Privacy by Design using Agents and Sovereign Identities

Kalman C. Toth[1][0000-0003-4659-1654] and Alan Anderson-Priddy[2]

[1] NexGenID, Portland OR 97205, USA
[2] Portland State University, Portland OR 97207, USA
[1] kal@nexgenid.com, [2] alan@nexgenid.com

Abstract. Our architecture employs collaborating *trusted agents* that deploy *self-sovereign digital identities* to owners enabling them to prove who they are and protect their private and personally identifying information. To show that our identity architecture satisfies the principles of *privacy by design*, we have applied generally accepted systems and software engineering practices to identify privacy requirements and design views, and validated these design views against the privacy requirements.

Keywords: privacy by design, identity, security and authentication.

1 Introduction

The Internet has a serious problem with identity and privacy. We have witnessed an alarming growth in compromised privacy by way of large-scale breaches, identity theft, impersonation and fraud. A critical root cause is the enormous volume of private data collected by providers underpinning password provisioning and sustaining business models driven by advertising revenue. Trusted agents deploying self-sovereign identities promise to deliver privacy by design that enable users to manage their identities and private data.

2 Relating Digital Identity and Privacy

Identity and privacy are intimately connected. Tightly controlled by their owners, self-sovereign digital identities enable them to prove who they are. When the binding between a user and her digital identity or a user and her private data is compromised, her private data can become publicly known and/or used to impersonate her. Such risks can be significantly reduced by simultaneously binding users to their digital identities and their private data. Our architecture implements such bindings.

Fig. 1 depicts a trusted agent working on behalf of an owner and interoperating with other trusted agents. A trusted agent encapsulates authentication data of the owner, possibly using multiple factors, and controls the owner's digital identities contained therein. The identities have properties enabling trusted agents to digitally sign, encrypt and seal identities, transactions, local and remote private data, consent tokens, and other digital artifacts. Digital seals cryptographically bind owner identities and attestations to digital artifacts that the owner cannot readily repudiate.

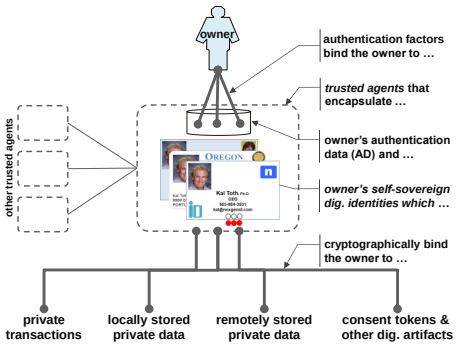

Fig. 1. Relating Digital Identity and Privacy

3 Privacy By Design

Early in the development of mission-critical systems, practitioners routinely define the requirements of the system, develop candidate designs, evaluate the design options, and settle on the one that best satisfies the requirements. Fig. 2 depicts our approach for Privacy by Design [1]. Our Privacy Requirements state (**A**) that the system is to support digital identities proving who users are while safeguarding their private data. Our System Design goal (B) specifies that users have devices with trusted intelligent agents [2] controlling and protecting their identities and private data. We have broken down our privacy requirements; identified four design views (Figs. 3-6); and traced these design views to the requirements they satisfy.

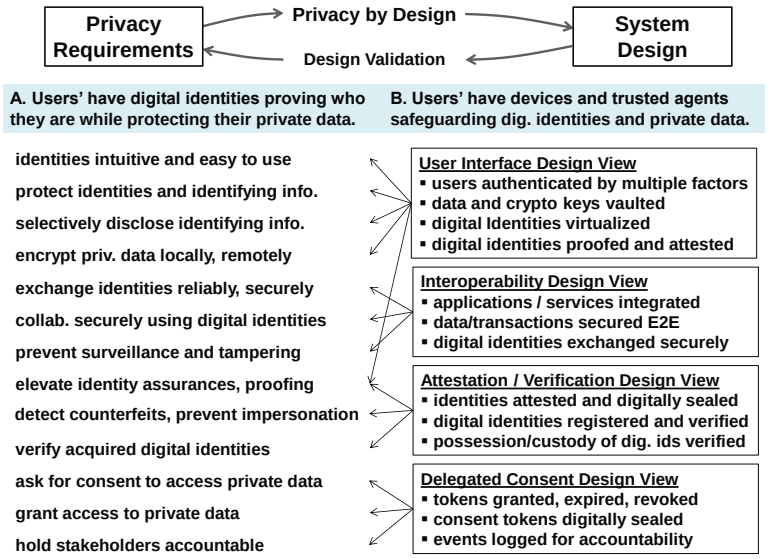

Fig. 2. Privacy by Design Process

User Interface Design View: Identity engines encapsulate authentication data enabling the owner to tightly control her digital identities. Identities are virtualized for ease-of-use and technology adoption; public/private key-pairs are bound to digital identities when created [3, 4]; the private keys of owners are not revealed; and agents reliably interoperate with the agents of other owners and service providers.

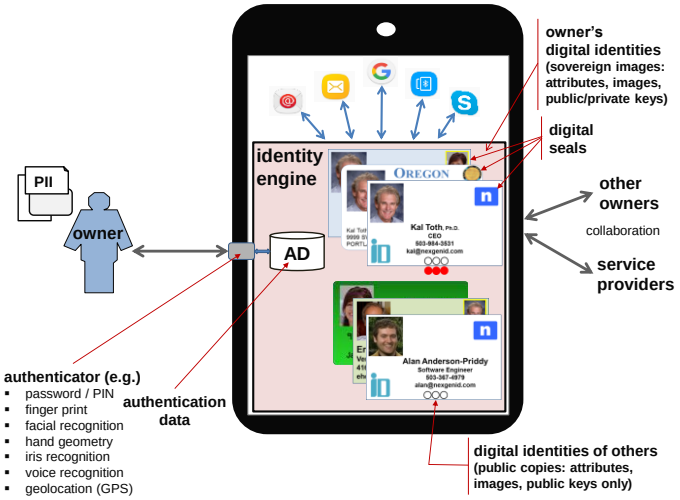

Fig. 3. User Interface Design View

Interoperability Design View: Identity engines are deployed between the Transport and Application Services Layers establishing an integrative identity layer across a given application context [3, 4]. Embedded protocols sign and encrypt transactions and leverage Diffie-Hellman [5] to securely exchange digital identities.

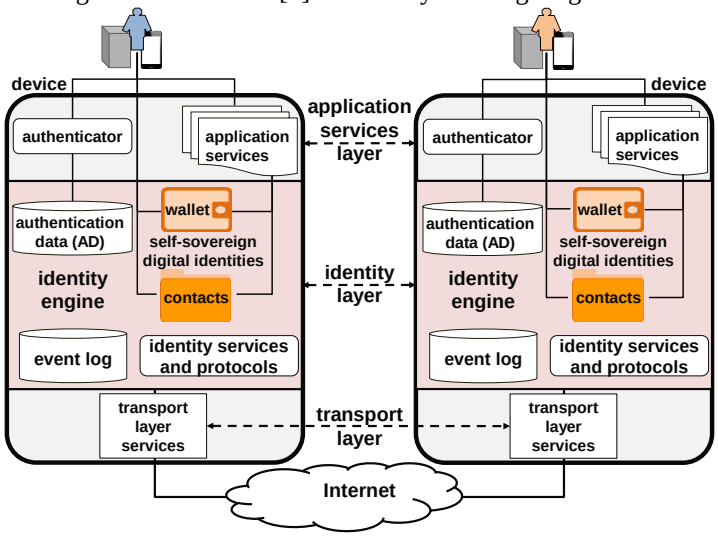

Fig. 4. Interoperability Design View

Attestation and Verification Design View: Assurances associated with digital identities are elevated when users proof, attest and digitally seal [3, 4] them. Collaborators verify digital identities by searching a proof-of-existence identity registry and/or by launching proof-of-possession and custody challenges [6].

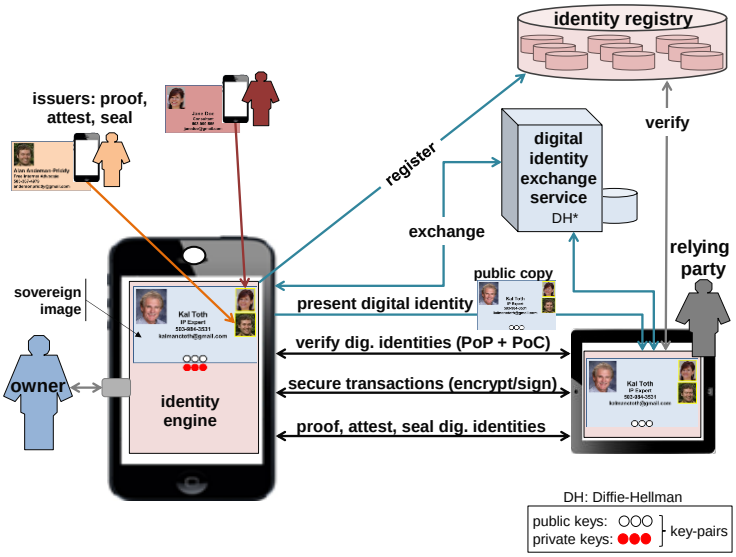

Fig. 5. Attestation and Verification Design View

Delegated Consent Design View: Prior art consent models are controlled by service providers. Our model enables owners to grant and monitor consent to access their remote private data using consent tokens digitally sealed by stakeholders.

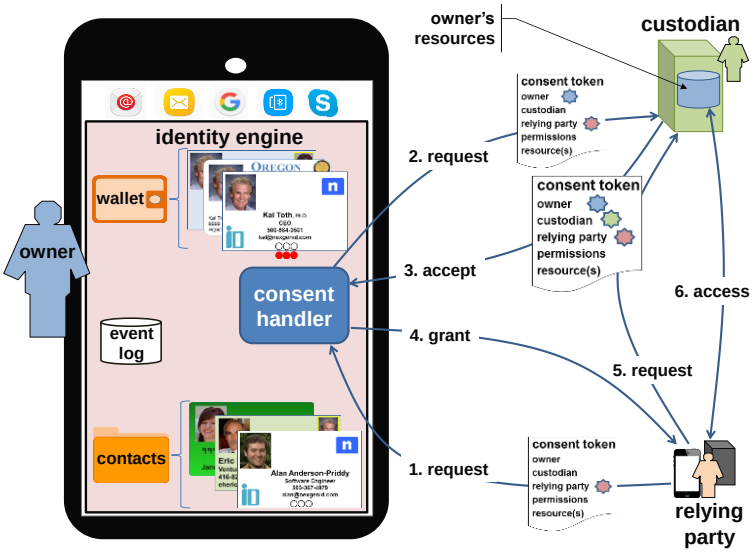

Fig. 6. Delegated Consent Design View

4 Concluding Remarks

Privacy by Design addresses the intimately related challenges of identity assurance and privacy protection. We have identified four foundation design views for NexGenID's identity architecture. Trusted agents and self-sovereign digital identities are simultaneously deployed to elevate identity assurances, enhance privacy, and strengthen security.

Future areas for study include using blockchain technology to distribute proof-of-existence identity registration across the web; adapting Signal's messaging protocol [7] to harden transaction security; and leveraging formal methods, trust zones, and trusted execution environments to elevate agent trustworthiness.

References

1. Ann Cavoukian, "Privacy by Design, The 7 Foundational Principles," https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
2. Hesslie Jones, "Accelerating The Future Of Privacy Through SmartData Agents, Cognitive World," *AI & Big Data*, Nov. 3, 2018.
3. Kalman C. Toth and Alan Anderson-Priddy, "Architecture for Self-Sovereign Digital Identity," *Computer Applications for Industry and Engineering (CAINE)*, Oct. 8-10, 2018.
4. Kalman C. Toth and Alan Anderson-Priddy, "Self-Sovereign Digital Identity: A Paradigm Shift for Identity," *IEEE Security and Privacy*, May/June 2019 issue.
5. E. Rescorla, "Diffie-Hellman Key Agreement Method", RTFM Inc., June 1999.
6. N. Asokan, Baltteri Niemi, Pekka Laitinen, "On the Usefulness of Proof of Possession," *2nd Annual PKI Workshop*, Apr. 28-29, 2003, pp.136-141.
7. Katriel Cohn-Gordon et. al., "A Formal Analysis of the Signal Messaging Protocol," November 2017, https://eprint.iacr.org/2016/1013.pdf.