CONSUMER DIGITAL IDENTITY

LEVERAGING DISTRIBUTED PRIVACY ENHANCING TECHNOLOGY

This paper explores current issues and opportunities in emerging identity markets, and describes the rationale and technology paradigms for designing a consumer–centric, privacy-enhanced system using modern distributed architectures. This paper was developed to accompany applied research developed by SecureKey under an applied research program of the Digital ID & Authentication Council of Canada (DIACC).

Table of Contents

ABOUT THIS DOCUMENT 3

EXECUTIVE SUMMARY 3

SYSTEM RATIONAL 4

ARCHITECTURAL AND PRIVACY PRINCIPALS 5

KEY STAKEHOLDERS 6

DIGITAL LOCK BOX PROVIDER (DLBP) 6
DIGITAL ASSET PROVIDER (DAP) 6
DATA CUSTODIAN 7
DIGITAL ASSET CONSUMER (DAC) 7
NETWORK STEWARD 7
THE USER 7

ARCHITECTURAL DETAILS 8

COMMERCIAL APPLICATION 10

CONCLUSION: A STRONG CUSTOMER PROPOSITION 11

About This Document

This document explores current issues and opportunities in emerging identity markets, and describes the rational and technology paradigms for designing a consumer–centric, privacy-enhanced system using modern distributed architectures. It was developed by the Digital ID & Authentication Council of Canada (DIACC) and SecureKey.

DIACC is a non-profit coalition of public and private sector organizations developing a digital identification and authentication framework. It was created following the federal government's Task Force for the Payments System Review.

SecureKey is a provider of identity and authentication solutions that simplify consumer access to online services and applications.

Executive Summary

The Commission on Enhancing National Cyber Security recently published its report on securing and growing the digital economy (December 1, 2016). The imperatives defined in the report were:

1. Protect, defend and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.
4. Build cyber security workforce capabilities.
5. Better equip government to function effectively and securely in the digital age.
6. Ensure an open, fair, competitive, and secure global digital economy.

Furthermore, the report emphasizes the needs for the administration to collaborate with the private sector on defining, implementing and defending a roadmap for i) improving the security of digital networks against denial-of-services, spoofing and others attacks on users and the nation's network infrastructure and ii) increasing the use of strong authentication to improve identity management

This document describes how SecureKey has developed a cloud-based identity ecosystem using elements of modern decentralized ledger (blockchain) technology to meet these requirements. The initial work was done in and applied research focused partnership of DIACC and Rutgers University Command, Control and Interoperability Center for Advanced Analysis (CCICADA) and concentrated on Model Definition, Business Analysis and Applied Research.

The identity ecosystem designed as a result of the research provides strong authentication while protecting individual privacy. It gives end-users control and convenience when sharing their digital assets with others in the ecosystem.

As such, the system complies with the guidance outlined in NIST Special Publication 800-63 and with DIACC's 10 Canadian Principles for Digital Identity Ecosystems. It is also aligned with the Privacy by Design Guidelines developed jointly between Canada and the Netherlands.

System Rational

A number of public and private sector organizations have implemented various identity management solutions to manage authentication and authorization privileges of their users within or across system and enterprise boundaries. Many of these current solutions rely on usage of Federated Authentication and Identity Networks Services provided by centralized broker architecture. These solutions allow end users to authenticate and/or provide their identity data claims using third party digital credentials they already have and trust, such as from their banks.

While currently deployed identity brokerage systems provide great utility to their participants, it has been noted that the principles upon which they are designed have several security and privacy limitations. Desirable improvements are further described in the “Privacy–Enhanced Identity Brokers” NIST whitepaper by Paul Grassi, Naomi Lefkovitz and Kevin Mangold, and in “Toward Mending Two Nation-Scale Brokered Identification Systems” whitepaper by Luis T.A.N Brandao, Nicolas Christin and George Danezis. Specifically, the architecture that addresses the issues mentioned above must reduce reliance on single point of trust and failure, and prevent any single party from tracking a user’s transaction, while maintaining an auditable trail that cannot be altered or used for data mining. The identity of the participant should also be protected using state of the art cryptographic technologies and protocols.

In addition, the proposed decentralized model described in this document also leverages well-known technology platforms and standards, and is available to the ecosystem participants leveraging an easy-to-license open source code-base maintainable by an established group of developers. It is designed to ease adoption and integration with book-of-record identity backend components, and to comply with established security, network communication and design requirements.

Architectural and Privacy Principals

The following are then the guiding principles to which the proposed system adheres:

1. No Centralized Authority: Both users and consortium members interact directly with the marketplace ensuring that there are no middle-man servers acting as a single point of failure or having the ability to tamper with the transactions.

2. Secured Blinded Infrastructure:
    a. Participants' identities should be guaranteed and protected using state of the art cryptographic technologies and protocols.
    b. All parties involved in a transaction should remain anonymous one another.
    c. Secure messaging between the network participants and/or the end user while remaining anonymous one another.
    d. Users' data is not accessed by the central infrastructure (except when required by court orders, legal investigations, or some other repudiation cases).

3. Decentralized, Secured and Private Data Architecture:
    a. Data storage, transaction endorsement and log and configuration rules are spread among all network participants.
    b. The network owner maintains financial auditing events in a private ledger with the related proofs of existence stored in a distributed ledger shared with all network participants.
    c. Each digital asset is encrypted with a split key, where the custodian holds part of the key and the user holds the other.

4. Privacy and Controls
    a. Users must always be in control. Data should be released encrypted and consent should be signed with keys that are in the users' control.
    b. Data at rest must not be linkable (unless an investigation has been authorized).
    c. Data in transit must be viewed by the minimum number of systems to satisfy the transaction endorsement policy (endorsement is where an organization has verified the validity of a transaction).
    d. User transactions (such as consent) should be linkable to a user during an authorized investigation (but not otherwise). Investigations should be authorized by a multi-organization scheme ("Break the Glass").
    e. Transactions should be endorsed by multiple organizations to be valid (to ensure that no single organization can create unauthorized transactions).

5. Book Keeping, Audit and Billing:
    a. A transaction history must be kept and cannot be altered.
    b. Auditable and decentralized architecture where billing can occur without the network being live.

Key Stakeholders

The solution enables users to utilize verified information from well-known trusted parties, such as banks, telecom service providers, governments and credit bureaus directly from their own personal devices.

To accomplish a wide-scale digital information marketplace, the ecosystem gathers partner organizations – Consortium Members – into a consortium. These members operate the system's platform, representing organizations that users already trust, such as their banks. They demonstrate validity of the user's information to the marketplace while also enabling access to this information.

The solution provides the network participants with a blinded secure data messaging service that allows the sharing of data as it is created or updated, but still leaves the user in control of the data flow. Once the user's information is available to the marketplace, it becomes a digital asset (DA).

Each consortium member is responsible for issuing one-use or re-usable digital asset(s) for users to share with online services – Digital Asset Consumers (DACs). This allows a user to provide reliable information from multiple sources and authenticate in a single transaction.

In order to preserve the strong user focused privacy properties of the system, partners running the marketplace infrastructure must be prevented from inspecting user records, tracking (or profiling) a user's activity, or being able to masquerade as a user (forge transactions).

Partners in the system may also be competitive entities in their industry, and therefore partners must be prevented from gaining any insight into another partner's, or partner's users', activities in the network.

Digital Lock Box Provider (DLBP)

The Digital Lock Box Providers are highly qualified and trusted organisations, which already have strong relationships with users. They maintain vital components of the ecosystem, providing the following functions:

- Introduce, educate and on-board users into the ecosystem.
- Authenticate the user during transactions with the network.
- Maintain the integrity and stability of the network by running essential components of the distributed network, including users' Digital Lock Box
- Provide tools to the user to support their network activities, including authentication, troubleshooting and account recovery.
- Act as the user's core identity provider/ primary Digital Asset Provider (DAP) in the network.

Digital Asset Provider (DAP)

The DAP provides information or services about their users via the consortium.

Data Custodian

The Data Custodian controls access to the data for the DAP. A set of associated auditors can access data used to audit transactions. However, to avoid a single point of trust, multiple auditors must co-operate to access transaction data for auditing purposes. Typically, DLBP can perform the role of Data Custodian.

Digital Asset Consumer (DAC)

The DAC is a relying party that needs to verify the user's identity before it can provide access to a resource, such as an online service.

Network Steward

This party founds the system, maintain the health of the distributed applications, and handles branding, contracting and billing. It also acts as a custodian auditor.

The User

The user is the individual that owns the identity information. Using a trusted user agent (UA), typically a smartphone application, the user controls how and when their identity information is provided to DACs.

Architectural Details

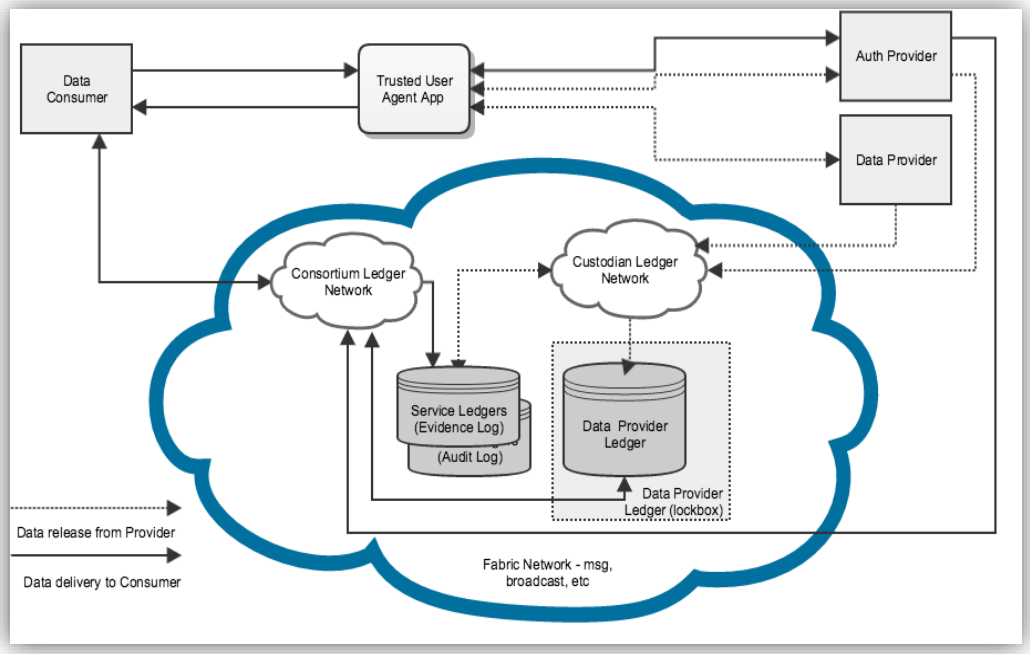
After a review of available state-of-the-art technologies to support all the above requirements, SecureKey decided that the system would be best implemented on a distributed ledger technology that provides transaction proof, maintains end user privacy and provides end user with full control of the data associated with his/her identity. The privacy enhancing cloud Identity Ecosystem is architected using a distributed database of cryptographically secured identity claims running at different trusted operational sites, eliminating central points of failure. To support transaction settlement and global state consensus, the system leverages a cryptographically protected distributed transaction ledger based on permissioned blockchain technology for recording actions in the system.

The new system in essence is a decentralized broker that:

1. Allows users to authenticate using a qualified provider they already use frequently.
2. Enables trusted remote interactions among organizations and users through a blinded marketplace, removing the need of having a centralized authority.
3. Provides capabilities to transfer verified user's identity/data, always under user consent.
4. Protects the participants' identities, and the user's right to privacy of interaction.
5. Implements necessary controls and audit trails to enable self-serve administrative functions while maintaining strict security, privacy and prevent tracking or profiling user's activities.

The main design concept is based on the implementation of a decentralized and asynchronous authentication flow between ecosystem participants, by moving several traditional broker functions to a Trusted User Agent (UA) that the user controls.

The following diagram shows the high-level system components and transaction flow in the system.



It is now in the user's power to instruct the User Agent in his/her control to accept and authorize requests originating from Data Consumers.

The Data Provider (DAP) no longer necessarily has to be online during a transaction, as a User is authenticated to his core provider on his own User Agent (represented by a secure mobile applications) in User Control. As the Data Providers will not necessarily be involved during a transaction, an Evidence Node is needed to certify that a user has control over a particular piece of data. In addition, an Auditor Node is also needed to allow all parties to be able to audit transactions they have performed (with special permissions).

The architecture proposes a model for such Evidence and Auditor nodes, where the Service Ledgers will ensure data integrity, including identifying the data publisher of recorded events and transactions details occurring in the Service, while protecting user and participant privacy and confidentiality. In addition, User Identifiers and User Data are stored in and protected by a secure container called Digital Lock Box. The encrypted Digital Lock Box is distributed in nature and as such, encrypted User Data may be stored at the particular Data Provider or within a distributed storage (with controlled access by the User Agent) based on the requirements of the specific scenario. The User's Authentication Provider (role played by DLBP) provides authentication to the Digital Lock Box.

The system also ensures that users only share data they have been issued from a trusted Data Provider, to the requesting, and legitimate Data Consumer (DAC), while maintaining the privacy and user consent requirements. To facilitate the validity of a transaction, the system implements a mechanism to attach a User's identity claim to an online transaction, like a digital watermark. Users sharing their digital assets with DACs must be authenticated by the Digital Lock Box Provider (DLBP). The cryptographic keys protecting the Digital Asset under users' control are only released when the user has properly consented to share their Digital Assets.

It is important to enable the system to retrieve user's transaction information in the event of an investigation and to provide this information while protecting the system from abuse. This is achieved using multiple ledgers within the distributed ledger system. A global public ledger is shared by the entire consortium, while multiple private ledgers are accessible by subsets of consortium members. These private ledgers hold segments of transaction information that link transactions to specific users, and make it possible for investigators to audit transactions. However, the information is divided between different private ledgers to avoid a single point of trust. The distributed ledger is used to store immutable entries proving that the transaction records exist, making all data verifiable without making identifying details readable. Viewing it requires co-operation from multiple parties to ensure that no single organization has access. By storing data this way, the Network Steward can create billing and remittance reports without being allowed to link transactions to particular users.

Commercial Application

The decentralized broker technology allows individuals to share their identity information quickly for access to business and government services. They can use the system to log into services without creating new passwords or IDs, and can enable organizations to share, update or validate their attributes with other organizations on their behalf.

These capabilities serve several scenarios, including:

- A government validating that a citizen's bank account belongs to them.
- A citizen validating their income with a financial institution by referring to government records.
- Creating verified accounts in sharing economy environments such as P2P marketplaces and rental services.
- Fast authentication for background checks and employment screening.
- Providing passenger information for transport services.
- Signing permission forms and contracts.

A key benefit for users is the ability to update their identity information at a single point as their circumstances change, without having to manually inform tens of different institutions.

SecureKey's ecosystem approach to identity and access management initially targets service providers such as banks, Telcos and government organizations, all of which have struggled with inefficient, cumbersome and insecure methods to validate identity. This approach will reduce fraud rates and increase transaction completion rates by reducing user friction.

Over time, it will appeal to a variety of industries ranging from real estate to travel and healthcare. Any high-volume transaction environment, particularly those using online transactions, can benefit from this decentralized broker approach.

The ecosystem approach will gradually scale out as more of these organizations participate over time. Canada's leading banks have already agreed to support and participate in the ecosystem together with Telcos and various levels of government.

The adoption process is designed to be relatively easy for all parties. Individuals using the service need little more than a mobile phone, while DAPs and DACs can use industry-standard protocols such as OAUTH, Open ID Connect or REST APIs.

DAPs share usage revenues when DACs use DAP's verified attributes from the service. DACs receive a price list for attribute bundles that they may request from the consortium and The Network Stewart bills them for their usage before paying corresponding revenue shares to the DAPs, retaining a percentage for its role in the system.

DACs and DAPs both benefit by reducing customer friction, decreasing fraud rates, and eliminating support costs. Consumers pay nothing.

The adoption process requires 'champions' to seed interest in the model. On the supply side, banks and other trusted data providers must begin offering high-assurance credentials and educating consumers. On the demand side, government agencies can lead by example, demonstrating the system's advantages.

Conclusion: A Customer Proposition

SecureKey has proven commercial experience in identity and access management through its work with the Canadian federal government and other national and global jurisdictions. Although blockchain technology is a new concept, SecureKey is basing its work on Hyperledger, a cross-industry initiative to build robust, open blockchain technology.

With the right set of trusted partners, the benefits of a distributed ledger approach to identity management has the potential to outweigh the adoption risks associated with a relatively new technology. The system's strong anonymity standards enable potential competitors to work together in the same ecosystem. Its decentralized nature eliminates single points of failure, dramatically improving resilience. Just as importantly, it maintains complete privacy for individual users while maintaining convenience and ease of access. This will provide network participants with a strong customer proposition.

For further information about DIACC applied research opportunities please contact info@diacc.ca.

For further information about the topics discussed in this paper please contact the applied research project lead Dmitry Barinov: dmitry.barinov@securekey.com.