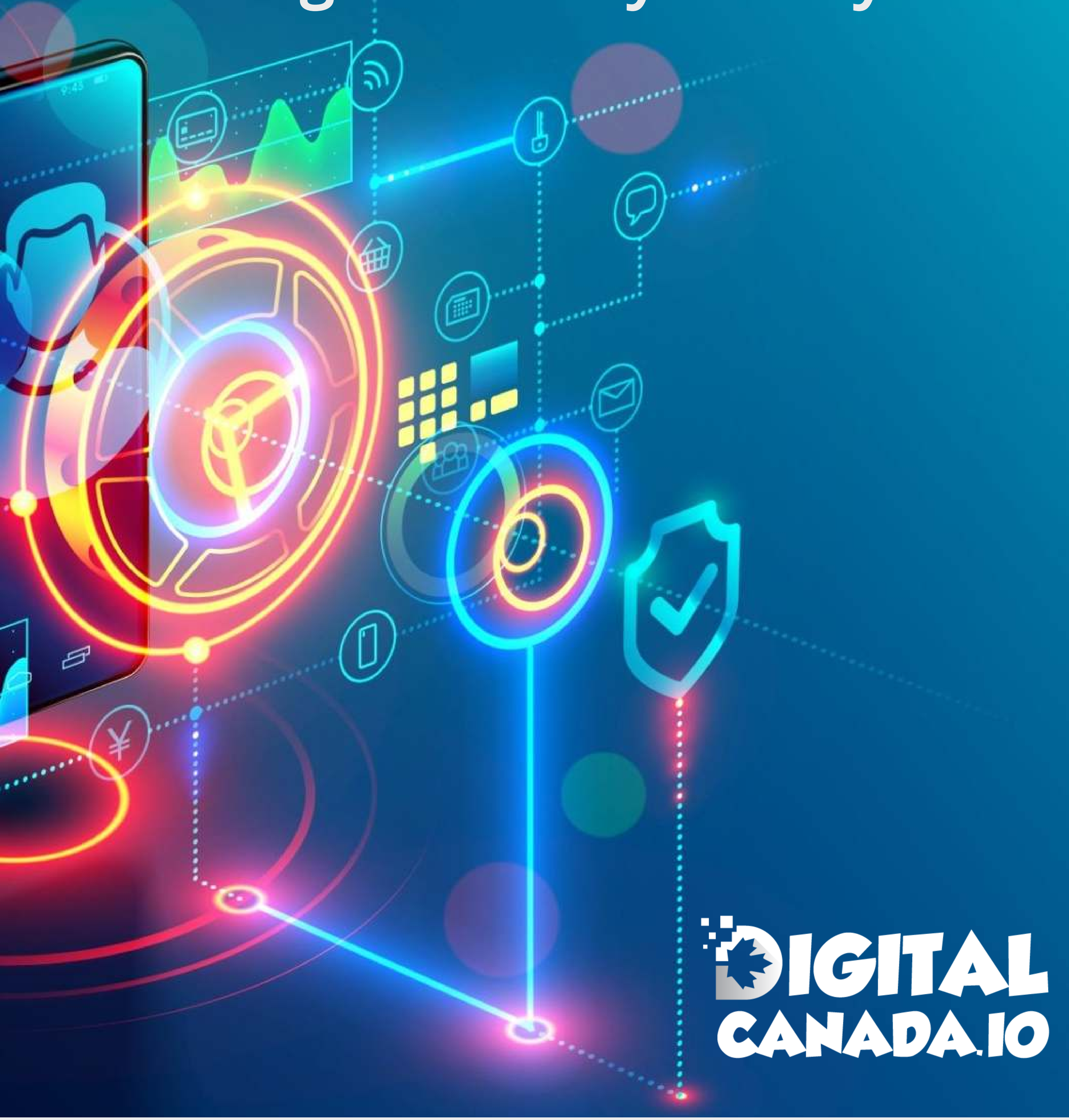
Building the Canadian Digital Identity Metasystem



DigitalCanada.ID

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 in 2006:

> The Identity Metasystem is an interoperable architecture for digital identity that assumes people will have several digital identities based on multiple underlying technologies, implementations, and providers.

Building the Canadian Identity Metasystem

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.

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:

> 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.

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

Digital Government Roadmap 2025

The keystone foundation for a digital nation is the online capability of the government – ‘Digital Government’.

With regards to the goal of Canada becoming the world’s leading digital nation, it is especially pertinent to highlight that as they reported in 2004, the nation **led as the world’s number one** at that time, in the field of E-Government, the precursor to Digital Government.

To regain this leadership position 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.

What is Self Sovereign Identity?

The critical role of Identity is easy to quantify – It is the keystone technology required to achieve the described ‘unified login system’.

Government programs like Gov.UK Verify are the early steps to better join up government systems via Identity as the common mechanism, so that access to online government services is much smoother and quicker.

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

Self-Sovereign Identity (SSI) is the cutting edge 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.

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, highlighting 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'.

The Decentralized Identity Metasystem

The profound impact the technology will have goes well beyond just public sector IT systems, it represents the most significant evolution of the Internet since DNS, enabling a similar global addressing system but for people and their data. In the same way DNS is implemented through a system of registrars and administered via ICANN, so a similar system will be grown to scale and manage a global network of decentralized identities.

The growing adoption of SSI will form what visionary Phil Windley describes as an "Identity Metasystem", a global addressing system akin to what DNS facilitates for web domains but for user data, with the required governance administered by the Sovrin network.

In essence it represents a wholesale 'upgrade' to the Internet itself, such that these powerful features are built right into it, in the same way HTTP is the common protocol for sharing web information. For example as Namecoin describes the DNS is the current backbone identity system, it translates domain names into IP addresses. It works very effectively but it's really quite an old technology and thus is ideal for this type of upgrade.

Brave New Coin writes about how it will enable what the whole Internet has been calling for, entirely user-centric data portability.

Users want the same frictionless experience and control of how their data is used with each and every organization they interact with, from governments through social media sites. An Identity Metasystem will achieve this through a generalized evolution of the Internet to this end.

The Paypers reports on Identity experts defining this as a new layer of the Internet:

"The current Open Systems Interconnection model (OSI) of the internet stack has 7 layers, 1) Physical, 2) Data Link, 3) Network, 4) Transport, 5) Session, 6) Presentation and then 7) Application. SSI technologies are so fundamentally new that they create a whole new layer just for individuals and users — this is called Layer 8. In this layer, identifiers are managed and owned by individuals and companies. Verifiable credentials can be issued to the identifiers, which can then be shared with any number of services they might interact with."

Key open standards include the W3C's 'DID' specification: Decentralized Identifiers, explained in this Evernym webinar.

> At a superficial level, a **decentralized identifier** (**DID**) is simply a new type of globally unique identifier. But at a deeper level, DIDs are the core component of an entirely new layer of decentralized digital identity and public key infrastructure (PKI) for the Internet.

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*.

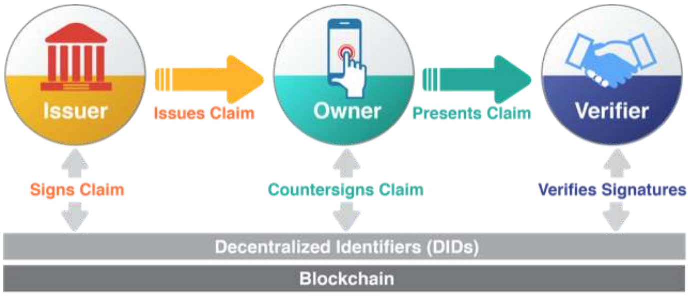
In particular, at 6m50s he describes how the Indian identity scheme 'Aadhaar', a centralized government program, violates over a decade of first-world Identity best practices, with few laws against profiling, discrimination and abuse by law enforcement.

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.

Blockstack offers this proposed definition of Blockchain Identity: *A blockchain identity (or blockchain ID) is a generic term used to refer to any identity on the blockchain. Users can have one blockchain identity or many and can register them just like one would register domain names or accounts on Facebook or Twitter.*

In his blog Paul Payam Almasi describes the key relationship to and the role the Blockchain will play, noting a key industry insight:

"As cryptocurrency exchanges like Binance and Coinbase begin to onboard more and more users, they will have the incredible luxury of linking someone's off chain identity with their blockchain identity. This creates a perfect onramp towards a self sovereign identity model."



In their guide SearchSecurity highlights:

“In all models of identity management, a digital identity requires identifiers, which ensure the user is who they say they are. However, with self-sovereign identity, identifiers do not need an intermediary. This means that a user’s self-sovereign identity can be registered to a claim, such as a block on a 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.

ACE

Led by visionary Mike Brown they are building ‘ACE’, the Alberta Credential Ecosystem, a local collaboration of organizations beginning to adopt SSI and achieve integrated services through sharing SSI credentials.

BC Orgbook

British Columbia’s OrgBook 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.

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

BLOCKCHAIN REVOLUTION
HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD
DON TAPSCOTT
and ALEX TAPSCOTT

Leading Canada's Blockchain Revolution

Don Tapscott is the original Digital Economy guru, literally writing the book. Fast forward twenty five years and Don is still charting the future, a path that could lead Canada to becoming the world's leading digital nation.

In 2016 Don published the Blockchain Revolution, describing how this technology innovation represents nothing less than the second generation of the internet and holds the potential to transform money, business, government and society.

These exemplar case studies demonstrate how Canada not only has the vision but also the engineering capability to pioneer this staggering level of digital transformation and 'Lead Canada's Blockchain Revolution'.

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, 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.

The EU has published research reports and explanatory videos to encourage widespread take up. As New Yorker magazine highlights describing Estonia as the Digital Republic:

"They do so through the "once only" policy, which dictates that no single piece of information should be entered twice. Instead of having to "prepare" a loan application, applicants have their data—income, debt, savings—pulled from elsewhere in the system. There's nothing to fill out in doctors' waiting rooms, because physicians can access their patients' medical histories."

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.

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

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

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.

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.

Alberta
Credentials
Ecosystem

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.

Building a Local Identity Ecosystem

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

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.

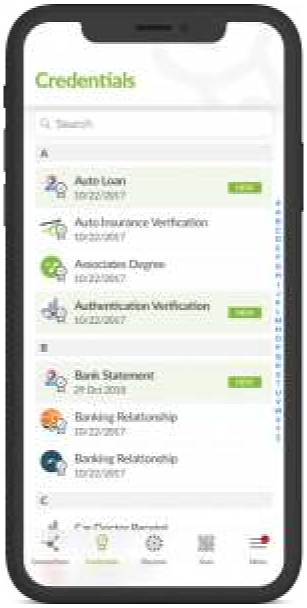
ACE : Building Localized Self-Sovereign Identity Ecosystems

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.



Credentials

Search

A

Auto Loan
10/22/2017 NEW

Auto Insurance Verification
10/22/2017

Associates Degree
10/22/2017

Authentication Verification
10/22/2017 NEW

B

Bank Statement
29 Oct 2018 NEW

Banking Relationship
10/22/2017

Banking Relationship
10/22/2017

C

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.

PCTF

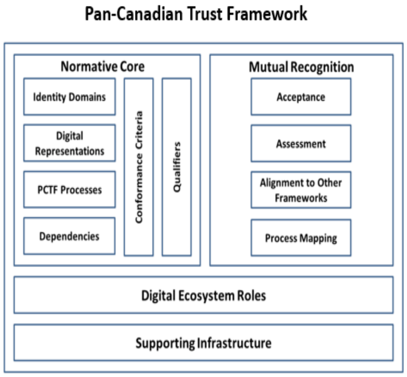
In this learning lesson Tim Bouma, Senior Policy Analyst Identity Management for the Canadian Government, shares an overview of the PCTF: Pan-Canadian Trust Framework.

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.

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.


Pan-Canadian Trust Framework
Normative Core
Identity Domains
Digital Representations
PCTF Processes
Dependencies
Conformance Criteria
Qualifiers
Mutual Recognition
Acceptance
Assessment
Alignment to Other Frameworks
Process Mapping
Digital Ecosystem Roles
Supporting Infrastructure