Open Banking: Will Decentralized Identity Satisfy Needs and Risks?

Kal Toth, Sovereign Image Inc.[1] for IdentityNorth Winter Workshop, Feb. 17-18, 2021

Stimulated by GDPR[2] and governed by PSD2[3], **Open Banking** was motivated by expanding market opportunities and increasing customer choice. Open application programming interfaces (APIs) enable emerging mobile apps and online services to exploit data and transactions held and managed by banks. Exploiting this data increases privacy and security concerns for banks and their customers. Currently, most online banking systems authenticate their customers using passwords augmented by a second factor such as text messaging and email. Some have suggested that in the not too distant future, such schemes will not be adequate for online banking, but that **Decentralizing Identity** to customers has the potential of mitigating privacy and security risks for emerging **Open Banking** systems.

This article explores the following pertinent questions:

- **A.** What lessons have been learned about identity technology that inform **Open Banking**?
- **B.** What requirements are being proposed for **Open Banking** and mitigating anticipated risks?
- **C.** Will **Decentralizing Identity** satisfy **Open Banking** requirements and mitigate these risks?

A. Lessons-Learned about Identity Technology that Inform Open Banking

Presumably, open banking will require higher levels of identity assurance than currently deployed for online banking:

a) Remote password authentication, even when augmented with second factor schemes, is nevertheless vulnerable to several attack vectors.
b) Commercial single sign-on and identity provisioning technologies such as OpenID Connect[4], OAuth and Facebook Connect[5] pose well-known private data collection and surveillance risks.
c) PGP[6], using client-side digital certificates and public/private key encryption, strongly encrypts transactions, prevents phishing attacks, but has enjoyed limited success because of weak usability properties.
d) Used in the government sector, PIV[7] and CAC[8] smart cards having X.509 digital certificates cryptographically bind users to online web services, but their devices need integrated or tethered smart card readers.
e) In the commercial sector, FIDO[9] (Fast Identity Online), a W3C standard, leverages biometrics and public-private encryption to authenticate holders but requires them to acquire special purpose authenticators.
f) Privacy-enhancing technology (e.g. Microsoft U-Prove, IBM Idemix, ABC4Trust and IRMA)[10] have developed techniques for preventing private data correlation and leakage across users and issuers, and zero knowledge proofs (ZKPs) for minimizing data disclosure, but limitations include usability and commercial availability.

These lessons-learned inform **Open Banking** about how to deploy digital identity technology. The most noticeable common thread for success is that public/private key encryption technology is consistently exploited {(c), (d) and (e)}. Given online banking customers use increasingly feature-rich personal devices for online banking, digital identities can exploit built-in encryption mechanisms; built-in wireless connectivity (NFC) {off-setting limitation (d)}; and built-in biometrics {off-setting limitation (e)}. Items (c) and (f) reinforce how important usability is to the successful adoption of identity technology. In other words, a user-oriented identity data model is critical for empowering users with digital identities they can intuitively use to prove who they are and secure their private data and transactions.

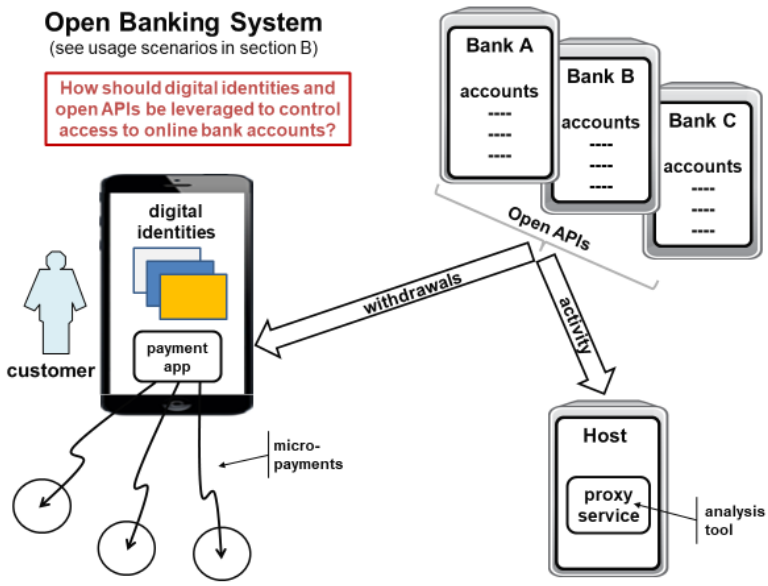
B. Open Banking Requirements and Risk Mitigation

Two usage scenarios are described below to provide context for the discussion that follows. The user (customer) has multiple bank accounts hosted by a banking system supporting open APIs. The banking system, the customer's device, and the described third-party web service are assumed to deploy a trustworthy execution environment.

---

[1] Sovereign Image Inc. https://www.sovereignimage.com
[2] General Data Protection Regulation (GDPR) http://www.gdpr-info.eu
[3] Second Payment Services Directive (PSD2) http://www.openbankproject.com/psd2/
[4] OpenID Connect https://openid.net/connect/
[5] Facebook Connect: https://en.wikipedia.org/wiki/Facebook_Platform
[6] Pretty Good Privacy (PGP) uses public/private encryption technology to secure email https://en.wikipedia.org/wiki/Pretty_Good_Privacy
[7] Personal Identity Verification (PIV) credentials are used to access federally controlled facilities and information systems
[8] Common Access Cards (CAC) are smart cards used by military personnel and contractors to access information systems
[9] WebAuthn https://www.w3.org/TR/webauthn-2/ implements FIDO protocols for handheld authenticators securing web transactions
[10] This papers addresses a wide range of identity and privacy-enhancing technologies https://pomcor.com/techreports/PrivacyPostures.pdf

Micro payment app: Installed on the customer's personal device (e.g. smart phone or PC), this app uses an open API to process transactions against the owner's bank account, plus a wireless interface (e.g. NFC) to issue payments, for example, to transponders, vending machines or point-of-sale terminals. The app is tamper-resistant, trusted, tightly controlled by the owner, and can be disabled. The owner can use a gesture, PIN or biometric to activate the device.



Online proxy service: This is a proxy of the customer running on a web hosting service accessing her online bank account by way of an open API. Once activated, her proxy can run continuously until deactivated. In this case, the proxy is given read-only access to the customer's bank accounts. The proxy can read the owner's banking data, conduct financial analysis, and push alerts to the owner. As above, the proxy is tamper-resistant, trusted, and can be disabled. Security risks are partially mitigated because the proxy is granted read-only access to her banking data.

Principle Open Banking Requirements for Digital Identity

[1] *Reducing or eliminating dependence on remote access passwords is probably a top priority for* ***Open Banking****.*
[2] *Privacy and security risks are among the top risks* ***Open Banking*** *systems must mitigate.*
[3] *Digital identities are to cut across organizations and sectors, and are to be portable.*
[4] ***Open Banking*** *leverages an identity model governing specification and the transfer of digital identities.*
[5] *Digital identities specify the customer's identifying and private information and control critical operations, namely, creating, proofing, updating, retiring, revoking, expiring, backing-up and recovering digital identities.*
[6] *Integrity of digital identities must be adequately protected from tampering and secured when transferred.*
[7] *In-person and remote identity-proofing and documents align with identity assurances when onboarding.*

These **Open Banking** requirements need to be clarified:

[8] *Usability requirements when specifying, showing, exchanging, verifying and using digital identities.*
[9] *Limiting disclosure when presenting digital identities and delegating express consent.*
[10] *Maintaining the provenance and integrity of digital identities and other data.*

C. Will Decentralizing Identity Satisfy Open Banking Requirements and Mitigate the Risks?

Over the last few years, several architectures decentralizing identity to users have emerged. Examples include:

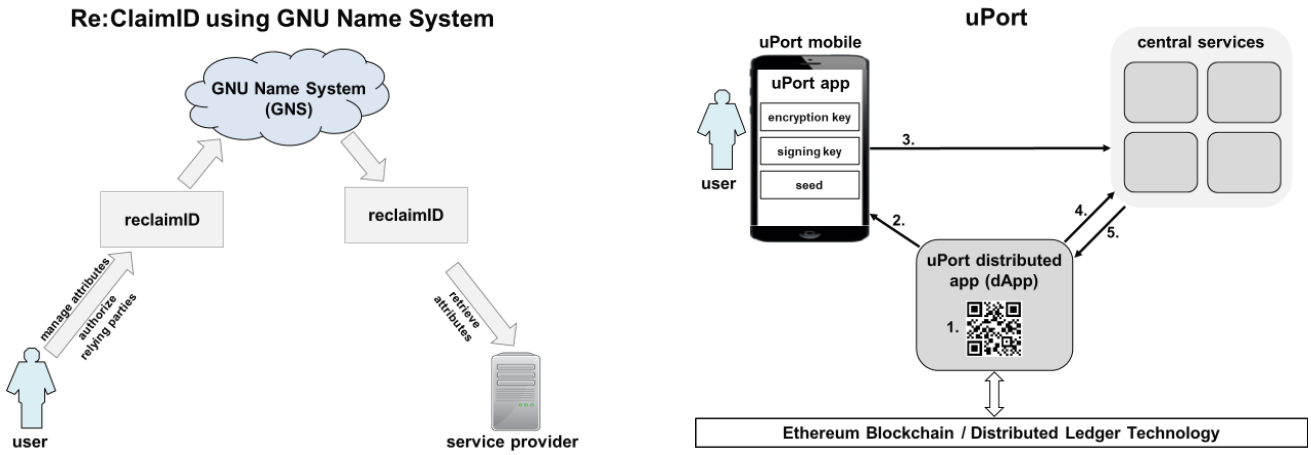
Re:claimID[11] leveraging the GNU Name System (GNS) and attribute-based encryption; uPort[12] exploiting Etherium's distributed ledger technology, a blockchain solution; and Sovereign Image architecture[13] harnessing interoperating identity agents. Sovrin and Evernym[14] have developed DLT (blockchain) solutions which are not addressed herein.

These solutions variously refer to "digital identity", "self-sovereign identity", "self-sovereign digital identity", "identity credentials", "digital credentials", "electronic credentials", "e-credentials", or simply "credentials". Although some writers have distinguished between these terms, the subtle differences are not discussed. This article refers to "digital identity" and "digital identities", occasionally mention they are sovereign or self-sovereign (owner-controlled).

The following paragraphs position **Open Banking** requirements and concerns about risk in the context of three decentralized identity technologies, namely, ReclaimID, uPort using Ethereum, and Sovereign Image. The indexed headings in this section directly reference **Open Banking** requirements **[1]** to **[10]** listed in section **B**.

---

[11] Re:claimID and the GNU Name System https://ieeexplore.ieee.org/document/8456003
[12] uPort and Etherium https://medium.com/uport/different-approaches-to-ethereum-identity-standards-a09488347c87
[13] Sovereign Image, https://www.sovereignimage.com
[14] Sovrin and Evernym https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf



[1] ***Reducing or eliminating dependence on remote access passwords is probably a top priority for Open Banking.***

Decentralizing Identity: Using distinct technical implementation strategies, ReclaimID, uPort and Sovereign Image leverage public/private pairs to decentralize digital identity to users. In each case, public keys are associated with identifying the digital identity owner, while private keys are secrets held by the identity owner. These architectures have the potential of replacing remote access passwords because discovering a private key from the public key is much harder to achieve than breaking a password.

[2] ***Privacy and security risks are among the top risks Open Banking systems need to mitigate.***

Risk Mitigation: Decentralizing identity to users distributes the attack surface thereby reducing the relative risk of privacy loss over centralized and federated identity solutions. A ReclaimID user could unintentionally encrypt a given attribute with the public key of the wrong service provider. Ethereum's permissioned (public) blockchain could be penetrated to extract the identifier of a uPort user subsequently attacking her digital identity. A Sovereign Image identity agent owner could disregard warnings and unknowingly submit her identity containing sensitive identifying information to a party whose identity is unknown and could be malicious.

[3] ***Digital identities are to cut across organizations and sectors, and are to be portable.***

Consistency Across Platforms: ReclaimID proposes service providers using identities (attributes actually) encrypted and deposited in a GNU Namespace System (GNS) to authenticate users. uPort proposes user-to-provider on-chain and off-chain applications using identities stored in a public Ethereum blockchain to authenticate users. Sovereign Image proposes organically building a virtual identity layer using identity agents that deploy digital identities used to mutually authenticate users and providers across web services. The relative technical and usage merits and risks of these technologies need to be carefully examined.

[4] ***Open Banking leverages an identity model governing specification and the transfer of digital identities.***

[5] ***Digital identities specify the customer's identifying and private information and control critical operations.***

Identity Data Model: Sovereign Image uses a common identity data model to structure and specify digital identities including identifiers, attributes, images and public/private encryption key pairs. This model extends W3C's Verifiable Credentials model[15] for machine-readability and portability incorporating cryptographic keys and operations for three distinct capabilities. Digital identities are securely written into a proof-of-existence identity registry when created, updated, deleted and revoked used by relying parties to verify them. Sovereign Image's proof-of-existence registry could potentially exploit the properties of a blockchain technology such as Ethereum. Presumably, ReclaimID and uPort have implemented similar identity data models.

[6] ***Integrity of digital identities must be adequately protected from tampering and secured when transferred.***

User Bindings and Control: ReclaimID assumes that users control their computing platforms and thereby their private keys. uPort simply indicates that users should be locally authenticated to guard against loss or theft. Sovereign Image's identity agents encapsulate the device owner's authentication data (e.g. PINs, biometrics), provide assurances to replying parties that the owner remains in control of digital identities by means of proof-of-possession and proof-of-custody challenges, secures and maintains the integrity of digital identities within the context of the identity engine, and signs, seals and encrypts private data and transactions.

[7] ***In-person and remote identity-proofing and documents align with identity assurances when onboarding.***

Identity Proofing and Attestation: Sovereign Image explicitly supports in-person and remote identity-proofing and describes procedures and mechanisms for proofing users and cryptographically binding attestations to digital identities to elevate associated identity assurances which are aligned with NIST's[16] identity and authentication assurance levels. Neither uPort nor ReclaimID describe such features and capabilities.

---

[15] W3C Verifiable Credentials https://www.w3.org/TR/vc-data-model/
[16] NIST SP 800-3-3 Digital Identity Guidelines, identity and authentication assurance levels https://pages.nist.gov/800-63-3/sp800-63-3.html

[8] ***Usability requirements when specifying, showing, exchanging, verifying and using digital identities.***

Usability: uPort uses QR codes to read digital identifies while ReclaimID does not explain how users manage their identities. Sovereign Image uses identity agents and the common identity data model to render virtualized identities that mimic the "look and feel" of identities used in the physical world. When meeting in-person, owners can show their digital identities and scan associated QR codes to transfer their digital identities. They can also use a web service to securely exchange their digital identities, and verify that presented digital identities exist and are in the possession and control of their owners before using them.

[9] ***Limiting disclosure when presenting digital identities and delegating express consent.***

Disclosure and Consent: ReclaimID uses attribute-based encryption which limits the risk of disclosure to unauthorized parties. uPort maintains meta data of digital identities on the public blockchain possibly leaving a residual risk that malicious attackers could compromise digital identities. Sovereign Image exploits digital identities to encrypt private data stored locally and remotely. Digital identity owners can decide which digital identities to disclose and what private and/or identifying information to reveal. Delegating consent to disclose and access data is achieved by circulating a consent token among stakeholders (requester, data owner, data custodian) who use their digital identities to create digital seals affixing commitments to a consent token that they cannot repudiate.

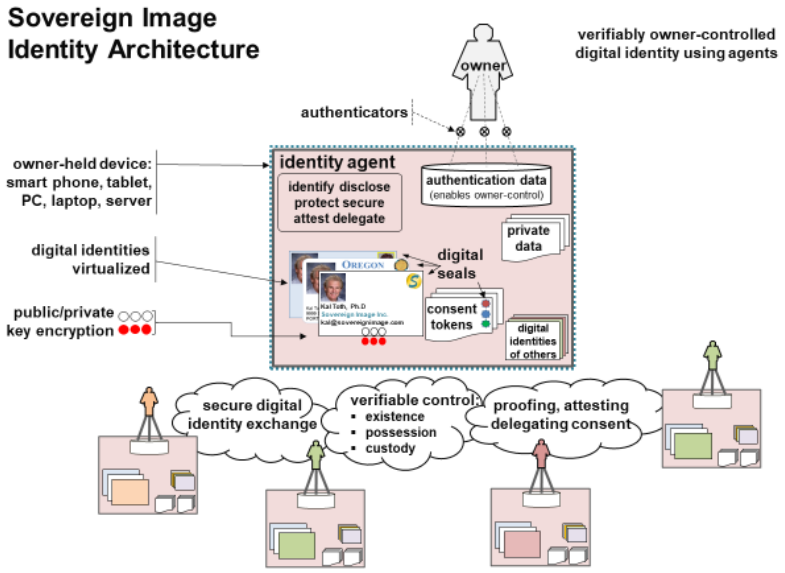
[10] ***Maintaining the provenance and integrity of digital identities and other data.***

Provenance and Integrity: Provenance and integrity of system data can be maintained by exploiting distributed database systems, change management systems, checksums, and blockchain technology (distributed ledgers). uPort exploits Ethereum to maintain the provenance and immutability of digital identities. Sovereign Image will exploit such alternatives, including blockchain technology, to maintain digital identities, consent tokens, and proof-of-existence registry records.

Licensing: ReclaimID and uPort offer open source licenses. Sovereign Image intends to create and make available a common reference model to guide open source development.

Additional Risk Mitigation Measures

Having decided on a suitable strategy for decentralizing identity, additional improvements can be incrementally introduced. For example, engineering-in software trustworthiness, enhancing privacy by minimizing data leakage, and hardening security through automated key rotation by deriving ephemeral encryption keys from long-term keys.



Critical Success Factors for Digital Identity Deployment			
Usability	**Control**	**Disclosure**	**Identity Assurances**
Digital identities mimic real-world identities that are intuitive and easy to use.	Relying parties can verify that digital identities exist and controlled by their true owners.	Owners can readily control what data they reveal and delegate and can expire and revoke access.	By way of in-person and remote proofing, owners can acquire identity assurances that are visible and intuitively meaningful.