DIACC

BC Government's Verifiable Credential Issuer Kit

Proof of Concept Report

Table of Contents

About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada **(**DIACC**)** is a non-profit coalition of public and private sector leaders who are committed to developing a Canadian digital identification and authentication framework that will secure Canada's full and secure participation in the global digital economy.

DIACC innovation papers focus on current issues and opportunities in the digital identity ecosystem. DIACC innovation papers are guided by the DIACC's 10 Digital ID & Authentication ecosystem principles and by the priorities of DIACC members. DIACC papers provide insights to business, legal, and technical audiences in Canada and around the world. DIACC papers are not endorsements and do not represent a qualified organization's opinion of the DIACC. DIACC innovation papers are pragmatic and address real-world issues; are open and transparent; vision future opportunities; communicate learning from past projects; are authored by DIACC member domain experts with real-world expertise.

About the Author

Dave McKay is the Co-chair of the Innovation Expert Committee at the DIACC. He specializes in decentralized systems in his work as an Identity Architect at Northern Block, Professor at the George Brown College Blockchain Development Program, Technical Lead at the Ryerson University Cybersecurity Research Lab, and Executive Director at the Canadian Credential Network. Dave worked on the Northern Block response to the call for private sector participation in this project.

Executive Summary

The DIACC Proof of Concept (POC) using the Government of British Columbia's (BC) Verifiable Credential Issuer Kit project demonstrated an open-source code base as a tool to support the adoption of decentralized identity in government and industry across Canada and internationally. The concepts explored in this POC showed the current state of viability for the use of Self-Sovereign Identity (SSI) as a way to issue government authenticated documents. The open approach that BC took to this POC played a role in enabling an industry engagement in the project.

Introduction

The intent of this report is to communicate the project drivers, what the POC demonstrated, the experience and learning of the participants, and how governments might proceed to implement digital identity in their own programs. This report uses a narrative approach to summarize the results of this POC. This report provides strategic and operational insights regarding the results of this POC for other government entities that are interested in building a POC or production system using SSI. The report was written based on a set of interviews with people who were part of this initiative. The interviewees subjects included government staff, vendors who responded to the call to collaborate, and observers from within the identity management industry.

POC Inspiration

In the United States (US), the Department of Homeland Security worked with vendors to research and implement networks that demonstrated an SSI model. Most SSI models include the notion of a mobile wallet, cloud agent, and network. Early research and implementation helped to demonstrate verifiable credentials and decentralized identifiers using W3C standards. This work demonstrated a potential method to break the problem of authentication centralization.

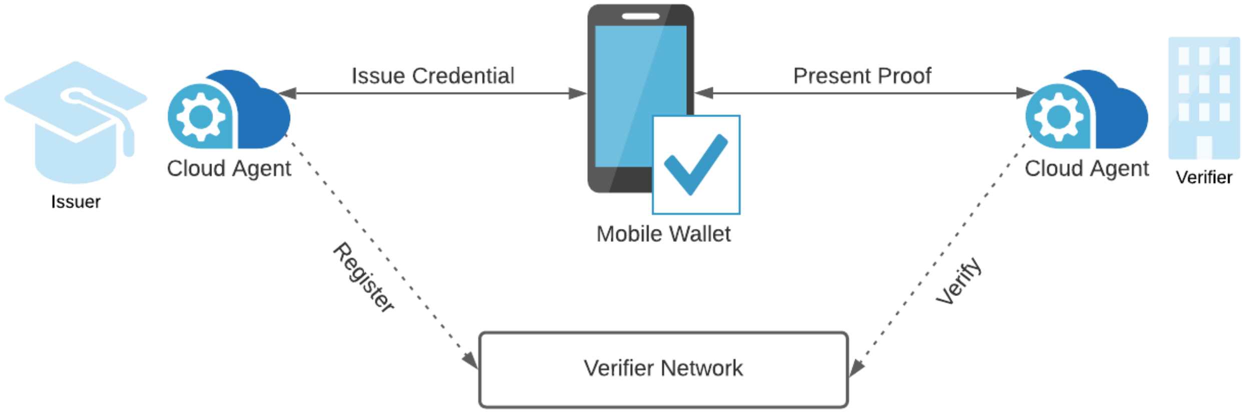
The Verifiable Credential Issuer Kit, an open-source kit built by the Government of BC, was created as a tool for governments and other interested parties to begin to experiment with issuing government authoritative documents. The goals of the Verifiable Credential Issuer Kit were to:

- showcase the potential utility of the technology,
- demonstrate a mechanism to enable residents to gain access to public sector authoritative data using technology that is interoperable around the world,
- demonstrate the BC government's commitment to solving related issues, and
- elicit a response from at least two vendors to develop wallets that could consume the issued credentials.

What Was Built

The output of the Verifiable Credential Issuer Kit POC was a demo container that could be installed by trusted organizations to use the service with their own systems or to connect with a network that the BC government had stood up. The advantage of the network-based approach was that trusted organizations could use elements of SSI systems from existing vendors to inform the services that the BC government was developing.

The Verifiable Credential Issuer Kit encompassed a selection of technology that can be deployed to issue a government-issued verified person credential. The Verifiable Credential Issuer Kit involved creating a user profile and then inviting that user by email to connect and receive their credential. The system was based on the Aries Cloud Agent for Python (ACA-py) that the BC government had helped to develop. The Verifiable Credential Issuer Kit used a variety of emerging technologies to make it easier for participants to build a test environment and to start issuing their own version of the credentials. The BC government extended the project to add in other POCs for how that verified person credential could be used with other government systems.



The approach to developing this POC was unique. The POC was conducted in an open and transparent manner using the neutral good governance of the DIACC, rather than developing a public sector Request For Proposals (RFP) process. The intent from the start was to make this an open development project. All of the code developed was made available for use with an open source license and accessible through Github. Some of the development was funded by bounties using the BC Code With Us program. Developers and development organizations external to the DIACC and BC government were invited to take part in the development or to follow the progress.

This was the first open project to demonstrate using the components of an SSI system to exercise the trust triangle using a Canadian Government issued credential. An individual could connect, receive a credential, and present that credential to another trusted system. Implementing an open source code-based system, allowed other parties to learn and to treat the Verifiable Credentials Issuer Kit POC as a reference design for building their own systems. A number of the vendors that participated in this POC expressed gratitude for the access to the open-source Verifiable Credentials Issuer Kit.

When the POC was up and running, vendors who were all using the same code base had an interoperability sandbox that could be used to mimic the response of an actual Verifiable Credentials Issuer system.

Response From Industry

Many of the subjects who were interviewed for this report indicated that participation in this POC was informative and enlightening. POC participation helped those subjects to better understand the impact and the value proposition that the technology explored in the POC could have on the marketplace. The POC demonstrated interoperability possibilities when participants are leveraging an agreed-upon technology stack.

The use of the technology explored represents a new paradigm. There were challenges in communicating the intent of the POC and how and why companies could interact with it. The initial vendor response was slow, however, the knowledge-based information-sharing community facilitated by the DIACC was instrumental to the engagement of more responses. The POC was developed through a series of regular DIACC hosted teleconferences where interested parties could participate. By the fall of 2020 the response to the Verifiable Credential Issuers Kit was confirmed and meetings were attended by active participants who were sharing experiences. By having a government entity behind this and running it in an open environment, the POC was able to attract vendors but it still highlighted the on-going challenges for the need to define appropriate commercial models that can be leveraged.

The following vendors responded with working systems:

- Northern Block
- Interac/2Keys
- Yoti
- Applied Recognition
- Vlinder

Each of these vendors demonstrated a mobile digital wallet as a proof of concept or as an alpha of a commercially releasable application. See Appendix A for more information on each vendor and a link to a repository of videos of each system being demonstrated.

Name Jane Doe

AssureID: Doc Authentication ✓

Face ID: Liveness Test ✓

Face ID: Match Score 100 ✓

Licence Number D6101 - 50707 - 51120

Date of Birth 1975/11/20

Identity Proof

Driver's Licence
Issuer: Northern Block Inc.
08/01/2020

Name:	Jane Doe
Date of Birth:	1975/11/20
Number:	D6101 - 50707 - 51120
Class:	C
Issue Date:	2019/05/28
Expiry Date:	2024/05/28
Address:	123 Any Street, Toronto, ON, M0M 0M0

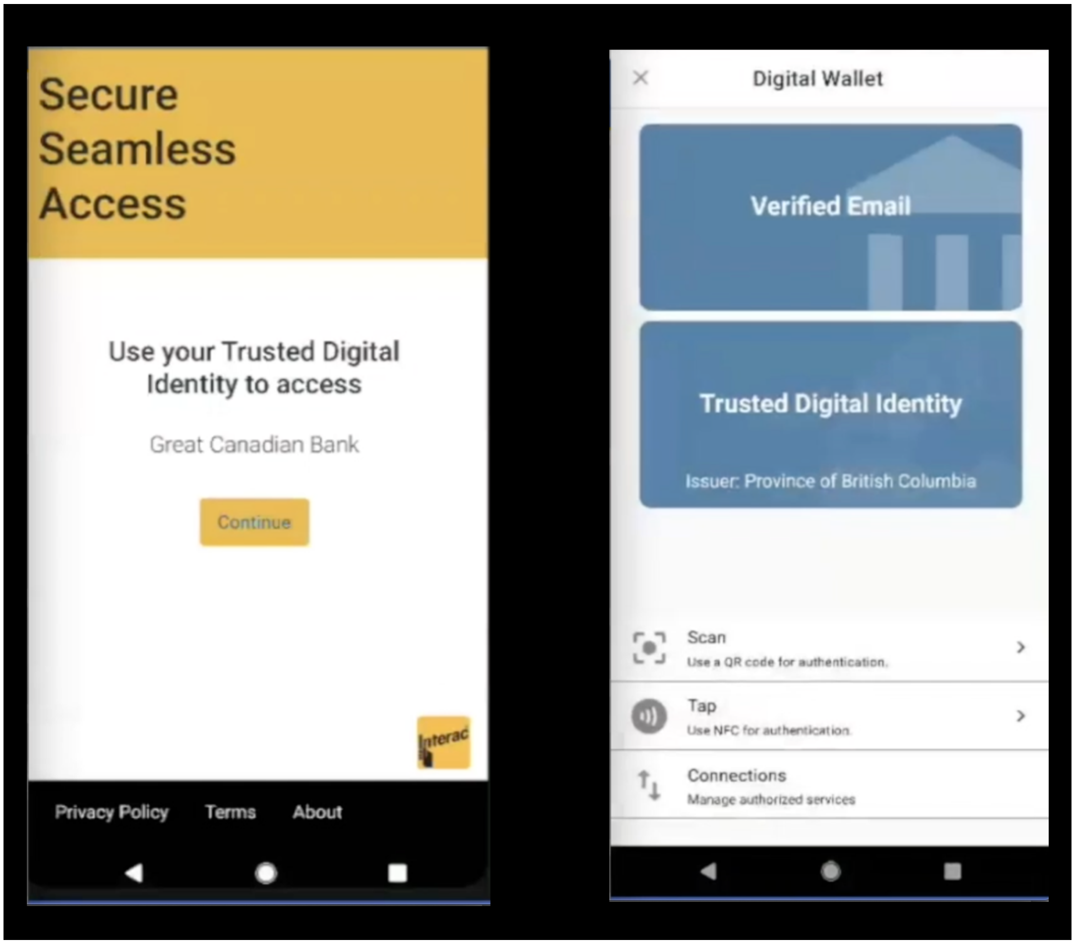
Welcome, Jane Doe!

Education Certificate
Issuer Ryerson University
Expiry Date N/A

Passport
Issuer: Northern Block Inc.
08/02/2020

Organization Connection Proof
Issuer ABC Company
Expiry Date N/A

Northern Block NB Orbit Wallet


Secure
Seamless
Access

Use your Trusted Digital Identity to access

Great Canadian Bank

Digital Wallet

Verified Email

Trusted Digital Identity

Issuer: Province of British Columbia

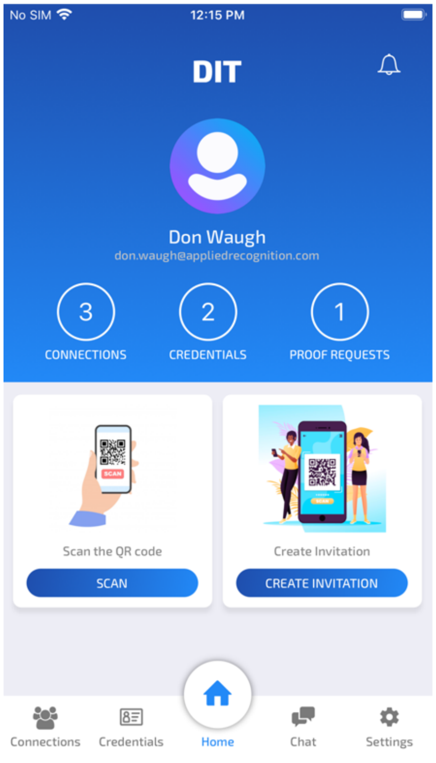
Scan
Use a QR code for authentication.

Tap
Use NFC for authentication.

Connections
Manage authorized services

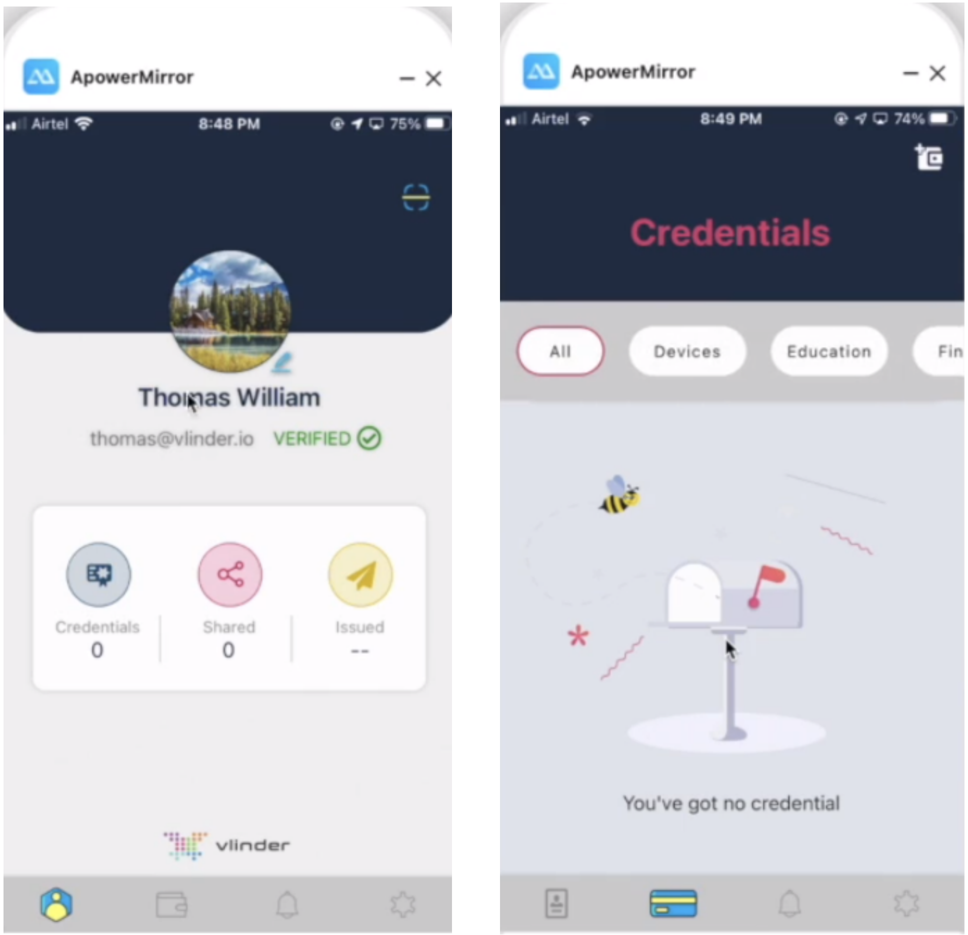
Interac/2Keys Wallet

Yoti Wallet



Don Waugh
don.waugh@appliedrecognition.com

Applied Recognition DIT Wallet



Vlinder Klefki Wallet

Key Learnings

The BC government team's biggest takeaway was that open participation and collaboration with the private sector can have a huge payoff. They also learned to allow for time for external parties to catch up and to digest what has been presented to them. In a project like this, rather than building one giant RFP at the outset, the system can be built using an iterative agile approach with calls for tech development when identified. They also discovered that some trusted organizations will judge things based on the look of the user interface rather than the underlying utility. Some potential respondents were turned off by the rudimentary interfaces and the lack of a polished setup procedure. In looking at what was built and the response, human-centred design is going to be important going forward with SSI systems.

The BC team was able to learn what can drive companies to adopt this technology. Demonstrating a mockup of a government-issued credential was a tipping point. In the eyes of the private sector participants, this was a way to break the catch-22 of a decentralized system - "If no one has any credentials to issue, then why create a wallet to store them?". From their perspective, if the government is involved, then the effort is worthwhile. The POC benefitted from the use case it handled. The workflow of the government issuing a credential to a citizen who can then take it to be verified by another party (possibly private sector) helped light the imaginations of companies involved in the response.

The vendors were able to learn what is involved in standing up their SSI offerings and what it takes to make sure that they are interoperable. By seeing the government reference systems, vendors were able to make their own architectural decisions that could take into account existing working open systems.

Recommendations

From the experience of this project, the participants have some recommendations for other government and private sector projects in the decentralized identity space.

Open collaboration leads the way

Keep the public informed about projects you are undertaking. Consult with the public and private companies and take into account their thinking. Collaborate on open source initiatives.

Do not stay in a silo, be interoperable, and have a target with an international scale

Without diverse collaboration, solutions will be siloed. Entities should think beyond their region and our country to ensure that solutions will work at an international scale.

Open projects are motivational for all parties involved

Working in collaboration fosters connections that can provide a better outcome for your project. Private industry will be enthused to be heard and to offer up help in accomplishing tasks.

Find ways to proceed that take into account market dynamics

Private industry needs to be agile and take into consideration what the market wants. Government projects need to take that into account and focus on areas where they can support and embrace innovation as well as issuing credentials that can be used to improve the security and reliability of commercial transactions.

Industry determines commercial viability and sustainability

The industry respondents identified wallets as a single component in a larger system of issuing and verifying credentials. The wallet appears to be sustainable in the context of a larger system. Innovations in issuing and verifying may drive changes to wallet operations. The marketplace of ideas is a critical driver of innovations that inform wallet design features.

Resources that may help to stimulate choice of wallets within the ecosystem:

- A roadmap of when / how public sector issued verifiable credentials would become available.
- The feature and functionality requirements that must be present in a wallet for the public sector to trust that wallet.
- Demonstration of PCTF compliance, for example through the DIACC Voilà Verified Trustmark program.

Government strength for issuing credentials

Compliance with legislation is critical to a functioning and stable transactional environment. Governments are positioned as natural issuers of machine-readable verifiable credentials that represent authoritative proofs to enable companies to comply with regulatory requirements and business practices.

Government can foster innovation with support

Government can play a huge role in supporting adoption. Governments need to participate in alliances to inform technical standards, policy governance, and to invest in projects that align with government priorities.

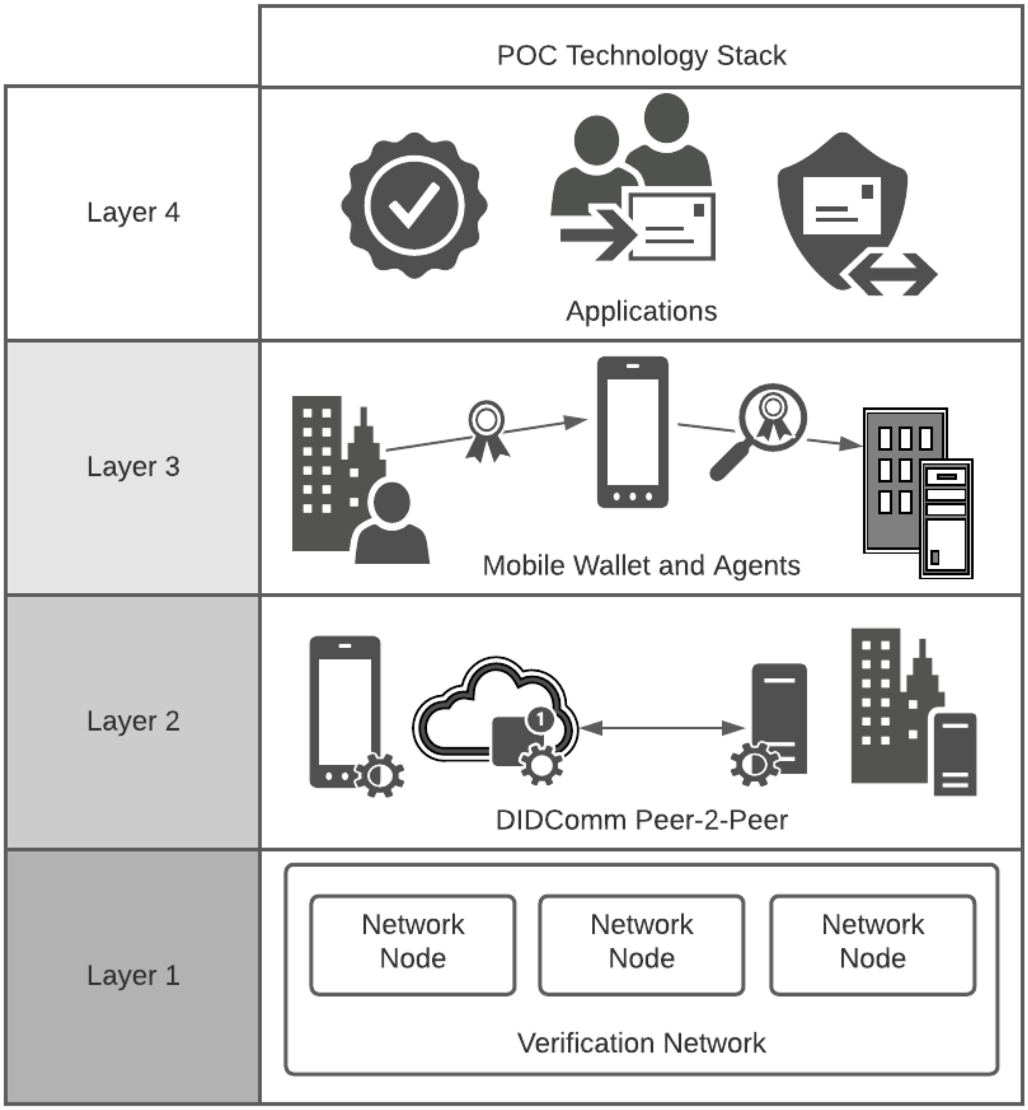
Always be interoperable

Every effort should be made to ensure that local systems can work with the systems used in other regions and with private industry. Systems that are not interoperable provide less value and may be ignored and deemed a waste of resources.

Get involved with the governance of networks and registries

Parties that are interested in the larger ecosystem of digital identity using self-sovereign identity should consider joining and contributing to efforts to build and operate these systems and their ongoing governance.

1. The public utilities layer governance is seeking trusted organizations to be stewards and trust anchors to operate the network in a distributed environment.
2. The provider governance layer can use the input of governments to help establish standards for credential transport, credential representations, and selection of cryptographic signatures to use.
3. The credential governance framework requires governance that sets compliance around privacy and security of the credentials and connections in the possession of holders and trusted organizations.
4. Governments can play a very large role in the ecosystem governance frameworks by becoming trusted registrars on trust registries of standard credential schemas and verified registries of known government, academic, charity, and financial institutions.



Legislation changes may be needed to enable digital identities and verifiable credentials

Governments should review legislation that does not take a “people first, digital first” approach to enable digital identities and credentials. Legislation that requires in-person signing, paper-based documents, or notaries should be reviewed to see if this new technology can streamline these processes and become compliant.

Conclusion

This project sought to test the adoption viability and interoperability of public and private sector interoperability of verifiable credentials in Canada. The work-in-the-open nature of this project enabled diverse public and private sector initiatives to gain strategic and operational insights regarding interoperability by working together. There are many open-source and private initiatives available to work with. See Appendix A for a listing of projects that were an inspiration or were inspired by this project.

For further information about the topics discussed in this paper, or to join the DIACC community, visit www.diacc.ca or contact info@diacc.ca.

Appendix A - Participating Vendors

Vendor	Northern Block
Contact	Mathieu Glaude, mathieu@northernblock.io
Offering	NB Orbit Wallet: ● https://northernblock.io/products/ssi-digital-wallet/ NB Orbit Issuer, Verifier and Onboarding Platform: ● https://northernblock.io/products/ssi-enterprise-cloud/ Northern Block presented an early version of the NB Orbit suite. It consists of a mobile wallet application and an issuing platform. The NB Orbit issuer, verifier and onboarding platform is currently based on the ACA-py agent that is used in the Verifiable Credential Issuer Kit. The wallet and credentials issued on this platform are compatible with the POC.
Website	https://northernblock.io/
Video	https://www.youtube.com/watch?v=rl8yt6V3p0U

Vendor	Interac and 2Keys
Contact	Andrew Johnston, ajohnston@2keys.ca
Offering	Interac and 2Keys presented a technology demonstration of a Digital Wallet mobile app that included acceptance of a government-issued Verified Person digital credential, end-user authentication via facial recognition, end-user authorization of credential presentation, and an open standards-based interface -- OpenID Connect -- for relying parties. Interac and 2Keys also provided some example relying party applications to demonstrate how the Verified Person credential could be used by private-sector ecosystem participants, and how biometric authentication could be used to improve confidence in the identity of the end-user.
Website	https://www.interac.ca/
Video	https://youtu.be/aso4RPQs5xM

Vendor	Yoti
Contact	Leigh Day, leigh.day@yoti.com
Offering	Yoti demonstrated the ability for a Yoti app user to ingest a government-minted credential from the Blockchain into the Yoti app, display it as a verified credential, and share it with a relying party by means of 'shooting' a QR code.
Website	www.yoti.com
Video	https://youtu.be/_G2_KDVLVvU

Vendor	Applied Recognition Corp.
Contact	Don Waugh, don.waugh@appliedrecognition.com
Offering	Applied Recognition presented an alpha version of a self sovereign wallet that integrates Ver-ID face recognition directly into the wallet. Applied Recognition recognized the security issues in the use of passwords by self sovereign wallet versus how credentials and wallets need to be secured. The integration of Ver-ID face recognition solves several issues for wallet owners, credential issuers and relying parties including: ● Protection of the wallet and the wallet holder from identity theft. ● Automation and augmentation of identity verification for issuers and relying parties. ● Binding face biometrics to verifiable credentials ensures that only the

	bonafide owner can open their credentials. ● Provides assurance to relying parties that the credentials presented are coming from the bonafide owner and not an imposter. The wallet was tested using both the BC Government test sites on the Sovrin Staging and BCovrin networks demonstrating interoperability between separate networks. Applied Recognition has now licensed Ver-ID to the Digital Identity Trust Foundation. who will make the wallet freely available to consumers to advance and secure digital identities and verifiable credentials.
Website	www.Appliedrecognition.com/sovrinwallet, https://digitalidentitytrust.org/
Video	https://vimeo.com/548476945

Vendor	Vlinder
Contact	Malini Srinivasan, info@vlinder.io, malini@vlinder.io
Offering	Klefki is a blockchain based secure, frictionless platform that enables trust, inclusion and efficiency to the ecosystem of Public and Private enterprises Klefki Enables individuals to: 1. Own Identity 2. Accept credentials from Issuers and Store Security in mobile wallet 3. Share credentials with Verifiers by consent, on demand basis 4. Disclose selective details of credentials (Proofs) as opposed to actual sensitive data Enables Issuers to: 1. Issue Credentials directly to Citizen’s wallet 2. View list of Credentials Issued in dashboard Enables Verifiers to: 1. Verify Credentials of Citizens directly with Citizens Klefki adheres to key standards including but not limited to: 1. W3C standards 2. GDPR 3. India’s Data Protection Bill Klefki Wallet (iOS): ● https://apps.apple.com/us/app/klefki/id1546129401

	Klefki Wallet (Android): ● https://play.google.com/store/apps/details?id=io.vlinder.klefki Klefki Product Link: ● https://klefki.io/#product Klefki Enterprise Platform (Issuer/Verifier Ecosystem): ● https://generic.klefki.io/login
Website	https://vlinder.io/
Video	Klefki Platform: ● https://vlinderdeveloper.wistia.com/medias/3wsjyd0vvu Klefki Real Estate DIACC: ● https://vlinder-uxdeveloper.wistia.com/medias/00poxjn0nk