoalliance.org.

NIST Special Publication 800-63A, “Digital Identity Guidelines, Enrollment and Identity Proofing”, January 2017, https://doi.org/10.6028/NIST.SP.800-63a.

Hesslie Jones, “Accelerating the Future Of Privacy through SmartData Agents”, Cognitive World, *AI & Big Data*, Nov. 3, 2018.

Ann Cavoukian, “Privacy by Design, The 7 Foundational Principles”, https://www.ipc.on.ca/wp-content/uploads/Resources/ 7foundationalprinciples.pdf.

Ann Cavoukian, “Consumers bear the cost of their privacy protection,” *Globe and Mail*, Sept 7, 2018.

Copyright 2020 Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy

Sovrin Foundation, “Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust,” Version 1, January 2018, https://sovrin.org.

World Wide Web Consortium (W3C), “Verifiable credentials data model 1.0: Expressing verifiable information on the Web”, W3C Recommendation 19 November 2019.

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

N. Asokan, Baltteri Niemi, Pekka Laitinen, “On the Usefulness of Proof of Possession,” *2nd Annual PKI Workshop*, Apr. 28-29, 2003, pp.136-141.

E. Rescorla, “Diffie-Hellman Key Agreement Method”, RTFM Inc., June 1999.

Kalman Toth, Alan Anderson-Priddy, “Architecture for Self-Sovereign Digital Identity,” *Computer Applications for Industry and Engineering*, New Orleans, LA, Oct. 8-10, 2018.

Kalman Toth, Alan Anderson-Priddy, “Self-Sovereign Digital Identity: A Paradigm Shift for Identity,” *IEEE Security and Privacy*, Vol. 17, No. 3, May/June 2019.

Kalman Toth, Alan Anderson-Priddy, “Privacy by Design using Agents and Sovereign Identities”, Information Security and Privacy Protection Conference (IFIP-SEC), Work in Progress and Emerging Technology Track, Lisbon, Portugal, June 25-27, 2019.

Kalman Toth, Ann Cavoukian, Alan Anderson-Priddy, “Privacy by Design Identity Architecture Composed of Identity Agents Decentralizing Control over Digital Identity”, Open Identity Summit (OID) 2020 Proceedings, May 27, 2020.

Kalman Toth, Ann Cavoukian, Alan Anderson-Priddy, “Privacy by Design Identity Architecture Using Agents and Digital Identities”, Annual Privacy Forum (APF), Lisbon, Portugal, Oct. 2020, paper accepted for publication in a forthcoming issue of Springer.

Author Bios

Kal Toth is a professional engineer registered in British Columbia with a Ph.D. in electrical and computer systems engineering from Carleton University, Ottawa, Canada. His industry and academic experience with the likes of Hughes Aircraft, CGI Group, and Portland State University spans the fields of digital identity, privacy and security; software engineering; and distributed database systems and networks. He can be contacted at kalmanctoth@gmail.com.

Ann Cavoukian, Ph.D. She is three-term Information and Privacy Commissioner of Ontario and is widely acclaimed for her contributions to Europe’s General Data Protection Regulation (GDPR) addressing the principles of Privacy by Design. Past Executive Director of Ryerson University’s Privacy and Big Data Institute, she now leads the Global Privacy and Security by Design Centre in Toronto. She can be contacted at ann.cavoukian@gpsbydesign.org.

Alan Anderson-Priddy has an M.Sc. degree in software engineering from Portland State University in Oregon. His professional experience includes software and systems consulting, technology research and development, enterprise software integration, and software prototype development. He can be contacted at andersonpriddy@gmail.com.

Copyright 2020 Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy

ANNEX

Video Segments 1-9 Depicted Below

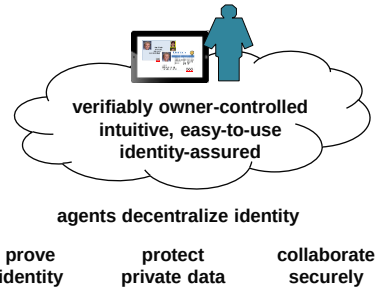
Privacy by Design Identity Architecture
Verifiably Owner-Controlled Identity using Agents

IdentityNORTH 2020 Virtual Annual Summit
Toronto, Canada, June 17-18, 2020

Kalman C. Toth Ph.D Ann Cavoukian Ph.D Alan Anderson-Priddy M.Sc.

Presentation Outline

Boosting Solution Strength
Issues and Opportunities
Leveling the Playing Field
System Concept
Privacy by Design
Design Views
Capabilities

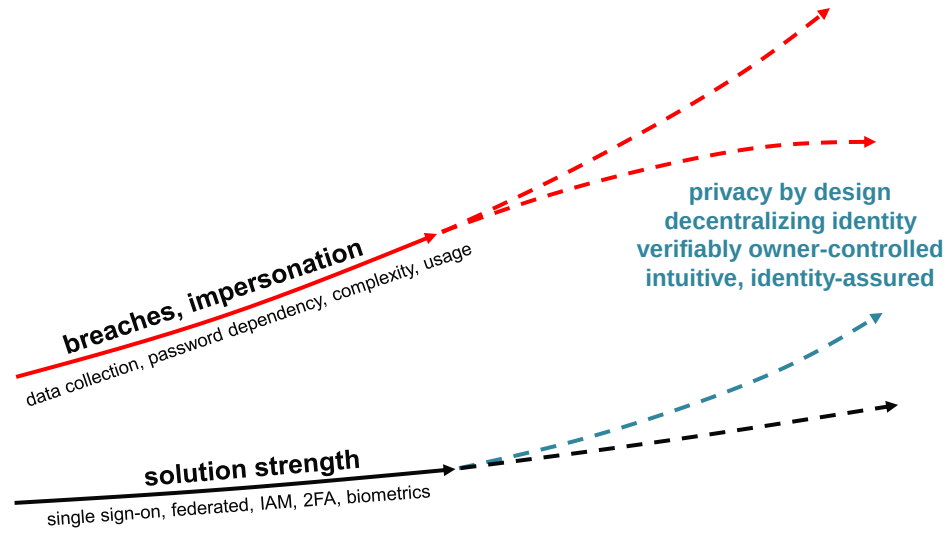


Toth, Cavoukian, Anderson-Priddy, "Privacy by Design Identity Architecture Using Agents and Digital Identities", Annual Privacy Forum (APF), October 2020, Lisbon, Portugal, accepted by Springer for publication.

Toth, Cavoukian, Anderson-Priddy, "Privacy by Design Identity Architecture Composed of Identity Agents Decentralizing Control over Digital Identity", Open Identity (OID) Summit 2020 Proceedings.

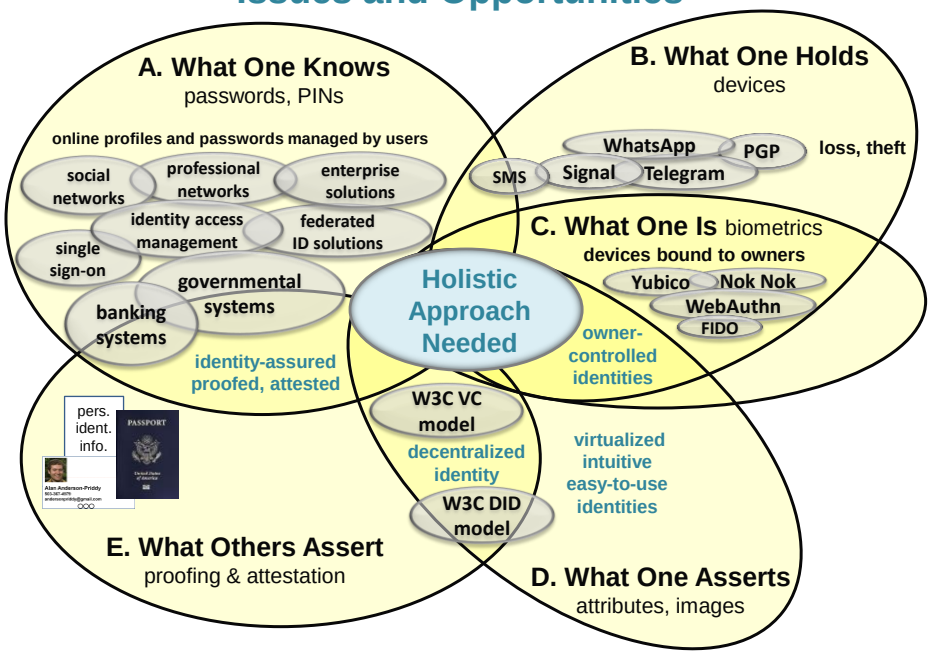
Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

Boosting Solution Strength, Flattening the Curve



Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

Issues and Opportunities

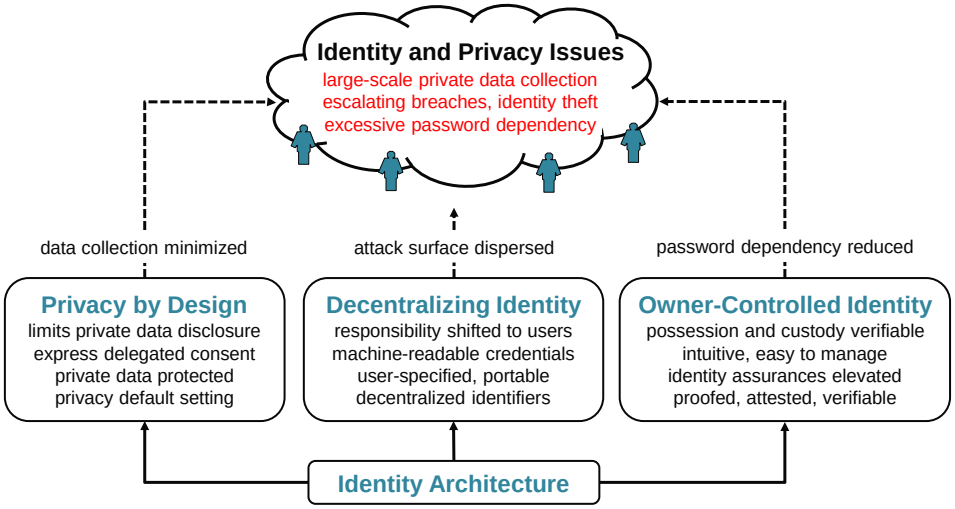


Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

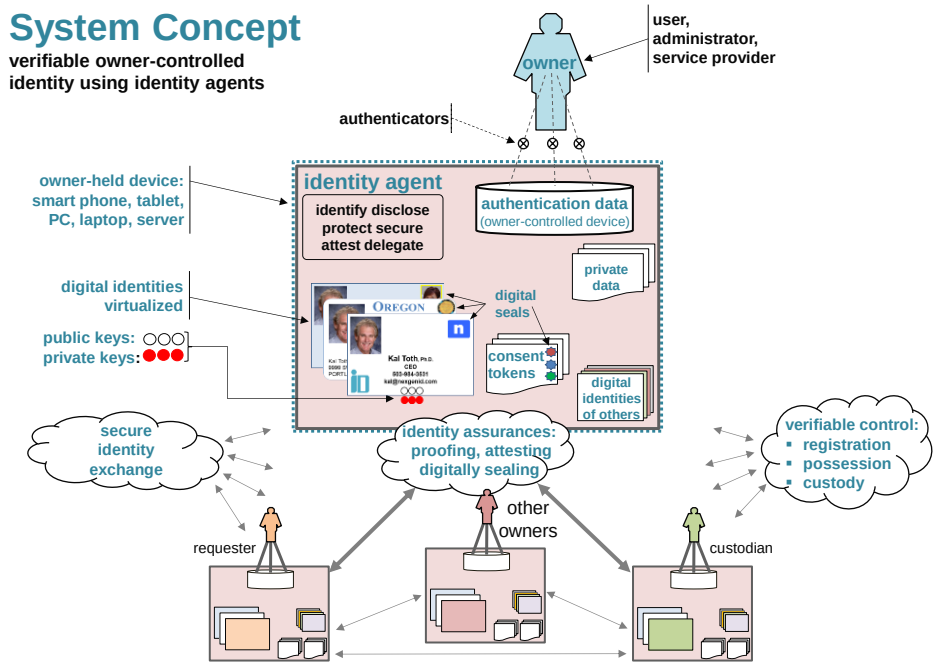
Leveling the Playing Field

2018 Facebook: 87M private records breached

Berners-Lee: take back power from the big Internet players … shift control to users

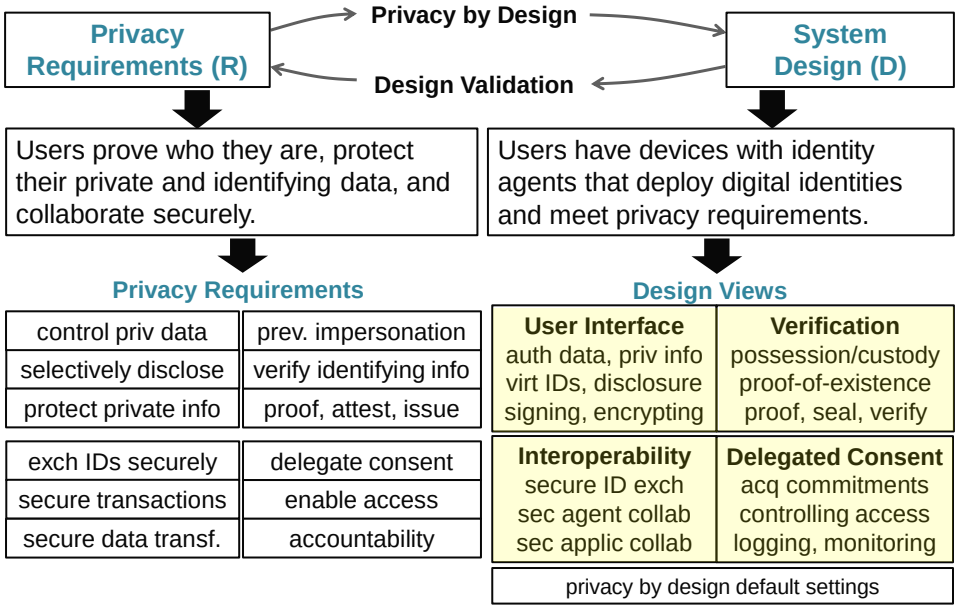


Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture



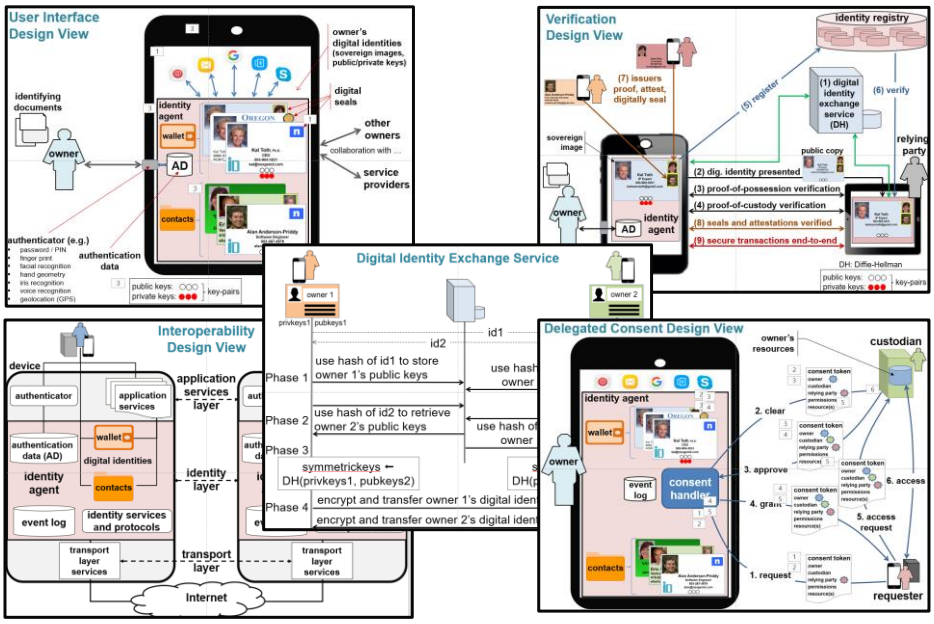
Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

Privacy by Design Process



Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

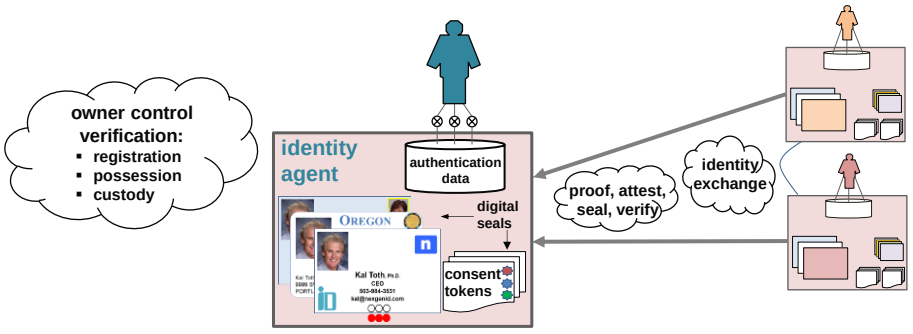
Design Views



Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

Capabilities, User Empowerment

- ✓ **Empowerment** - privacy, security, impersonation prevention
- ✓ **Virtualized digital identities** - usability, intuitive ease-of-use
- ✓ **Digital identity exchange** - secure, convenient transfers
- ✓ **Owner Control** - encapsulated authentication data, devices controlled
- ✓ **Verifiable owner-control** - existence, possession, custody
- ✓ **Elevating identity assurances** - proof, attest, digitally seal
- ✓ **Acceptability of assurances** - verify digital seals, attestations



Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture

Closing Remarks

- users control their identities
- identities verified by others
- intuitive, easy to use
- identity-assured by others

identity agent

Kal Toth, Ph.D
linkedin.com/in/kaltoth/
kalmanctoth@gmail.com

Ann Cavoukian, Ph.D
Global Privacy and Security Design Centre
Ann.Cavoukian@gpsbydesign.com

Alan Anderson-Priddy, M.Sc.
andersonpriddy@gmail.com

Thank You!

Narrator: Connie Kirk

Available on Request and Online

- Narrator's script, bios, reference materials and screen shots in a single document
- Materials published by the authors available via **linkedin.com/in/kaltoth/** and by email

Copyright © 2020 Kalman C. Toth, Ann Cavoukian, Alan Anderson-Priddy, Privacy by Design Identity Architecture