Sign In Canada and Digital Identity

Update for:
ADM Service And Federating Identity Committee

August 26, 2020

Po Tea-Duncan

A/Executive Director, Cyber Security

Office of the Chief Information Officer

Digital Identity

What is it?

*A **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.*

Trusted 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.

Canada's Digital Identity Vision

The Government of Canada is building a digital identity ecosystem for the nation...

...to be leveraged by all GC departments and agencies, other jurisdictions in Canada (provinces, territories, municipalities) and Canadian partners (private sector & other countries)...

Other

Academia   Banks

Local Gov't   Telcos
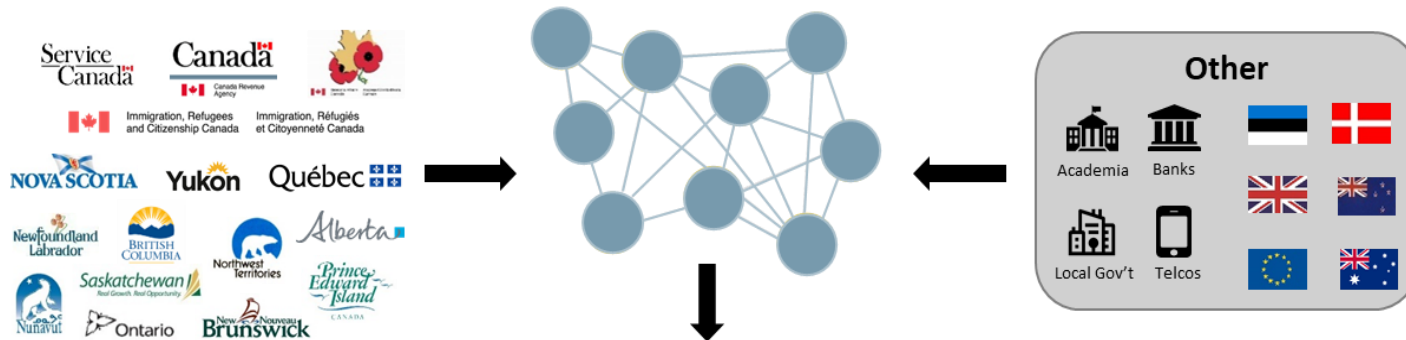
...to deliver services and issue digital identities to Canadians...
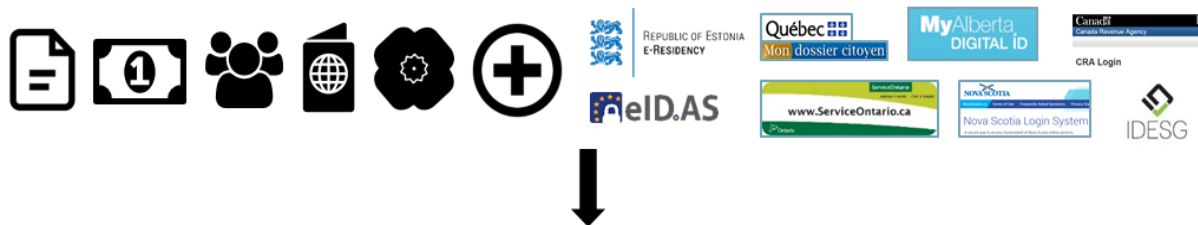
...so they can access services seamlessly, anytime, anywhere and on any device.

Today's GC Cyber Authentication Solution

- In operation since 2012, enables clients to sign-in to >100 GC services

- Consists of two managed (contracted) services:
  - **GCKey**, which is the GC-branded credential
  - **Credential Broker Service**, enables login via 16 Canadian banks

- Enterprise service is mandatory for online applications offered to the public for which authentication (sign-in) is required

- Uses 'anonymous' credentials (i.e. not bound to identity)

- Once signed in, users enroll with programs individually
  - Identity process is in program space

- Each dept/agency maintains own chooser page and integrate with each credential provider separately

Credential count at end of June 2020:

12.2 million GCKeys and
*9.6 million bank credentials*

Evolution: Sign In Canada

- Provides a common chooser screen for all GC applications

- Improves user experience

- Continues to accept current anonymous credentials (GCKey and Banks)

- Ensures continued access to GC services

- Enables acceptance of trusted digital identities

- Supports interoperability with other jurisdictions

- Enables clients to switch their credential while preserving program enrolment

- Uses open technology standards (e.g. OAuth, OIDC)

- Enables use of new technology (e.g. digital wallets, verifiable credentials)

# High-level Architecture of Sign In Canada

Current State

- Users can sign in with a GCKey, banking username/password or CRA Login
- Each department/agency must maintain its **own sign in page** (duplication of effort)
- **Inconsistent** user experience
- Digital identities would need to be added department-by-department
- Security concerns with **legacy technology**
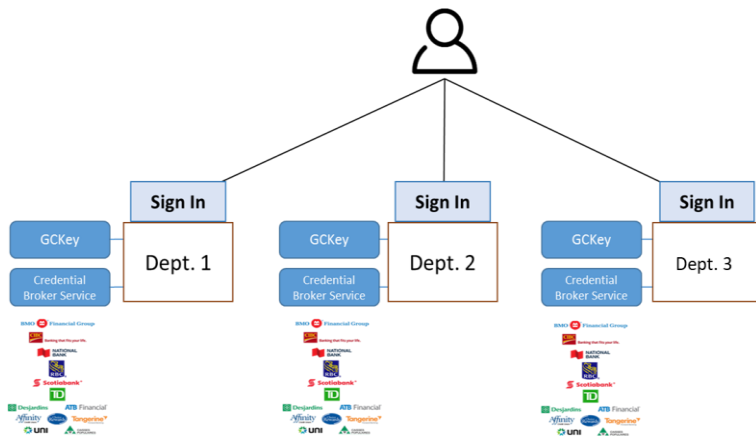
Future State
(endorsed by GC EARB March 2018)

- Enables **use of trusted digital identities** from other jurisdictions
- **Continued support** for existing GCKey and bank credentials
- **Single integration point** for departments and agencies
- **Common sign in page** for consistent user experience
- **Support** for modern tech and **cloud applications**
- Updated **security & privacy** features

7
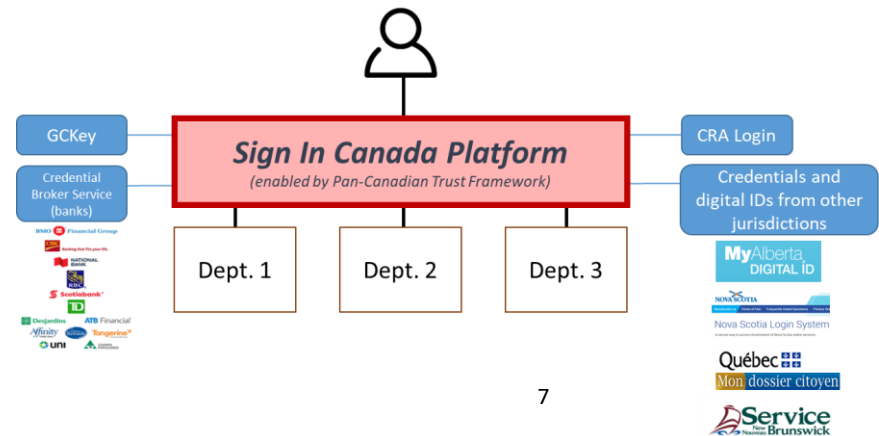
Current Challenges for Canadians

Enrolment process for many GC services*:*

Complete an online application form

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

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

Canadians see government as one entity, but are forced to have separate, varying interactions with departments and agencies to access services

Process to apply/access services not intuitive, convenient, or user-friendly for Canadians, requiring separate accounts multiple usernames and passwords
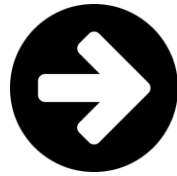
There is a lack of communication between jurisdictions to coordinate seamless service delivery for Canadians

How Sign In Canada Will Work

User navigates to Canada.ca site

Menu of sign in choices is presented
(Eg. Provincial Trusted Digital ID; banking credentials; GCKey; CRA login)

User can access any GC service with a single sign on

Sign In Canada will be the common access point through which Canadians can quickly and securely access GC services using their trusted digital identity

Standardized application of Pan-Canadian Trust Framework ensures consistent protection of personal information and privacy across all jurisdictions

Improved user experience, enabling them to re-use their digital IDs and only provide their personal information once, with consent 8

Sign In Canada Minimal Viable Product (Release 1)

OCIO build of core Sign In Canada product successfully demonstrated:

- Common login screen for all GC services to enhance user experience

- Integration with existing GCKey and banking credentials

- Integration with two provincial Digital Identities (BC and AB)

- Integration with social logins (Microsoft and Google)

- Ability to 'translate' SAML to OIDC so depts/agencies can use new digital IDs without the need to change/upgrade existing applications

- Ability to integrate new cloud-based applications

- Seamless user experience as depts/agencies transition to Sign In Canada (i.e. no need to re-enrol in services)

- Ability for depts/agencies to "customize" list of credentials offered to clients

- Single integration point where depts/agencies can streamline integration with multiple digital ID and credential providers

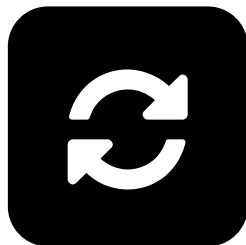- Enables clients to switch their credential while preserving program enrolment

Aug 4 - Sign In Canada in production with GCKey and Credential Broker Service

Benefits

Look/feel continuity for Canadians

Canadians can continue uninterrupted use of existing GCKey and banking credential from a consistent sign-in screen GC-wide
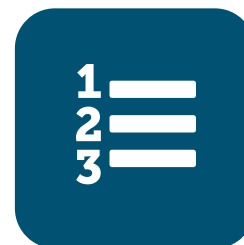
Facilitates credential evolution

GC can evolve GCKey and banking credential quickly via new procurement with minimal transition costs due to central integration point

Single point for provincial integration

Digital IDs from other jurisdictions (e.g. Alberta, BC) can be integrated at one spot and instantly usable by all departments and agencies
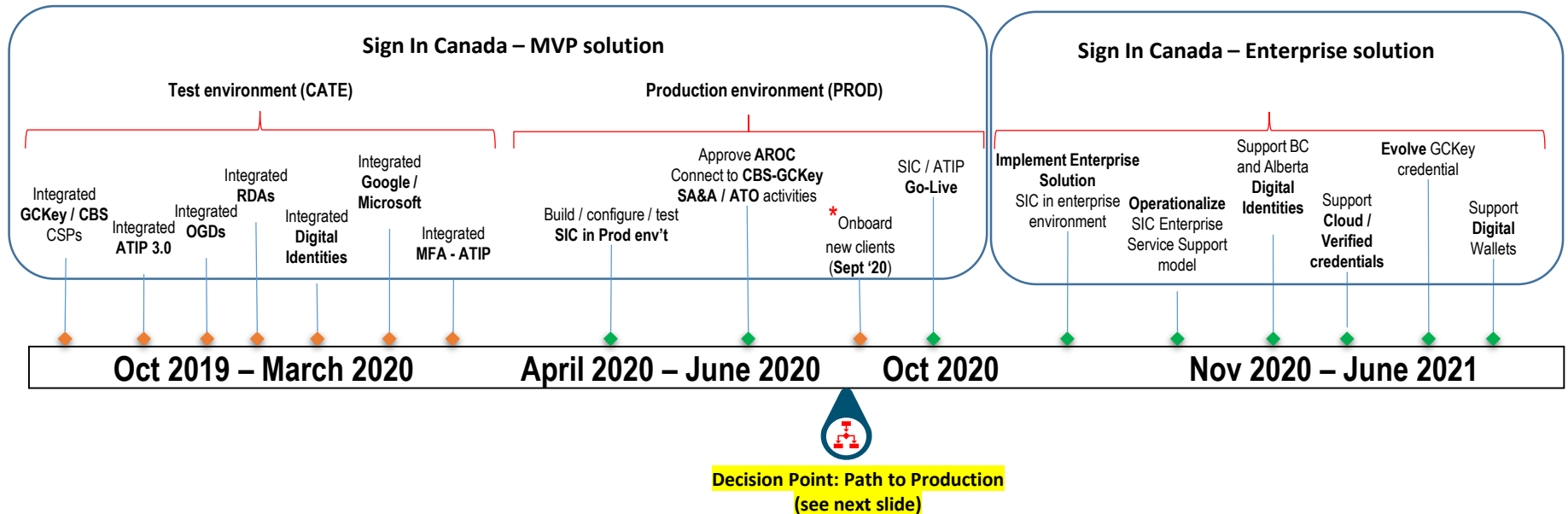
Alignment with Digital Standards

Platform will be built iteratively using open source software, open standards, and in collaboration with departments and users

Sign In Canada is foundational to the OneGC initiative

Proposed Sign In Canada (SIC) Roadmap

Sign In Canada – MVP solution

Test environment (CATE)

- Integrated **GCKey / CBS** CSPs
- Integrated **ATIP 3.0**
- Integrated **OGDs**
- Integrated **RDAs**
- Integrated **Digital Identities**
- Integrated **Google / Microsoft**
- Integrated **MFA - ATIP**

Production environment (PROD)

- Build / configure / test **SIC in Prod env't**
- Approve **AROC** Connect to **CBS-GCKey** **SA&A / ATO** activities
- * Onboard new clients **(Sept '20)**
- **SIC / ATIP** Go-Live

Sign In Canada – Enterprise solution

- **Implement Enterprise Solution** SIC in enterprise environment
- **Operationalize** SIC Enterprise Service Support model
- Support BC and Alberta **Digital Identities**
- Support **Cloud / Verified credentials**
- **Evolve** GCKey credential
- Support **Digital Wallets**

Oct 2019 – March 2020	April 2020 – June 2020	Oct 2020	Nov 2020 – June 2021

Decision Point: Path to Production (see next slide)

Legend
- ◆ Client onboardings
- ◆ Product Milestones

GCKey = GC Branded Credential

CBS = Credential Broker Service (e.g. Banking credentials)

OGDs = Other Gov't Dept.'s integrated in the Test env't include: TC, IRCC, IRB, CRA, ESDC, ISED, etc.

RDAs = Regional Development Agencies integrated in the Test env't include: FedDev Ontario, WED

Digital Identities = My Alberta Digital Identity (MADI) and BC Services Card

* Departments have expressed interest in onboarding into new Sign in Canada Platform including IRB, FCAC, CCCS, CRA, etc.

Annex

Additional Context

- Federal/Provincial/Territories (FPT) Deputy Minister (DM) Table on Service Delivery Collaboration deemed digital identity a top priority

- Pan-Canadian commitment made to establishing a federation of digital identities under the Whitehorse Declaration (signed by Joint Councils in February 2019)

- Ongoing international collaboration (Digital Nations, World Bank, etc.) with goal of mutual recognition of digital identity

- Completed assessment of My Alberta Digital ID against Pan-Canadian Trust Framework (now live as option to log into My Service Canada Account)

- Initiated Sign In Canada Proof of Concept (in-house build) in May 2019, endorsed by Trusted Digital Identity Committee and GC EARB

Future User Experience

A trusted digital identity…

| From Any ID Partner	On Any Device	Through Any Platform	For Any Service
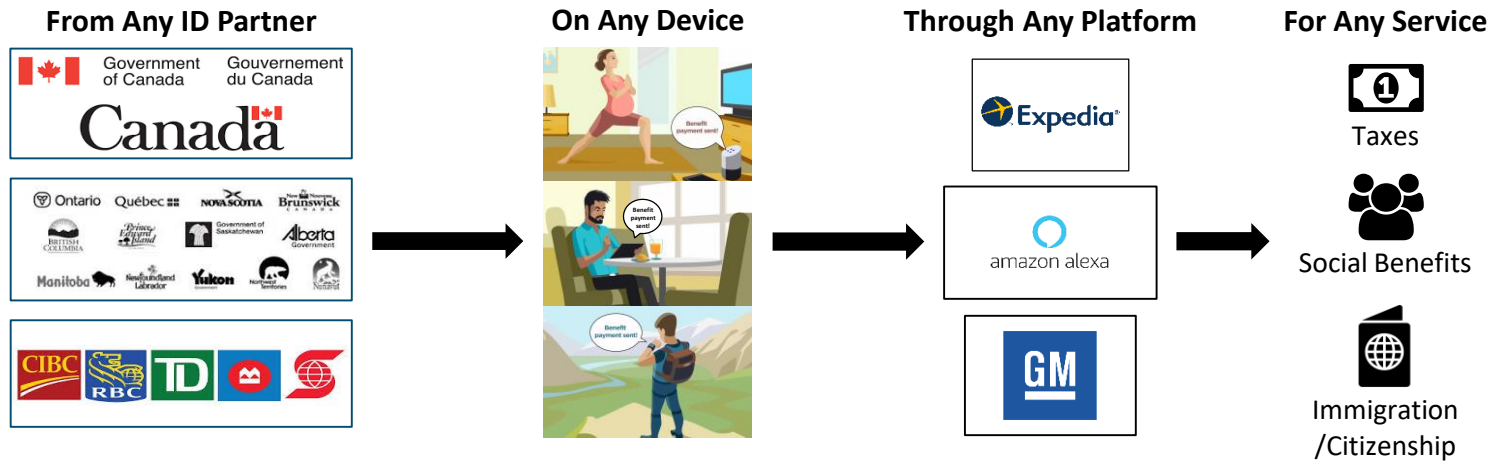
- Canadians can sign in once using their trusted digital identity to instantly access services across GC departments and across jurisdictions on any device
- Trusted digital identity will enable one-time identity-proofing (tell us once), streamline government processes and create a better user experience for Canadians to access services anytime, anywhere and on any device.
- The digital identity ecosystem can be leveraged by any partner, such as other GC departments, provinces or territories, banks, etc. to validate/verify the identities of their clients
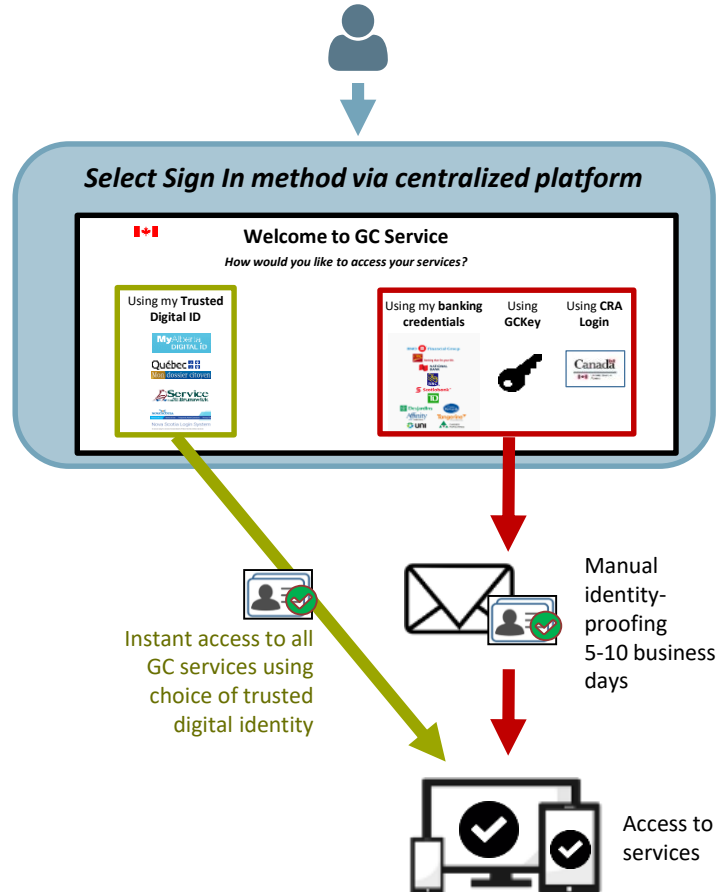
Evolution of GC Digital Identity

Current State
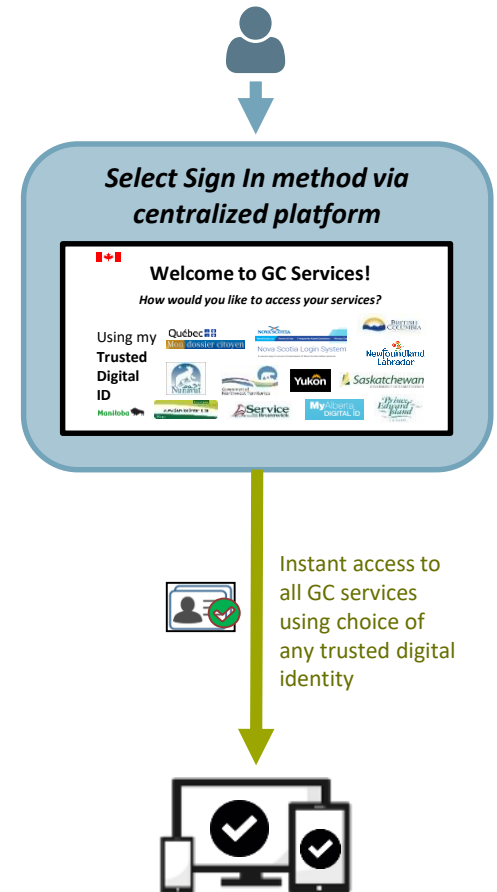**(2 sign-in options, manual identity-proofing)**
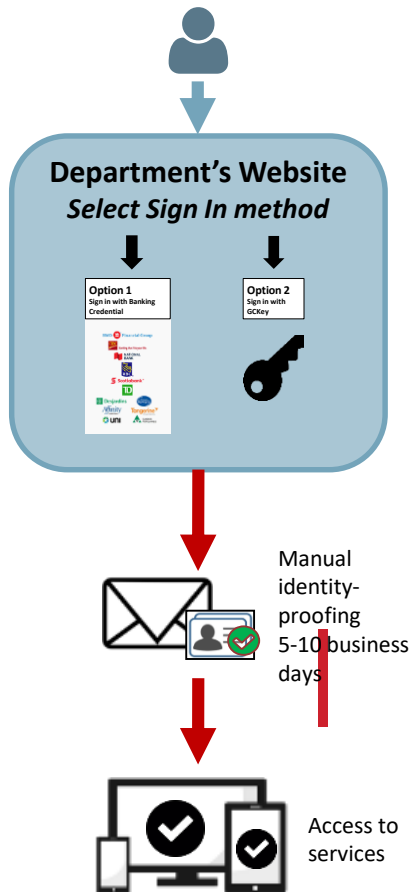
Transition
(Additional option to sign-in with trusted provincial IDs & bypass manual identity-proofing)

Future
(Full acceptance of all available trusted digital IDs, eliminating need for manual identity-proofing)

Sign In Canada: Alignment to GC Digital Standards

Design with users ✓

Working with UX experts, and performing user research

Iterate and improve frequently ✓

Agile approach (e.g. proof of concept, iterative)

Work in the open by default »

Open and transparent with non-sensitive code/data

Use open standards and solutions ✓

Use of open source (e.g. Gluu, Linux, OIDC)

Address security and privacy risks »

Security built-in by design (privacy analysis underway)

Build in accessibility from the start »

Leveraging accessibility templates (analysis underway)

Empower staff to deliver better services ✓

Use of innovative tools and technologies

Be good data stewards ✓

Supporting Tell Us Once approach (maximizing data reuse)

Design ethical services »

Analysis underway

Collaborate widely ✓

Continued collaboration with jurisdictions (Alberta, BC) and internationally (Digital 9 Nations, World Bank, etc.)