



Consumer Digital Identity Leveraging Blockchain

Delivering a Distributed Privacy
Enhanced Identity Ecosystem

The Commission on Enhancing National Cyber Security report from December 1st, 2016 emphasized the importance of securing and growing the digital economy. In line with the recommendations from this document, and in compliance with the Digital ID & Authentication Council of Canada's (DIACC) **10 Canadian Principles of a Digital Identity Ecosystem**, SecureKey Technologies entered into a multiphase program with DIACC and the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) to evaluate, develop, and deliver a solution for enabling distributed privacy enhanced identity ecosystems.

This paper summarizes the work done as part of Phase 3 of the program, concentrating on the “Commercialization of the Verified.Me project,” and building upon the recommendations from the Applied Research completed in Phase 2 which are further described in this **white paper**.



Table of Contents

04 >>>

About this document

05 >>>

Executive summary

07 >>>

The commercialization phase

16 >>>

Lessons learned
for the DIACC community

18 >>>

References

About this Document

This document has been developed as a companion paper to support the findings of the Implementation (second) phase of work that was performed by SecureKey as part of its application for DHS Applied Research grant through the DIACC.

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 Global Privacy by Design guidelines developed jointly between Canada and the Netherlands.

Contributors to this project and paper include DHS S&T, 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.

DHS works to secure the United States from any threats. The S&T Directorate monitors technology threats and rapidly capitalizes on technological advancements, developing solutions and bridging capability gaps at a pace that mirrors the speed of life.

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

Executive Summary

The Verified.Me service, offered by Secure-Key and developed in cooperation with seven of Canada's major financial institutions – BMO Bank of Montreal, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank, and TD – is a Blockchain-based digital identity verification network that aims to provide the foundation for a truly digital economy. In order for high value services and processes to be brought online, there must be a digital exchange that provides trusted identity and reliable digital claims in a secure and private manner to participants in the network.

For example: when applying for a credit product at a financial institution today, an individual must go, in person, to a financial institution branch's agent with an application and a variety of documents to prove that individual is who s/he claims to be. The agent processes the application and performs an identity proofing exercise on the individual to have

confidence in his/her identity. The individual typically presents government issued identification documents. The bank accepts the application if the identification “looks right.” The issuer of the document (passport office or DMV, for example) is never notified of the individual's desire to open a bank account – the individual's activity is kept private from the issuer(s) of the identity document(s).

In this example, the application can be completed online; the processing of the application can be done by bank IT systems, and the associated identity verification from the collected sources can be cross-checked with online services. But what cannot be done is the verification by the bank of the identity of the individual presenting reliable digital identity credentials. Therefore, this service – and many like it that rely on identity proofing or confidence – rely upon tedious “in person” processes.

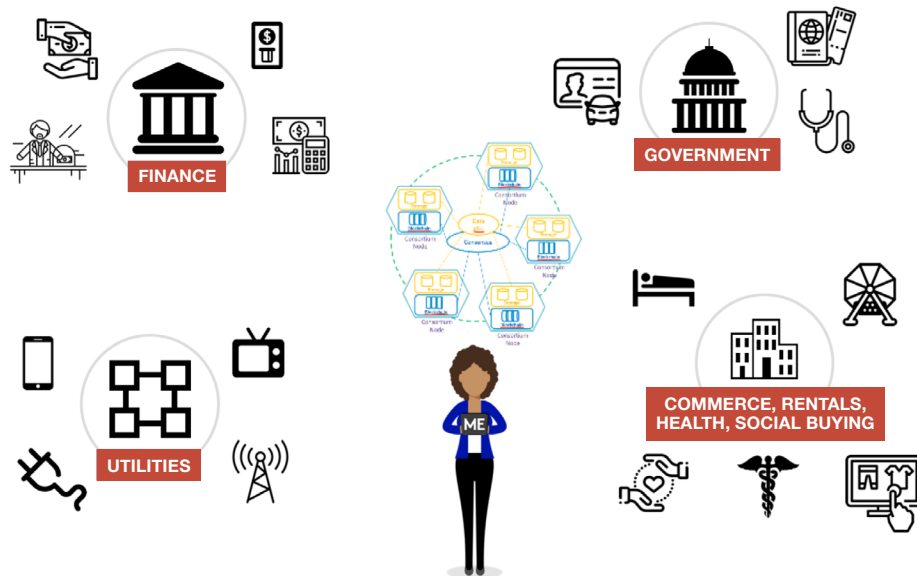


To solve that problem, the Verified.Me service allows a user to collect and present verified digital assets in a trusted and reliable manner, to and from all participants in the digital identity network. The service acts as the exchange network for a user's digital assets. It guarantees:

- A user's right to privacy of activity;
- A user's right to decide when and what information about themselves is shared between organizations;
- All digital assets are cryptographically protected for confidentiality and integrity;
- All digital asset exchanges and transactions are cryptographically auditable;
- There is no central point of failure or central point of trust: a distributed network of trusted organizations run a cryptographically protected consensus protocol that collectively determines the state of the network, the participants, the digital assets and the users and;
- All participant activities in the network are permissioned, authenticated, and auditable.

Identity in the Future

Utilizing Strong Distributed Ledger Capabilities



PROS

- No Data visible to network operator
- No central database or honeypots
- No central point of failure
- Triple Blind - PRIVACY
- Cannot track user across relying parties
- Scalable
- Resiliency to DDOS

The Commercialization Phase

The project Phase 3 – Commercialization consisted of several deliverables aligned with the core Architectural and Privacy Principals identified in Phase 1 - Applied Research, as well as with the deliverables from Phase 2 – The Implementation, which are summarized by the corresponding white papers accessible through the provided links below:

PHASE 1

Architectural and Privacy Principals:

- a. No Centralized Authority
- b. Secured Blinded Infrastructure
- c. Decentralized, Secured, and Private Data Architecture
- d. Privacy and Controls
- e. Bookkeeping, Audit, and Billing

Corresponding white paper available [here](#).

PHASE 2

The Implementation:

- a. System Assumption Evaluation and Deployment Architecture documents
- b. Digital Asset Licensing and Distribution
- c. POC Coding and Transaction Flows / Screens
- d. iOS and Android User Agents (Mobile Apps)
- e. PoC Deployment and demos
- f. Optional usage of Biometric Authentication and Windows Secure Element

Corresponding white paper available [here](#).

PHASE 3

Commercialization:

a. Program Frameworks

- Program Governance Framework including participants eligibility assessment and approval processes
- Roles and Responsibilities of each participant
- Network Framework (Solution Architecture, Security, Regulatory, Privacy, Contracting, Operations, and Ecosystems and Operating Model)

b. Production System:

- Service Description (Use Cases and Functionalities for Launch, Roadmap)
- System Components and Deployment Environments (including Solution and Deployment Guides)
- Operations Monitoring and Support

c. Go to Market

- Market / Consumers Surveys and Testing
- Marketing Approach

d. Service KPIs

e. Commercial Launch

- Partners and Use Cases

f. U.S. Pilot

✧ The Commercialization Phase

The first deliverable of the project concentrated on the development and establishment of proper Governance and Network Frameworks necessary for a proper commercialization of the service, as well as clearly defining the roles and responsibilities.

The second deliverable of the project focused on the productization of the components developed during Phase 2, establishment of a distributed production environment for these components to be operated by the Service Hosts, and establishment of necessary operation support tools and processes to monitor and maintain the overall health of the network.

The third deliverable of the project concentrated on the Go to Market activities leading to the Commercial Launch.

Phase 3 also included the operation of a pre-production pilot in the U.S. with local business partners willing to evaluate the solution developed by SecureKey under this program in consideration of a commercial launch in the U.S.

Governance and Network Frameworks

1. The Network Operator participates in the runtime operation of the Ledger Network and maintains the financial transaction log for billing settlement for the Network Participants. It manages the participant registration (Service Host, DAPs, and DACs) and the policy configuration as set out by the Consortium. It also provides operational support and monitoring of Network specific components to help maintain the health of the Network as a whole. The Network Operator is also in charge of sales, marketing, and contracting

activities, and actively participates in the Consortium that defines and approves of the operating rules and policies for the Network. In Canada's Verified.Me Network, SecureKey is the Network Operator.

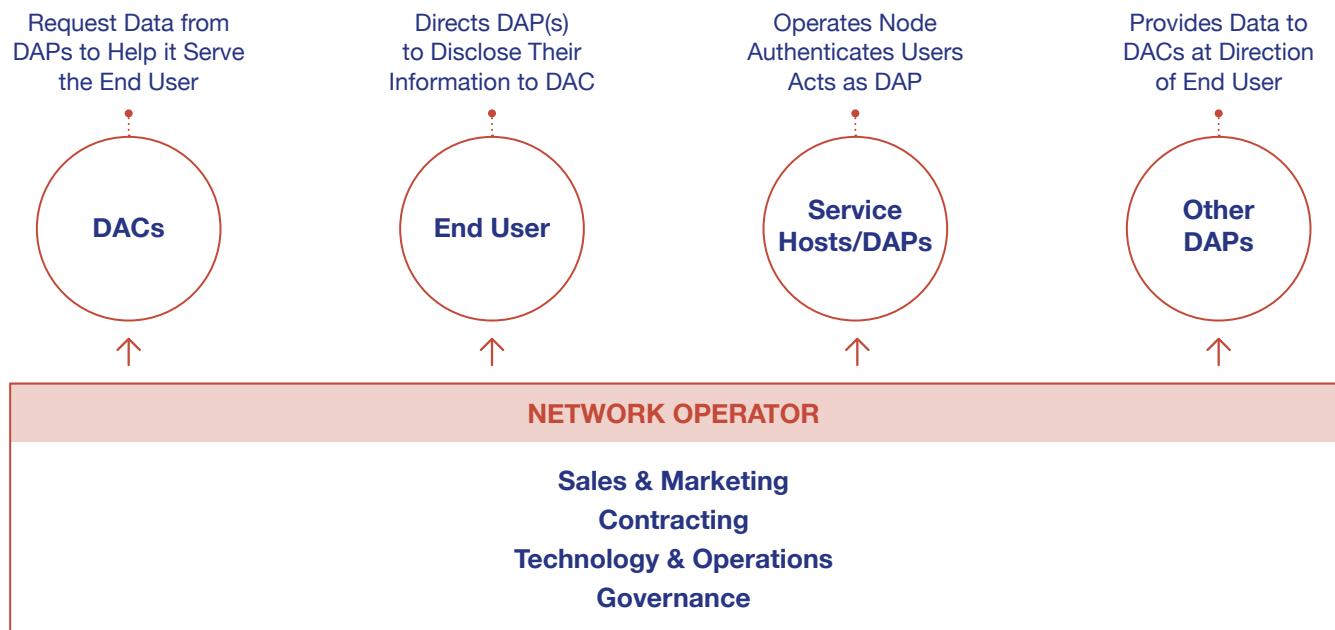
2. The Service Hosts are the backbone of the Network, providing authentication services, lockbox management, and license management interfaces to the user agent, as well as hosting the required distributed Ledger Nodes that make up the Network. They are also able to provide verified attributes about their end users. Together with the Network Operator, they actively participate in the Consortium that defines and approves of the operating rules and policies for the Network. They are highly trusted and regulated organizations that already have an active relationship with end users. In Canada's Verified.Me Network, these organizations are seven of the country's major financial institutions.

3. The Digital Asset Providers (DAP) act as data sources for the Network, providing end user verified data through Digital Assets allowing a user to share their account-related information from multiple sources in one authentication and licensing/consent action.

4. Digital Asset Consumers (DAC) act as data consumers that request Digital Assets from users, and once the user consent is recorded, collect the Digital Asset data related to the user from the service Ledger Network.

5. The End User used the Network User Agent (Mobile App or Web Client) to select and authenticate with the Service Host of their choice and directs DAP(s) to disclose their information to DAC.

Roles & Responsibilities



Proper Contracting Framework and corresponding agreements had to be developed to enable each participant in the Network.

This contracting framework was built using a “Hub 'n Spoke” contracting model to avoid point-to-point agreements between participants while limiting the overall liability between them.

To participate in the Network, each participant must comply with the Compliance Framework defined by the Network Consortium using the following key principles:

1. Avoid point-to-point vendor assessments

2. Self-attestations:

Backed by third party assessment covering requirements, preferred

Backed by independent/internal assessment covering requirements, acceptable

3. Evidence of self-attestation to be available to all ecosystem participants for review

Network Operator

- SOC 2 Report
- Self-attestation to:
 - NIST Cybersecurity Framework
 - Harmonized Base Control set - Specific NIST SP 800-53 requirements (entity type specific)
- Notification, cooperation obligations, and procedures for managing incidents

Service Hosts

- Self-attestation to:
 - NIST Cybersecurity Framework
 - Harmonized Base Control set - Specific NIST SP 800-53 requirements (entity type specific)
- Notification, cooperation obligations, and procedures for managing incidents

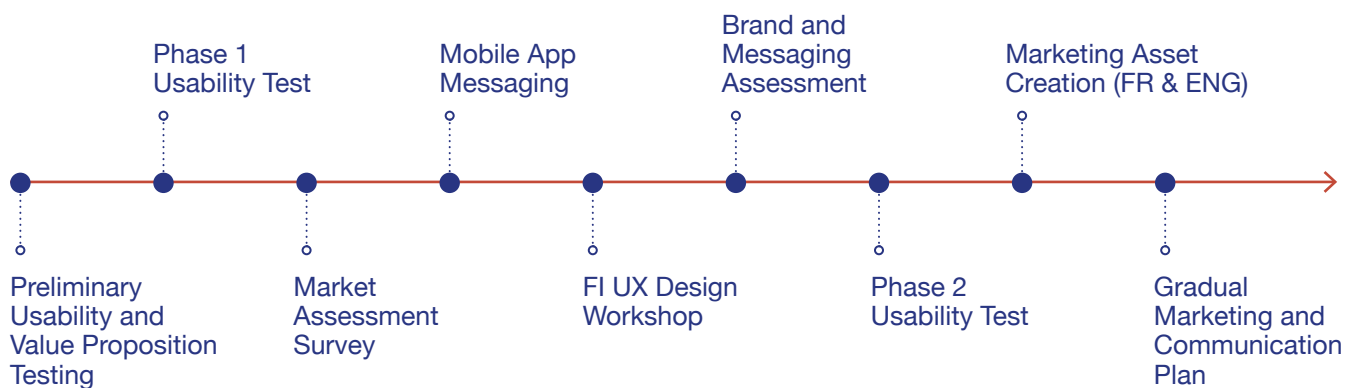
DAPs & DACs

→ Self-attestation to:

- “Short form” of requirements (commitment to best practices, technical and operational safeguards, etc.)
- Notification, cooperation obligations, and procedures for managing incidents

The Brand Journey

SecureKey orchestrated key activities to assess the market opportunity, brand, messaging, and mobile app usability, subsequently creating consumer support marketing assets and an overall gradual marketing communication plan as depicted in following diagram:



* The Commercialization Phase

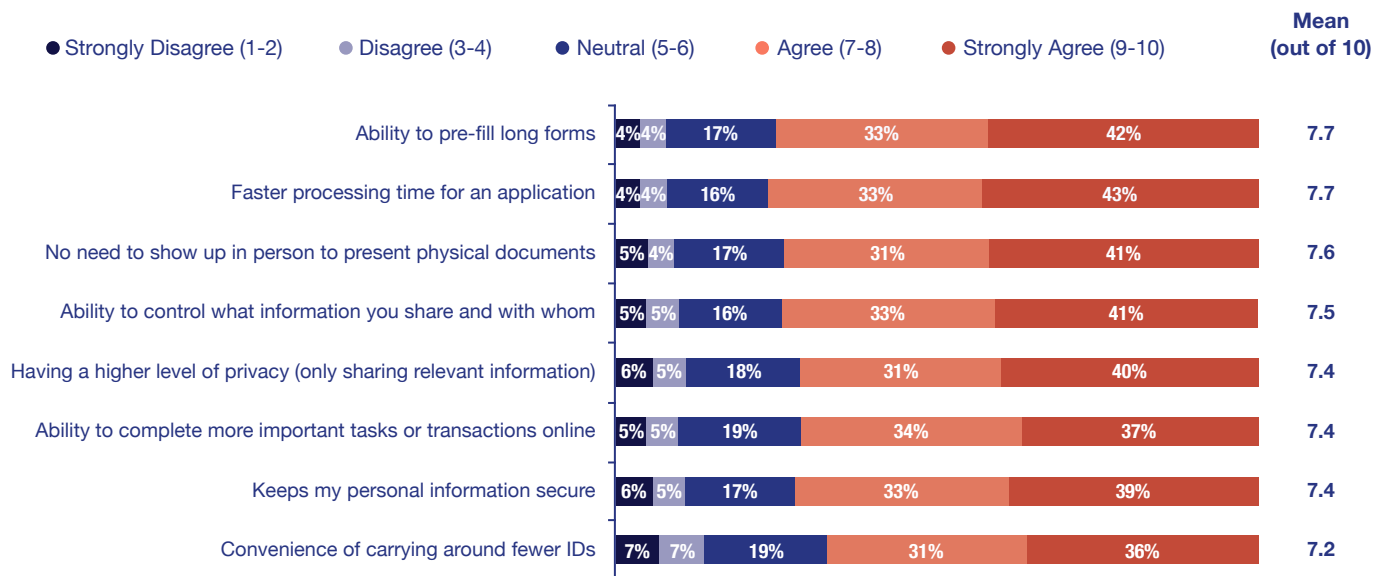
These activities included:

- A third-party agency approved by the Consortium participants, experts in marketing research, user experience (UX), and customer experience to assist in a series of consumer market and usability testing studies;
- Iterated usability testing over time to improve the customer experience and app usability;
- Engagement of the Consortium UX design teams through working groups and dedicated workshops to provide input into the Verified.Me mobile app UX;

- Overall absorption of test and research feedback, implementation, and re-testing to validate direction and changes made; and
- Creation of all marketing assets in both English and French, going through necessary reviews and approvals with Consortium marketing and legal teams.

Among many things, the market study and consumer surveys allowed SecureKey to segment the eligible population into four categories, confirm the perceived benefits from an end user perspective, and subsequently build the various marketing assets. See example of the perceived benefits of using Verified.Me below.

Perceived Benefit of Using Verified.Me



Business Model and Marketing Approach

Another very important aspect of building an ecosystem is to clearly define the business model and marketing expectations for each ecosystem participant. This is paramount for enabling fast adoption of the service, where each participant understands clearly what is in it for them.

The diagram below summarizes the marketing expectations from each participant as well as how the data and fees would flow through the network while maintaining privacy between them:



DIGITAL ASSET CONSUMERS (DACs)

Role: drive transactions with end consumers

Tactics: promote Verified.Me available in channels, leverage common general messaging and assets, assist in customer education, allow use of brand in marketing

Optional: marketing commitments identified in contract negotiations, i.e. fund independent marketing campaigns

.....> Asset flow
.....> Free flow



NETWORK OWNER (SecureKey)

Role: overall accountability to coordinate and promote marketing activities

Tactics: provide messaging guides, marketing assets, coordinate campaigns, contribute group and independent funds on above-the-line campaigns, provide MDF for Service Hosts

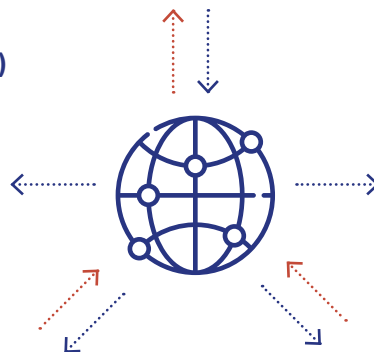


CHANNEL PARTNERS

Role: raise awareness and drive adoption by DACs

Tactics: leverage SecureKey B2B marketing assets, sales team education, etc.

Optional: develop value-add services and integration components to ease onboarding



SERVICE HOSTS (FIs)

Role: promote consumer awareness and adoption, enable DAC use cases, help to kick-start ecosystem

Tactics: leverage existing consumer relationships for education and promotion, contribute funds for above-the-line campaigns, allow use of brand in marketing

Optional: act as a channel partner to attract DACs



DIGITAL ASSET PROVIDERS (DAPS)

Role: encourage consumers to create connections and DACs to consume bundles

Tactics: support Verified.Me messaging and communications

Optional: provide additional direct-to-consumer offerings

Gradual Launch Approach

We agreed with the Consortium members on a gradual launch approach, allowing us to properly introduce the service to the market.

As part of this third deliverable, SecureKey provided a production version of the mobile application, available for iOS and Android platforms through commercial app stores, and integrated launch customers and partners to the production system while making it available to end users.

The service was launched on May 1, 2019 and generated a substantial amount of international press coverage – both mainstream and trade – and inbound requests confirming the interest of the Canadian Market.

Read the full announcement [here](#).



Media Launch Summary

102,194,434
Total impressions



479
Stories



40
International Stories
including U.S., France, India, Lebanon,
the Netherlands, Singapore and the U.K.



76
National Stories



Coverage
in **8 provinces**
and **2 territories**



Social media
was buzzing

ON 113 stories with
16,723,008
impressions

QC 36 stories with
18,887,573
impressions



App Store Ratings
More than 50% of reviews
are 5 stars

Initial capabilities and use cases

There is a cyber problem; identity is broken and the impact of identity fraud is massive.

The only real way to ensure we are dealing with the correct individual at the time of a transaction is to implement an identity proofing scheme that enables the validation of 'What I Am', 'What I Have' and 'What I Know' capabilities. It is essential that we combine the strong and actively managed credentials that financial institutions provide (What I Know) together with telco data on the phone a consumer is using, e.g. validation of the user's SIM card and whether it has changed (What I Have), and the ability to validate government documents and match against live faces (What I Am). These are the initial pillars of a proper digital identity network.

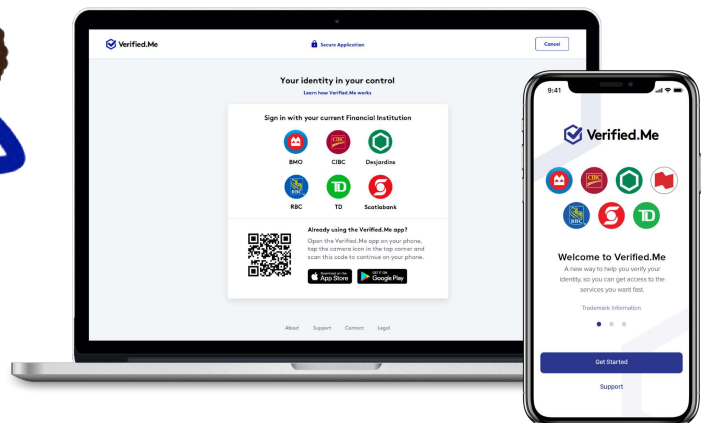
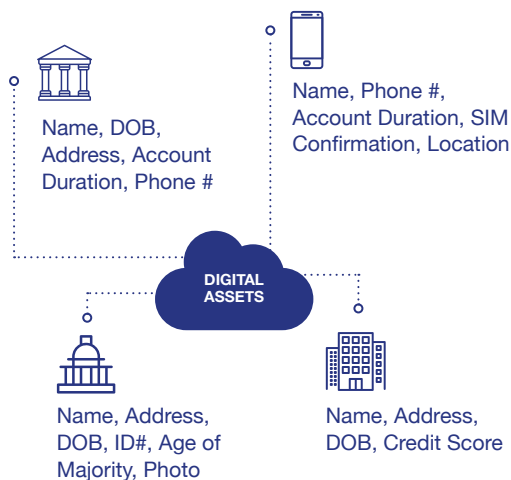
By combining the security capabilities of government, telco, and financial institutions while raising the bar on security, Verified.Me is a service strong enough to be trusted by institutions to allow individuals to share their data.

Once authentication is strong enough, a citizen can be enabled to share data from multiple sources in a single transaction. It is important that the network never sees that data and that no copies of the data are stored in the network.

Our learning in Canada is that to increase efficiency in the system multiple data sets need to be shared in a single transaction.

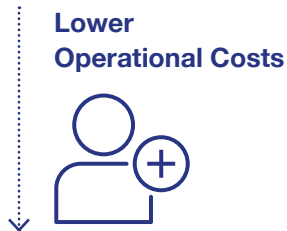
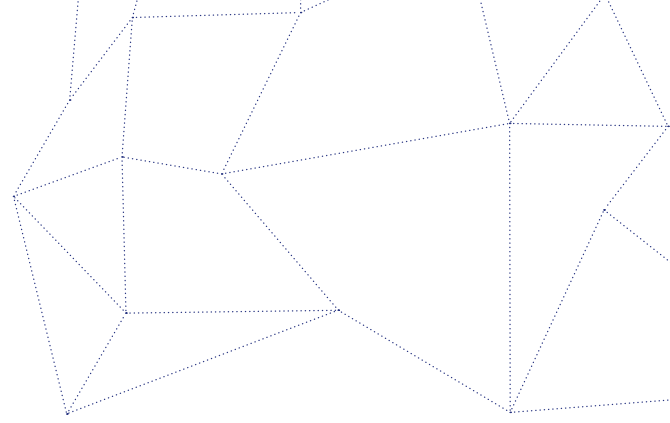
A bank, for example, requires identity validation, income validation, and credit score validation to approve a mortgage. A landlord requires identity validation, income validation, and a background check. A health provider requires identity and health card validation.

Identity & Other Claims



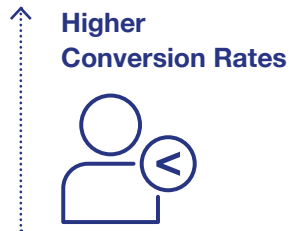
* The Commercialization Phase

Such a broad ecosystem truly enables consistent, real-time identity assurance across all touchpoints of a digital transaction, whether it is being used for initial Sign-Up, on-going Sign-In, or necessary Step-Up during more sensitive transactions:



SIGN-UP

Sign-Up supports the new account opening/enrollment (both standard retail accounts or KYC regulated accounts)



SIGN-IN

Sign-In supports a single sign on use case where the end user uses Verified.Me to log into the Relying Party (DAC) web/mobile app.



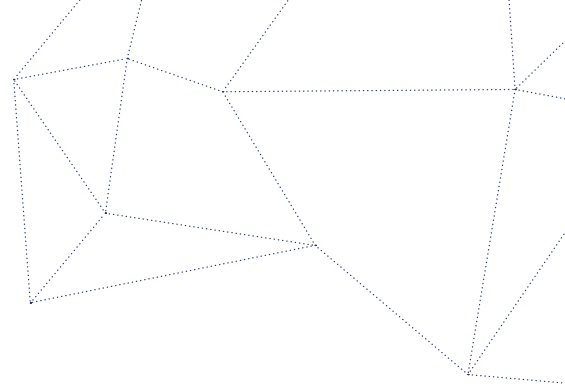
STEP-UP

Step-Up provides a Verified.Me supported flow for providing stronger identity validation during risk potential transactions with the Relying Party (DAC)





Lessons Learned for the DIACC Community



Commercializing any new product or service is a complex task requiring the coordination of many interdependent and intra-dependent partners. Bringing a national digital identity network online, one could argue, is even more challenging than a normal software product launch, because the Verified.Me service is an ecosystem of trusted partners allowing end users to exchange personal information with confidence, privacy, and security.

To do this, SecureKey collaborated with seven of Canada's major financial institutions to provide the backbone of the network, sought trusted partners to provide additional end user information, engaged organizations looking for better ways to remotely interact with prospective and existing customers, and developed a mobile application to put the end user at the centre of their digital identity world.

The challenges and lessons span a wide range of topics including legal, governance, technology, operations, and design. The following are a few key observations that emerged during the commercialization phase.



1 Network Business Model

The “Hub 'n Spoke” contracting model was used to avoid point-to-point agreements between participants and limit the overall liability between them. The network operator is the hub ensuring network contract integrity and consistency of terms across parties. The time and effort to build the contract architecture and templating was significant. The key here is

avoiding point-to-point agreements, which over time would be very difficult if not impossible to manage with a large and growing ecosystem.

One of the more complex topics supported by the contract framework is the liability model. The Verified.Me ecosystem is a “zero-liability” model, meaning at a top level that the data is provided as is and there is no contractual warranty that the data provided is accurate. Striking the right balance across the parties according to the role they are playing in the network takes time and requires careful definition. This balance was highlighted when an organization plays multiple roles in the network (i.e. provides and consumes data) and contract conditions presented on one side then had to be honoured on the other.

The risk management framework and ongoing governance of the ecosystem was also a critical part of the commercialization process. Without consensus on information security standards and requirements for each role and DAC/DAP eligibility rules (i.e. permitted uses) there would be no trusted network. This is a distinguishing factor from other “open” networks and underwrites the intrinsic and economic value of the Digital Identity Ecosystem.



2 User Experience

Shifting focus to how the end user interacts with the Verified.Me service, a substantial amount of work, research, and testing went into all aspects of the mobile application

user experience, consent, and service support model. The decision to provide a mobile application, in fact, was a significant direction that took several turns over the course of the project. Ultimately, based on usability research, branding and product development, the decision was made to support a Secure-Key mobile application. While that in and of itself raised the issue of “yet another app,” it also solved a number of key design issues around consent management and user understanding of the relationship between their financial institution and the user’s interaction with partners in the Verified.Me service.

The process of refining and enhancing the mobile experience during the commercialization phase was lengthy and, in some cases, involved a number of financial institutions. In the section above discussing the brand journey, you will see reference to several usability test iterations, messaging, and market assessments. At one point, a “design summit” was organized to include experts from financial institutions and SecureKey, with the objective of collectively and creatively designing optimal user experiences. This allowed the user to collect and present verified digital assets in a trusted and reliable manner, ensuring the user has clear understanding of what is happening during a transaction. This was a challenging activity to organize and execute but was effective in answering several key design questions that were required to move the product and service forward.



3 Service Operations

From a programmatic and service Go to Market perspective, the coordination, alignment, and execution of bringing all parties together

to go live on a single date was substantial. The program management team was pressed to guide all the technical, business, and operations teams from all partners through the launch date. It’s easy to overlook the planning and execution complexity that was required across several organizations and within each of those organizations and lines of business. A strong PMO, with good relationships with partner PM teams, is essential for managing and extinguishing the inevitable fires that spring up as the program drives toward a go live date.

The processes needed to support the ongoing management of the ecosystem – adding new parties, monitoring, and managing changes, incidents, and end user support – are not menial. Designing, testing, and operationalizing these processes is a long-term driver of end user and partner satisfaction. It does not take much to turn a user off and have them delete an app, likely never to return. Accordingly, these underlying services must be slick and frictionless.


Without understating the obvious, bringing a Digital Identity Ecosystem to market based on new distributed ledger (blockchain) technology, where very few production applications are working successfully, presented another set of challenges. Creating a nationally scalable infrastructure that is performant and resilient to the many cyber threats on top of this new technology is another matter altogether. The baseline plan was adjusted several times to accommodate additional time needed to manage operational, infrastructure, security, and compliance requirements in this evolving technological landscape. Many people and countless hours are to be expected if a similar effort is to be undertaken in the future.

References

- <https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/>
- <https://verified.me/>
- <https://www.securekey.com>
- <https://diacc.ca/principles/>



 DIACC.ca
 info@DIACC.ca
 @mydiacc

 720 King Street West,
Suite 302, Toronto, ON,
M5V3S5