Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Canada

Canadian Digital Identity

Prepared for 2018 International Identity Summit
Seattle, Washington

Ken McMillan

August 2018

Draft v0.8

Background

Focus on digital government

In February 2018, Canada joined the Digital 7, a group of the most digitally-advanced countries in the world whose mission is to harness digital technology for the benefit of citizens.

D7
NEW ZEALAND

In July 2018, The Honourable Scott Brison was appointed Minister of Digital Government, in addition to his existing appointment as President of the Treasury Board.

In July 2018, Alex Benay, the current Chief Information Officer of the Government of Canada, was elevated to a deputy minister-level position to support the Honourable Scott Brison in his new role as Minister of Digital Government.

The Government of Canada is making digital government a priority

Digital identity

What is it?

***Trusted digital identity** is an electronic equivalent of who you are as a real person, used exclusively by you, to receive valued services and to carry out transactions with trust and confidence.*

Digital Identity confirms that ‘you are who you say you are’ in an online context.

Why does it matter?

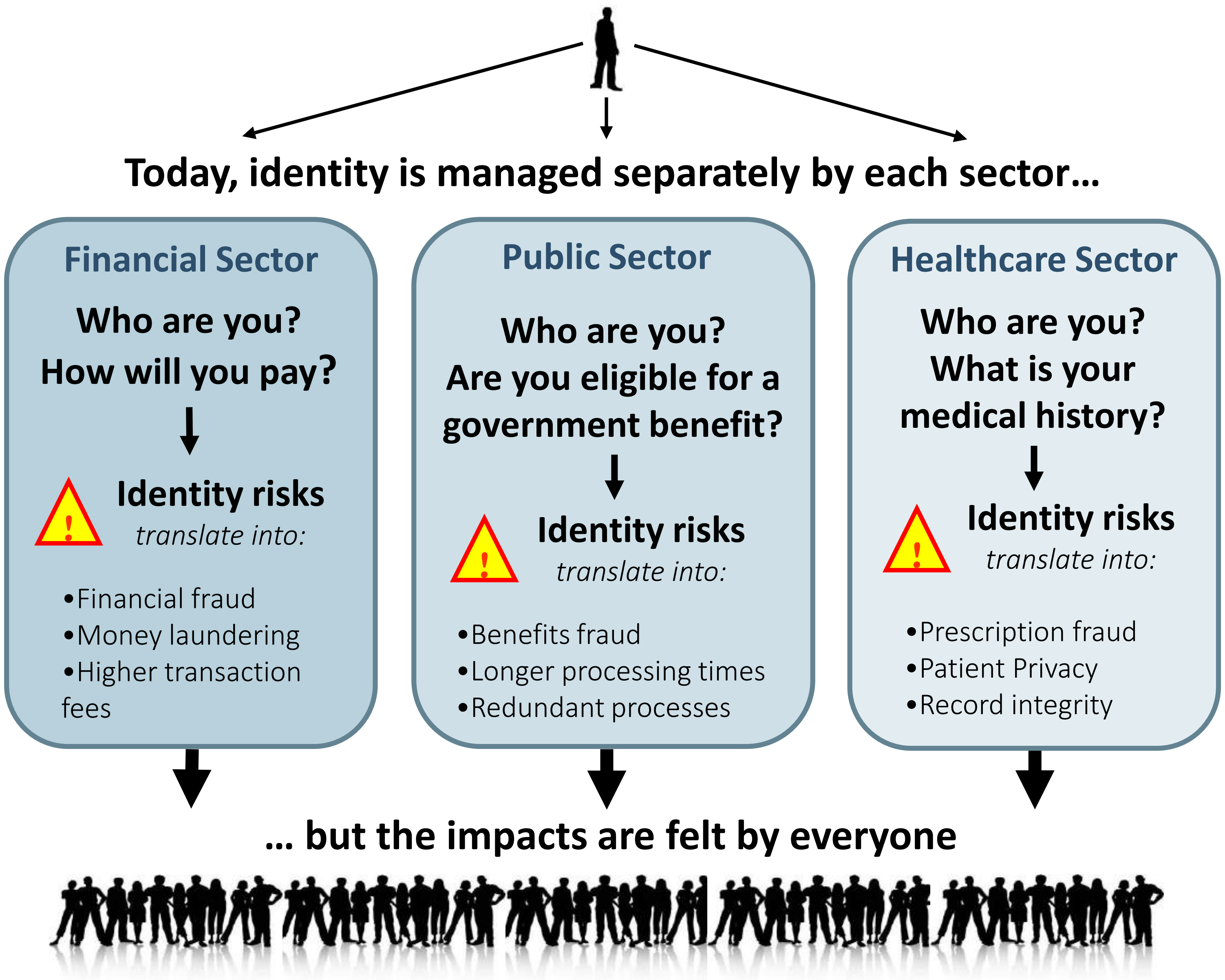
Digital Identity is the foundation to moving more services online, where our citizens expect to be.

What (many of) you are up to:

Country	Program	Details
Estonia	National ID Card	• **Mandatory**, centralized state administered, single ID number, issued card used for electronic authentication
Denmark	NemID	• **Mandatory** national electronic ID and digital signature infrastructure developed in cooperation with the banking sector, operated by a private provider for the government and Danish banks.
United Kingdom	Gov.UK Verify	• **Voluntary**, certified private companies, built and maintained by GDS, approx. (4M uptake, expected 25M) • Policy authority recently moved from Cabinet office.
India	UIDAI (Aadhaar)	• **Mandatory**, centralized state administered, single ID number, 120M issued, biometric authentication
New Zealand	RealMe	• **Voluntary**, state administered (NZ DIA, Electronic Verification Act), username/password • In operation (uptake 250K reported in January 2017)
Australia	Trusted Digital Identity	• **Voluntary(tbc),** federally administered (AUS DTA), • Beta recently announced
European Union	eIDAS	• **Regulation** set of standards for the European Single Market (in force September 2014) • Private sector "Trust services market" is still immature; confusion with public sector services

"Only 3% [of countries] have foundational ID schemes that can be used to access a collection of online and offline services."
WORKING PAPER Digital Identity: the current state of affairs, BBVA Research [2018]

Current Canadian Challenges



Today, identity is managed separately by each sector…

Financial Sector

Who are you?
How will you pay?

Identity risks *translate into:*

- Financial fraud
- Money laundering
- Higher transaction fees

Public Sector

Who are you?
Are you eligible for a government benefit?

Identity risks *translate into:*

- Benefits fraud
- Longer processing times
- Redundant processes

Healthcare Sector

Who are you?
What is your medical history?

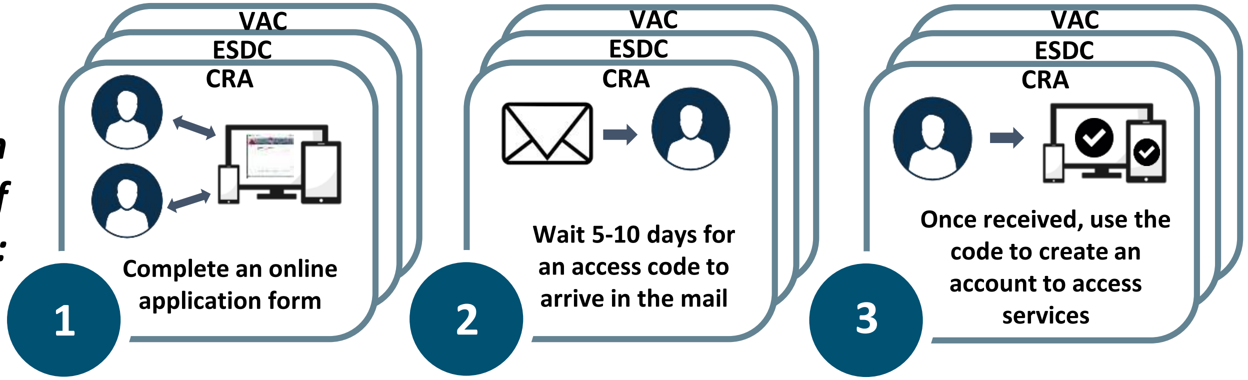
Identity risks *translate into:*

- Prescription fraud
- Patient Privacy
- Record integrity

… but the impacts are felt by everyone

Current Government of Canada Challenges

For each Government of Canada service:



VAC
ESDC
CRA

1
Complete an online application form

VAC
ESDC
CRA

2
Wait 5-10 days for an access code to arrive in the mail

VAC
ESDC
CRA

3
Once received, use the code to create an account to access services

- Canadians see the government as a single entity, but are forced to have separate and varying interactions with each department and agency to access services
- The process to apply for and/or access services is often not intuitive, convenient, accessible or user-friendly for Canadians, requiring separate accounts for each service and multiple usernames and passwords
- There is a lack of communication and information standardization between jurisdictions to support seamless service delivery for Canadians

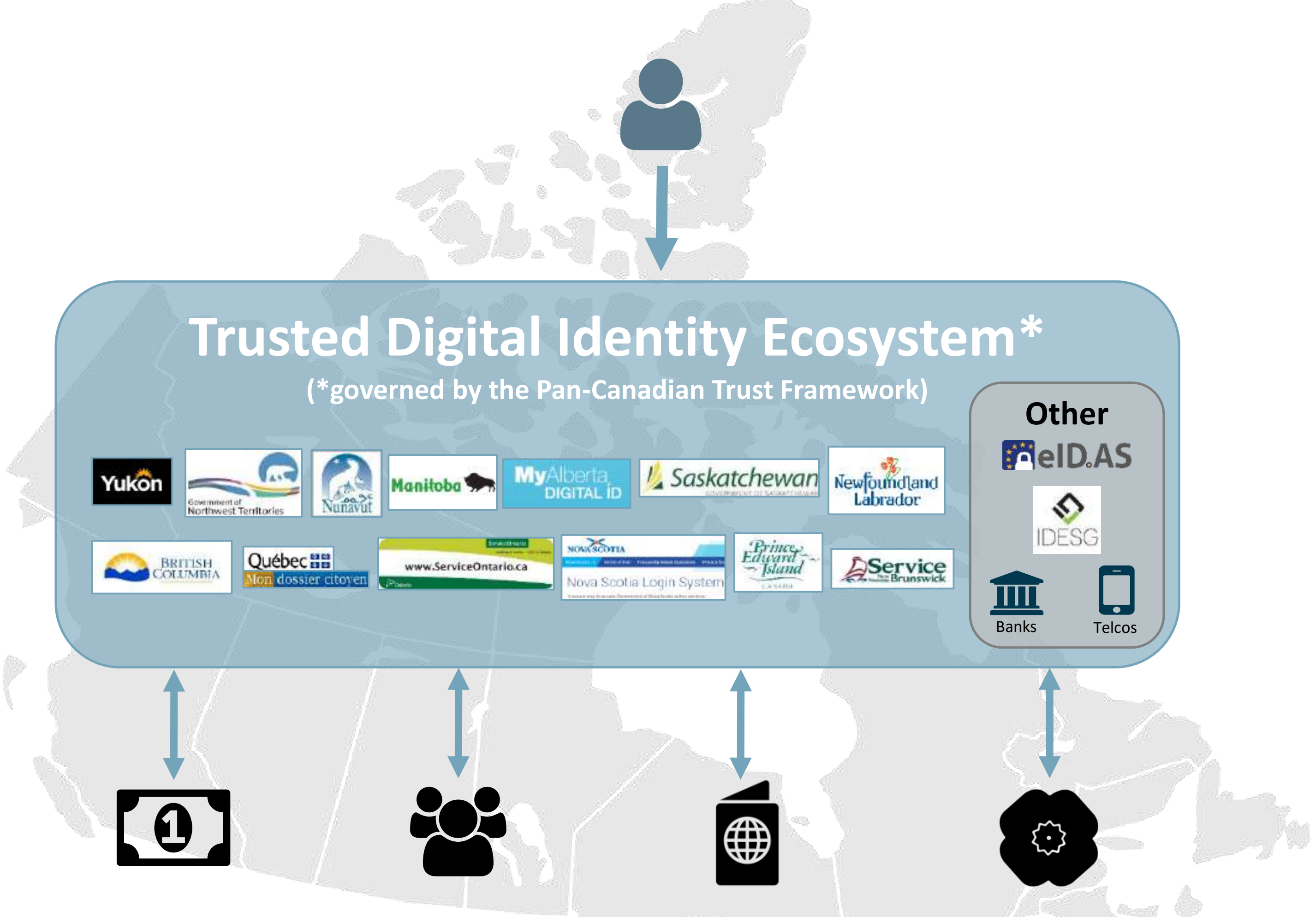
Drivers for Digital Identity

There are a number of key drivers for adopting a pan-Canadian approach to digital identity:

1. **Citizen expectations –** Canadians want convenient, quick and reliable access to government programs and services, such as only having to provide their personal information once or only when necessary, with consent
2. **Security –** The threat environment is evolving and becoming increasingly sophisticated, requiring proactive protection strategies
3. **Privacy –** Canadians place a high value on privacy and want to know about and provide consent to the use and disclosure of their personal information
4. **Service Delivery –** Canadians expect seamless service delivery regardless of which department or agency is delivering it
5. **Technology –** Adoption of new technologies and migration to common and shared services drives the need for a streamlined and common approach to digital identity

Canada’s Approach

Approach to trusted digital identity



Trusted Digital Identity Ecosystem*

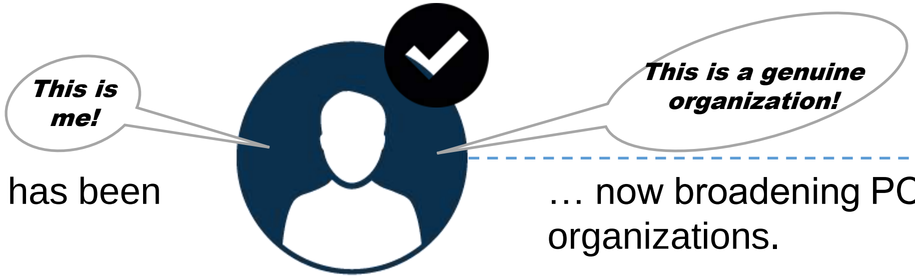
(*governed by the Pan-Canadian Trust Framework)

Other

The federal government vision is to build a federated, digital identity ecosystem where trusted digital identities are used to deliver services in a seamless manner on any platform, with any partner, on any device.

What is the Pan-Canadian Trust Framework?

Trusted Digital Identity



Initial PCTF focus has been individuals…

… now broadening PCTF focus to organizations.

PT Pilots

Is it the same person?

Verified Login ✓

Is it a real existing person?

Verified Person

Is it you providing your personal identity information?

Confirmation, Binding, Notice and Consent

VO Pilots

Is it a real organization?

Verified Organization

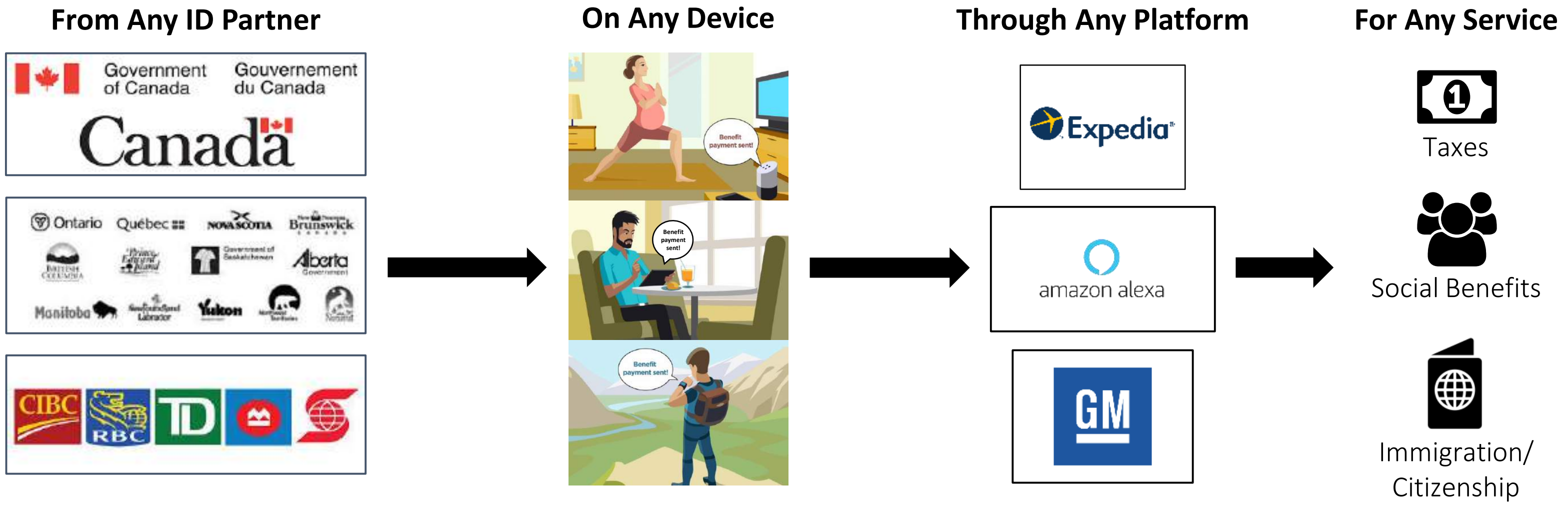
Pan-Canadian Trusted Infrastructure Component

Security, Privacy, User Experience, Communications

The Pan-Canadian Trust Framework is a set of standards and specifications to ensure that all jurisdictions abide by a common, agreed-upon set of rules to trust and accept each other's digital identities.

Destination user experience for Canadians

A trusted digital identity…



From Any ID Partner

On Any Device

Through Any Platform

For Any Service

Taxes

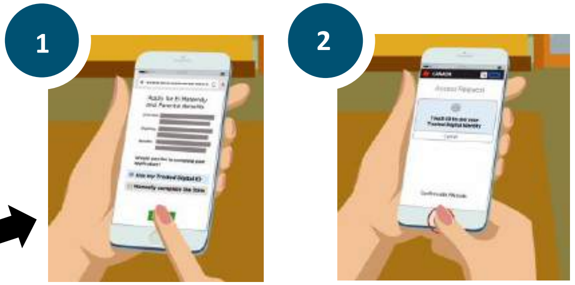
Social Benefits

Immigration/ Citizenship

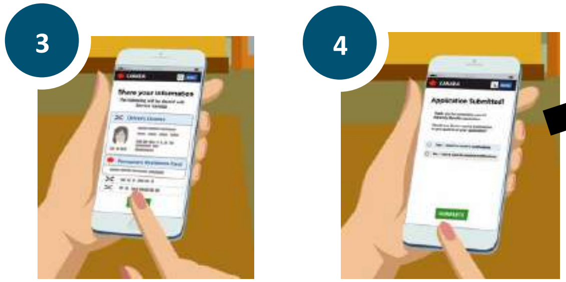
- Canadians can sign in once using their trusted digital identity to instantly access services across departments and across jurisdictions on any device
- There is no single point of failure as the digital identity ecosystem is federated across jurisdictions with Canadians being able to use their trusted digital identity to access services
- The digital identity ecosystem can be leveraged by any partner, such as other departments, provinces or territories, banks, etc. to validate/verify the identities of their clients

Digital identity use case: applying for benefits

Emily is having a baby soon and is applying for benefits. What if she could do all this at once from any device?



She'd start her application by confirming who she is using her Nova Scotia trusted digital ID.



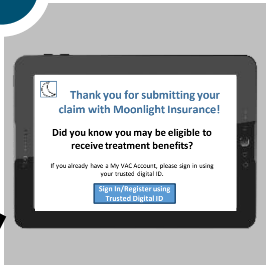
Then she'd consent to using personal information from her digital ID to complete the application.

Once her application is approved, Emily would be notified via her virtual assistance that the benefit payment has been sent to her bank account.

Digital identity use case: submitting a claim for veteran treatment benefits

Mohammed is a veteran and he is submitting a medical claim to his insurance company. He is told that he may be eligible to receive treatment benefits from Veterans Affairs and is given the option to Sign-In/Register with his Trusted Digital ID.

1

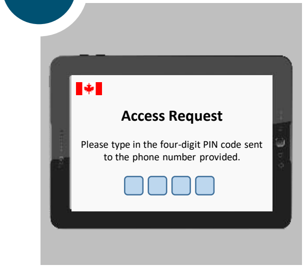


Thank you for submitting your claim with Moonlight Insurance!

Did you know you may be eligible to receive treatment benefits?

If you already have a My VAC Account, please sign in using your trusted digital ID.

2

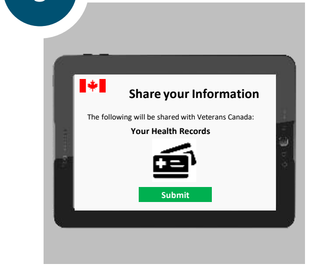


Access Request

Please type in the four-digit PIN code sent to the phone number provided.

He knows he is eligible for this benefit due to an injury he sustained while on active duty. He proceeds to sign in using his Québec Mon Dossier Citoyen digital ID and confirm his identity.

3

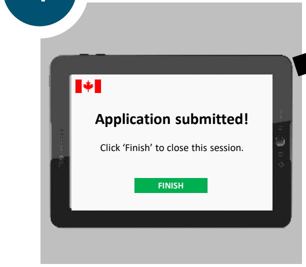


Share your Information

The following will be shared with Veterans Canada:

Your Health Records

4



Application submitted!

Click 'Finish' to close this session.

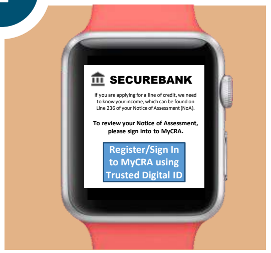
Then he consents to sharing his personal health records from his digital ID with Veterans Affairs to claim his treatment benefits.

Once his treatment benefits claim is approved, Mohammed is notified via a push notification on his tablet that the benefit payment has been sent to his bank account.

Digital identity use case: applying for a line of credit

Francois is applying for a line of credit from his bank and he needs to provide his income. He is told he can do this by obtaining a Proof of Income from CRA and he is given the option to Register/Sign-In using his Trusted Digital ID.

1

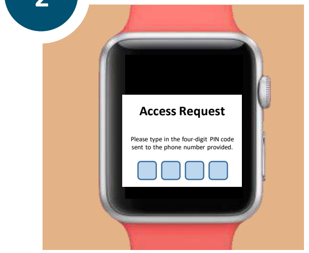


SECUREBANK

If you are applying for a line of credit, we need to know your income, which can be found on Line 236 of your Notice of Assessment (NoA).

To review your Notice of Assessment, please sign into to MyCRA.

2



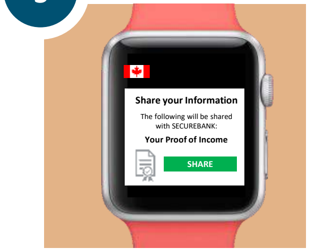
Access Request

Please type in the four-digit PIN code sent to the phone number provided.

□ □ □ □

He proceeds to sign in using his SECUREBANK trusted digital ID, confirm his identity and obtain a Proof of Income from CRA, which he chooses to store in his digital ID for future use.

3

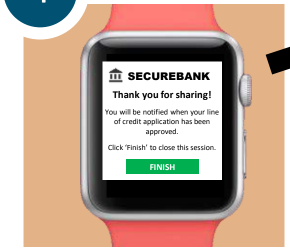


Share your Information

The following will be shared with SECUREBANK:

Your Proof of Income

4



SECUREBANK

Thank you for sharing!

You will be notified when your line of credit application has been approved.

Click 'Finish' to close this session.

Then he consents to sharing the Proof of Income he stored in his digital ID with his bank.

If everything checks out, Francois is notified by the bank on his smart watch that his application for a line of credit has been approved.

Current Projects/Pilots

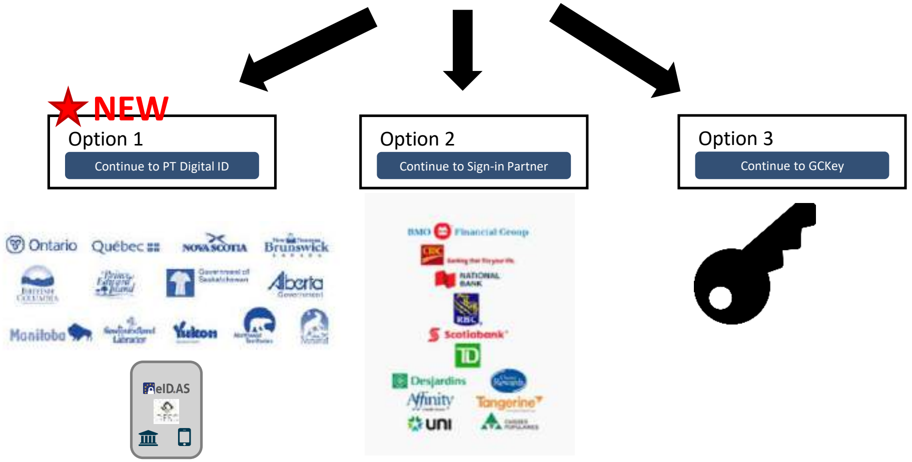
Provincial proof-of-concept

The success of our first PT pilot will allow other jurisdictions to have their digital identities accepted and used by the federal government.

Timeline: October 2018, other jurisdictions to follow

Emily navigates to the landing page for My Service Canada Account (MSCA).

She chooses to sign in to her MSCA and is presented with the two original sign-in options and **a new one, a provincial or territorial Digital ID:**



NEW

Option 1

Continue to PT Digital ID

Option 2

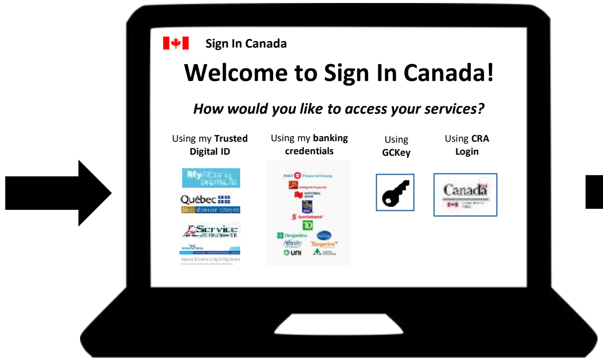
Continue to Sign-in Partner

Option 3

Continue to GCKey

Sign In Canada

Mohammed navigates to the landing page for Sign In Canada acceptance platform.



Sign In Canada

Welcome to Sign In Canada!

How would you like to access your services?

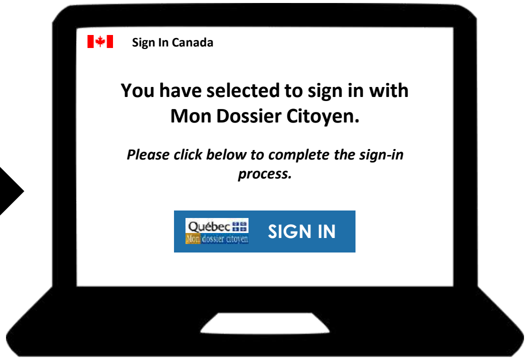
Using my **Trusted Digital ID**

Using my **banking credentials**

Using **GCKey**

Using **CRA Login**

He is presented with many sign-in choices.



Sign In Canada

You have selected to sign in with Mon Dossier Citoyen.

Please click below to complete the sign-in process.

He is a resident of Québec so he chooses to sign in with his Mon Dossier Citoyen digital identity.

Sign In Canada enables the “Tell Us Once” principle. It provides the common access point through which verified individuals can quickly and securely access services using their trusted digital identity.

Timeline: Contract award in Spring/Summer 2019; implementation in Fall/Winter 2019

Collaboration with Banks

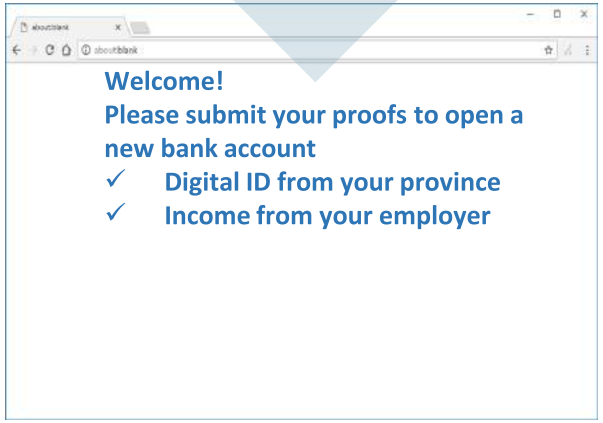
Working with banks to pilot the use of a trusted digital ID to streamline the process of opening a bank account.

This will reduce a citizen's wait time to open a bank account, lower the risk of fraud and lessen the burden on banks.

Timeline: TBC (dependent on amended regulations)

Opening a new account: From 40 minute in-person paper-based process…

…to a 40 second higher assurance digital process leveraging provincial Digital ID



Welcome!
Please submit your proofs to open a new bank account

- ✓ **Digital ID from your province**
- ✓ **Income from your employer**

Sum it up

Current Context and Challenges

Context

- The federal government's work in identity management dates back to 2008 with the launch of the Cyber Authentication Renewal Initiative; which led to the current mandatory service in use today (GCKey and bank credential login)
- Since then, the federal government has solidified its policy position on identity via:
  - *Directive on Identity Management (2009, updated again in 2017)*
  - *Guideline on Defining Authentication Requirements (2012)*
  - *Standard on Identity and Credential Assurance (2013, with supporting guideline in 2015)*
  - *Draft Pan-Canadian Trust Framework (2016)*

Challenges

- While the credential service in place today allows for a common sign-in to federal government services, programs must still conduct manual identity-proofing processes before a citizen can gain access
- Consuming trusted digital identities will reduce this burden, but there is a marked under-capacity within the collective governments to evolve the current solution into a digital identity ecosystem
- At their current bench strengths and levels of coordination, our governments can conduct pilots between individual jurisdictions and departments (e.g. using a provincial digital ID to use a federal department's services), but still need to develop the capability-maturity to scale and sustain at enterprise levels

Want to know more?

Ken.McMillan@tbs-sct.gc.ca
Director, Digital Identity
Cybersecurity