Consumer Digital Identity Leveraging Blockchain

Delivering a Distributed Privacy Enhanced Identity Ecosystem

This document explores and shares the experience of DIACC member SecureKey. In alignment with DIACC’s 10 Canadian Principles of a Digital Identity Ecosystem, SecureKey has entered into a multiphase program with DIACC and DHS to explore and evaluate a solution for enabling distributed privacy enhanced identity ecosystems. This paper has been developed for the purpose of enhancing community based knowledge sharing.

This paper summarizes the work done as part of the Phase 2 of the program concentrating on the “Development of the Core Features and Initial Proof of Concept”, and building up on the recommendations from the Applied Research completed in Phase 1 which are further described in the “Consumer Digital Identity” white paper.

Table of Contents

About this paper

Information in this report is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

For more information, please contact:

Anil John
Technical Director
Silicon Valley Innovation Program
Science and Technology Directorate
US Department of Homeland Security
Washington, DC, USA
anil.john@hq.dhs.gov

This content of this white paper is developed under the governance of the DIACC International Applied Research program. The International Applied Research program connects innovators that align with the DIACC Digital Identity Ecosystem Principles[1] with international applied research funding opportunities. The content of the paper was submitted by SecureKey and does not necessarily reflect those of the DIACC membership.

For more information regarding this program please contact:

Joni Brennan
President of the DIACC
Info@diacc.ca

Executive Summary

DIACC anticipates that multiple *Third-Party Identity Information Networks*, referred to as **Network(s)** in this paper, may become available in the near future. The purpose of this project is to explore implementation considerations regarding Networks. This companion paper was developed to identify and share lessons learned with the DIACC community as a valuable opportunity to inform the development of the Pan-Canadian Trust Framework by exploring an implementation of a Network.

This paper specifically explores a Network that is being implemented by SecureKey on Blockchain technology that aims to provide a foundational service to accelerate the digital economy. In order for high value services and processes to be brought online, it is envisioned that digital exchanges will provide trusted and reliable digital identity claims in a secure and private manner to participants in such an exchange.

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

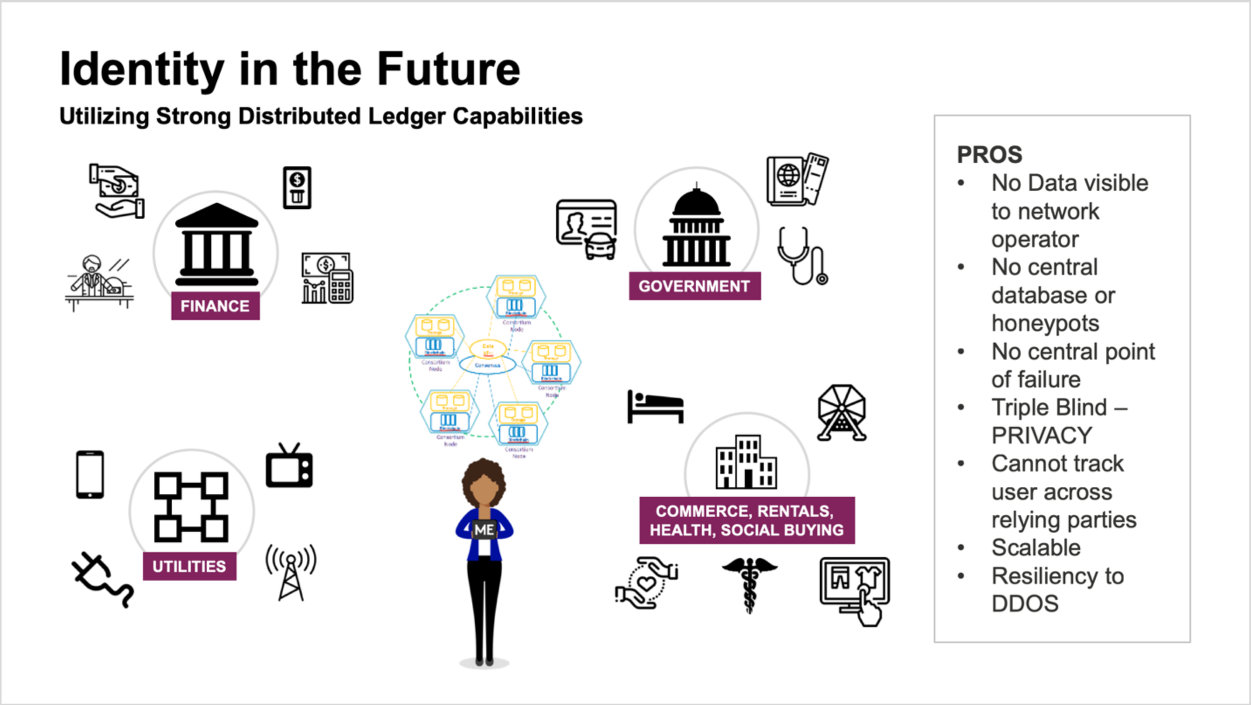
[1] https://diacc.ca/principles/

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 on 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 of 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 the above example, the application can be completed online. The processing of the application can be done by Bank IT systems. 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, identity proofing or confidence continues to rely on tedious "in person" processes.

To solve that problem, a Network service allows a user to collect, and present, verified digital assets in a trusted and reliable manner, to and from peer Network Participants. Networks have the potential to secure:

- A user's right to privacy of activity.
- A user's right to decide when and what information about themselves is shared between organizations.
- Cryptographic protection of digital assets for confidentiality and integrity.
- That all digital asset exchanges and transactions are cryptographically auditable.
- No central point of failure or trust: a distributed Network of trusted organizations run a cryptographically protected consensus protocol that collectively determines the state of the Networks, the Participants, the digital assets, and the users.
- Permissions, authentications, and auditability of Network Participant activities.



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

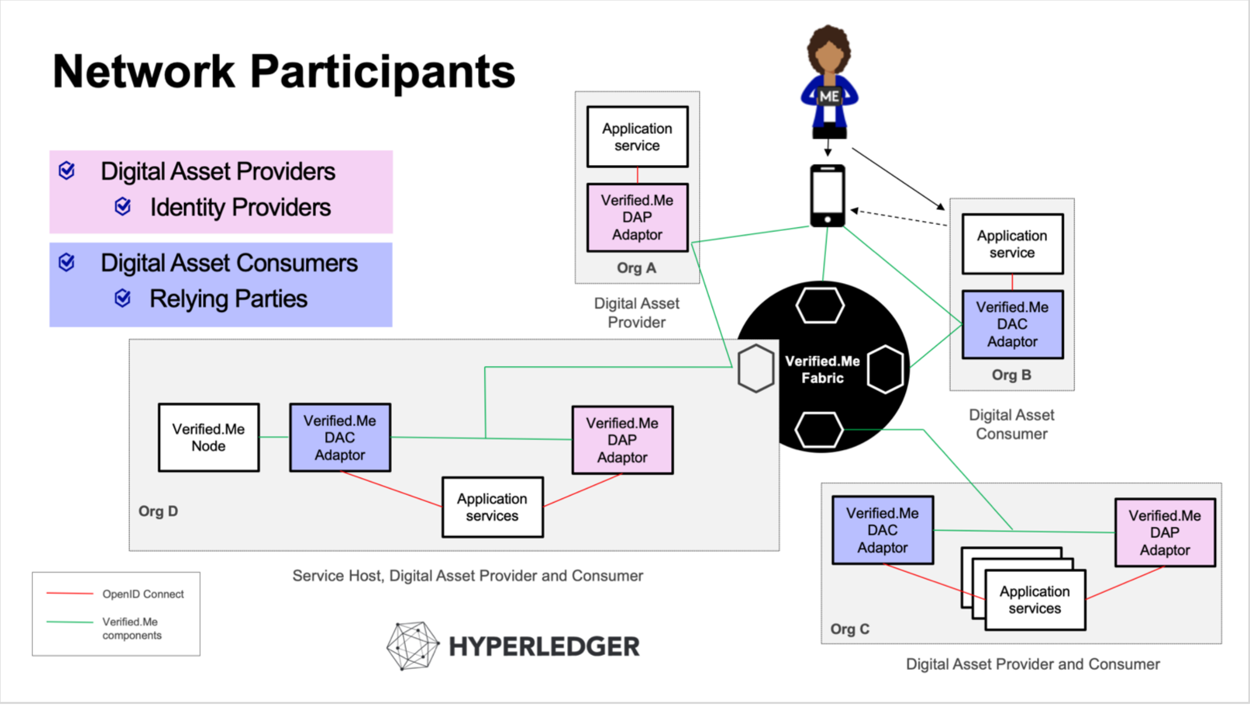
The Implementation Phase

The Applied Research Project Phases consist of six key deliverables that align with core Architectural and Privacy Principals.

1. 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. Book keeping, audit and billing

2. Phase 2 Implementation Key Deliverables:
   a. System assumption evaluation and deployment architecture documents
   b. Digital Asset licensing and distribution
   c. Proof of Concept coding and transaction flows/screens
   d. iOS & Android user agents (mobile apps)
   e. Proof of Concept deployment and demos
   f. Optional usage of biometric authentication & Windows secure element

All deliverables for the Implementation Phase have been completed with key outcomes as follows.

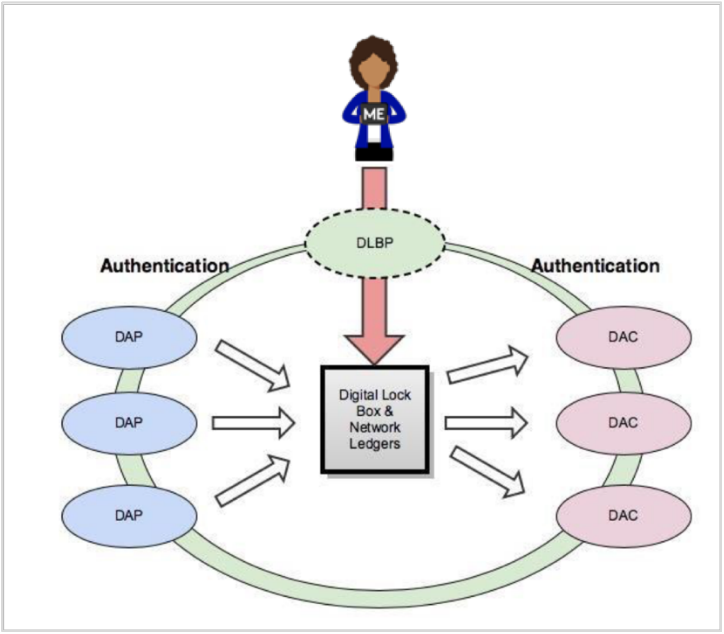


Exploring Network Principles

It is anticipated that multiple Networks may come into existence for user-controlled, secure, and privacy-enhancing exchange of identity information and interoperability of identity data and network communication represents an imperative opportunity to grow Canada's economy. To reduce uncertainty regarding implementation of Networks, this paper explores a specific Network instance called Verified.Me™ that is represented in various graphics throughout this paper. Terms introduced in this paper are specifically defined by SecureKey who are the performers of this Applied Research Project. This Network is an example of a "Digital Asset exchange" that allows users to authorize the exchange of shareable verified data between Network Participants (otherwise known as third-party data verifiers) in a secure and privacy preserving manner, under a common operating protocol without the need for Network Participants to integrate directly.

A user's shareable data in the Network are represented as Digital Assets. Digital Assets are associated to a user's network account, or Digital Lockbox. The Digital Lockbox is maintained by the Service Host/Digital Lockbox Provider (DLBP). A user authenticates to their Digital Lockbox via their Service Host/DLBP in order to manage and share their Digital Assets with Networks.

Network Participants do not communicate directly to exchange data. Network Participants rely on their Service Host/DLBP and the Ledger Network to authenticate the user and validate the data exchange policies. Providers of user data will receive a request for their user's account data from the Ledger Network and provide data to the Network for delivery to the Requesting Party.



High Level Roles and Interactions

A **User Agent** provides the user interface to the Network, including authentication, lockbox management, and licensing/consent workflows. The User Agent can be available either as a mobile application available on iOS and Android platforms, or as a web agent.

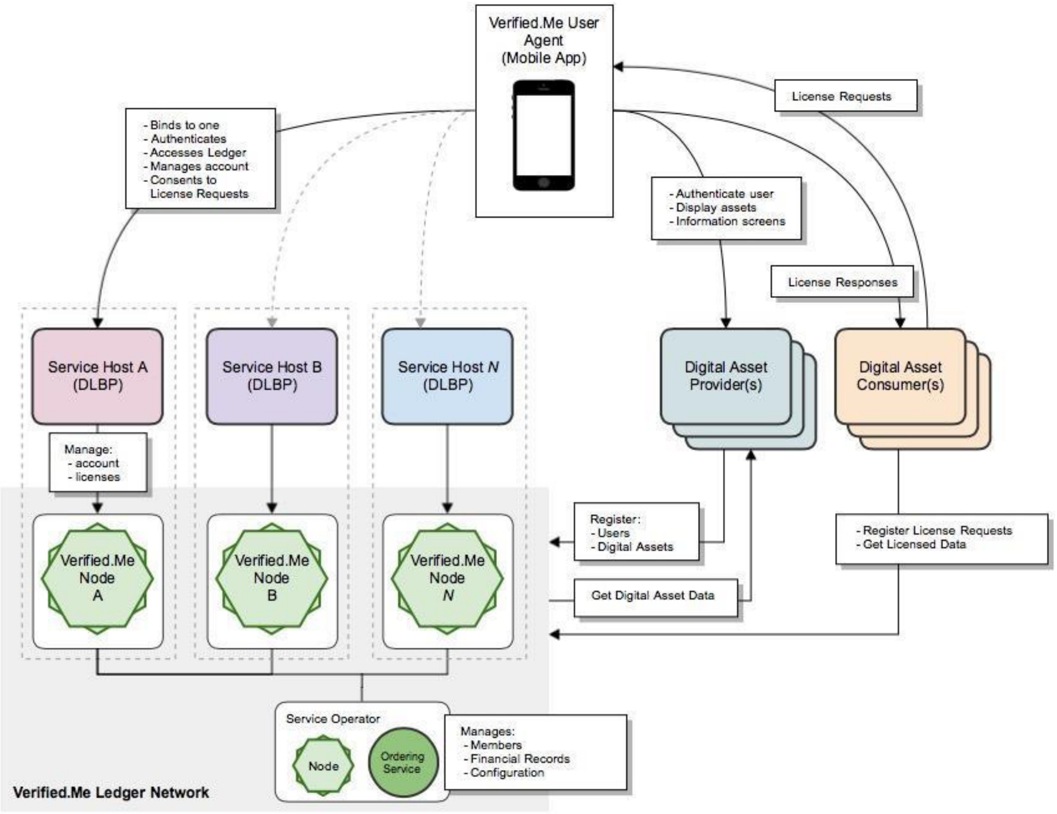
A **Digital Lockbox Provider (DLBP)** is a user's Network account which is stored on the Ledger Network. Service Hosts also typically make up the Consortium Organizations who determine the operating rules and policies for the Network. **Service Hosts/DLBPs** are the backbone of the Network, providing 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.

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

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.
Organizations participating in a Network can act as any combination of Service Host/DLBP, Digital Asset Provider, and Digital Asset Consumer.

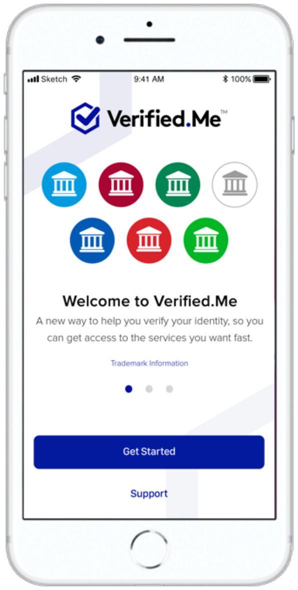
In this case the service **Ledger Network** is a distributed application and state database backed by HyperLedger Fabric blockchain technology. Each Service Host/DLBP runs a Node to support the Ledger Network, ensuring there is no central point of failure or single point of trust. Service Host/DLBPs, Digital Asset Provider and Digital Asset Consumers act as clients to the Ledger Network nodes. The Ledger Network stores the state of a user's lockbox and license grants. A user's internal DAP account information, or raw data, are never persisted on the Ledger Network.

The **Service Operator** participates in the runtime operation of the Ledger Network by supporting a shared component called the **Ordering Service**, and also by maintaining the financial transaction log for billing settlement for the Network Participants. The Service Operator manages the participant registration (ServiceHost/DLBP, DAPs, and DACs) and the policy configuration as set out by the Consortium Organizations. The Service Operator also provides operational support and monitoring of Network specific components to help maintain the health of the Network as a whole.



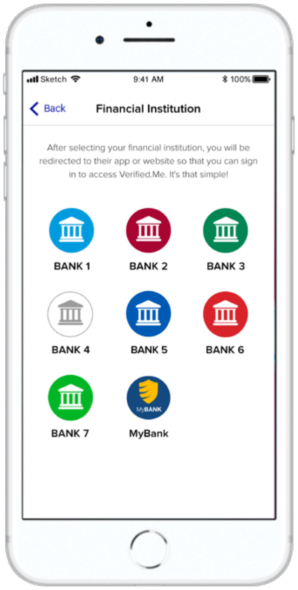
Core Use Cases and Demo Screens

1. **Registration:** A user should be able to create a new Digital Lockbox to register for the service. This is done by downloading the mobile app and linking it to a valid Service Host.

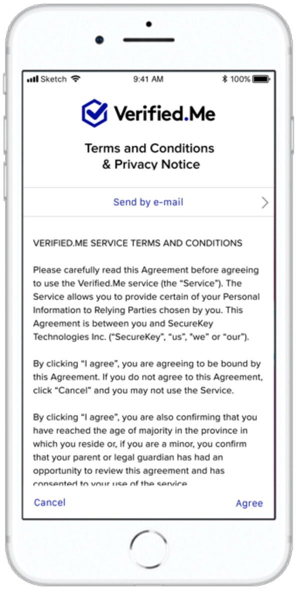


Welcome to Verified.Me

A new way to help you verify your identity, so you can get access to the services you want fast.



After selecting your financial institution, you will be redirected to their app or website so that you can sign in to access Verified.Me. It's that simple!



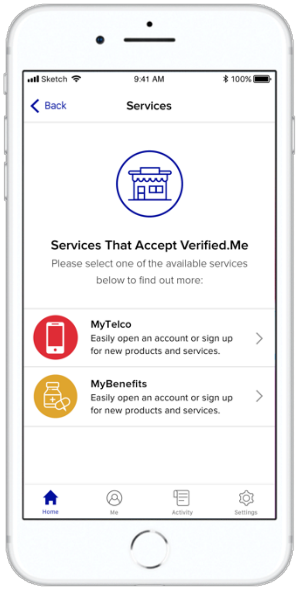
Terms and Conditions & Privacy Notice

VERIFIED.ME SERVICE TERMS AND CONDITIONS

Please carefully read this Agreement before agreeing to use the Verified.Me service (the "Service"). The Service allows you to provide certain of your Personal Information to Relying Parties chosen by you. This Agreement is between you and SecureKey Technologies Inc. ("SecureKey", "us", "we" or "our").

By clicking "I agree", you are agreeing to be bound by this Agreement. If you do not agree to this Agreement, click "Cancel" and you may not use the Service.

By clicking "I agree", you are also confirming that you have reached the age of majority in the province in which you reside or, if you are a minor, you confirm that your parent or legal guardian has had an opportunity to review this agreement and has consented to your use of the service



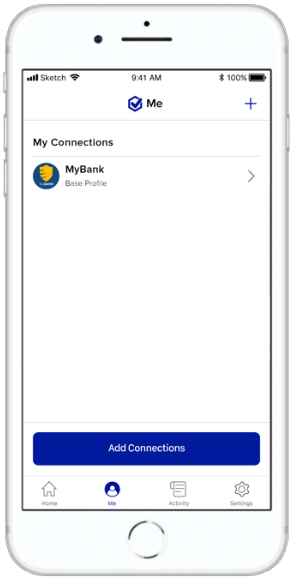
Services That Accept Verified.Me

Please select one of the available services below to find out more:

MyTelco
Easily open an account or sign up for new products and services.

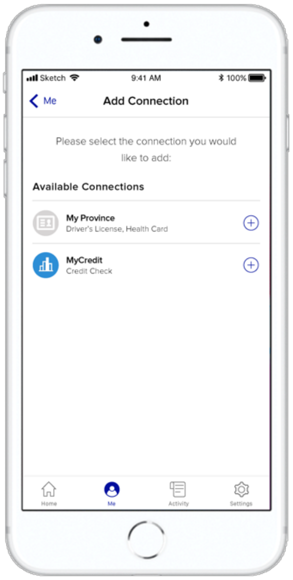
MyBenefits
Easily open an account or sign up for new products and services.

2. **Collect Digital Assets – Add Connection:** A registered user should be able access Digital Assets provided by other Network Participants who are acting as DAPs. This rounds out their Digital Lockbox profile and allows for faster transactions in the future.



My Connections

MyBank
Base Profile



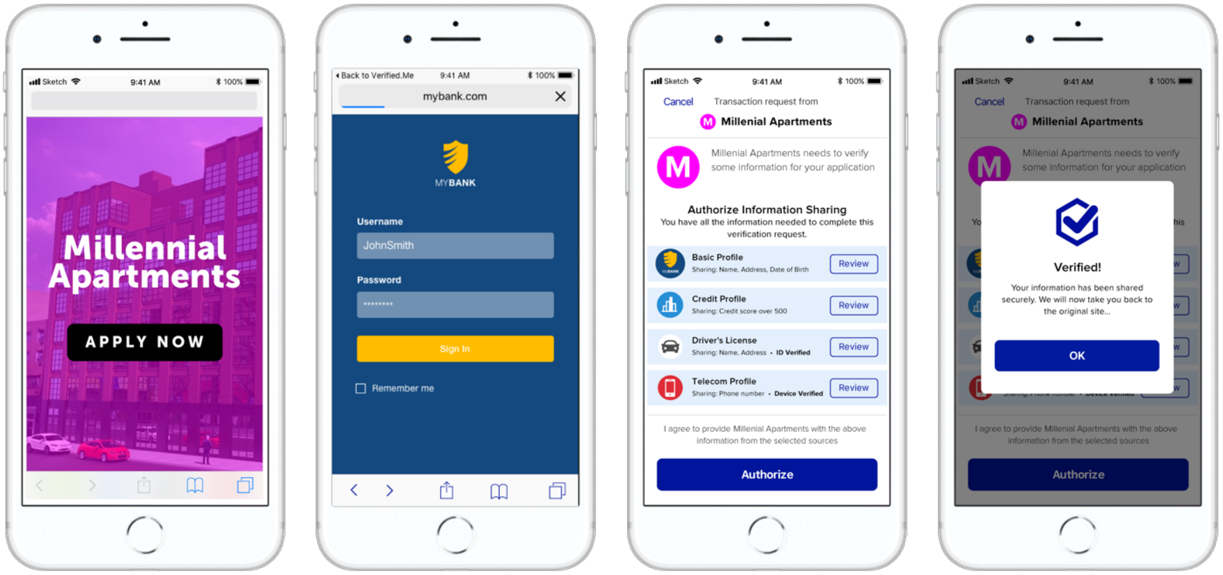
Please select the connection you would like to add:

Available Connections

My Province
Driver's License, Health Card

MyCredit
Credit Check

3. **Share Multiple Digital Assets in one Action:** A user should be able to share their Digital Assets with valid Network Participants who are acting as DACs. Users should be able to share multiple Digital Assets from potentially multiple sources in a single transaction without requiring multiple authentications at each DAP.



Username: JohnSmith

Password: ********

Transaction request from

Millenial Apartments

Millenial Apartments needs to verify some information for your application

Authorize Information Sharing

You have all the information needed to complete this verification request.

Basic Profile
Sharing: Name, Address, Date of Birth

Credit Profile
Sharing: Credit score over 500

Driver's License
Sharing: Name, Address • **ID Verified**

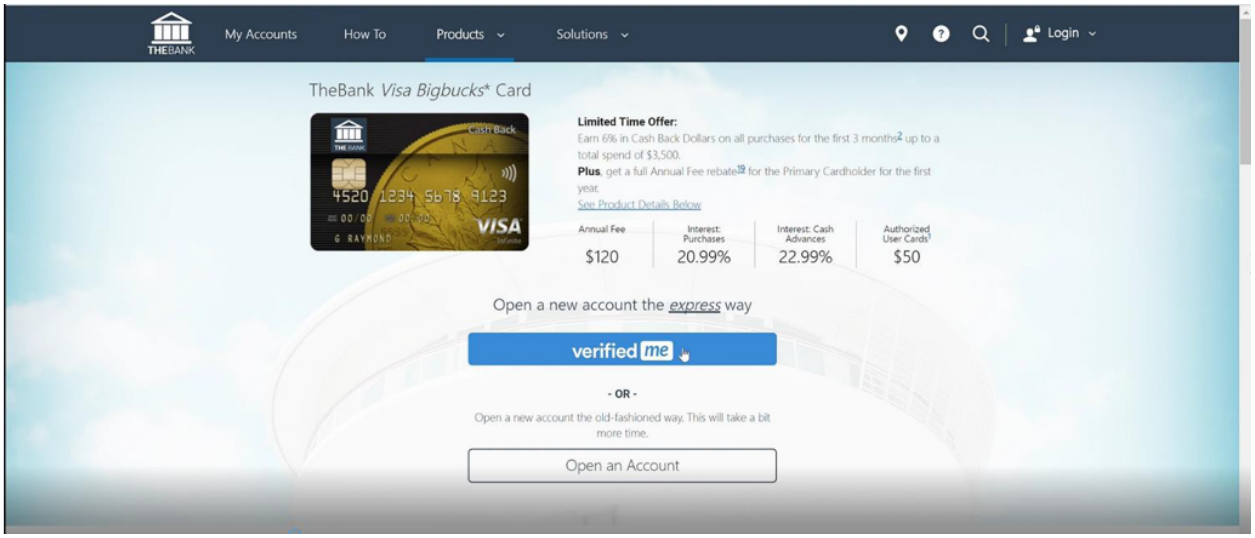
Telecom Profile
Sharing: Phone number • **Device Verified**

I agree to provide Millenial Apartments with the above information from the selected sources

Verified!

Your information has been shared securely. We will now take you back to the original site...

4. **Manage Digital Assets:** A user should be able to view and manage their Digital Assets registered in the Network.
5. **Transaction History**: A user should be able to review their transaction history of events and consent actions they participated in from the mobile app.
6. **Report a Problem:** A user should be able to inspect the details of past transactions they have taken in the Network and be able to report a possible mis-use of their information to their DLBP for resolution.
7. **Delete Account:** A user should be able to delete their Digital Lockbox and all its contents if they choose to stop using the service.
8. **Biometric Authentication and Windows Secure Element:** The addition of traditional web browser capabilities complements the mobile app, enabling consumers to access online services faster, such as opening bank accounts or applying for a new credit card online in seconds, with added privacy and security. It is important to ensure that the digital identity ecosystem is not limited to only one device (mobile). Through SecureKey's work with Intel Corporation, consumers are able to assert identity information straight from their Intel® Core™ processor-based desktop or laptop using Intel® Software Guard Extensions (Intel® SGX) technology. This extends the option for consumers to verify their identity directly from a laptop or desktop. Intel SGX® add extra protections and integrity of sensitive code and data without disrupting the ability of legitimate system software to schedule and manage the use of platform resources.



TheBank *Visa Bigbucks** Card

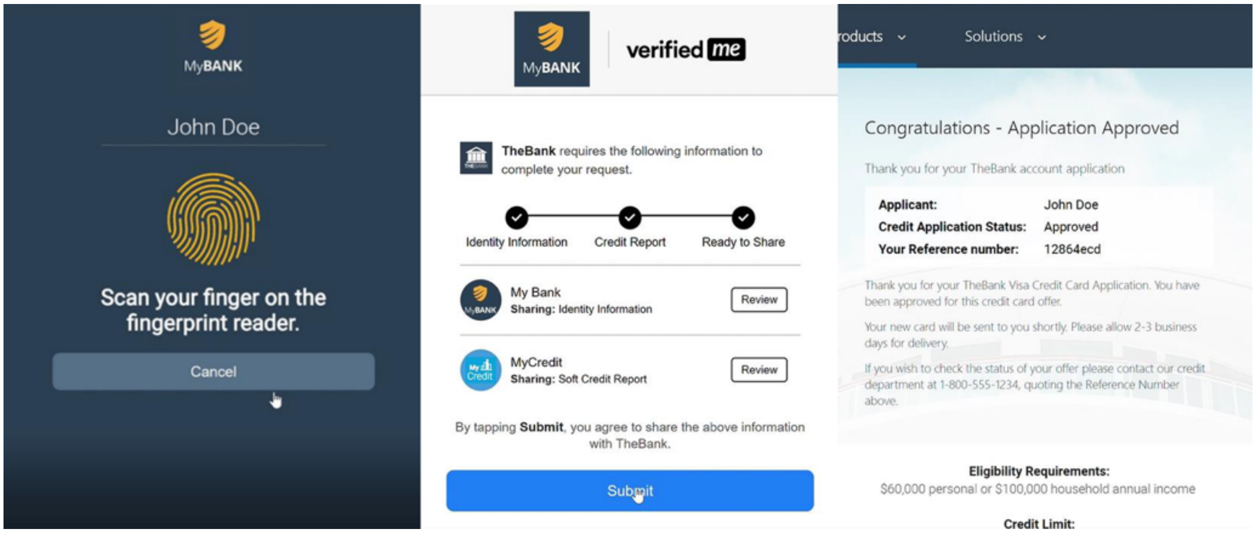
Limited Time Offer:
Earn 6% in Cash Back Dollars on all purchases for the first 3 months[2] up to a total spend of $3,500.
Plus, get a full Annual Fee rebate[19] for the Primary Cardholder for the first year.
See Product Details Below

Annual Fee	Interest: Purchases	Interest: Cash Advances	Authorized User Cards[1]
$120	20.99%	22.99%	$50

Open a new account the *express* way

- OR -

Open a new account the old-fashioned way. This will take a bit more time.



John Doe

Scan your finger on the fingerprint reader.

TheBank requires the following information to complete your request.

Identity Information — Credit Report — Ready to Share

My Bank
Sharing: Identity Information

MyCredit
Sharing: Soft Credit Report

By tapping **Submit**, you agree to share the above information with TheBank.

Congratulations - Application Approved

Thank you for your TheBank account application

Applicant:	John Doe
Credit Application Status:	Approved
Your Reference number:	12864ecd

Thank you for your TheBank Visa Credit Card Application. You have been approved for this credit card offer.

Your new card will be sent to you shortly. Please allow 2-3 business days for delivery.

If you wish to check the status of your offer please contact our credit department at 1-800-555-1234, quoting the Reference Number above.

Eligibility Requirements:
$60,000 personal or $100,000 household annual income

Credit Limit:

Digital Asset Licensing and Distribution

A Digital Asset in the Network is a collection of data linked to a user. Digital Assets are defined by a Schema, or Type. The Type defines the bundle of information that can be collected in a request for that Digital Asset. For example, the Base Profile Digital Asset Type contains personal identification and contact information related to the user. The variety of Digital Asset Types makes up the set of information that can be collected about a user through the Network in a request.

Digital Assets are sourced, or provided, by partners in the Network acting as a DAP. A user can have multiple Digital Assets from a variety of providers.

The Digital Asset record in the Network is a set of references that 'point' to the source (DAP) of the data and links these references to a Digital Lockbox. No real data values are stored in a Digital

Asset record in the Network.

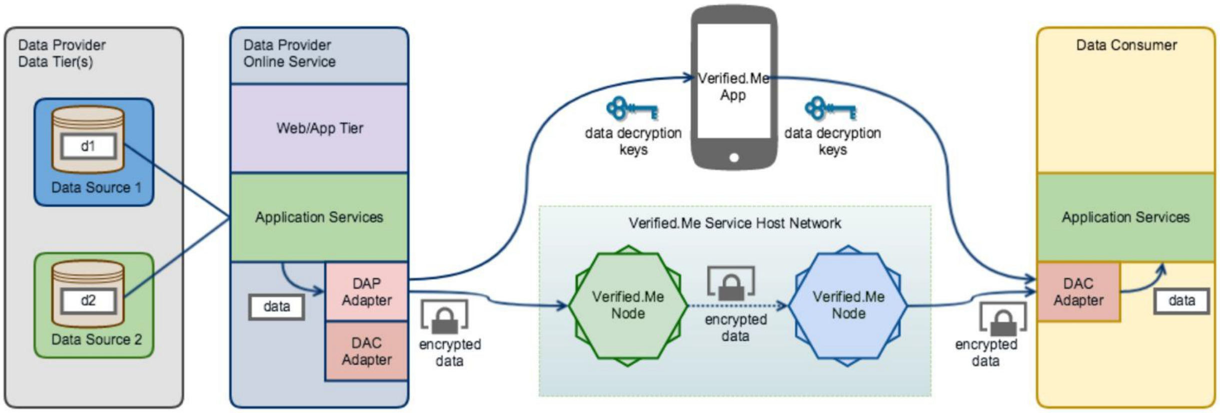
Users are required to authenticate to their Digital Lockbox in order to prove ownership of their Digital Assets.

A user registers at a DAP to authorize access to their information through the service. The DAP then issues one or more Digital Assets to the user.

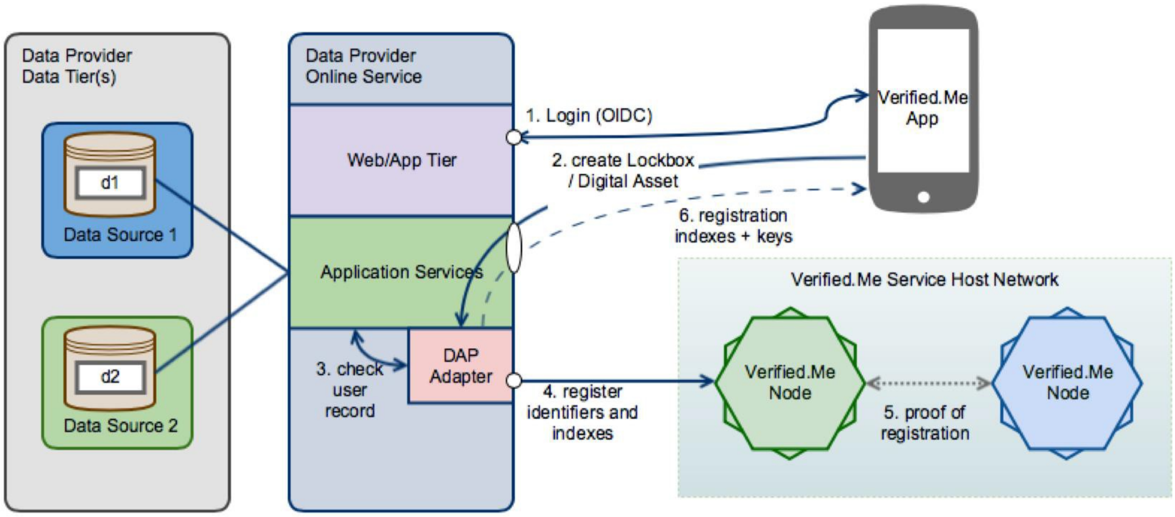
Partners in the Network that consume user information are called Digital Asset Consumers (DACs). When a user agrees to share their Digital Asset with a DAC, they are licensing their Digital Asset to that DAC through the service.

The service manages Digital Assets and licenses to facilitate the exchange of user information in a secure, private, reliable and robust manner through the Network.

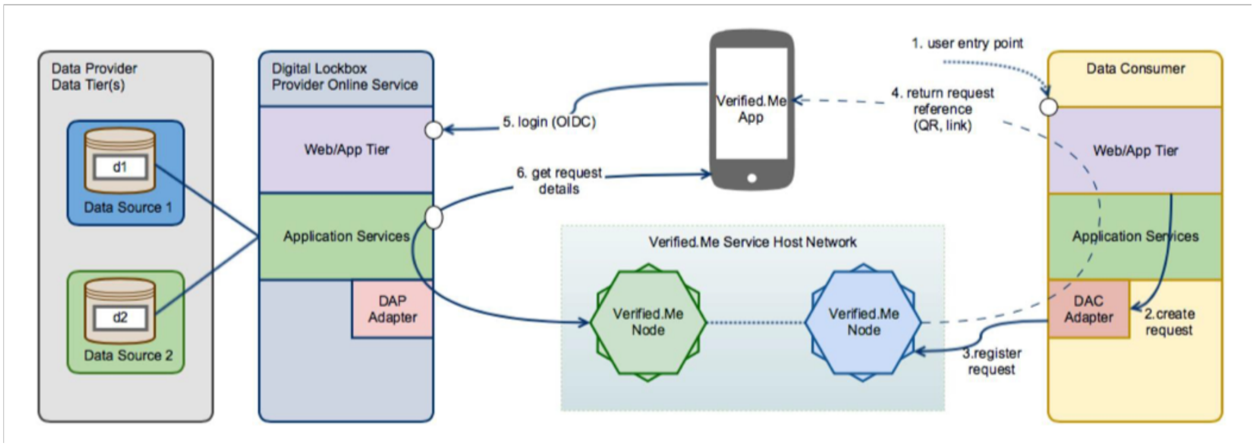
1. High Level Data and Key Flow



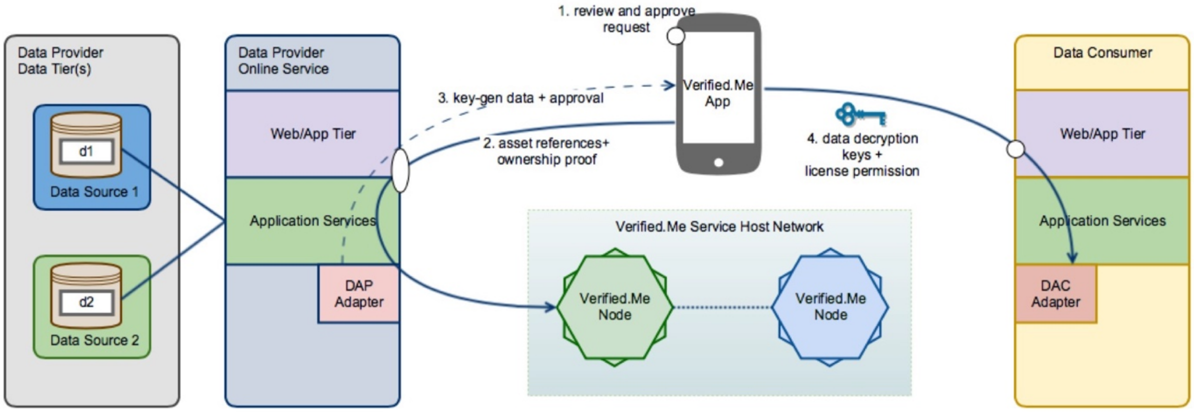
2. Registration



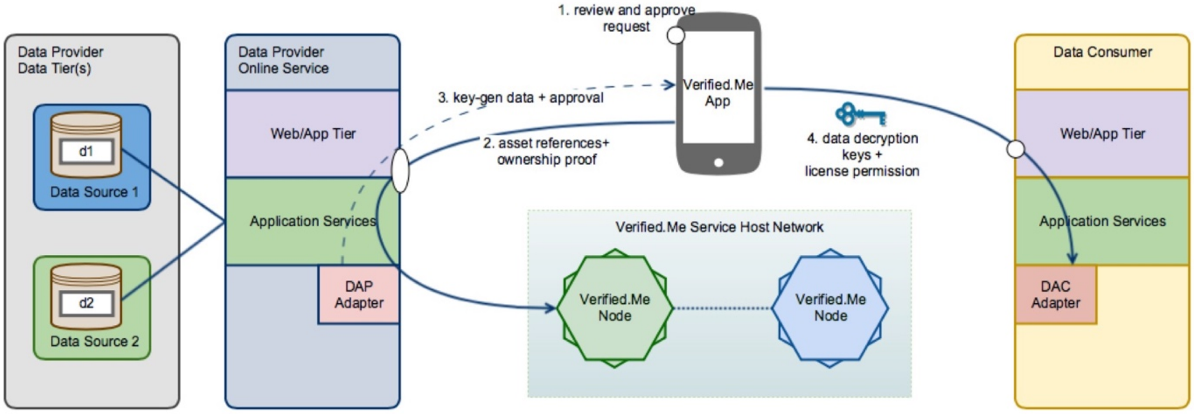
3. Transaction Step 1: Request



4. Transaction Step 2: User Licensing



5. Transaction Step 3: Fulfillment



Lessons Learned for the DIACC Community

DIACC's mission is to unlock and harness Canada's full potential in the Digital Economy by delivering a Digital Trust Framework of standards and practices collectively known as the Pan-Canadian Trust Framework. The Pan-Canadian Trust Framework is developed by Canada's public and private sector community and published by the DIACC in order to accelerate Canada's economic growth by securing interoperability of Digital Identity services and solutions including Third-Party Identity Information Networks. The learnings of this applied research project provide a valuable opportunity to inform the Pan-Canadian Trust Framework by exploring an implementation of a Third-Party Identity Information Network.

Given the scope of the deliverables in Phase Two, a number of key learnings were identified during the implementation and development activities. The high-level focus of the lessons learned centered around the need for Networks to perform with speed, convenience, and aligned with the expectations of today's digital users – clearly users will have low tolerance for slow transaction response times and making sure the user has clear understanding of what is happening during these transaction – the user experience must support allowing the user to collect, and present, verified Digital Assets in a trusted and reliable manner. This is a short list of key findings focusing on two primary areas – system/implementation and user experience.

When implementing a Network, at a high level the following requirements were identified:

1. To ensure a seamless user experience, Networks must prioritize speed and efficiency with regards to processing of transactions.

2. The user experience with regards to handling T&C, also requires management with tools to allow the user to review and reference them in the future if needed.

3. Implement a recovery profile feature, allowing users to recover their digital relationships and previous history.

4. Enhance participant on-boarding process with support and integration materials.

References

1. https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/
2. https://verified.me
3. https://www.securekey.com
4. https://diacc.ca/principles/