Building the Canadian Digital Identity Metasystem

DIGITAL CANADA.IO

DigitalCanada.io

Building the Canadian Digital Identity Metasystem

Alex Benay describes how a national Digital Identity program is a keystone foundation for a Canadian digital economy blueprint, enabling Canada's trusted digital identity vision.

As Neil Parmenter from the Canadian Bankers Association explains it would provide a universal framework, an ecosystem, for accelerating digital capabilities across all industries such as Digital Banking.

The concept of an 'Identity Metasystem' has been under development for twenty years.

Microsoft Identity guru Kim Cameron defined the concept in 2006 and more recently 'Self Sovereign Identity' guru Phil Windley describes it's evolution up to today's cutting edge progress and innovations like SSI.

Tim Bouma, Canada's SSI expert, builds on this to add the further definition of its role as a Global Verification Network: ***"A network to independently verify without reliance on trusted intermediaries."***

Identity Networks

In their blog 'Why Canada Needs a Digital ID Framework' DIACC describes a compelling argument for accelerating the development and adoption of a Canadian digital identity system.

The mission of the DIACC is to unlock interoperable capabilities of the public and private sector to secure Canada's full and beneficial participation in the digital economy by fulfilling the following strategic goals aligned with their 10 Principles for an Identity Ecosystem.

They define the implementation of this ecosystem through 'Identity Networks':

Building the Canadian Digital Identity Metasystem

"Some countries, such as the Nordics, have a history of collaborative approaches to digital identity that is suitable for regulated services. In the case of the Nordics, the banks have over several years provided "BankID" services for use in financial services, government services, and the wider economy. Several other initiatives – some national, some international – are seeking to create similarly robust and ubiquitous digital identity networks in other regions.

These identity networks will allow digital identities to be portable, they will help to detect and reduce fraud, and they will provide mechanisms to ensure identity data is up to date. They will create collaborative environments where the needs of all stakeholders (not just a few) are met. The work of the DIACC, and in particular the Pan-Canadian Trust Framework, is helping to ensure that this is accomplished in identity networks in Canada and internationally."

DIACC estimates a $15 billion value to the Canadian economy through implementation of this ecosystem, building a rising tide that floats all boats of improved trust and security across government, banking and other online transactions.

For example they highlight that during this time of coronavirus crisis there is a massive rise in remote working, a trend that is likely to continue, and that too presents risks that identity would address. Canada as a nation of digital identity would be better prepared to continue working in the event of future crisis and is thus a critical infrastructure that should be invested in accordingly.

Spotlight on Mastercard

One example of a member participating in DIACC is Mastercard, demonstrating the point that banking would be one of the industries that benefits from the rising tide. Canada has fallen behind in key markets like Open Banking and it is a trend where identity is a central enabler. They describe:

Building the Canadian Digital Identity Metasystem

> Identity is what makes our existence in the world official: it is how countries recognize and see us, and it establishes citizens' rights to national benefits. It is also the foundation for participating in the economy, and more importantly, to help grow the economy.

and their own identity standards, notably their model for digital identity, a method for embodying privacy-by-design and enabling digital interactions to occur with minimal data exchanged and only when needed. It will safeguard data and the use of data effectively such that the users are in control, with a person's identity securely bound to their smartphone.

Overview of the PCTF: Pan-Canadian Trust Framework

The primary standards for building Canada's Digital Identity Metasystem is the 'PCTF'.

In the feature video Tim Bouma Senior Policy Analyst Identity Management for the Canadian Government, shares an overview of the PCTF: the Pan-Canadian Trust Framework.

Tim explains that the Canadian Government's Identity strategy has been under development for over a decade, evolving from a program to a user to now a Self Sovereign view for Digital Identity, and that is an ongoing process of innovation, with key goals of a pan-Canadian, technology-agnostic model.

A key design requirement for their framework is the ability to integrate with numerous existing legacy systems, those that operate via centralize and federated architecture.

The model itself is a combination of agreed concepts, process definitions, conformance criteria and an assessment framework, to enable acceptance of trusted digital identities, and is accessible as an open source Github repository.

Early adopters include the Canada Revenue Agency and the Provinces of BC and Alberta. These are traditional system integrations but they set the scene for adopting digital wallets and Self Sovereign Identity.

Anchors and Rails of a Digital Nation - Forging Self Sovereign Identity in the Age of the Blockchain

To realize a world-class Digital Government Canada has set itself an ambition of:

"Digitize all public-facing government services so they are accessible by web and mobile phone and available behind a unified login system by 2025."

A number of technologies, from Cloud computing through AI, will play an important role in achieving that goal, with the central linchpin being Digital Identity.

It will make possible the described unified login system, among other core capabilities that provide the keystone foundation for an entirely digital nation, and the cutting edge innovation of this field is 'SSI' – Self Sovereign Identity.

What is Self Sovereign Identity?

Self-Sovereign Identity (SSI) represents the ultimate evolution of Digital Identity technologies and architecture to underpin and enable such government ID systems. As the name suggests the key principle is that Identity systems are not operated centrally by one organization, but rather the user themselves are in control of their own Digital Identity and personal data.

Sovrin provide this introductory article explaining SSI – They are central to this trend, operating the membership organization, a collection of 'stewards', who work together to ensure the integrity of the network much in the same way DNS is regulated. Via his blog tech industry luminary Phil Windley describes their launch.

Anchors and Rails of a Digital Nation - Forging Self Sovereign Identity in the Age of the Blockchain

One of Canada's foremost experts in the field Tim Bouma identifies the current landscape of Government Identity systems in Canada in his blog Canada: Enabling Self-Sovereign Identity.

He highlights how many are implementing similar approaches to the UK's Verify system in terms of centralized or federated models, with SSI adoption being at the very early stage, and in another blog articulates a vision of how this will provide for the 'Anchors and Rails of a Digital Nation'.

Identity in the Age of the Blockchain

An explosive field of potential lies in the intersection with the Blockchain. In his Reboot the Web of Trust presentation Christopher Allen defines this headline theme of *Forging self-sovereign identities in the age of the blockchain*.

In particular, at 6m50s he describes how the Indian identity scheme 'Aadhaar', a centralized government program, violates over a decade of first-world Identity best practices, with few laws against profiling, discrimination and abuse by law enforcement.

To avoid these pitfalls Allen says a key objective was to utilize the same tools used to protect buyers, sellers, traders and auctioneers to protect the helpless, documenting these principles into his defining white paper The Path to Self-Sovereign Identity, which was presented to the United Nations.

Anchors and Rails of a Digital Nation - Forging Self Sovereign Identity in the Age of the Blockchain

Canada's Global Opportunity

The opportunity and real potential for Canada to become the world leader in the field of SSI is demonstrated through the local expertise and pioneering projects that are well ahead of anything being done elsewhere.
Canada boasts world-leading exemplar case studies for the role of Self Sovereign Identity for Digital Government scenarios, including the ACE and BC Orgbook projects.

The User-Centric Verifiable Digital Credentials Challenge is intended to accelerate this momentum, and grow adoption across many more use cases.

"The Treasury Board Secretariat of Canada (TBS) and Shared Services Canada (SSC) are seeking a standardized method to issue and rapidly verify portable digital credentials across many different contexts, thereby reducing human judgement error, increasing efficiency and ensuring digital credential veracity using cryptography."

The Github repo provides a detailed knowledge base explaining the program, and is also further explained in this document.

Use Cases and Vendors

The winning vendors are documented here, which lists the use cases they intend to implement and demonstrate:

Anchors and Rails of a Digital Nation - Forging Self Sovereign Identity in the Age of the Blockchain

- **Bluink –** Demonstrate eID-Me interoperability with Decentralized Identifiers (DIDs), WC3 Verifiable Credentials, and JSON-LD specifications.
- **Aviary Tech –** Demonstrate how cannabis licensees can use their government issued verifiable credentials to coordinate directly with the federal supply chain, rather than relying on the many integrations currently required.
- **SecureKey –** Enable users to share verified data from trusted partners including banks, telcos, insurance, and credit agencies. Issuing organizations will be able to create official digital credentials.
- **Terrahub –** Independently, cryptographically and rapidly verify an individual's ability to perform a job or enter a site without the need for 3rd party verification.
- **TrustScience –** Demonstrate how a set of credentials containing the information (e.g., time of hiring, time of termination, employer, employer id, citizen id) along with the metadata are managed in a wallet controlled by a citizen and also be stored by the employer to be transmitted to the Canadian government.
- **2Keys –** Demonstrate how issuers of evidence of foundational identity (birth certificates or permanent resident cards) can issue a digital equivalent (verifiable credential) that supports enrolment and delegation processes using verifiable credentials and supports an omni-channel approach to allow a user to present verifiable credentials online or in-person with the ability to cryptographically verify the provenance of the credentials whether connected or offline.

This webinar replay shares detailed demos of all the pilots.

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

Canada is beginning to develop their own version of a "Tell Us Once" Digital Identity policy, an approach pioneered in Europe by the likes of Estonia.

This is a policy where having provided your data to one government agency, you'll never be asked for it again from another, defined explicitly through legislation.

Canadian Digital Government

Canada's adoption of the principle includes a first project for online direct deposits. Their future looking Canada150 site explores the idea that this represents the future of their online government, and as the feature video shows they're seeking to socialize the idea across the Canadian public sector to encourage further adoption.

Via their 'OrgBook' project British Columbia offers a technology blueprint for achieving this approach.

This is for a use case of business registrations, a very powerful case study that harnesses the latest technology innovations including the Blockchain and Self-Sovereign Identity.

Red Tape Reduction

As their case study explains a primary motivation for the project is to greatly reduce the bureaucracy associated with small business administration.

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

Small businesses in Canada face a daunting work load – Companies with less than five people pay C$6,744 per worker just meeting regulations.

Even a sole proprietor in Canada must use at least three different tax numbers, and starting a new business is like navigating a maze with three levels: local, provincial, and federal.

The core benefit of a Tell Us Once approach is eliminating the need for citizens to repeatedly populate workflow forms with data they have already provided to another agency. In Estonia for example your tax return application application is pre-populated with data from other databases, indeed the requirement to do so is mandated by law.

How to reduce this type of bureaucracy to boost economic output is a key research focus for the EU, who have been conducting extensive research into this, publishing this report.

Verifiable Organizations Network

The OrgBook project sought to bring this same efficiency to small business applications for British Columbia, launching the 'VON' – Verifiable Organizations Network.

The OrgBook is a repository of web-searchable public credentials, instances of VON issuer/verifier agents, the equivalent of "Permit to Operate" documents posted on businesses' walls. It acts as a digital marketplace, matching organizations applying for permits to those who issue them, verifying the integrity of that process through Self-Sovereign Identity methods.

The register is a decentralized, Self-Sovereign identity network built on Blockchain technology, using the Sovrin Foundation's Sovrin Network as the underlying Identity Registry Network.

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

As an organization goes through the online application processes to acquire registrations, licenses or permits, the services get proofs (and their associated verified claims) from verifiable credentials already stored in OrgBook about the organization. Once a service completes the approval process and decides to issue the organization a registration, licence or permit, they issue that public verifiable credential digitally to OrgBook about the organization.

This saves the users from having to re-type the information for each service (and eliminates typos in the data). Each service can trust the information because it comes from a trusted source, cryptographically proving:

- The information was issued by the issuer.
- The information was issued to OrgBook.
- The information has not been tampered with (was not forged).
- The information has not been revoked.

Blockchain and Self-Sovereign Identity

An especially helpful primer to this technology and case study is offered through this webinar (below) from John Jordan of the British Columbia ID team, one of the first governments to pioneer adoption of Blockchain and Self-Sovereign Digital Identity technologies for government use cases.

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

Particularly noteworthy points include:

- Enacting the legislation required to underpin the technology framework for Identity-enabled digital services.
- How previous Identity approaches (the “old technology”) resulted in semi-digital versions of the offline paper-based process, resulting in yet more multiple online accounts, an effect greatly exasperated by the many levels of government citizens must interact with to complete one process (eg. business permits etc.)
- A Continuous Integration capability enabled by RedHat Openshift-based Government as a Platform architecture.
- Starting off with a proof-of-concept to trial key technologies like the Blockchain, in conjunction with DIACC and based on an early version of the Hyperledger Fabric.
- How the key is to approach design models as an Ecosystem, the ‘Decentralized Identity Solar System’.

ACE : Building Localized Self-Sovereign Identity Ecosystems

The core principle of building an Identity Ecosystem is the collaborative integration of multiple organizations.

What is particularly notable about this effect is that they are being developed at multiple levels – For example Sovrin is building a global network for regulating the exchange of Self Sovereign Identity-based data, and then also at the national level organizations like DIACC are developing a Canadian policy framework and system.

Furthermore there are even regional initiatives, SSI pioneers are also developing localized ecosystem collaborations.

In Alberta the state owned bank ATB Financial is building 'ACE', the Alberta Credential Ecosystem, a local collaboration of organizations beginning to adopt SSI and achieve integrated services through sharing SSI credentials, an initiative led by Mike Brown.

> The power of ecosystems are key to an exponential future! #SUCanSummit
> The Alberta Credential Ecosystem is an example of how we're embracing a future of Self Sovereign identity #SSI and #blockchain to give individuals control of their identity
>
> — Mike Brown (@mike_brown_yyc) April 23, 2019

Building a Local Identity Ecosystem

What this highlights is that both global and local collaboration is key.

ACE : Building Localized Self-Sovereign Identity Ecosystems

Where global ecosystems like Sovrin enable the core inter-operation, there is still a need for localized collaborations to operationalize these capabilities, even in the simple terms of building partner relationships through meet ups and workshops. From these comes the realization of how and where to apply the technology to best deliver mutually beneficial business results.

Presenting to the SSI Meetup community, Mike explains the journey thus far for developing ACE.

The principle objective has been to form a collaboration network of local organizations, what Mike defines as a 'multi-sided marketplace', including universities, utilities, telcos, local and city government, to identify where they have intersecting business processes that would be well served through an SSI-integrated workflow.

Having modeled these scenarios they have then developed Proof of Concept prototypes. For example working with Telus, the local telco, they linked a banking credential to enable a new account opening process. With IBM and Workday they linked the other way, connecting a new employee onboarding process to payroll banking set up.

Future work includes an in-depth review of digital wallet options and the role they will play in enabling user-centric services for citizens, in particular how best to address the critical issue of key management.

Presenting at the Hyperledger Global Forum Mike shared this lightning talk that showed these developments within an overall context for the bank, with SSI being one of five main focus areas, the others being inter-banking operations, enterprise solutions, cryptocurrencies and payment solutions.

ACE : Building Localized Self-Sovereign Identity Ecosystems

The key dynamic of 'Self-Sovereign Identity' is that it is decentralized versus centralized, achieved through 'DID' open standards. Rather than a single, central database of Identity information users themselves hold, manage and present their own digital credentials, via digital wallets such as Evernym's Connect.me.

This mirrors the physical world, where users carry their credential documents like their drivers licence in their wallet.

Furthermore programs like Alberta's then localize this collaboration, providing a community vehicle for participants to zero in on the specific use cases they want to digitally enable through SSI, such as how local Telecomms, Government, Healthcare and Insurance organizations might interoperate to facilitate shared business processes.

Transforming Canadian Education through the Blockchain and Self Sovereign Identity

The building block of digital identity ecosystems are ‘verifiable credentials‘ and Education is an ideal sector for illustrating their practical application.

Our school diplomas and university degrees are credentials that every one can easily relate to and understand the societal value of, and with the rise in fake certificate fraud an obvious demonstrator of the need for the assured integrity of these documents.

Hence this is a keynote use case for Self Sovereign Identity.

Digital Certificates and Badges

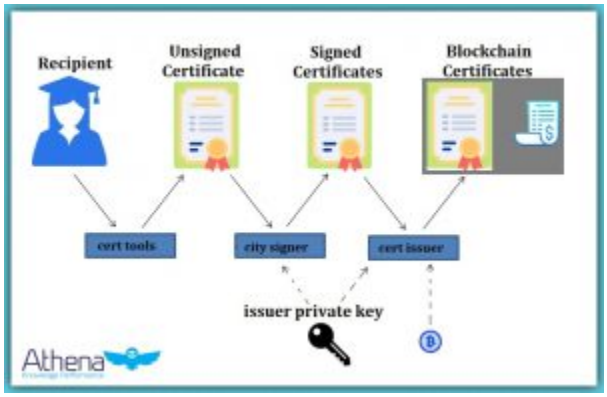
The role and value of digital certification in today’s modern world can most simply be described visually:

This example highlights their immediate value to employment, how they can be modular and very specific to workplace roles – an AWS Solution Architect is a very well defined function, and not only does the digital certificate validate the required skills have been achieved but they can also be used to socially promote the fact we have them, increasing our chances of securing such a job.

Transforming Canadian Education through the Blockchain and Self Sovereign Identity

Blockchain

The purpose of introducing the Blockchain into the mix is to add another layer to enhance the validation aspect of this, ensuring the authenticity of certificates and badges.



The types of innovation that seem to be focusing on this type of use case include 'Blockcerts', an open source blockchain project for enabling a Universal Verifier that will verify any Blockcert issued by any institution, anywhere in the world.

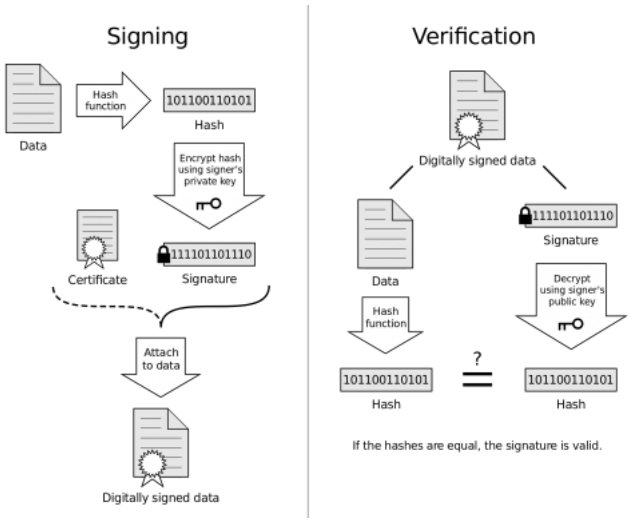
Via their Medium article UniversaBlockchain explore the scenario of Blockchain in Education.

They highlight keynote problems like the high rates of medical school diploma falsification as pain points a technology like Blockchain is ideal for tackling in some form, among a wave of other transformative benefits for the sector as it ripples through all workflow areas related to HR, resume checking, et al.

Athena builds on this some, notably detailing the core signature process that underpins the integrity of the record, as a comparison to traditional paper-based approaches:

Transforming Canadian Education through the Blockchain and Self Sovereign Identity

- Blockchain-enabled digital certificates are immutable and cannot be forged
- The records are stored on a distributed ledger, hence certificates can be only evaluated by anyone who has access to the blockchain
- Since the records are stored in a shared distributed ledger, the certificate can still be validated even if the organization that had issued it no longer exists
- The digital certificates stored in the ledger can only be destroyed if all the copies in every system are destroyed.



In his Medium blog Timothy Ruff provides an excellent, detailed summary of this interconnected ecosystem will begin to take shape with SSI as the keystone foundation.

Transforming Canadian Education through the Blockchain and Self Sovereign Identity

He explains how:

- Organizations like the T3 Innovation Network, within the U.S. Chamber of Commerce, are developing Learning and Employment Records, powered by the same VC standards and technologies that enable self-sovereign student ID, with the same issue, hold, verify model to/from an SSI wallet, which they call a "learner wallet" for simplicity.
- This will help reduce and eliminate student fraud. Once organizations realize they can receive cryptographic proof directly from the student, they can lessen their reliance on passwords, social security numbers, and other personal information.

Digitary – Power to the People

Digitary is a vendor specializing in combining SSI with digital certification, and offers a suite of features for managing academic credentials and digital badges.

As this news highlights one of the first customers to harness this capability is the Association of the Registrars of the Universities and Colleges of Canada (ARUCC), choosing Digitary as the solution provider for the Made for Canada National Network. This has been followed by launching 'MyCreds', a national, bilingual credential wallet supported by a comprehensive website for Canada's post-secondary community and learners.

This initiative means the Canadian higher education community is creating the very first online platform and national credential wallet for post-secondary learners. Once fully operational, the Network will enable 3 million learners across the country to access and share their official digitized post-secondary transcripts and credentials online – anytime, anywhere.

As CTO Takis Diakoumis writes:

Transforming Canadian Education through the Blockchain and Self Sovereign Identity

"Portable learner credentials and the ability to securely assert claims to knowledge is the key enabler in ensuring this freedom of movement across places of learning and work. In exploring the next sustainable ecosystem for learners, we begin to note the technological evolution of self-sovereignty and the broader reimagination of our digital identity."

"SSI enables the sharing of data in a new, controlled and trusted way, a way where no one can take it away or switch it off. A new foundational connection between institutions and learners is formed where we can completely reimagine the learner relationship, for life. The enormous impact is beyond any one sector. It is about human connections and digital trust; about how we relate to the world around us and where learners become the cornerstone of the next digital revolution."

A New Paradigm for Education

The impact of this technology will go far beyond simply securing the integrity of the issued certificates, it will provide a foundation for the wholesale transformation of how education is provided. This Cointelegraph article explores the nature and details of this transformation.

Blockchain and Digital Credential experts Christopher Allen and Kim Hamilton Duffy explain how a key trend is 'personal data agency' – To date academic credentials like degrees and transcripts are held centrally, and individuals must navigate a number of challenges and approvals to obtain access to and share them for employment purposes.

They can also be changed, deleted and shared without consent or knowledge of the individuals, and so the advent of the Blockchain era will see users take direct control and ownership of their records, and via technologies that ensure their integrity. This would be hugely impactful in scenarios like immigration, where an increasing number of migrants that either have lost their credentials or for whom it is impossible to tell if their documents are valid.

This will enable a "peer to peer" approach to learning. Christopher Allen highlights:

> "This makes it possible for there to be P2P [peer-to-peer] competency credentials, from fellow students, teachers, co-workers, clients, contractors, employers — not just educational institutions."

In other words not only can a single individual be the teacher providing the education but also the 'institution' certifying the student has learned the skill accordingly. Their own reputation as an expert in the field would underpin its' legitimacy.