



# **ONEGC PLATFORM:**

#### SINGLE WINDOW TO GC DIGITAL SERVICES

#### **NIEM Business Architecture Committee September 16, 2020**

#### Prepared by:

- Digital Enablement Directorate
- Office of the Chief Information Officer of Canada
- Treasury Board of Canada Secretariat



## **GC DIGITAL VISION**



"The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device.

Digitally, the Government of Canada **must operate as one** to benefit all Canadians."

GC Digital Operations Strategic Plan

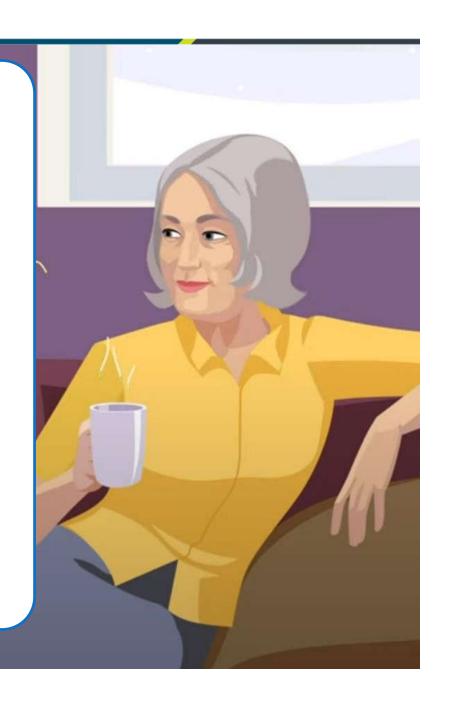
#### THE REASON



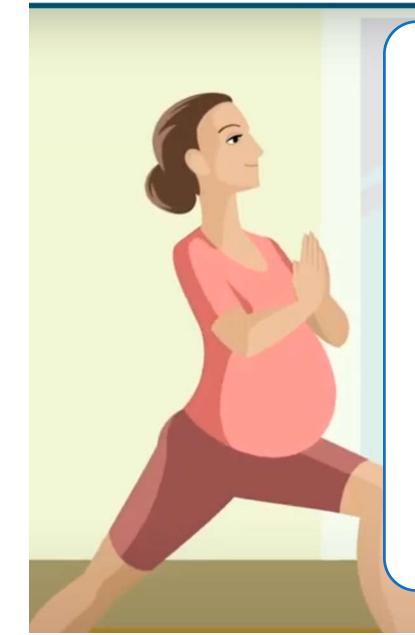
- Today, there are 56 different places to log in to a government account
- That's pretty frustrating for a population that's used to having everything from the latest meme to a full grocery order available in just a few clicks
- With this initiative, we're exploring ways to reduce those 56 login screens to a single place that seamlessly connects Canadians to their government services

## THE SOLUTION

- OneGC Platform
- A central hub that will connect and orchestrate the GC's common digital platforms and departmental services to enable users to:
  - have a centralized view of their information
  - manage their profiles
  - provide transparency regarding who has access to their information



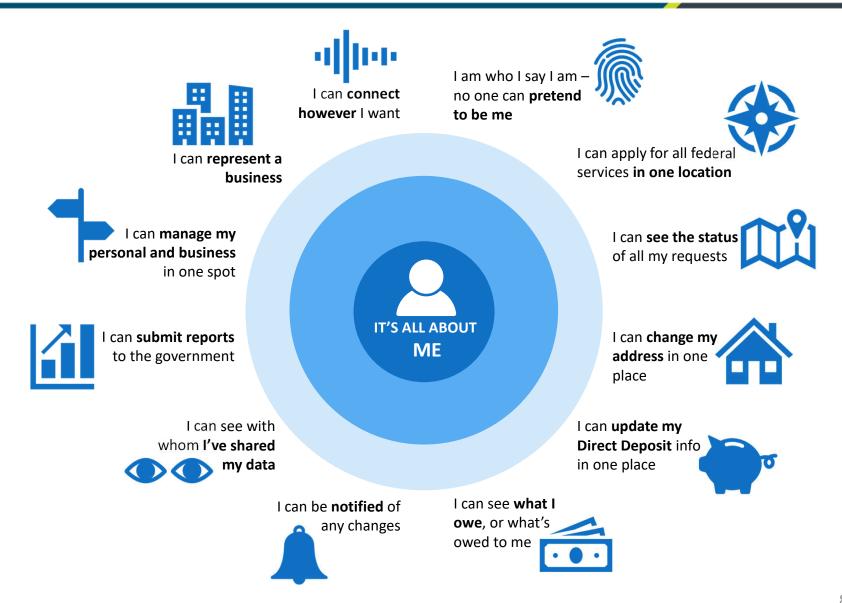
## **EXPECTED OUTCOMES**



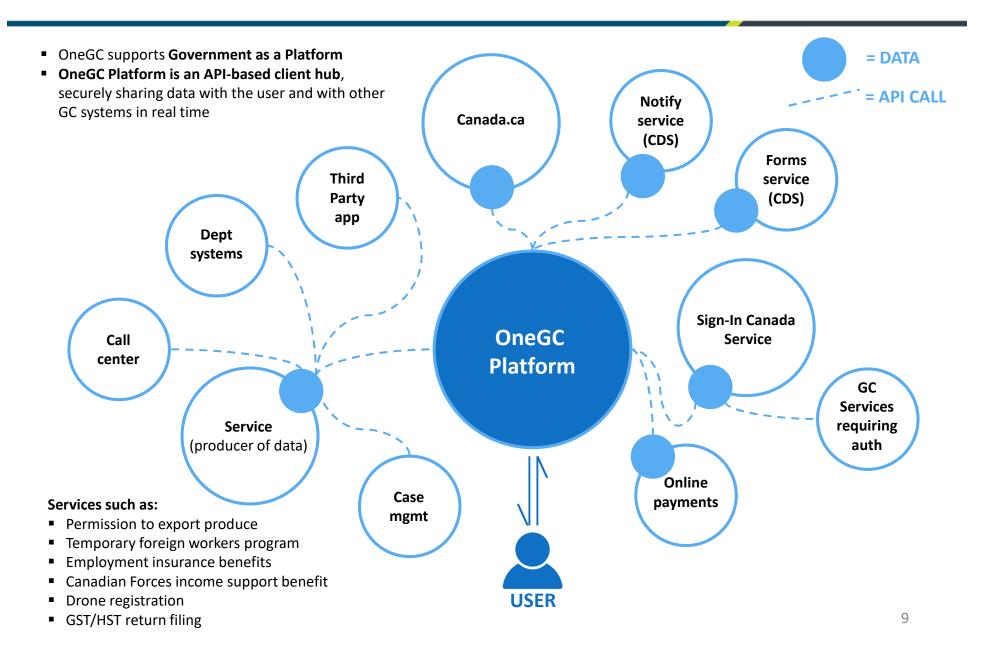
- The public has access to all federal government services via a single online window
- Users only need to share their information once with the GC (Tell Us Once principle)
- Services are delivered in a consistent and reliable manner, reducing user effort and frustration, and building trust and confidence



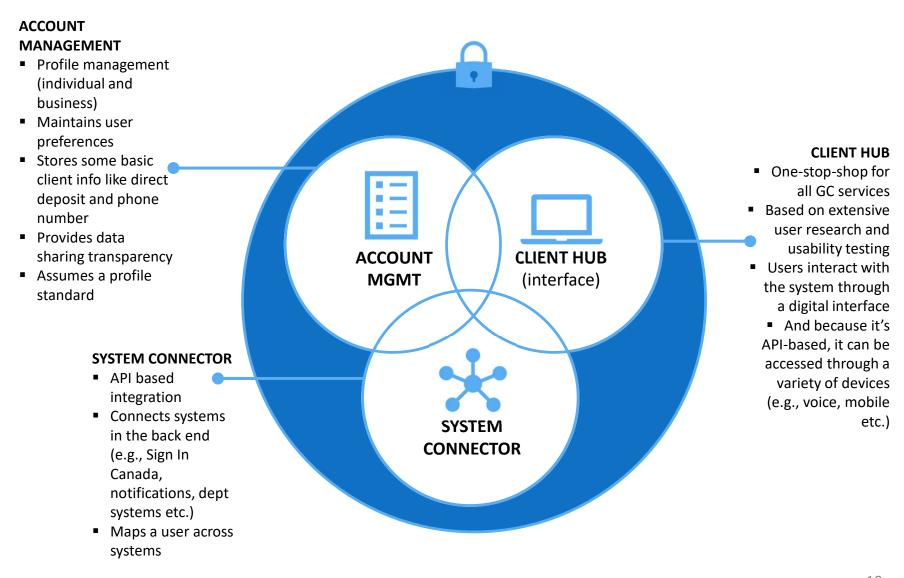
# A SINGLE ONLINE WINDOW, WHERE...



## THE BEAUTY OF DATA REUSE



### **ONEGC PLATFORM COMPONENTS**



#### DATA MODELS BEING EXPLORED

#### **CENTRALIZED**

**DATA AUTHORITY** 



A single central solution stores and manages core citizen profile data (legal name, gender, address, marital status, dependents, citizenship). A single organization is responsible for administering this data, including providing support services such as help desk, data verification, and data quality management.

#### **FEDERATED**

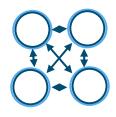
**DATA AUTHORITIES** 



A single data authority will be designated for each context portion of citizen data (life data, residency/citizenship data). Each data authority is responsible for administering their portion of the citizen data and mapping that data to records in other data authorities through some form of a record key (single or federated). This model has been used by Estonia.

#### **DISTRIBUTED**

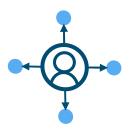
**DATA MANAGEMENT** 



Each Department manages their own version of the citizen's data. A central service hub can still provide a common interface for the citizen and some mechanisms to broker data sharing between Departments. Each Department makes the determination on what to do with an update.

#### **SELF-SOVEREIGN**

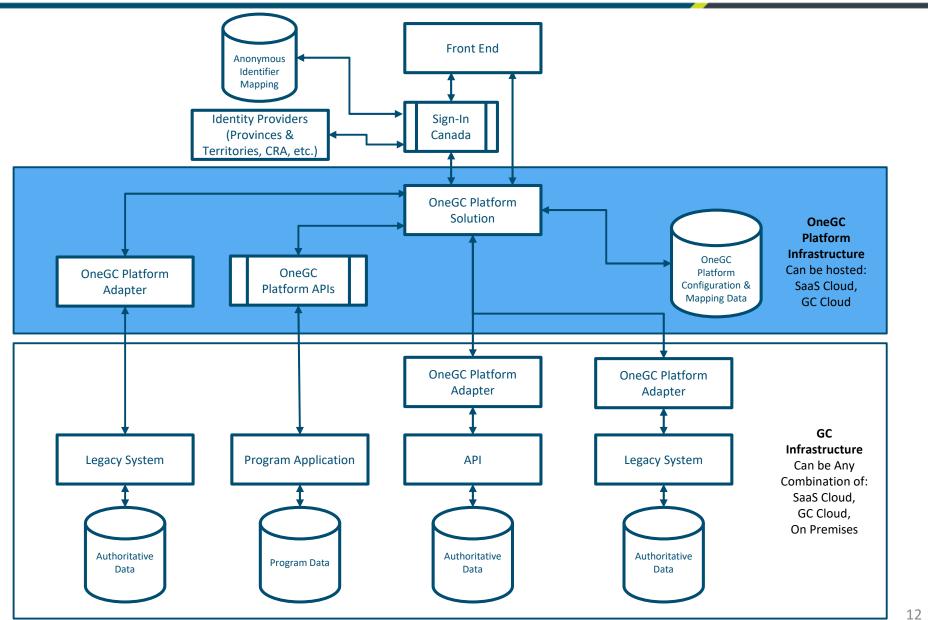
DATA AUTHORITY



The individual/businesses manages their own version of verifiable proofs for identity and associated information. They present their proof(s) to departments based on enrollment in services and level of assurance required, and the departments verify their claim.

Departments continue to operate as-is with data sharing as required (e.g. legal/public safety reasons).

## **ONEGC PLATFORM ARCHITECTURE**





### PHASE 1: EXPERIMENTATION



- **2. Researched** common user patterns and existing UX work (e.g., through Canada.ca)
- **3. Designed wireframes** (interactive visuals) to test user expectations for each use case
- **4. Conducted usability testing** on the wireframes to test user behavior (not their opinions)

- **2. Conducted an environmental scan** to determine who's doing what and how
- 3. Partnered with vendors to experiment with various modern, API-based client hub/portal solutions
- **4. Explored system integration** with legacy systems

#### WHAT WE DISCOVERED – UX INSIGHTS



- Providing multiple unfamiliar sign-in options results in confusion
- 2. Most users **do not read** even extremely brief and simple **statements of consent**, but assume data is shared by default
- Participants **reacted positively** to the convenience of **having data shared across departments** especially for businesses
- Successful task completion was largely driven by participant age, their digital literacy, and their emotional state
- Participants were **eager for the experimental prototypes to become available,** demonstrating enthusiasm for simplified digital services from the Government of Canada

#### WHAT WE DISCOVERED – TECH INSIGHTS



- An API-based platform is a common technical approach for delivering a single online window
- Data doesn't need to be stored repeatedly everything can be mapped in the back end
- Solutions advertised as low-code still require significant tech investment for integration and testing
- Most challenging part of the technology is the **integration with** legacy systems but it can be done
- Digital credentials and wallets are rapidly emerging approaches and technologies worth exploring

An API-based platform is a common technical approach
for delivering a single online window



- Of the solutions explored none were set up to be the single monolithic system of record
- Data is retrieved (via Application Programming Interfaces (APIs)) for display to the user,
   but not stored within the system
- These platforms support multiple authoritative or non-authoritative sources of data
- The approach minimizes the need to retain multiple copies of the data
- We are not alone. Governments and NGOs are already leveraging API-based platforms to successfully delivery valuable services to citizens and stakeholders. For example:
  - Province of Saskatchewan
  - State of Michigan
  - CERN (Conseil européen pour la recherche nucléaire)

# Data doesn't need to be stored – everything can be mapped in the back end



- The platforms could easily integrate with identity providers and data can be used from authoritative sources (e.g., provinces, territories or banks) without being stored centrally
- A single unique identifier isn't required everything can be mapped in the back end and anonymous identifiers can be used to maintain that mapping
- Common identifiers, such as the business number, can be used to make linking to existing services simpler
- Platform solutions can also manage consent for the sharing of data. The consent settings are stored centrally and are shared with the various programs depending on the user's preference
- Users have real-time, as needed, access to their data, regardless of which government program holds that data

Solutions advertised as low-code still require significant tech investment for integration and testing



- Low-code/no-code approaches provided by the platforms can work for some business users if all the integration points are built and the business users have some basic technical skills
- **Developers and system integrators (SIs) will still be essential** to enable modern integration methods with legacy systems
- Commercial solutions don't have strong support for automated testing, so the need for manual testing remains high
- Each solution had its own jargon and way of provisioning workflows and integrations, which are not directly transferable from other technologies. This requires platform operators to go through training

Most challenging part of the technology is the
 integration with legacy systems – but it can be done



- Getting data to/from the legacy systems becomes the most complex part of these solutions
- Legacy system data must be exposed to allow for real-time data access
- Various technical solutions and patterns can be employed aside from modernizing the legacy solution:
  - Adapters provide native connectors and capabilities for mapping and transformation (can be deployed on different infrastructure and network zones for security purposes)
  - Legacy wrapper services are written to serve as an interface between legacy and the single window solution (and other solutions requiring data in realtime)

Digital credentials and wallets are rapidly emerging
 approaches and technologies worth exploring



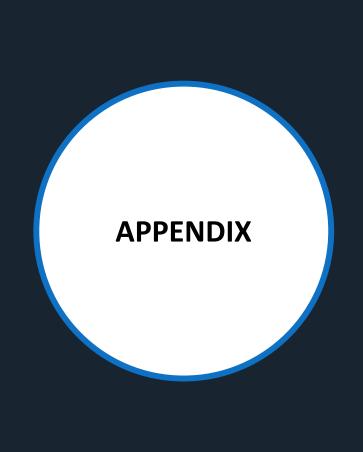
- Some experimentation was conducted with the self-sovereign data model using **digital credentials and wallets** (which could complement a federated model using APIs)
- Standards exist and continue to evolve, but more investment in standardization is needed to ensure widespread interoperability
- Successful proofs of concept have been completed across numerous jurisdictions including British Columbia, Alberta, Canada (Innovation, Science and Economic Development Canada and Transport Canada), United States (USA), and the United Kingdom (UK)

#### **FUTURE PHASES WILL...**



- Adopt a product-based approach that is outcomes-based, puts
   the user first and supports an agile delivery methodology
- **Confirm an approach to data management** that considers common data standards and different data model approaches
- **Explore policy and legislation** related to privacy, consent and data sharing
- Understand the user journey across all touchpoints in order to address points of friction, such as accessibility
- Invest in technology that is API-based, prioritize API development and support the evolution of data exchange with legacy systems





## **OUR GUIDING PRINCIPLES**

#### Our work is guided by the Government of Canada Digital Standards



Everything we do is in the open



User community, technology, and business are all active participants working closely together



Product
management
approach with
continuous
iteration and
delivery, focused on
the needs of the
user



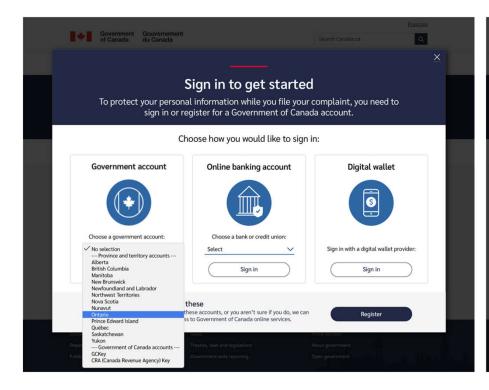
**Experimentation mindset** removes
constraints and
allows for a
"sky's the limit"
perspective

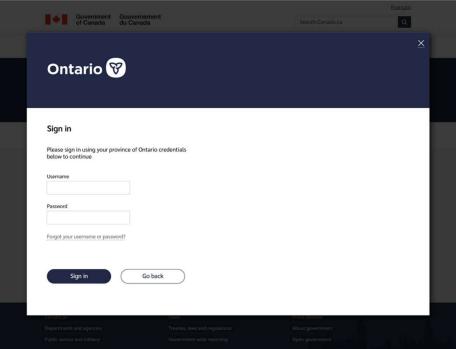


We are leveraging the work of our partners like OneGC Council members and F/P/T clusters

# WHAT IT COULD LOOK LIKE (I)

User changes address in context of completing a task (filing a labour standards complaint)

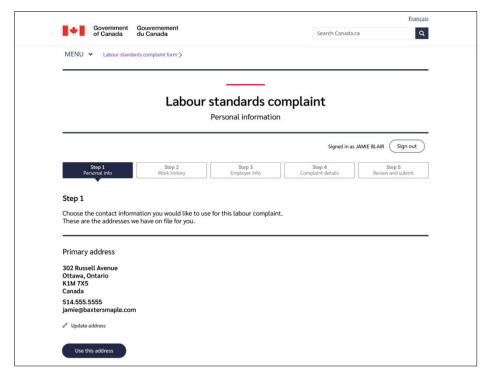


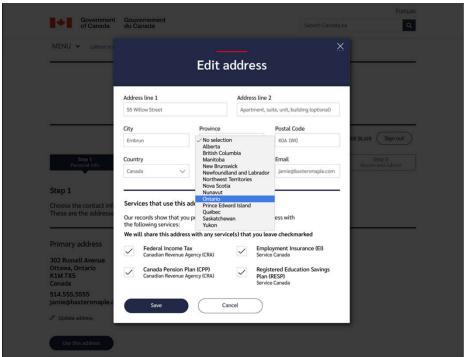


User is prompted to sign in – they can use one of several methods including GCKey, online banking, provincial or territorial credentials, or a digital wallet

# WHAT IT COULD LOOK LIKE (II)

User continues with filing a labour standards complaint, and notices that the address on file is an old one which needs to be updated





User opts to change the address (which is then shared across various services based on the user's preference)...

# WHAT IT COULD LOOK LIKE (III)

...and continues with the task (filing a labour standards complaint). The address change will be reflected in the user's dashboard next time they sign in.

