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

Canada

TELL US ONCE/SINGLE WINDOW PROTOTYPE: *RESEARCH THROUGH DESIGN*

TECHNICAL REPORT

Prepared by:

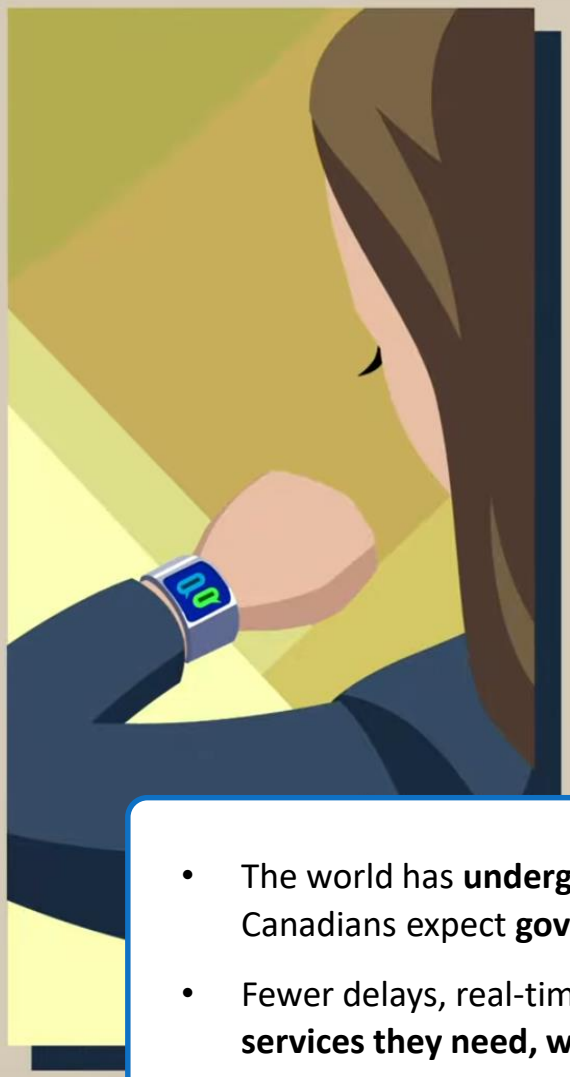
- Office of the Chief Information Officer of Canada
- Treasury Board of Canada Secretariat
- 2020

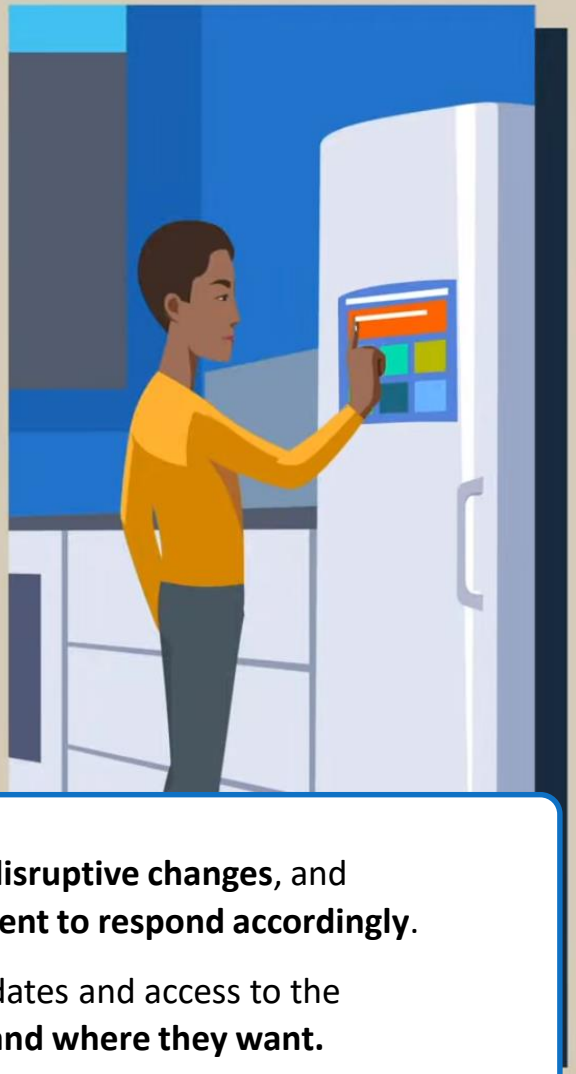
TELL US ONCE
OVERVIEW

TELL US ONCE: a key pillar of our digital future

- Yesterday's government delivered **services by analog**.
- **Long wait times and siloed service delivery** were normal.
- Telling the government **key pieces of information repeatedly** was not only common – it was expected.

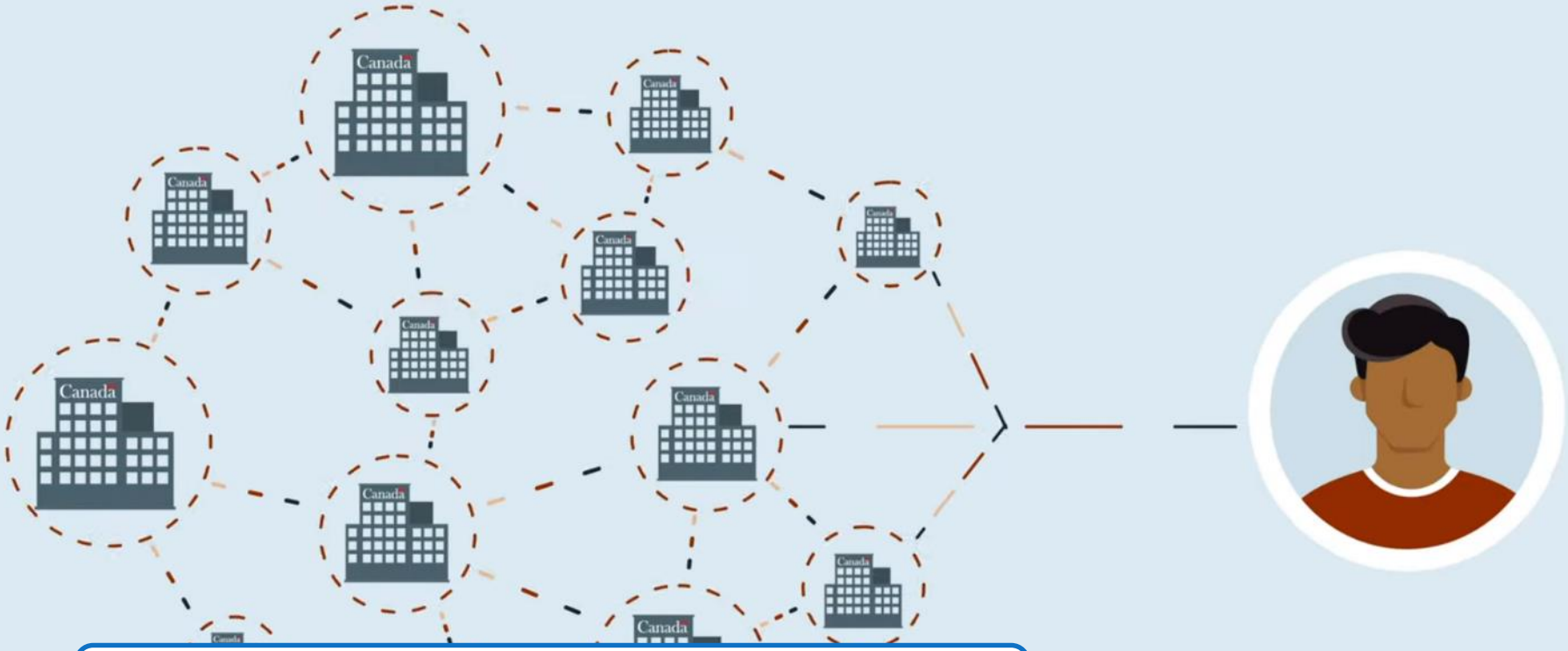
TELL US ONCE: a key pillar of our digital future





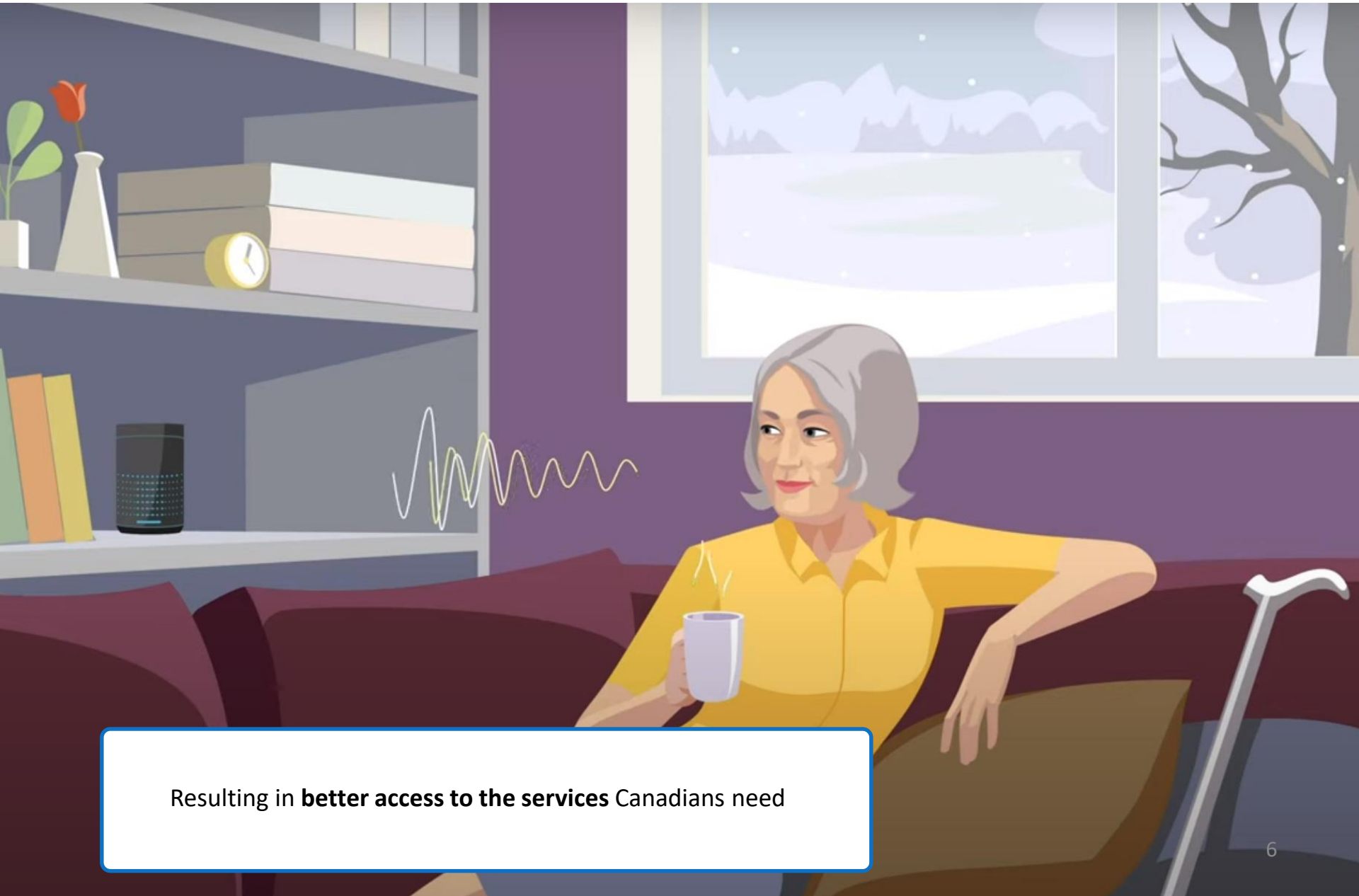
- The world has **undergone disruptive changes**, and Canadians expect **government to respond accordingly**.
- Fewer delays, real-time updates and access to the **services they need, when and where they want.**

TELL US ONCE: a key pillar of our digital future



- What if government could **re-imagine its service relationship with citizens**.
- “Tell Us Once” is a key pillar of our digital future, this approach means **citizens only need to tell government their information once**.

TELL US ONCE: a key pillar of our digital future



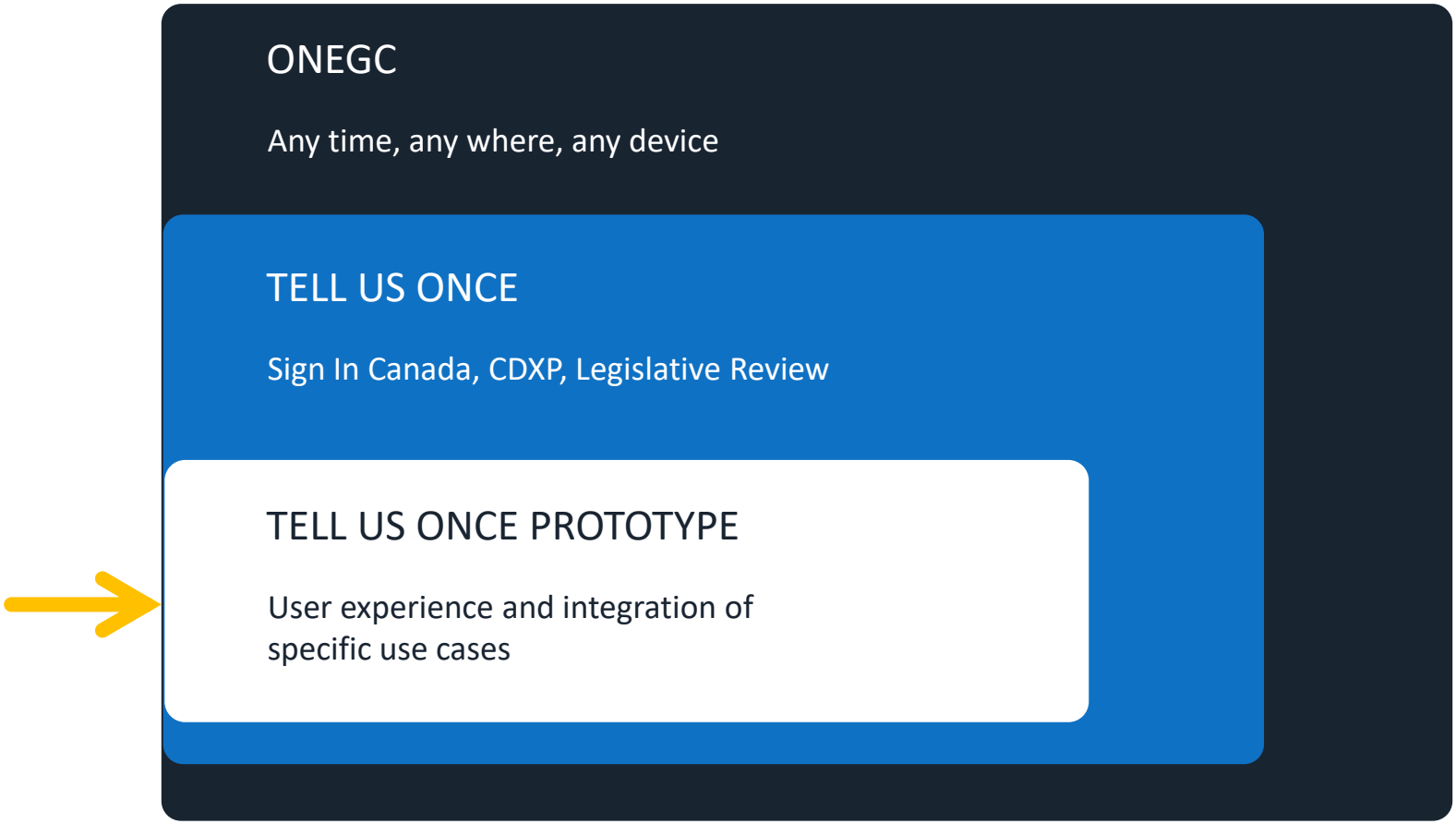
Resulting in **better access to the services** Canadians need

PROJECT BACKGROUND

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've been exploring ways to reduce those 56 login screens to **a single place that seamlessly connects Canadians to their government services.**

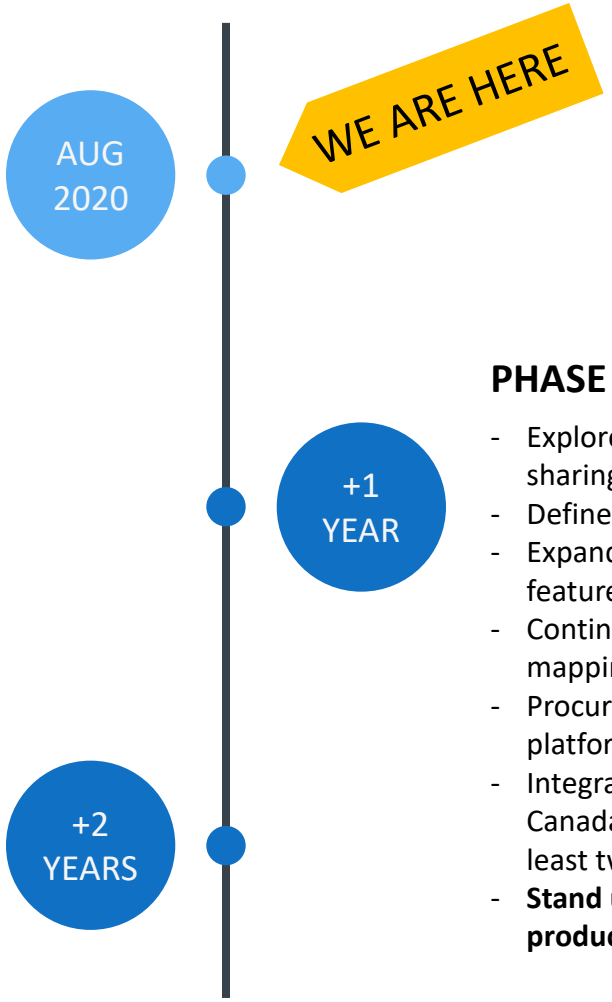
THE HIERARCHY



THE JOURNEY

PHASE 1: CRAWL

- Experiment with four use cases
- Determine a happy path for users
- Land on a preferred technology
- Collect and analyze data to help inform future direction
- **Publish findings and develop list of recommendations**



PHASE 2: WALK

- Explore privacy, consent, and data sharing policies and legislation
- Define a data sharing model
- Expand use cases to include common features such as direct deposit
- Continue with usability testing and mapping the user journey
- Procure a client-hub integration platform
- Integrate with Sign In Canada, Canada.ca, account mgmt., and at least two GC services
- **Stand up alpha version in production**

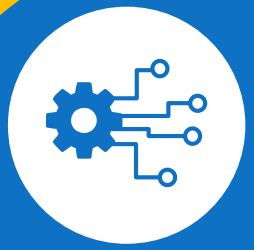
PHASE 3: RUN

- Onboard additional GC services, encouraging dept. to make their services available through APIs
- Continue refining user experience based on usability testing
- Incorporate new common services such as notifications, forms, and wallets etc.
- Tackle necessary policy and legislative changes as required
- **Launch beta version in production**

WE WANTED TO BETTER UNDERSTAND

FOCUS of this REPORT

+



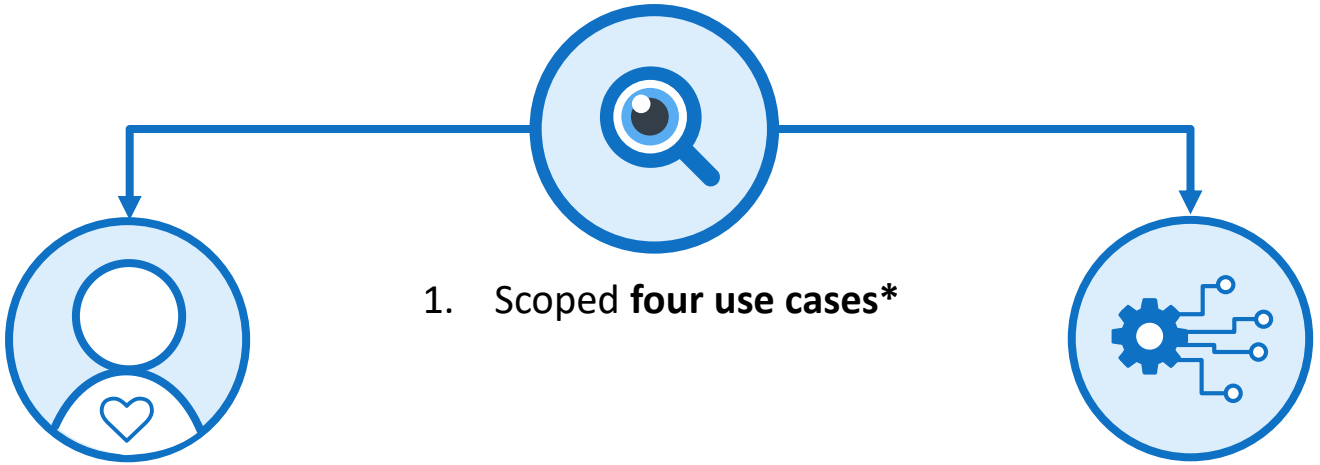
USER EXPERIENCE (UX)

What does Tell Us Once **look like to the end user**?

TECHNOLOGY

How do we best support **integrated and interoperable service delivery** across GC through Tell Us Once?

OUR SIX MONTH EXPLORATION



1. Scoped **four use cases***

USER EXPERIENCE

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)

TECHNOLOGY

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
5. **Examine solution alignment** with the current Pan Canadian Trust Framework (PCTF)

Use case details: slides 17-20

ASSUMPTIONS WE MADE

USER EXPERIENCE

- Consent must be given prior to sharing info
- Not constrained by existing policies or legislation
- When a service is selected on the non-authenticated side this information will be passed through to the authenticated side
- Web channel only
- User triggered changes and updates
- Users consist of both individuals and businesses
- Scope is limited to Canadian residents

TECHNOLOGY

- Leveraging APIs & messaging
- Open interop standards
- Non-production data for testing
- Cloud hosting possible
- Connectivity enabled through test services

WHO WAS INVOLVED

PROJECT LEAD

- TBS OCIO **Interoperability**

PROJECT TEAM

- **TBS OCIO**
  - Identity
  - Cyber Security
  - Enterprise Architecture
  - Privacy
  - Policy
  - Talent Cloud

- OneGC Partners
  - **ISED**
  - **CRA**
  - **ESDC**

- TBS
  - **Legal**
  - Canada.ca (**SCMA**)

CAPABILITIES EXAMINED

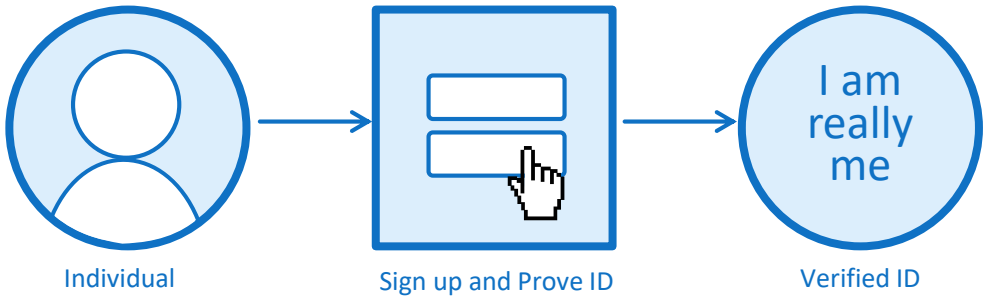
Find information		Manage account		Manage services		
Discovery external to GC	Site navigation inside GC	Account creation / sign in	Account maintenance	Service enrolment	Service request processing	Receive service output
		Canada.ca	Profile information maintenance	Submit a request/apply for a service		
		Portal solution	Assign representatives/ Verified relationships	Submit a request/apply for a service bundle		
		Digital wallet solution		Credential mapping		
		Sign in and mapping credentials		Information sharing and consent		
		Identity proofing				
		Create or connect basic profile information				
		Verifiable proofs				

USE CASES

USE CASE 1

VERIFIED INDIVIDUAL

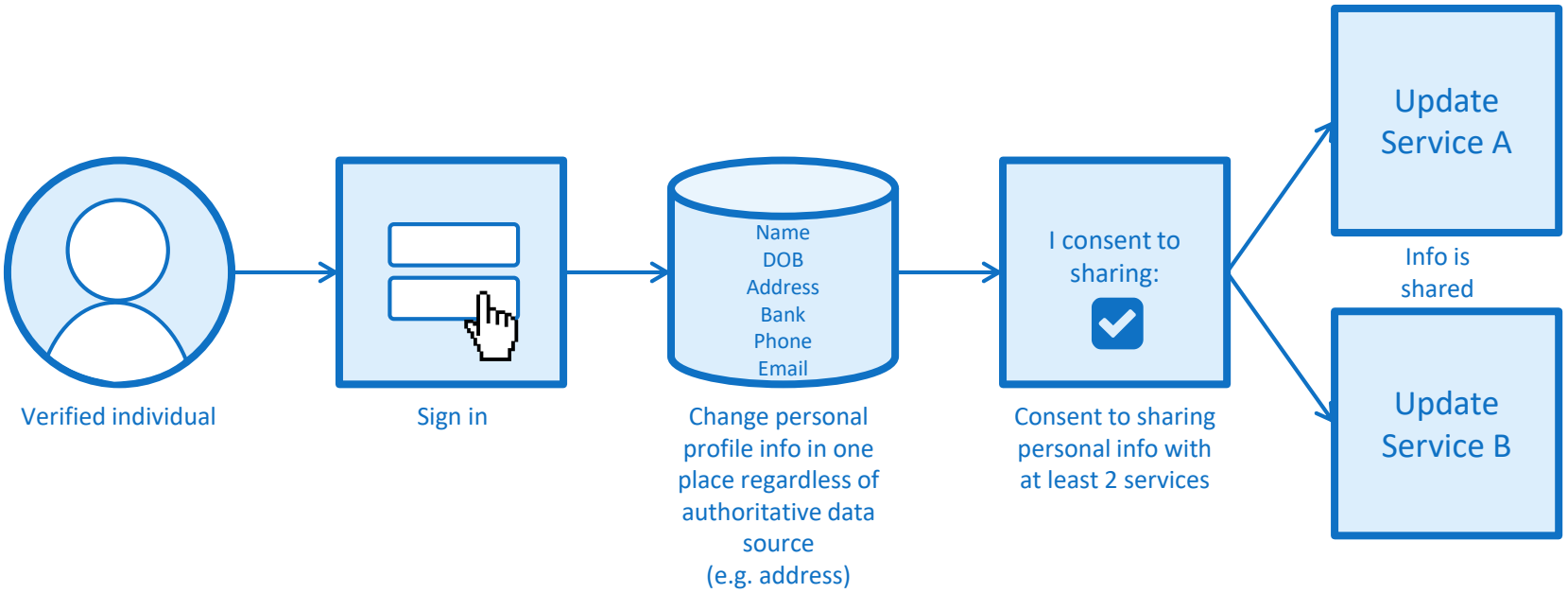
Authenticate and prove identity of an individual



USE CASE 2

INFORMATION SHARING

Self serve client profile management*

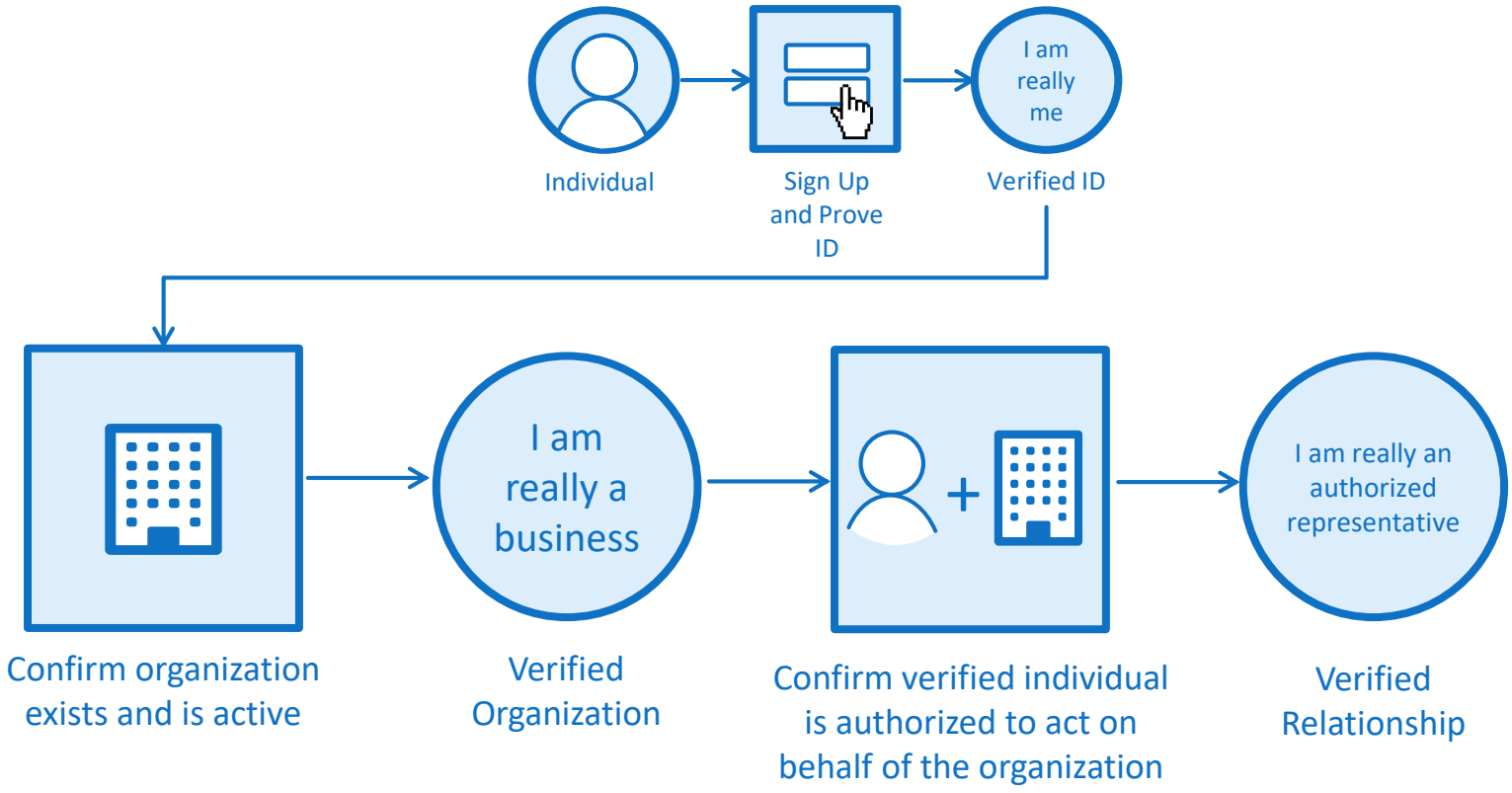


**Use case 2 screen views are located in the annex*

USE CASE 3

VERIFIED ORGANIZATION AND RELATIONSHIP

Verify the existence of an organization and link it to an individual

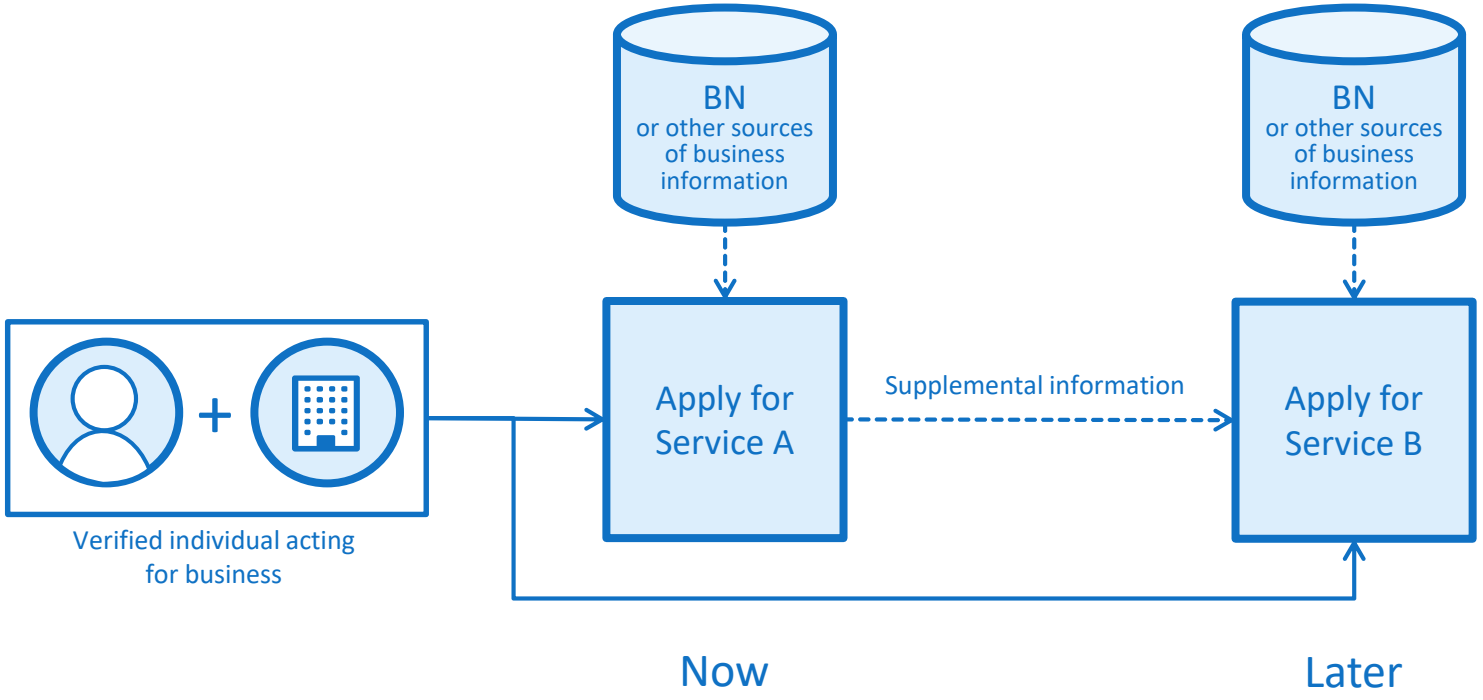


**Use case 3 screen views are located in the annex*

USE CASE 4

BUSINESS INFORMATION SHARING

Enrol in two business facing services leveraging the business number and other common data elements*



*Use case 4 screen views are located in the annex

TECH
APPROACH

OUR TECH APPROACH - SUMMARY

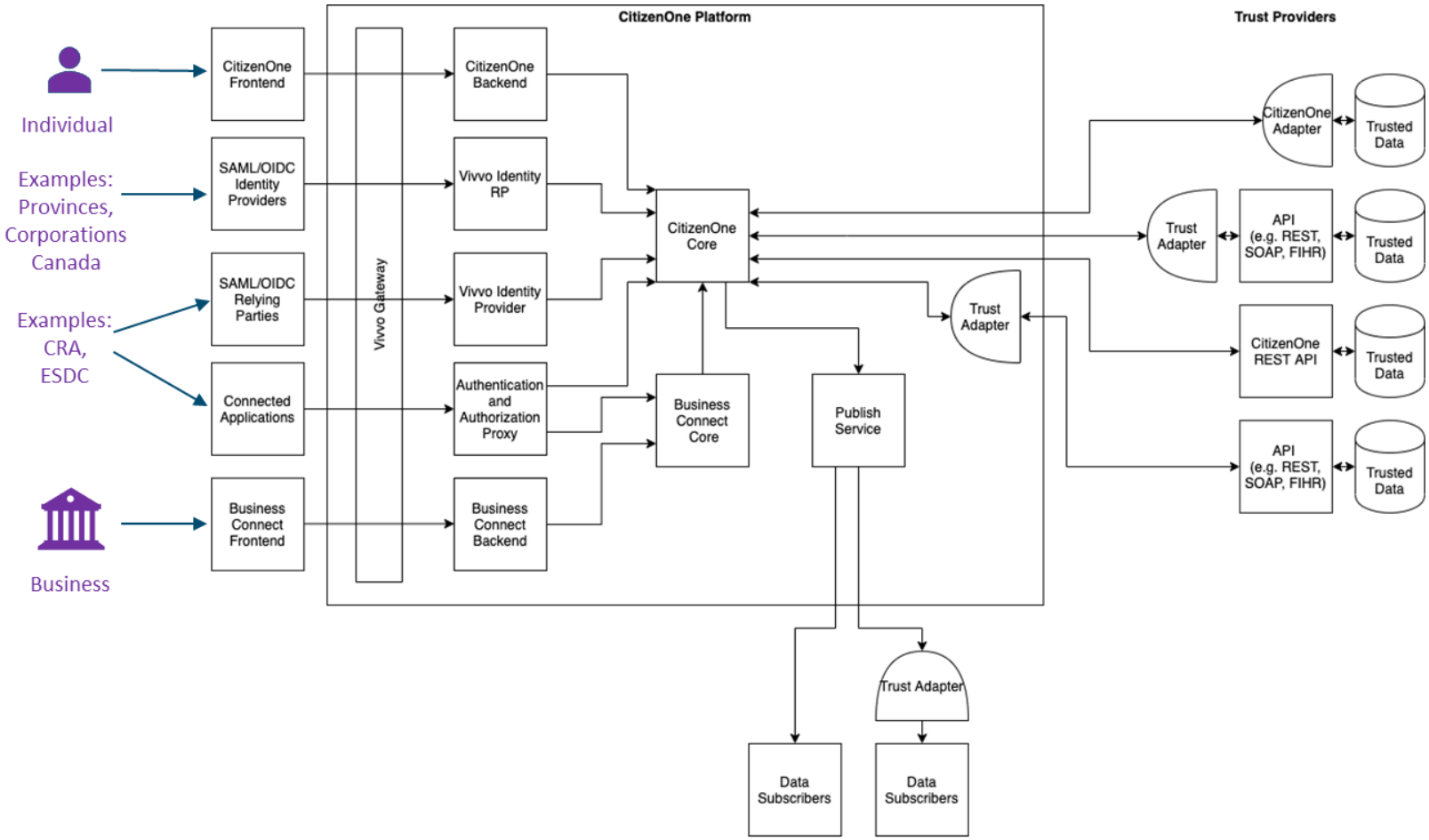
- Conducted an **environmental scan** to see who's doing what out in the wild
- Tested three **API-based single window solutions** in a sandbox
  - Vivvo CitizenOne
  - Salesforce
  - ServiceNow
- **Reviewed integration** with identity providers
- Explored the use of **digital credentials** held in digital wallets to prove identity and to exchange verifiable information
- Set up **mock services and authoritative data sources**
- Explored the **ability to integrate with legacy systems** using stubbed versions of real interfaces
- **Ran traffic through** with dummy data

THREE SOLUTIONS – DEEP DIVE

- The three solutions examined (Vivvo CitizenOne, Salesforce, and Servicenow) are the result of **different product evolutions and perspectives**:
    - Vivvo CitizenOne is designed to help goverments deliver digital services
    - Salesforce originally focused on Customer Relationship Management (CRM)
    - ServiceNow originally focused on IT Service Management (ITSM)
- Commonalities in these platforms include **identity**, **workflow**, and **integration** capabilities
- All solutions are **API-based** platforms deployed in the **cloud**
- Vivvo CitizenOne was extended through the **Build In Canada Innovation Program (BCIP)**
- Workshops and other material can be found on the GC Collab page: https://gccollab.ca/file/group/2134454/all

**Examples of data models are presented in the annex*

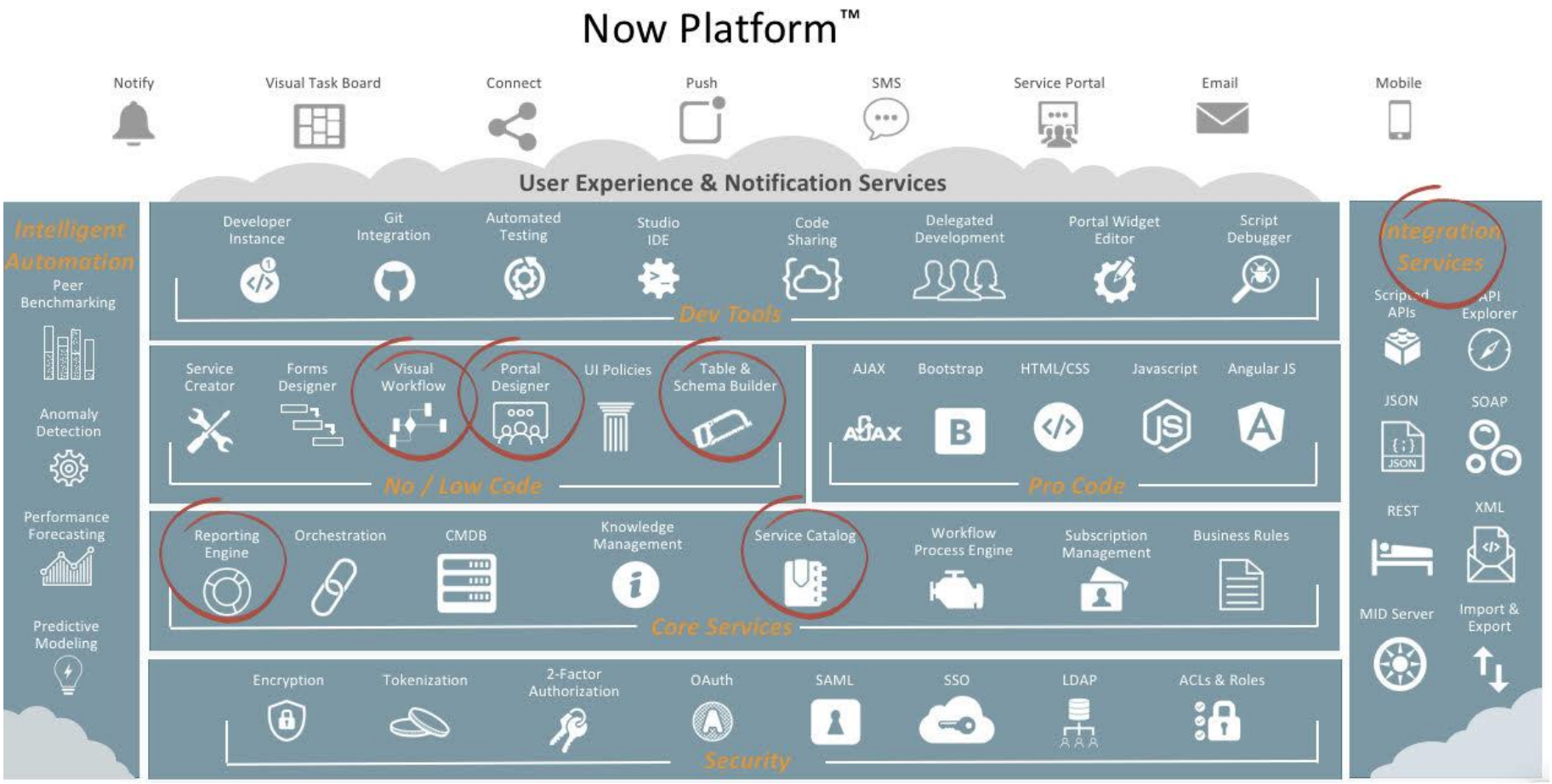
THREE SOLUTIONS – VIVVO CITIZENONE



THREE SOLUTIONS – SALESFORCE

The red text indicates the highlighted features for a single online window

THREE SOLUTIONS – SERVICENOW



The circled areas indicate focused areas of technical workshops and hands-on testing

IDENTITY INTEGRATION – DEEP DIVE

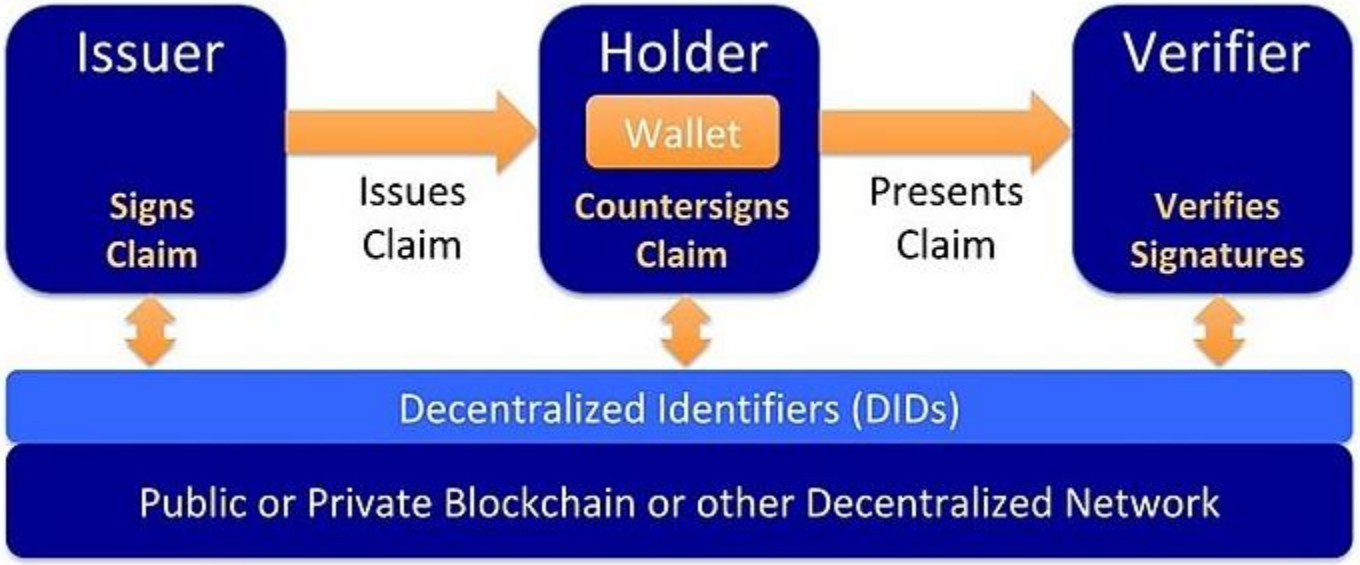
- Reviewed integration with identity providers
- The GC already has digital identity solutions in mind with **Sign In Canada** and has established digital credentials like GC Key
- It was reviewed whether these platforms could **integrate with 3rd party identity providers** (e.g. Sign In Canada)
- Sign-in options were stubbed and tested as part of Use Case (UC) 1, including CRA and a provincial login using SAML and Open ID Connect protocols

Pending Vivvo screenshot of login partners screen

**Examples of data models are presented in the annex*

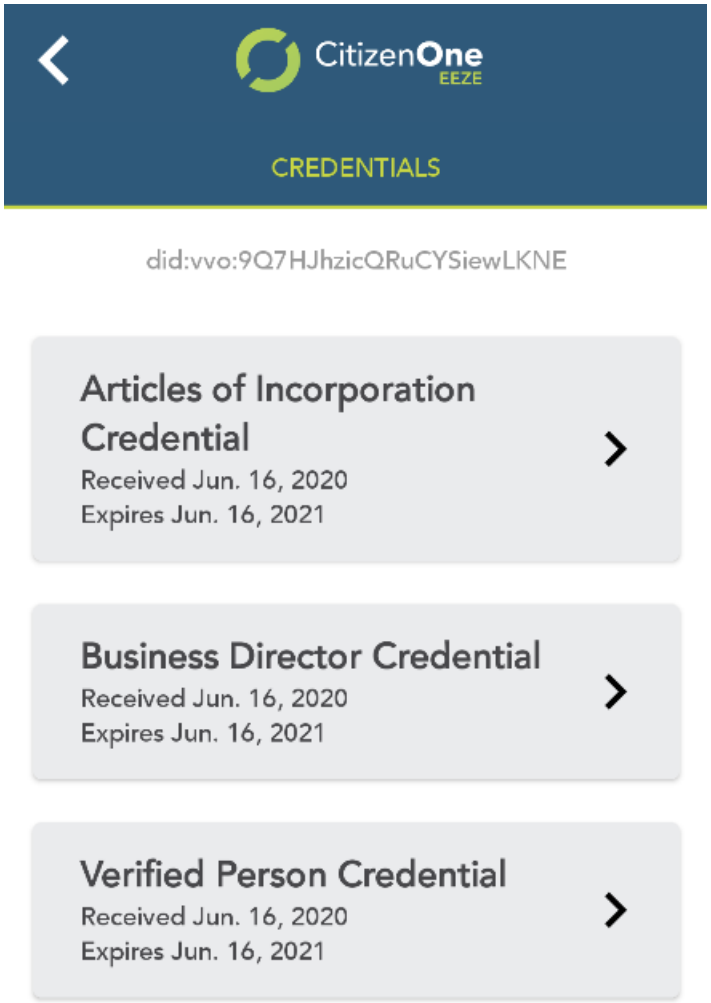
DIGITAL WALLETS – DEEP DIVE

- Explored the use of digital credentials held in digital wallets to prove identity and to exchange verifiable information
- **Digital credentials and wallets** enable individuals to store their data on their personal devices and provide it for verifications without the need to rely on a central repository
- The **user is in control** of their information and to whom they give it (similar to documents held in physical wallets)



Graphic from Wikimedia Commons

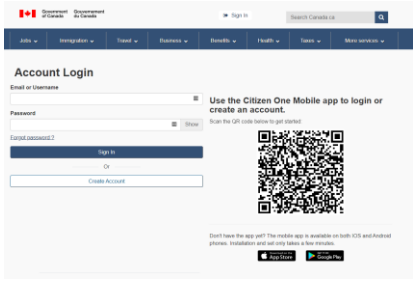
DIGITAL WALLETS – DEEP DIVE

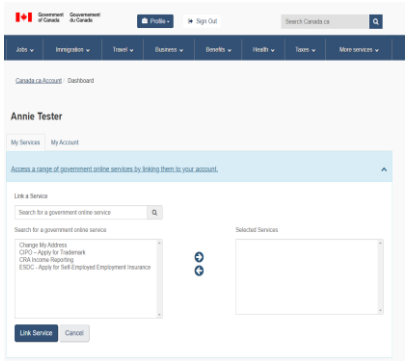


- Digital Wallets were explored using the Vivvo CitizenOne mobile application
- The digital credentials and wallet were based on **standards** from the Worldwide Web Consortium (W3C) such as Verifiable Credentials and Decentralized Identities
- Used the mobile device's secure enclave to protect credentials and cryptographic private keys in the mobile wallet [see Annex for further technical details]
- The current version used proprietary credential collection and presentation protocols, but Vivvo is in the process of adopting DIDComm to enable greater interoperability
- The digital credentials and wallet were primarily used for Use Cases 3 and 4

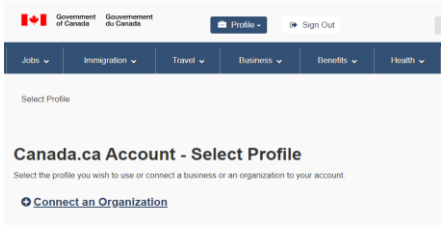
DIGITAL WALLETS – USE CASE 3

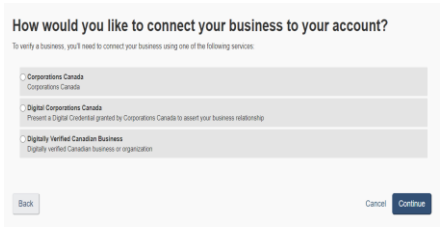
Users verify their identity, relationship with a business and role as a director using digital wallet credentials.



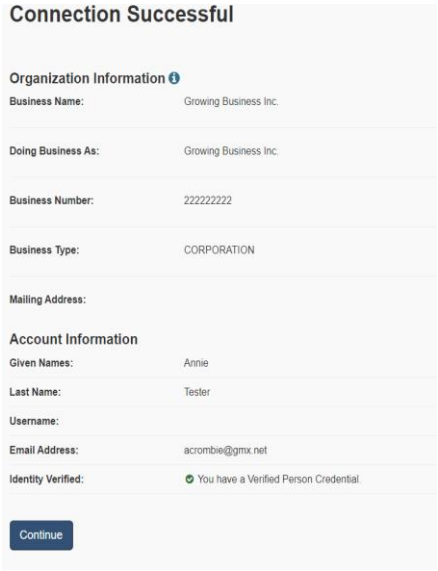


At CitizenOne, scan the QR code with the mobile app to log into personal account





Link business account to personal account using credentials provided in digital wallet.



Confirmation of successful linking of business account to personal account.

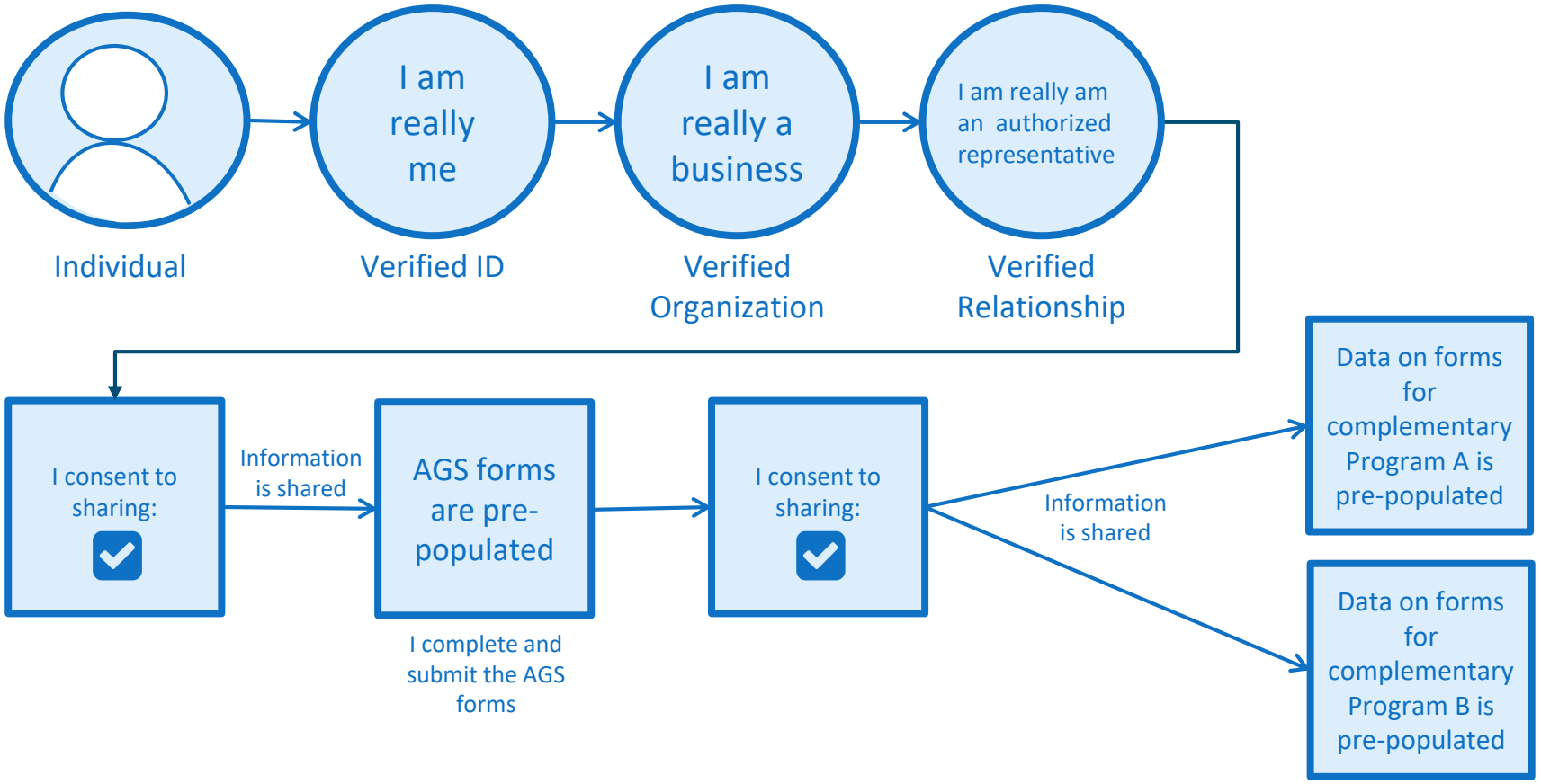
LEGACY INTEGRATION – DEEP DIVE

- Explored the **ability to integrate with legacy systems** using stubbed versions of real interfaces
- Integration with existing GC systems to send or retrieve data will be required
- Explored capabilities addressing **legacy system integration** and **modern integration** methods
- Some **Application Programming Interfaces (APIs)** were used, e.g. Canada Post address completion
- Insufficient time to implement connectivity to the GC applications for testing but used **stubs of real interfaces** as much as possible
    - Included Corporations Canada, CRA Business Number (BN) Lookup, and ISED Accelerated Growth Services planned future API specs
- Where interfaces were not available, stubs were created based on real data attributes collected that would be feasible to share in the future, e.g. CRA business data

USE CASE 4 – TESTED WITH VIVVO PLATFORM

With valid digital credentials established:

- Pre-populate Accelerated Growth Services (ISED program) forms with CRA data
- Pre-populate complementary programs forms with AGS data




TECH
INSIGHTS

TECH INSIGHTS – SUMMARY

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

2. **Data doesn't need to be stored repeatedly** – everything can be mapped in the back end

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

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

5. **Digital credentials and wallets** are rapidly emerging approaches and technologies worth exploring

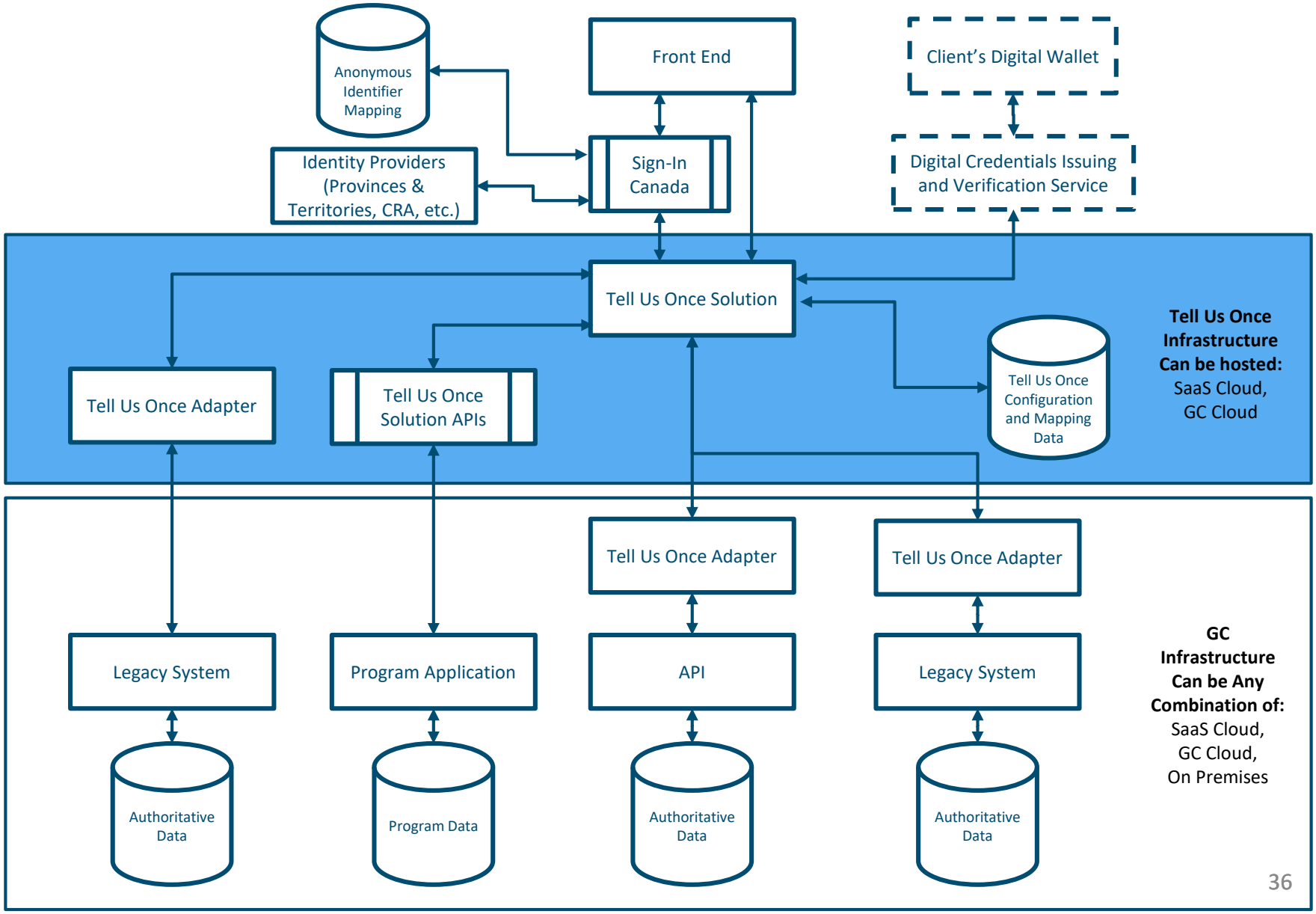
TECH INSIGHTS – DETAILS

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

- Of the three solutions explored (Vivvo CitizenOne, ServiceNow, and Salesforce) **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)

*Examples of data models are presented in the Annex
** Additional examples can be found in the Annex

API-BASED PLATFORM ARCHITECTURE



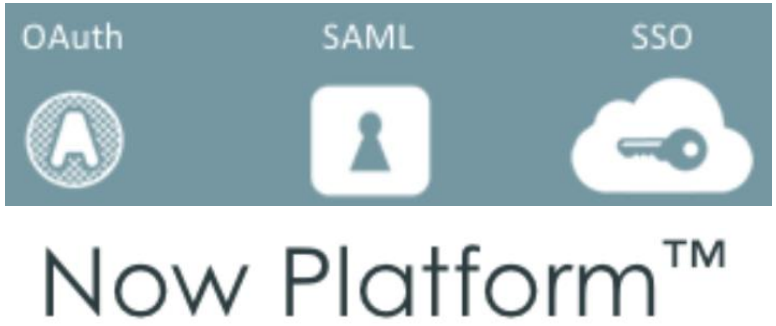
TECH INSIGHTS – DETAILS

2. 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

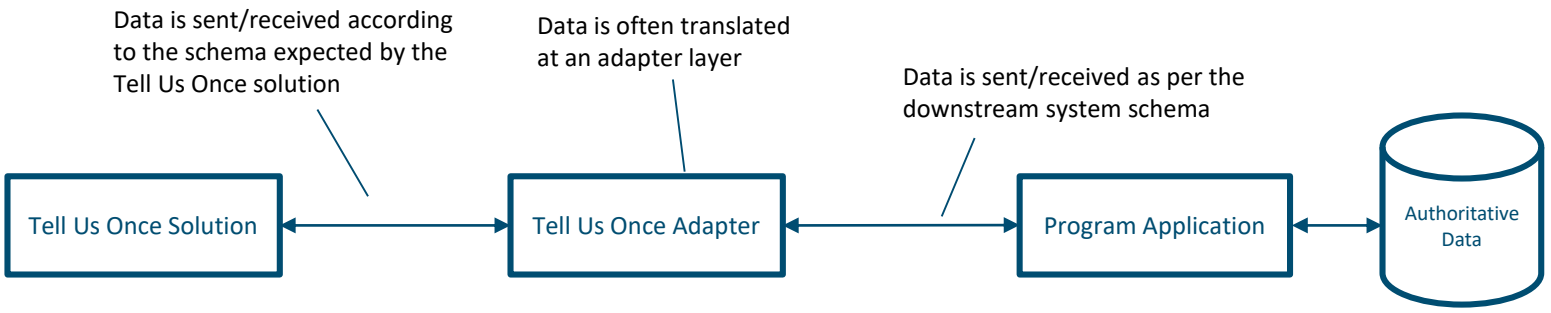
IDENTITY PROVIDER INTEGRATION

- Platforms could **support integration with an identity provider** like Sign In Canada
- It was found that there is broad support for **industry standard protocols** such as SAML and OpenID Connect in support of **integrating with 3rd party identity providers**
- This extended to Single Sign On (SSO) capabilities within the platforms



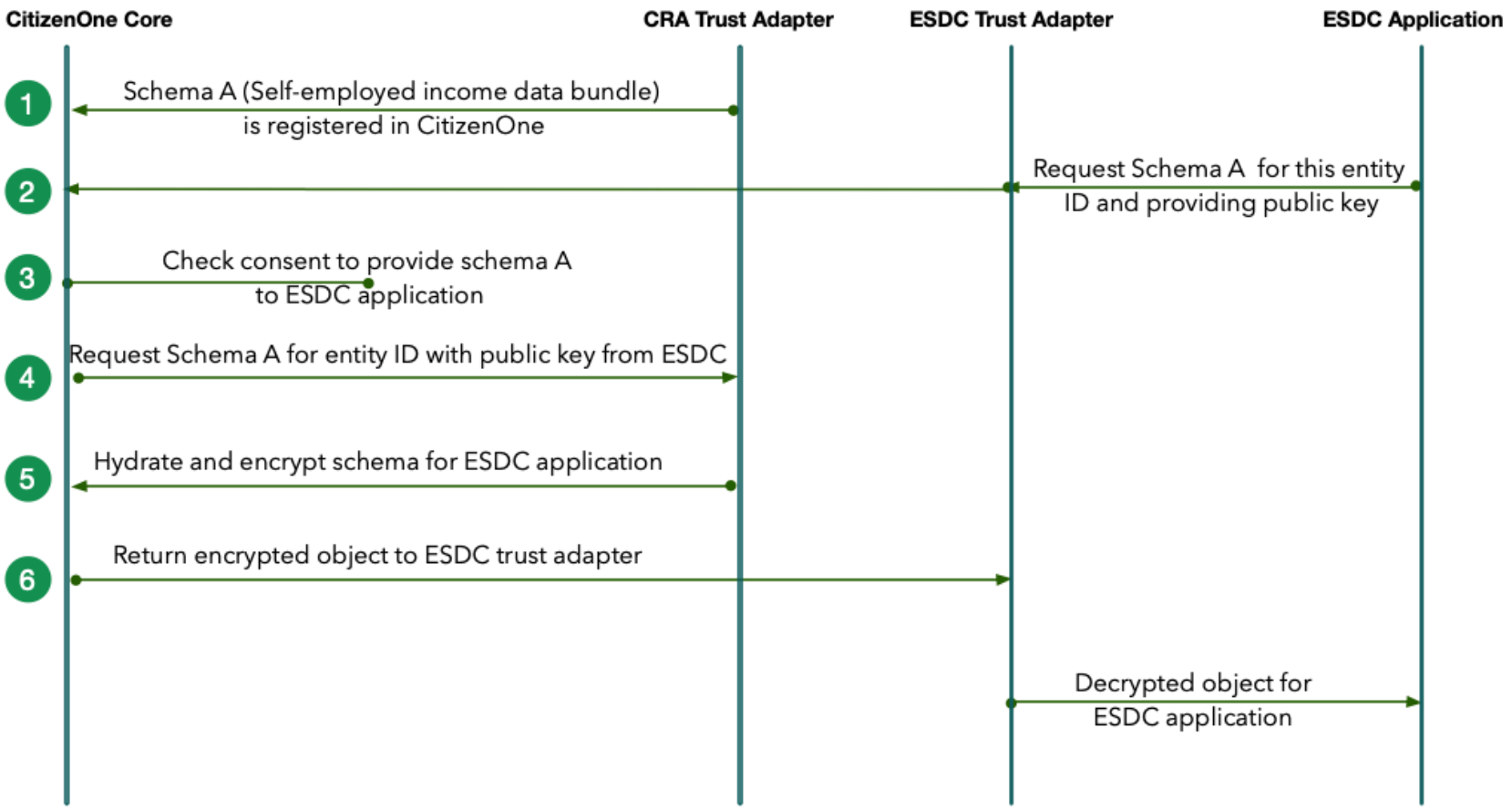
DATA MAPPING

- The API-based platforms **do not expect** a single schema implemented by all downstream systems
- Data inconsistencies are **expected** from downstream sources
- A common schema for elements in maintained through **mapping**
- This mapping could be executed by the central solution, an adapter, or some other component between the platform and the downstream systems



VIVVO CITIZENONE – DATA FEDERATION EXAMPLE

This data federation example shows how platforms could be used to enable **data sharing securely** without exposing that data to the core solution



TECH INSIGHTS – DETAILS

3. 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**

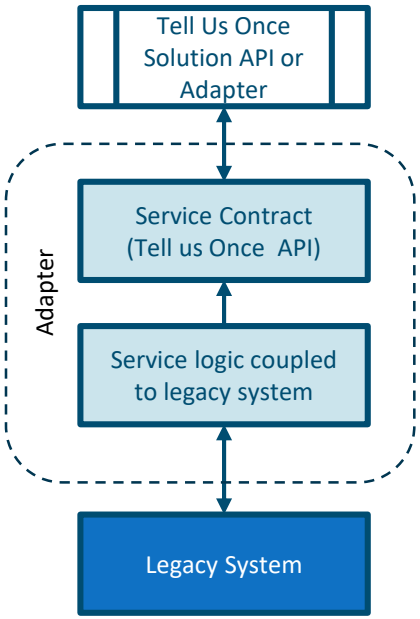
TECH INSIGHTS – DETAILS

4. 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 real-time)

LEGACY INTEGRATION

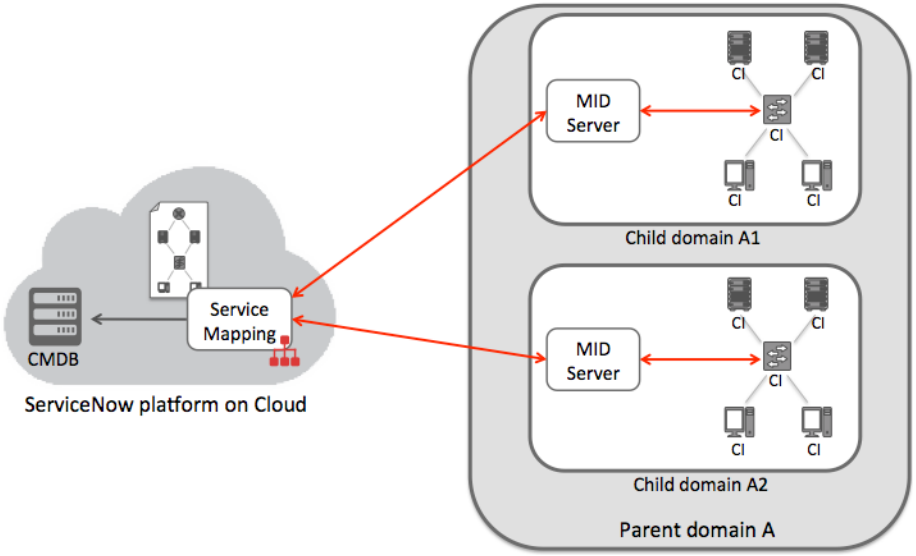
- The API-based platforms used **adapters** to act as intermediary connectors when standard protocols like REST and SOAP cannot be implemented



- These nodes can be deployed in the **same network zone** as the application component and can be customized to work with the application's specifications
- The nodes communicate with the central solution in a standard fashion, keeping the solution's configuration **streamlined and consistent**

INTEGRATION USING QUEUES

- ServiceNow used **queues** rather than synchronous requests to ensure communication is **always calling out** from the more secure network zones
- Adapters in these zones referred to as MID Servers **call out to queues** to check for requests
- These requests are executed, and if any information is requested it is **sent as a request payload** rather than a synchronous response
- Performance implications for real-time citizen and business interactions would need to be examined for this type of model



TECH INSIGHTS – DETAILS

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

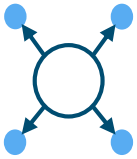
- Some experimentation was conducted with the self-sovereign data model using **digital credentials and wallets** (which could complement a federated model using APIs)
- Standards exist and continue to evolve, but **more investment in standardization is needed** to ensure widespread interoperability
- 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)*

**Details on digital credentials and wallets initiatives can be found in the Annex*

ANNEX

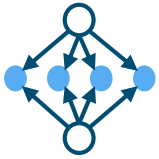
DATA MODELS*

CENTRALIZED
DATA AUTHORITY



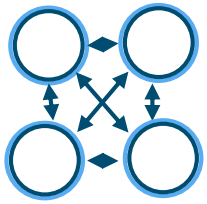
A single central solution stores and manages core citizen profile data (legal name, gender, address, marital status, dependents, citizenship). A single organization is responsible for administering this data, including providing support services such as help desk, data verification, and data quality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

FEDERATED
DATA AUTHORITIES



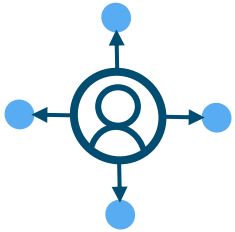
A single data authority will be designated for each context portion of citizen data (life data, residency/citizenship data). Each data authority is responsible for administering their portion of the citizen data and mapping that data to records in other data authorities through some form of a record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

**Data models were consulted with GC Data and Interoperability Communities of Practice*

SINGLE WINDOW INITIATIVES

Below are some sample government and non-profit single window initiatives:

- Argentina
- Estonia
- Province of Saskatchewan
- State of Michigan
- State of Ohio (for businesses)
- New South Wales (Australia)
- CERN (Conseil européen pour la recherche nucléaire)

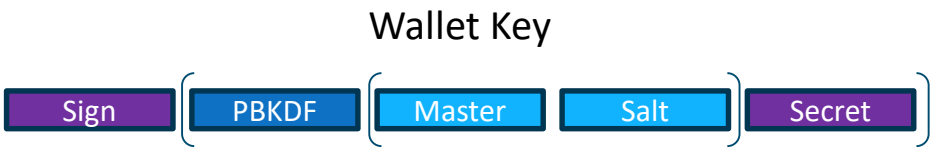
DIGITAL CREDENTIALS AND WALLETS INITIATIVES

Below are some sample government initiatives related to digital credentials and wallets:

- Known Traveler Digital Identity (Transport Canada with Netherlands)
- Innovation Solutions Canada Challenge (TBS/SSC)
- Opening a Business Bank Account (ISED with BC/AB/Banks)
- Digital Infrastructure Recommendations (ISED/TBS/Bank of Canada/TC/BC/AB/ON/QC)

Note: FPTM Joint Councils are also working on establishing a national sandbox to facilitate joint collaboration on digital credentials and wallets

DIGITAL WALLET PROTOTYPE – WALLET KEY



Functions

Sign

Secure Enclave Sign Operation
Purpose: Ensures the wallet is secured with data that never leaves the Secure Enclave (Reduces in memory attach vector)

PBKDF

Password Based Key Derivation Function
Purpose: Produces a hash that is computationally expensive. (Reduces vulnerability to brute force attacks)

Data

Master

User Generated Password
Purpose: Provides a means for the user to secure and access their Wallet. Is stored in the Keychain.

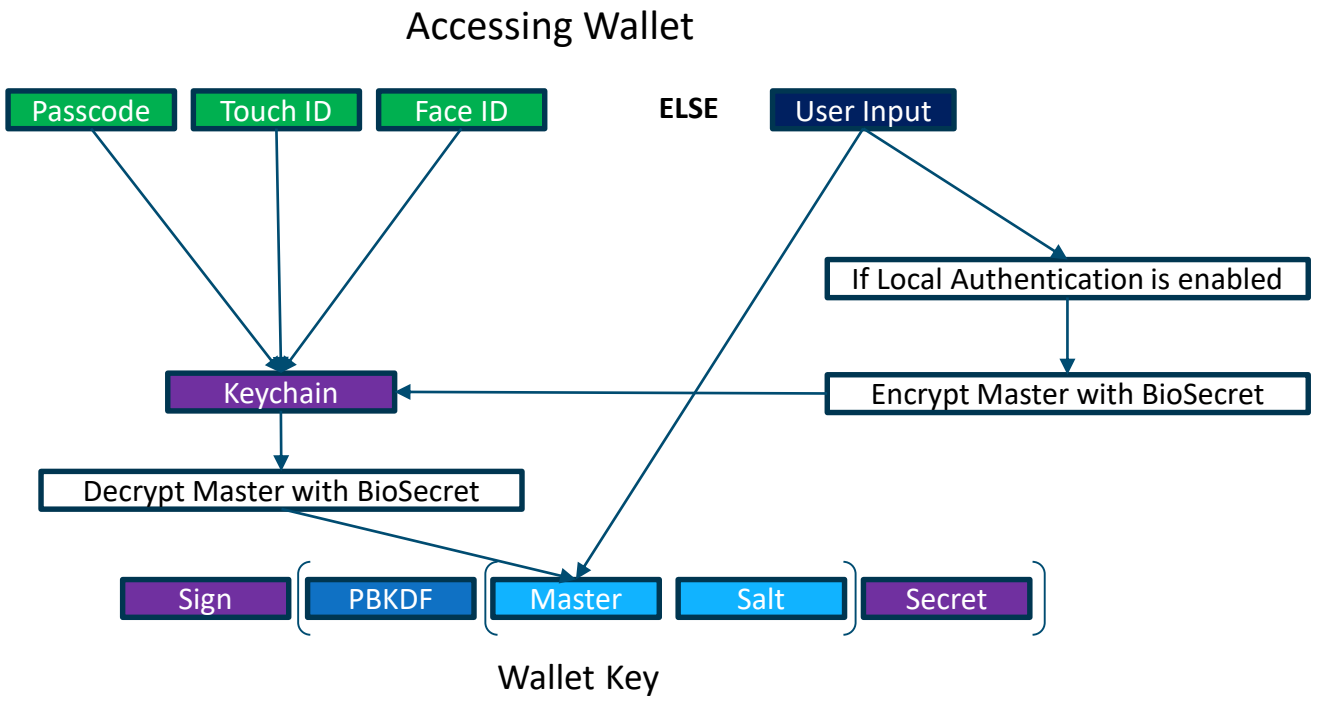
Salt

Device Generated Salt
Purpose: Uniquifies the hash produced from the PBKDF. Is stored in the Keychain. (Prevents Rainbow Table attack vectors)

Secret

Secure Enclave Secret
Purpose: Is a private key that cannot leave the devices Secure Enclave. Works with the Sign Operation.

DIGITAL WALLET PROTOTYPE – ACCESS



Term	Definition
Master (Password)	The primary password created by the user when creating a wallet. Or when accessing the wallet without Local Authentication.
Local Authentication	Passcode, TouchID, and FaceID
BioSecret	A secret in the Secure Enclave that invalidates and is unrecoverable if Local Authentication is changed or disabled
Secret	A secret in the Secure Enclave that is not associated with your Local Authentication