An Ecosystem Approach to Frictionless Digital Identity

SECURE KEY

Overview

The Commission on Enhancing National Cyber Security recently[1] published its report on securing and growing the digital economy. Amongst its priorities, the report emphasizes the need 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-service, spoofing and others attacks on users and the nation's network infrastructure, ii) increasing the use of strong authentication to improve identity management, and iii) delivering a frictionless experience to citizens while accessing Government services.

The identity ecosystem designed by SecureKey in accordance with this research combines strong authentication while enhancing individual privacy protection to a new level. It gives end-users control and convenience to share verified digital assets from trusted, and often regulated, organizations such as banks, telecom service providers and governments with others in the ecosystem to prove they are who they say they are, right from their personal devices. The back-end infrastructure is built on top of a private distributed ledger (blockchain) to maintain trust, security, privacy and auditability across the ecosystem. IBM recently announced a collaboration with SecureKey to scale this secure, private and trusted platform for citizens globally.

Customer Need

For citizens, proving identity is incredibly difficult today – it's inconvenient in the physical world, and fraught with friction in the digital world where the risk of fraud and identity theft is higher.

It does not have to be this way. Citizens should be able to log into Government e-services without having to create new passwords or user IDs. Citizens should not be required to show up in person at a kiosk or send pictures of confidential documents to prove who they are during initial onboarding, or wait days to be granted access. It should be easy and cost efficient for the Government to authenticate a citizen accessing services either in person, online or on the phone with a high level of trust, security and privacy.

A number of public and private sector organizations have implemented various identity management solutions relying on usage of Federated Authentication and Identity Networks Services provided by centralized broker architectures. While these systems provide great utility to participants, the principles upon which they are designed have several security and privacy gaps. Architectures must do more to protect the identities of participants by eliminating any reliance on single points of trust, control and failure, and by preventing parties from tracking a user's transactions. They must also maintain an immutable auditable trail without exposing user data that could be mined.

Our Approach

The ecosystem approach developed by SecureKey and its ecosystem partners is based on a privacy-enhanced, triple-blind distributed architecture that relies on the following key principles, which also comply with the guidance outlined in NIST Special Publication 800-63:

- That no data is visible to the operator of the network.
- That there is no central database or "honeypot" of data.
- That there is no central point of failure.
- That there is privacy so that an Identity Provider cannot tell where an identity claim is being used (e.g. imagine if the government knew every time a citizen went to the liquor store).
- That there is no way to track an individual across relying parties.

The SecureKey ecosystem leverages well-known technology platforms and standards, and is available to participants using an open source code base that is maintained by an established group of developers. The ecosystem has an easy-to-license model and proven deployments.

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. The sharing model developed puts users in control of the data flow by asking for his/her consent every single time, while clearly articulating what is being shared, with whom, when, and under what context, preventing users from oversharing information.

Specific information about a user available within the ecosystem becomes digital assets (DAs). Each consortium member is responsible for issuing one-use or re-usable DAs for users to share with other services. This allows a user to provide reliable information from multiple sources, and authenticate in a single low-friction transaction.

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

[1] December 1, 2016

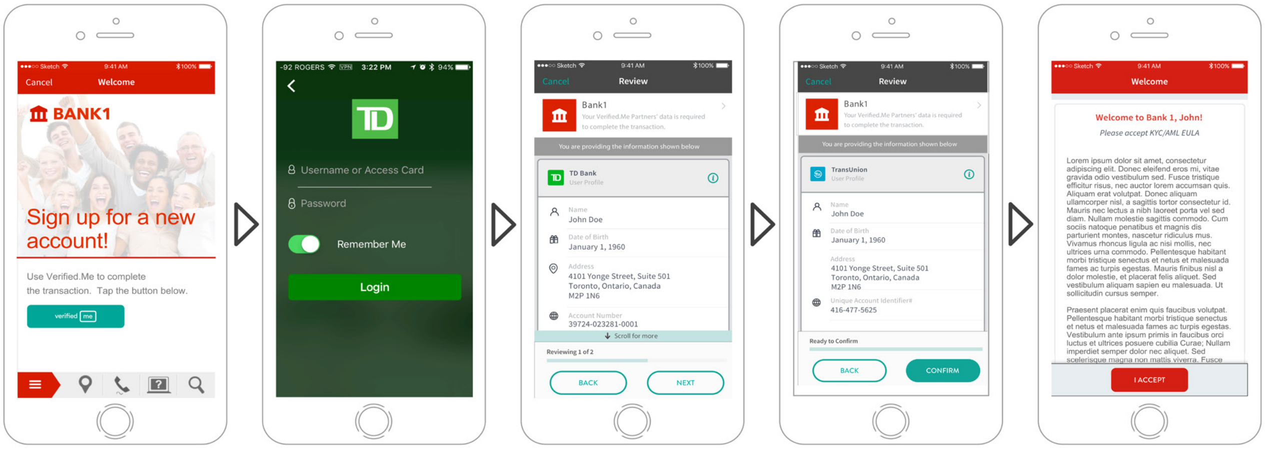
Benefits

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 prove who they are. To increase the level of authentication, the system enables claims from multiple parties to be layered together along with multiple authentication factors - e.g., what you have (your phone), what you know (your well remembered and secure bank login), and what you are (biometrics like comparing to government facial records) without increasing friction. To accomplish a wide-scale digital information ecosystem, partner organizations are gathered into a consortium. These members operate the system's platform, representing organizations that users already trust. They demonstrate validity of the user's information to the ecosystem while also enabling access to this information. This federated identity ecosystem can be used for three transaction types – first, it allows individuals to share their verified identity information quickly for initial onboarding to business and government services. Second, they can use the system to log back into services without creating new passwords or IDs. Third, it can enable organizations to share, update or validate a customer's 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 all ecosystem participants is that a single simple user behaviour can be leveraged across interaction channels to create a high level of identity certainty with low friction.

The User Experience



Sign up for a new account!

Use Verified.Me to complete the transaction. Tap the button below.

Bank1
Your Verified.Me Partners' data is required to complete the transaction.

You are providing the information shown below

TD Bank
User Profile

Name
John Doe

Date of Birth
January 1, 1960

Address
4101 Yonge Street, Suite 501
Toronto, Ontario, Canada
M2P 1N6

Account Number
39724-023281-0001

Reviewing 1 of 2

Bank1
Your Verified.Me Partners' data is required to complete the transaction.

You are providing the information shown below

TransUnion
User Profile

Name
John Doe

Date of Birth
January 1, 1960

Address
4101 Yonge Street, Suite 501
Toronto, Ontario, Canada
M2P 1N6

Unique Account Identifier#
416-477-5625

Ready to Confirm

Welcome to Bank 1, John!

Please accept KYC/AML EULA

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec eleifend eros mi, vitae gravida odio vestibulum sed. Fusce tristique efficitur risus, nec auctor lorem accumsan quis. Aliquam erat volutpat. Donec aliquam ullamcorper nisl, a sagittis tortor consectetur id. Mauris nec lectus a nibh laoreet porta vel sed diam. Nullam molestie sagittis commodo. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Vivamus rhoncus ligula ac nisi mollis, nec ultrices urna commodo. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris finibus nisl a dolor molestie, et placerat felis aliquet. Sed vestibulum aliquam sapien eu malesuada. Ut sollicitudin cursus semper.

Praesent placerat enim quis faucibus volutpat. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nullam imperdiet semper dolor nec aliquet. Sed scelerisque magna non mattis viverra. Fusce

Competitive Advantage

This ecosystem approach to identity and access management initially targets service providers such as banks, telecom service providers and government organizations, all of which continue to rely on physical identification methods, creating inefficient, cumbersome and insecure validation methods. The ecosystem approach combines information typically siloed in industry verticals (e.g., a mobile network operator validating a device and account pairing) to the betterment of all participants to reduce fraud rates and increase transaction completion rates by lowering 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 approach.

The ecosystem approach will gradually scale out as more of these organizations participate. Canada's leading banks have already agreed to support and participate in the ecosystem, together with telecom service providers and various levels of government. IBM recently announced its support of the Securekey approach. This type of collaboration across financial institutions, government agencies, telecom service providers and others will scale both in other individual markets and, eventually, at a global scale.

Next Steps

This approach is the first of its kind, and we are working to develop new open standards to enable global solutions. In addition, we are engaging with further like-minded organizations to broaden the partner base for citizens to have widespread access to the services they need.

SECURE KEY