Ontario Digital Service (TBS) & Infrastructure Ontario

Digital Identity Market Engagement

Report on Key Findings from the Phase 1 Consultations (For Distribution)

January 2021

Infrastructure Ontario

Ontario

Engagement Notes

The mandate was to conduct a consultation process with variety of business stakeholders to start understanding their perspective on digital identity, key elements of the ecosystem, and role of government

Considering the importance of Ontarian adoption in the overall success of the ecosystem, public consultation is crucial to help in prioritizing use cases / verticals and identifying right conditions to drive adoption

Even though, the market consultation has provided some perspective on governance, business case, operating model, investment model, etc., these need to be defined and matured while executing prioritized use cases

The learnings from these initial pilots / use case launches will enable the government to scale the ecosystem with key conditions of success and performance indicators in place

Engagement Facts

12	139	68	5	100+
Weeks	Invitations Sent	Organizations Participated	Roundtable Discussions	Industry Experts Engaged

Executive Summary

1 A high-level analysis identified 16 benefit streams from the vantage points of individuals, businesses and Government – **at full scale, realizing these benefits could unlock ~$20 billion (directional based on further analysis) of economic value per year, with ~$8 billion directly attributable to Government**. Further analysis requires as part of the go-to-market strategy

2 **Five categories of insights were identified**, to help formulate views on a preferred business model to better position the Province to access the indicative value:

1)Government cannot do this alone
2)Value is driven by adoption, and adoption is driven by end-user participation
3)The funding model can be self-sustaining
4)Prioritize speed over perfection
5)Requires a dedicated team on an ongoing basis with buy-in across ministries and Government

3 **Key Next Steps:**

1) Develop an approach for public consultation, in order to understand behaviour-based user personas and the associated perceived value of specific digital, allowing for prioritization of use cases and industry clusters; and
2) Develop partnership model structures and test them, in order to determine how to optimally structure a future operating model, identify public and private sector partners to deliver end-to-end prioritized use cases, and to continue development of the business case for the ecosystem, including the associated financial model.

Unlocking maximum value from a Digital Identity ecosystem requires Ontario to closely collaborate with public and private sector stakeholders, and this engagement was the first step in that direction

OBJECTIVE

The Province is looking to develop a **Digital Identity (DI) ecosystem for both people and businesses to enable secure access to services anytime, anywhere, and from any device**. To realize the vision, the Province is looking to consult relevant public and private sector stakeholders in order to –

- Identify and assess the potential business model(s)
- Understand key elements to develop a successful partnership structure, including leveraging adoption to drive greater private sector participation and monetization
- Discuss case studies and key learnings from private sector experience and other jurisdictions

ONTARIO ONWARDS

This initiative is part of the Action Plan, which is a roadmap to improve the overall functioning of government at a rapid pace, based on lessons learned during the ongoing COVID-19 pandemic. The Action Plan outlines how government will:

- Make public sector services and service delivery **modern** and **customer focused**;
- Make public sector **digital and data- driven** and put data at the centre of government decision-making; and
- Increase **efficiency, effectiveness and speed** of government operations and decisions.
- https://www.ontario.ca/page/ontario-onwards-action-plan

MARKET CONSULTATION OVERVIEW

Engage like-minded public and private sector players to understand their perspective on digital identity, high value use cases, and where they are on the journey

Share Ontario’s point of view and gather perspective from key stakeholders on necessary elements in maturing the digital identity ecosystem

Devise a go-forward approach leveraging the public-private partnership including ecosystem offering, governance, technology, investment models and monetization approaches

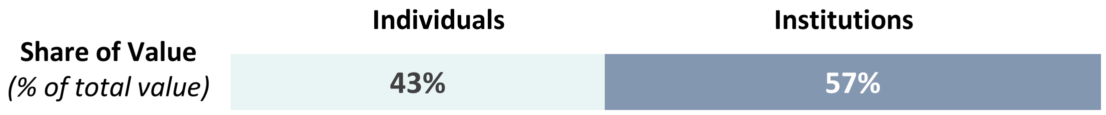
At scale, Digital Identity can unlock up to ~$20B of value for Ontario alone based on our bottom-up analysis with ~$8B directly attributing to the government

McKinsey & DIACC Analysis

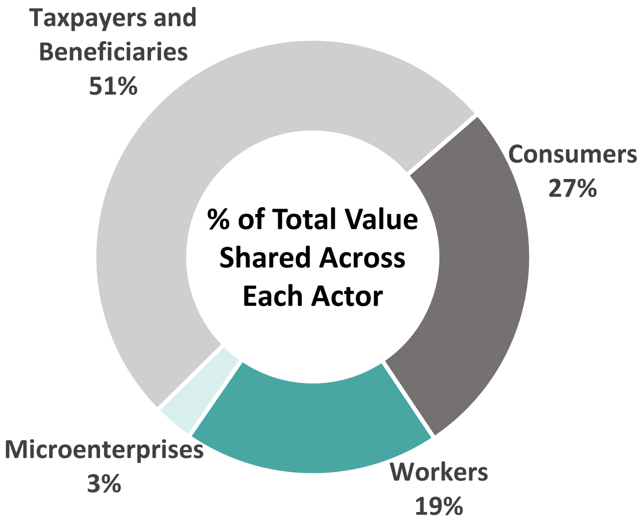
$8-$25B

(1-3% of GDP)

Based on studies by DIACC and the McKinsey Global Institute (extrapolating from the U.K. data), Ontario can generate between **1-3%** of GDP equivalent value through the **Digital Identity** ecosystem[1].



Outlined below is how the **Digital Identity** ecosystem can unlock value for individuals as they interact with firms, governments, and other individuals through a variety of roles…



Taxpayers and Beneficiaries; value achieved by individuals during interactions with public providers.

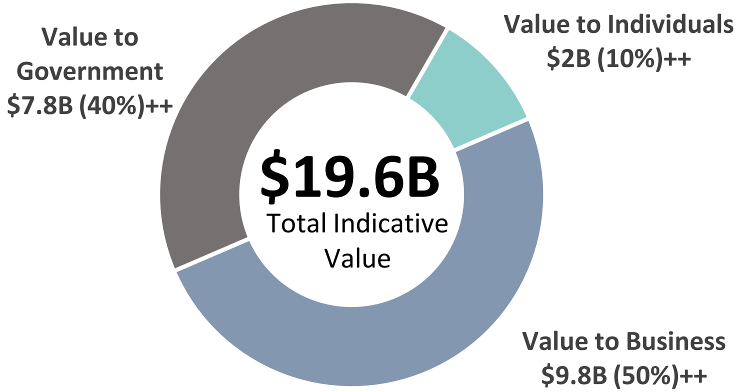
Consumers; value achieved by individuals during interactions with commercial providers.

Workers; value achieved by individuals during interactions with employers & the labour force.

Microenterprise; value achieved during interactions with consumers.

Internal Bottom Up Analysis

Our internal rough order of magnitude analysis leveraging ~35 value drivers and 100s of data points from various sources such as DIACC, McKinsey Global Institute, World Economic Forum, and others estimates suggest **Digital Identity** can unlock up to **$19.6B** in economic value for Ontario.



Selected examples of potential value generated across government and business

$0.6B
Businesses can save by reducing the effort required to monitor retail-based fraud

$1.1B
Businesses can save by reducing customer onboarding and servicing costs

$1.2B
Value accrued to Government through efficient delivery of services and benefits

$0.9B
Value accrued to Government by improved credentialing and reducing benefit leakage / fraud

[1] McKinsey Global Institute – Digital Identification Report; U.K values used as a reference.

__Note:__ These are rough order of magnitude estimates; specific values and assumptions identified are indicative and are for illustration purposes to be validated in subsequent phases

We can distill the key insights from the market consultation process in the following five themes, and successful execution on these can create a much-desired value creation for the ecosystem

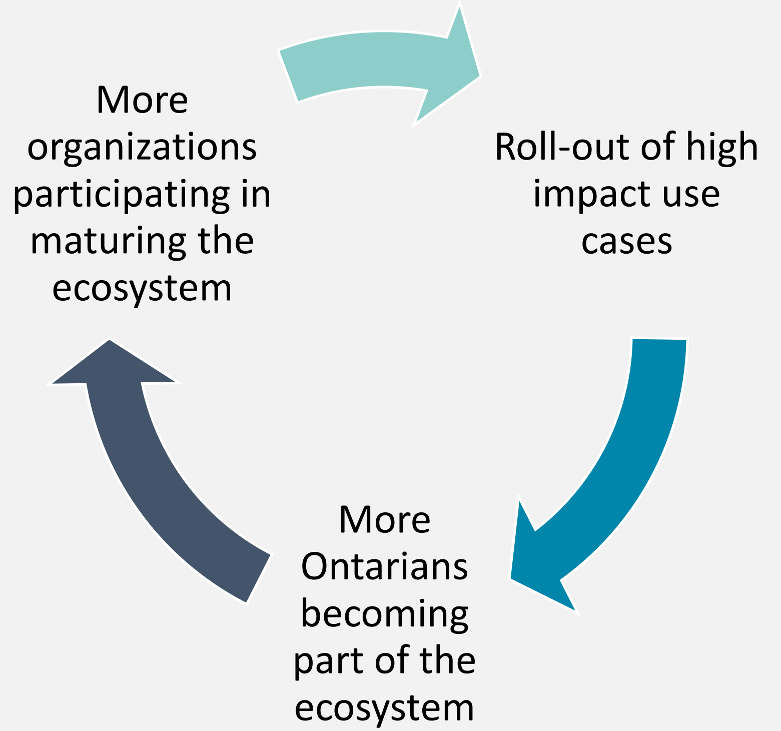
Business Model Themes

1. Government cannot do this alone
2. Value is driven primarily through end-user participation
3. The funding model can be self-sustaining

Execution Themes

4. Prioritize speed over perfection
5. Requires buy-in across ministries and Government and close collaboration with private sector

Enabling these five themes can lead to a virtuous cycle driving ecosystem maturity and adoption



More organizations participating in maturing the ecosystem

Roll-out of high impact use cases

More Ontarians becoming part of the ecosystem

Through the establishment of key partnerships, Ontario can create an efficient marketplace, reimagine government service delivery and drive economic growth, accelerating value to Ontarians

Create an Efficient & Secure Marketplace

By partnering with like-minded public and private sector organizations, Government can ***accelerate the creation of digital identity marketplace*** leading to:

- The ability for businesses and entities to ***execute transactions efficiently***
- ***Appropriate oversight and regulation*** to ensure security, privacy and inclusivity
- A ***financially viable platform,*** preventing any undue burden on taxpayers

Reimagine Government Service Delivery

The ability to securely verify a person's identity can provide exceptional capability to the government on ***how services are delivered*** in the future. For example:

- **Reduced reliance** on **in-person** transactions and physical credentials
- The ability to roll out completely ***new service delivery models*** e.g., outcomes based primary care
- ***Reduction in fraud*** while providing ***exceptional experience*** to Ontarians

Drive Economic Growth

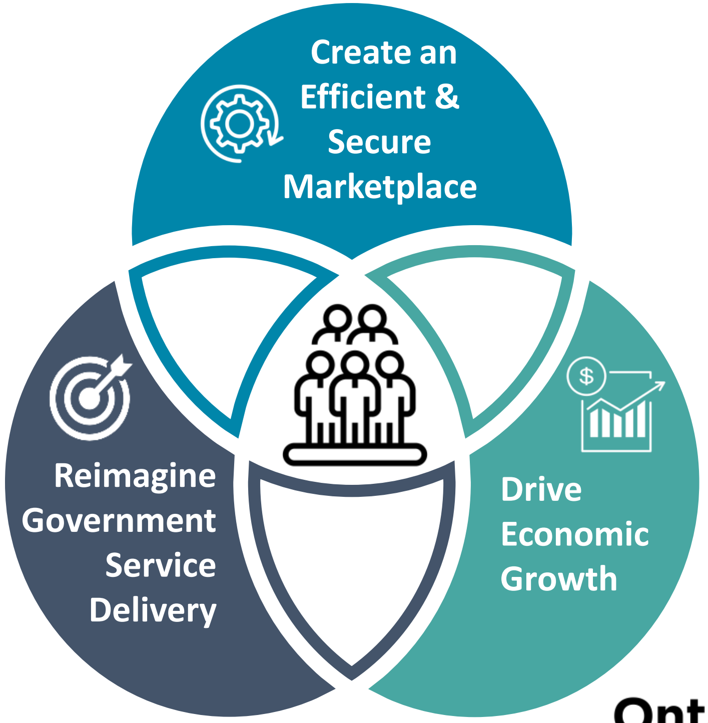
The ecosystem will drive ***innovation and attract investments*** as businesses may:

- ***Easily move to digital*** without being encumbered by the need of securing / managing user data
- Build ***new products and services,*** *which would* leverage capabilities provided by the digital identity ecosystem
- Redirect funds to ***higher value activities,*** driving economic growth

Convergence of the Ecosystem

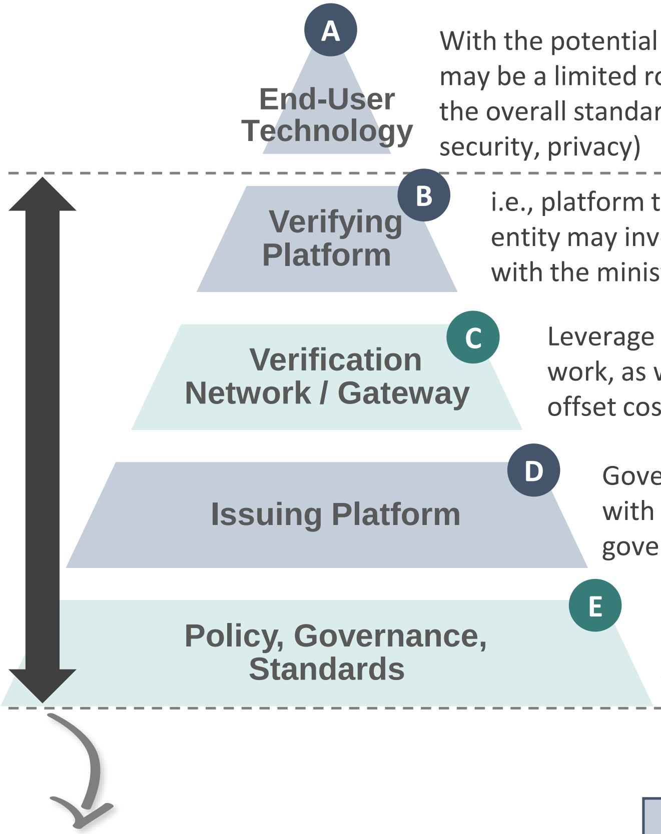
Greatest value to Ontarians is realized at the convergence of an efficient marketplace, reimagined service delivery, and economic growth :

- ***Provides Ontarians the opportunity to participate in a digitally native society*** in which accessing any kind of services becomes as easy as making a phone call
- ***Enables the launch of new digital services*** informed by advanced analytics in the matter of weeks rather than years
- ***Establishes the Province as a thought leader***, opening the door for future partnerships with other jurisdictions, across Canada and internationally


Create an Efficient & Secure Marketplace
Reimagine Government Service Delivery
Drive Economic Growth

1 Government cannot do this alone

The DI ecosystem can be divided into five core components, of which Government plays a role in four (B-C-D-E), though close collaboration with other entities is required to successfully establish infrastructure and enable broader user / stakeholder participation



A — With the potential for multiple wallets in market, there may be a limited role for government apart from setting the overall standards and guidelines (e.g., interoperability, security, privacy)

B — i.e., platform to verify credentials – Each organization / entity may invest on their own; ODS may need to work with the ministries to develop the best fit solution

C — Leverage broader National Digital Infrastructure work, as well as public-private partnerships, to offset costs and prevent duplication of efforts

D — Government will leverage technology in market, with market creating credentials based on government issuing the foundational identity

E — Close collaboration required to understand overall policy and governance needs, and to test/adopt standards.

Elements that may require direct role and investment by Government and ministries

▨ Mostly decentralized, associated technology and processes could be owned and managed by ***independent organizations / technology providers***

□ Associated technology and processes may require **closer public-private partnerships / alignment**

Considerations based on Market Consultation

A Most participants believe that government may not need to own the end user technology, though appropriate standards and approval processes needs to be in place to ensure security, privacy and interoperability of the solutions. Government should work in partnership with standards bodies in order to certify products.

Key components: Secure containers (e.g., digital wallets) that may sit on devices (e.g., phones)

B Focus on enabling multi-channel experiences to ensure inclusion, incenting businesses to leverage digital credentials across the economy to drive adoption and realize benefits.

Key components: Devices and technology to initiate verification / connect with the wallet & network

C There were mixed perspectives on government involvement in the verification network / gateway; however, there was consensus among respondents that interoperability of future networks / solutions is of paramount importance.

Key components: Actual network (could be blockchain based) to verify credentials

D Respondents indicated that a unified issuing platform across government can optimize government investment. When looking at issuance of credentials, it is important to examine more than one standard when building the credential itself.

Key components: Core back-office applications, Infrastructure, Databases, Integrations / APIs, and Change management; physical establishment and enrolment infrastructure may get owned and managed by ministries, as today

E The government must play a significant role in bringing different stakeholders together and enabling a consistent approach for the overall policy, governance and standards of the ecosystem, including establishing legal and regulatory frameworks.

Key components: Human resources to establish and maintain policy and governance, associated technology and real estate needs, and to collaborate with market to successfully adopt standards

Government = Ministries, Agencies, Premier's Office, etc.

Benefits can be realized across the three core operating models when viewed independently, however market feedback strongly suggested a hybrid approach to ecosystem operations, and leverage benefits from each model collectively

Centralized

Government is accountable for collecting user attributes, issuing digital credentials and authenticating users

- ✓ Model allows for perpetual integrity of information
- ✓ Private sector partners could participate by providing inputs, data sources, and/or assurance checks
- ✓ Potential to drive high levels of adoption, if participation is mandatory in order to access certain Government services
- ✗ Centralized storage of data reduces user privacy, given users do not have control over where their information is stored
- ✗ Significant responsibility for Government to setup and manage the service
- ✗ A centralized data repository can heighten security risks

Federated

Multiple accredited identity providers collect, store, and manage attributes / credentials and authenticate users

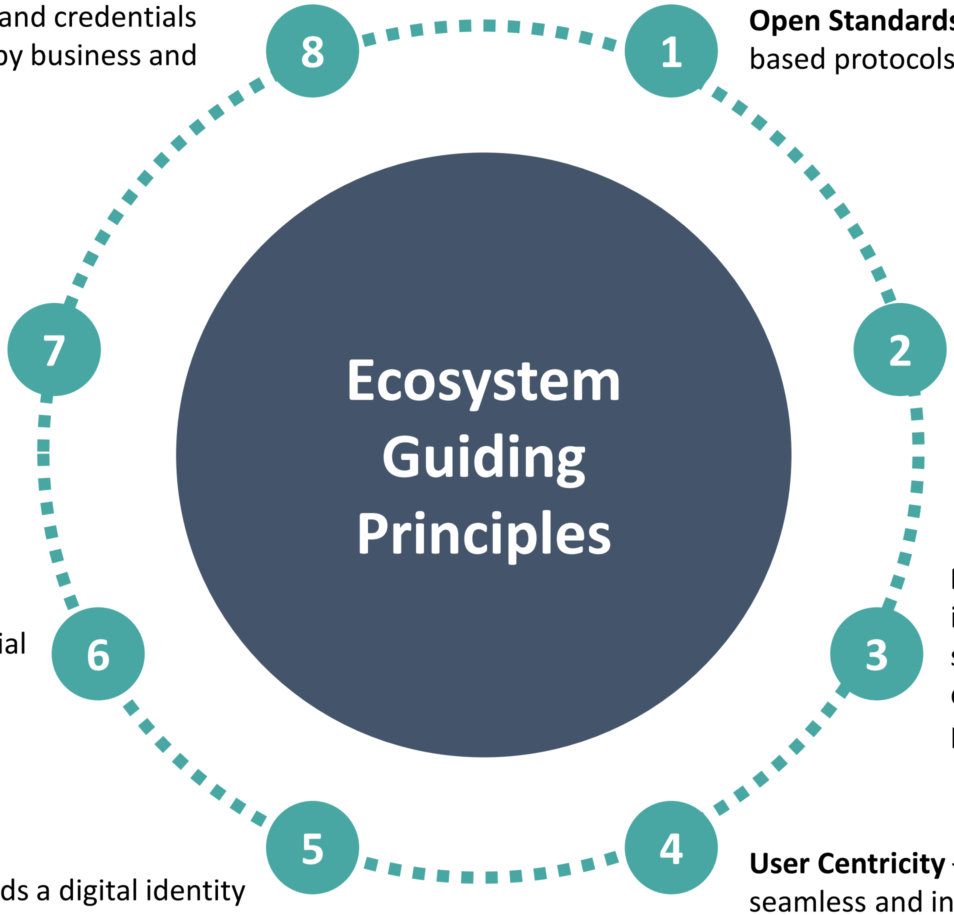
- ✓ Useful when large networks of providers have sufficient capability in identity proofing – could be helpful should identities cross jurisdictions
- ✓ Model helps to spread operating costs over a number of providers
- ✓ Responsibilities can be optimized based on who is best suited to own the scope (e.g., Government could issue identity credentials, while private sector can lead in other areas such as financial information, education credentials as well as enablement of use cases)
- ✓ This model enables a more flexible digital identity ecosystem, which provide organizations the opportunity to act as IDPs, and drive coherent policies / standards across the ecosystem
- ✗ Data / identity fragmentation across multiple entities could create confusion for end users

Decentralized

Any organization can play the role of identity provider as long as they abide by ecosystem rules and practices

- ✓ Completely open ecosystem with limited regulatory oversight
- ✓ Reduced influence over the ecosystem by any one stakeholder group
- ✗ Greater reliance on organic adoption, increasing overall uncertainty of adoption
- ✗ Significant effort required to educate the general public on the mechanics and benefits of the ecosystem
- ✗ Minimal channels for recourse should a user's identity be compromised, or they encounter a problem

The following eight guiding principles that are developed based on jurisdictional research and market consultation will serve as a bedrock as the ecosystem is built and matured



1 **Open Standards & Interoperable** – Built on open, standards-based protocols, and interoperable with international standards

2 **Robust, Secure and Scalable** – Ecosystem has state-of-the-art capabilities to prevent against fraud and identity theft, and is easily scalable

3 **Privacy by Design** – Systems, practices and infrastructure used in the ecosystem are designed to support privacy, promote user control over their own data and ensure personal and sensitive data is protected

4 **User Centricity** – Services enabled by the ecosystem are seamless and intuitive, leverage innovative technologies and are convenient and efficient

5 **Inclusive** – Anyone who wants or needs a digital identity is easily able to obtain one – ecosystem meets broad stakeholder needs

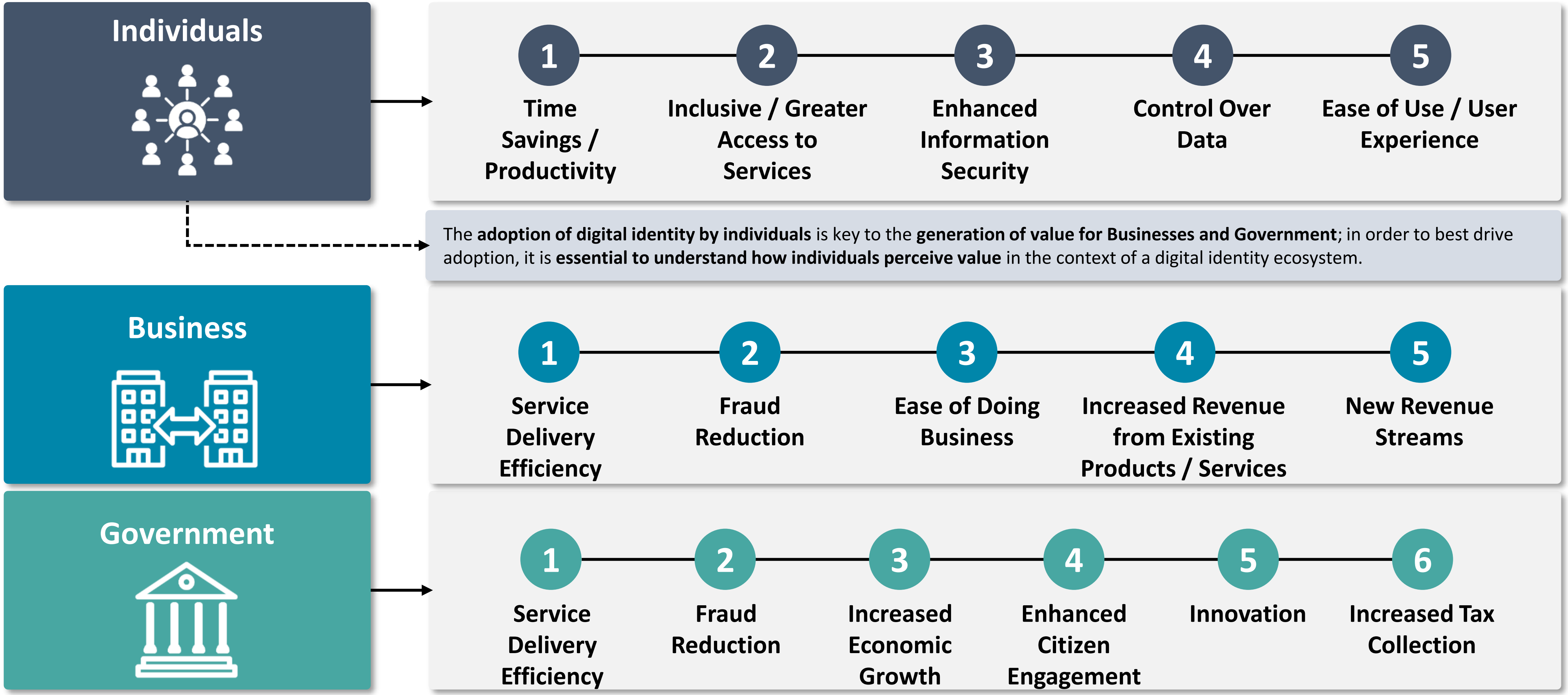
6 **Financially Viable** – Doesn't result in undue financial burden on taxpayers, and is open to competitive market forces

7 **Distributed** – Data is stored and maintained where it's created, by users and individual identity providers (IdPs)

8 **Verifiable Identity & Credentials –** Identity and credentials meet appropriate assurance levels defined by business and security requirements

2 Value is driven primarily through end-user participation

In order to generate greater value to ecosystem stakeholders, we must understand how individual users of the ecosystem perceive value, and focus on creating this value through initial use cases, which in-turn drives greater user adoption



Individuals

1. Time Savings / Productivity
2. Inclusive / Greater Access to Services
3. Enhanced Information Security
4. Control Over Data
5. Ease of Use / User Experience

The **adoption of digital identity by individuals** is key to the **generation of value for Businesses and Government**; in order to best drive adoption, it is **essential to understand how individuals perceive value** in the context of a digital identity ecosystem.

Business

1. Service Delivery Efficiency
2. Fraud Reduction
3. Ease of Doing Business
4. Increased Revenue from Existing Products / Services
5. New Revenue Streams

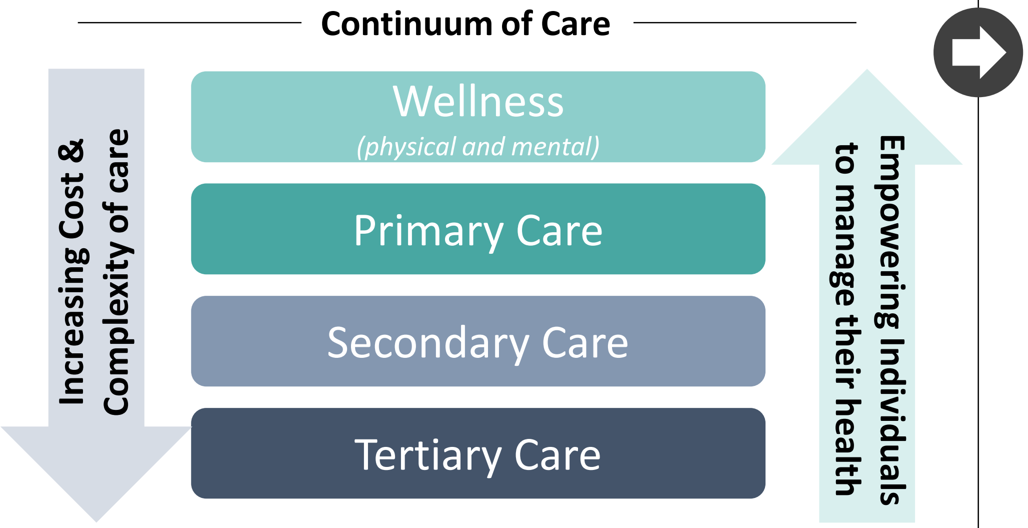
Government

1. Service Delivery Efficiency
2. Fraud Reduction
3. Increased Economic Growth
4. Enhanced Citizen Engagement
5. Innovation
6. Increased Tax Collection

2 Value is driven primarily through end-user participation

To enable amplification of value and a more structured rollout of the ecosystem, Government should focus on taking a vertical approach by maturing ‘clusters’ of use cases in a particular sector, such as healthcare

The province currently spends ~$65 Billion every year to provide healthcare to Ontarians, yet the system faces challenges with overall access to primary care as well as high wait times for specialist services. The cost and complexity of the system also increases significantly as we move further down into the continuum of care



With the increasing trend towards taking control of one’s own health, exponential improvements in health tracking and remote monitoring capabilities (e.g., smart glucose meters), and better coordination between a variety of providers, can allow Ontario to make a step change in both costs and quality of health services

Every 1% improvement in health care costs can save the Province upwards of $600 M while improving outcomes for Ontarians

Enabling Ontarians to easily understand all healthcare services and enrol in the appropriate ones

Seamless capture of consent and transfer of electronic medical records between a variety of providers

E-prescription as well as ability to view current / past prescribed drugs reducing unintended consequences

Remote patient monitoring actively triggering alert for earlier intervention

Telehealth and remote monitoring reducing the need of physical healthcare infrastructure

Better data capture enabling improved claims and reimbursements both for in and out of province patients

Analytics on cohorts of patients providing insights on new ways of care and innovation

Enabling moving from the current fee-for-service models to value based care models

3 The funding model can be self-sustaining

A number of different investment models were discussed during the process and the final solution could be a hybrid of the options presented below; private sector entities seemed to be willing to make investments as long as the business case and partnership structures are clear and compelling

Options discussed

- Government is the Sole Investor
- Public and Private Sector Entities Combine Investments
- Technology Providers are the Investors

Based on market feedback, **combining public and private sector funds** appears to be the preferred funding approach

- ✓ Shared funding model provides substantial **incentive for both public and private sector to ensure success** of the ecosystem
- ✓ Provides the **opportunity for improved collaboration across ecosystem participants**, with private sector providing leading edge technology and expertise and the public sector kick starting the ecosystem by enabling data use and financial support
- ✓ **Funding risk is shared across the public and private sector**, while private sector may be able to take advantage of public sector cost of capital through different means

The Role of Government

- There are multiple roles government could play in regards to the investment model:
  - a) Seed investor to enable primary as well as edge cases
  - b) Investments to mature internal capabilities
  - c) Providing grants for specific organizations
  - d) Providing funding incentives for smaller businesses

Recovering Ecosystem Investments

Ecosystem investments could be covered using a combination of maintenance and transaction fees to the participants followed by charges associated with establishing and retaining credentials; any potential model need to consider impact on small and mid size organizations to ensure they don't get excluded if the costs are too high plus should not have adverse effect on end user adoption especially the ones from underprivileged backgrounds (e.g., unbanked, undocumented, remote communities, homeless, refugees, Indigenous). Government could also recover ecosystem investments through taxes.

4 Prioritize speed over perfection

Use cases vary across sectors and can easily proliferate into a daunting implementation challenge, however even by starting with a single high-impact use case, there is opportunity to bring significant value to ecosystem users in a streamlined manner

Public Sector (Federal, Provincial, Municipal)

- ✓ Mobile Driving License, Registering vehicles (including farm vehicle)
- ✓ Municipal: applications, licenses & permits, inspection, rental, transit
- ✓ ServiceOntario services / e-services
- ✓ Other licenses (e.g., hunting, fishing, firearms)
- ✓ Grants & Benefits: EI benefits, social assistance, ODSP
- ✓ Vital events: Birth, Marriage, Death certs.

Financial Institutions

- ✓ Customer onboarding and verification
- ✓ AML / KYC Compliance
- ✓ Ability to securely access and share banking data without compromise
- ✓ Canadian and foreign tax reporting

Health

- ✓ Health – accessing and transferring medial records, POA
- ✓ Digital insurance, pharmacy, hospital
- ✓ Proof of vaccination

Most mentioned sectors / use cases

Travel

- ✓ Digital passports, NEXUS, travel / work visa
- ✓ Frictionless Travel: Airport, Hotel check-in, accessing services

Indigenous

- ✓ Verifiable Indigenous ID

Education & Certifying Bodies

- ✓ Regulated professional licenses (e.g., law society license)
- ✓ University degrees & High School diplomas
- ✓ Micro-credentials & digital badges

Telecom

- ✓ Identity Validation and proofing for new prospects
- ✓ Acting as a source of secondary / multi factor authentication

Legal

- ✓ Digital contracts, signatures, execution & compliance

Real Estate

- ✓ Registering / owning a property, home or business
- ✓ Rent apartment or houses, car rental

Other Businesses

- ✓ Ability to prove their relationship with a business (e.g., owner)
- ✓ Secure access to employees, customers, and other stakeholders
- ✓ Verification for businesses moving products and services online
- ✓ Eligibility to work, employment checks, onboarding
- ✓ Import / export licensing and documentation
- ✓ Business registration, permits & licenses
- ✓ Filing taxes

Ontario Residents

- ✓ Providing proof of age (e.g., alcohol, casino)
- ✓ Smart cities: monitor devices and sensors e.g., energy usage, air quality, traffic congestion
- ✓ Password less authentication; digital onboarding

5 **Requires buy-in across ministries and Government and close collaboration with private sector**

We recommend to start with the following next steps that complement the ongoing digital wallet implementation

1	**Launch public consultation** in order to understand behaviour-based user personas and the associated perceived value of specific digital, allowing for prioritization of use cases and industry clusters	January 2021
2	**Develop go-to-market and partnership execution strategy** in order to determine how to optimally structure a future operating model, and identify public and private sector partners to deliver end-to-end prioritized use cases	March 2021
3	**Implement digital credentials for prioritized use cases** to inform standards, governance and technology for the ecosystem.	Starting 2021
4	**Continue to monitor key ongoing activities** including standards design, policy and legislation development, as well as other program management and oversight activities – standards, policy and legislation require **close collaboration with federal, municipal, as well as other provincial entities**	Ongoing

5 Requires buy-in across ministries and Government and close collaboration with private sector

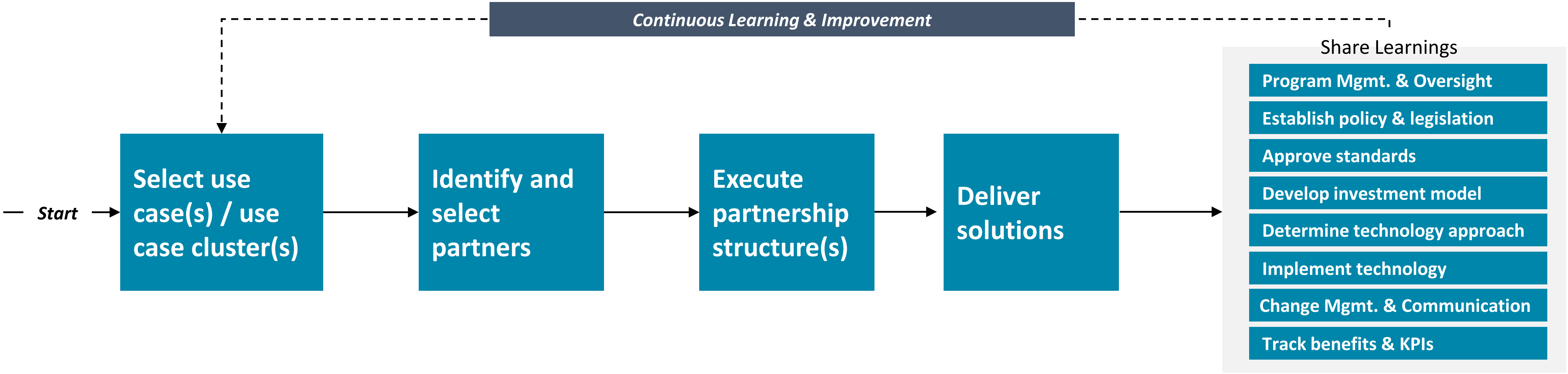
We will pick a few prioritized use cases and partners to deliver initial offerings, in parallel we will create a go-to-market strategy to drive implementation over the next few years

Why is this important?

- Key to the successful rollout of a digital identity ecosystem are strong partnership arrangements between Government and its ministries, and the private sector – this concept was further reinforced through feedback from market consultation and roundtable participants
- Partnerships can accelerate the creation of a digital identity ecosystem, leading to the ability for businesses and entities to execute transactions efficiently, appropriate oversight and regulation to ensure security, privacy and inclusivity, and a financially viable platform, preventing any undue burden on taxpayers

When will it happen?

- Initial work to commence over the first six months of 2021, with additional phases being rolled out subsequently as the year progresses


Continuous Learning & Improvement

Start

Select use case(s) / use case cluster(s)

Identify and select partners

Execute partnership structure(s)

Deliver solutions

Share Learnings

- Program Mgmt. & Oversight
- Establish policy & legislation
- Approve standards
- Develop investment model
- Determine technology approach
- Implement technology
- Change Mgmt. & Communication
- Track benefits & KPIs

APPENDIX

Market Consultation Insights – Summary

Here is a summary of some of the key insights on overall ecosystem and offering from the market consultation process

Ensure appropriate governance from the start

- Provide **fundamental protections** for data privacy and security, ensuring ‘privacy-by-design’ and offering users control over data
- Establish **consistent standards in consultation with various bodies**, simplifying the required technologies and experience, while also driving trust and adoption
- **Minimize identity fragmentation** by preventing too many identities spread across too many entities and reuse existing data points, attributes, and components, where possible
- Create a **communication channel** between ecosystem participants in order to simplify interactions between them
- Ensure **interoperability** as the ecosystem matures across jurisdictions, considering alternative credentialing standards and models to optimize user experience
- **Empower existing communities and regulatory bodies** to provide credential oversight, while providing domain-specific governance to enable specific needs (e.g., law society for lawyers)

Build services and offerings around Ontarians needs and aspirations

- Enable a **citizen-centric view** with a focus on high value use cases can help drive user adoption and engagement
- Prioritize **frequent & cumbersome private sector use cases** to drive adoption, while also providing incentives to organizations supporting citizen enrollment
- Leverage **existing use case flows** (e.g., driving license application) to drive enrolment, ideally those that are relatively seamless and secure
- Design **use case based attribute sharing** (e.g., road-side stop profile), permitting only relevant information to be shared to the Relying Party
- Introduce **awareness and engagement campaigns**, communicate the value and of the offering to Ontarians, while providing peace of mind around handling of sensitive information
- **Device possession during verification** with a clear understanding of what information is being requested before sharing

Focus on inclusion, control and simplicity

- Solutions should cover a range of attributes, offerings and features, to provide **maximum flexibility and accessibility**
- Provide **control and ownership over the identity**, offering users the ability to discard any credentials previously accepted and the option to abolish their digital identity if needed; there were differing views on the use of biometrics
- Focus on **inclusion of unbanked and undocumented Ontarians**, by building on existing municipal inclusion policies and considerations with the **ability to verify offline** especially in remote parts of the country
- Enable **digital attestations** to facilitate value-add use cases such as digital insurance slips and digital university transcripts
- Focus on **simplified User Interface** to be able to display relevant information in easily accessible manner

Here is a summary of some of the key insights on technology & operations from the market consultation process

Think Big, Start Small, Scale Fast

- Take a **Minimum Viable Product (MVP)** approach to deploying the ecosystem, while keeping the bigger picture in mind, in order to make incremental progress
- Consider the advantage of an **advanced end-user solution such as Wallet+** to generate greater interest in the ecosystem and potentially increased user adoption
- Enable **omni-channel capabilities** to provide capabilities to use digital identity across networks and devices
- Leverage **data analytics** to understand authentication behaviour, studying characteristics and approaches established by Financial Institutions and Telecoms
- Consider **owning the verification gateway** similar to the model developed by the Digital Transformation Agency in Australia
- **Open competition** among technology providers enabling innovation, lower prices, increased efficiency, a variety of offerings, and user-driven choice

Continue to iterate leveraging emerging technologies and standards

- Adopt a **Microservices Architecture** approach and leverage API based services, ensuring that the ecosystem can operate efficiently and quickly innovate via incremental improvements
- Facilitate **ongoing engagement** for continuous improvement and interoperability, while also providing a sandbox to allow partners to test new features and suggest improvements (i.e., build and learn use cases)
- Leverage **learning from existing projects** built on common standards, to accelerate implementation and reduce risks
- Continue to **monitor new standards** beyond verifiable credentials, to enable best practices related to scalability, security and privacy
- Allow for **platform extensibility** to enable future use cases such that key scenarios and services can evolve over time

Simplify and standardize where possible

- Create single identity issuance system across ministries allowing all organizations to maintain control and provenance over their respective issued credentials, while **leveraging a common infrastructure**
- Leverage **traditional access management standards**, to enable consistency when providing requisite details to a service as a means of verifiable proof
- Enable **tiered authentication** with more secure checks for higher risk transactions, to streamline authentication processes, and reduce bandwidth requirements.
- Create **appropriate safeguards** to protect user's identity, potentially leveraging concepts such as 'devaluing of information' and 'zero-knowledge proof'
- Even though including a **mobile number** as a key attribute may enable easy linkage to the account holder and quick verification, there are mixed perspectives on the same due to associated security concerns
- **Prevent duplication of information** to streamline platform operations and data capture

We also heard a few more considerations on regulatory framework and governance, as well as risks and mitigation strategies

Considerations to Establishing a Regulatory Framework

- Closely manage overall governance, as well as control and access to public assets
- Legislation ensuring the legal equivalency of Digital ID
- Review regulations requiring two pieces of ID
- Meeting national and international regulations such as EU AML laws
- Clear and well-defined liability model with appropriate penalties for misuse

Additional Governance & Authority Considerations

- Clarity on information sharing including which wallets or applications can hold credentials
- Third / neutral party oversight & full public consultation
- Eliminating systemic bias by collecting broad sociodemographic information or other necessary means
- Leverage existing working groups & infrastructure

Select Risks & Mitigation Strategies

Cybersecurity attacks

- Government should lead, manage and / or own security framework principles
- Decentralized digital identity solutions
- Secure PKI ID Management

Privacy violations

- Ensure built-in privacy provisions such as data minimization and proportionality, robust governance / controls, and an established rule of law
- High-assurance digital ID programs reduce the risk of credential forgery and unauthorized use
- Use double blind credential sharing between IdP and RP

Lack of standardization

- Leverage technical blueprints and standards produced by industry thought leaders
- Consider modular architecture separating the business applications, the wallet, data registry, and communication protocols

Lack of qualified resources

- Work with a partner with deployable infrastructure
- Consider modular architecture separating the business applications, the wallet, data registry, and communication protocols

Slow user and institution adoption

- Human centered design principals and tools are essential to driving enrollment and adoption

Market Consultation Insights – Detailed

Ecosystem & Offering

Ecosystem & Offering Insights (1 of 4)

1

Fundamental protections for data privacy and security

- ✓ Leverage ‘privacy-by-design’ approach to establish fundamental data security protections and implement a self-sovereign identity approach to provide users free control over what data is shared and with whom, when and the reason for access (unless related to national security or criminal behaviour). Engaging privacy experts early on could be highly beneficial
- ✓ Standards for guarding against intrusion leveraging a distributed data approach to avoid concentration of high-risk information

2

Citizen centric view with a focus on high value use cases

- ✓ Preparing a comprehensive list of use cases and identifying the highest priority ones (including the ones from the private sector) can drive user adoption and engagement
- ✓ Offering financial and other incentives to selected private sector participants can also drive furthering of use cases
- ✓ Develop a user centric experience identifying interaction points across the journey to ensure a consistent, intuitive, and compelling experience
- ✓ Use cases that involve young adopters (e.g., high school and universities) may accelerate the process

3

Cover a range of attributes, offerings and features

- ✓ The scope of offerings could go well beyond the basic biometric data (name, date of birth, address, phone, email, etc.) to any individual / business specific data or documentation that may benefit from being administered via a DI ecosystem as well as flexible enough to deviate from Eurocentric norms (e.g., people without first and last names, non-Latin alphabet characters, gender fluid ID categories). The solution may store a number of documents securely in digital format that are pushed directly by the organizations
- ✓ Some frequent examples included –

  ○ Driver’s licenses
  ○ Health data
  ○ Vehicle data
  ○ Social Insurance
  ○ Relationships
  ○ Criminal Record
  ○ Citizenship certificate
  ○ Educational certificates
  ○ Business – corporation number, ownership, board of directors, etc.
  ○ Photo of user
  ○ Digital signatures

4

Prioritize frequent & cumbersome private sector use cases to drive adoption

- ✓ Showing the value delivered through digital ID as-soon-as-possible may require identifying the touchpoints that are more frequent and cumbersome, with some of those residing within the private sector (e.g. Argentina worked with banks to transform the customer onboarding process to accelerate adoption).
- ✓ Scale the program by adding public and private sector use cases in parallel including providing incentives to organizations supporting citizen enrolment (e.g., Post offices in India).
- ✓ Involve RPs early on such as Elections Ontario, Liquor Control Board of Ontario, Ontario Cannabis Store, or Ontario Lottery and Gaming for age of majority verification, and selected private licenced retailers.

Selected Statements

As the orchestrator of the ecosystem, the government should define as many public-sector uses as possible and focus on adding attractive private-sector use cases early on. Including a wide range of private sector use cases is critical because this will drive regular user engagement and broad adoption.

DigiLocker, in India, is a digital platform for issuance and verification of paperless documents and certificates. Citizens are able to access the digital document locker through a unique verifiable identification number known as Aadhaar. Each DigiLocker account can store a variety of documents provided by different issuers, who are all connected to the DigiLocker platform. The benefits of such systems include simplified access, verification, renewal, and replacement.

Ecosystem & Offering Insights (2 of 4)

5 Leverage existing use case flows to drive enrolment

- ✓ Utilize seamless, but secure enrolment / registration processes using existing use case flows (e.g. during driving license issuance) vs. a decentralized enrolment process (e.g., dedicated campaigns for digital identity enrolment).
- ✓ Consider opt-out vs opt-in measures for enrolment can further drive adoption; some respondents advised to only go for an opt-in approach.
- ✓ Contactless methods such as video chat could also be used in issuing digital credentials to Ontarians.

6 Use case based attribute sharing

- ✓ The mobile driving license POC from Virginia allowed the credential holder to select the applicable use case, which would allow the relying parties to retrieve the appropriate information.
- ✓ For example, a road-side stop profile would release all the information found on physical license, whereas the age verification profile would release only the photograph and indicators of the holder is younger or older than a certain age.
- ✓ This design consideration reflected the learnings from a series of security and privacy threat assessments.

7 Consistent and Government-led standards

- ✓ Striving for a consistent and standardized method to identify individuals that is agreed upon with the key players could simplify the required technologies and overall experience
- ✓ Further, government-led foundational evidence of identities would play a key role in driving trust and hence the usage and adoption of digital identity services. This would also require a governance framework stipulating the legal, business and technical rules

8 Digital attestations to enable value add use cases

- ✓ Ability of a digital identity owner to offer their own attestation to a digital identity holder in the form of a verifiable credential would enable the likes of insurance companies to offer digital insurance slips and universities to offer credentials for digital transcripts

Selected Statements

Successful private and public sector collaboration leverage a collaborative framework and problem-centric challenge model. Individual challenges allow organizations to cluster around areas that they can contribute most, while the outcomes of challenges can be shared across collaborative members. These challenges are executed within an overarching public-private governance framework that has oversight and insight into all challenges.

Ontario must bring more to the ecosystem than just a wallet that contains trusted credentials. The approach of 'build it and they will come' has failed many times over in the digital ID space. Take the current mobile ID initiative available to Oklahoma residents for example; a mobile wallet that verifies identity and can store government issued digital versions of the state ID or driver licence. After being available for a year, at a cost of $0 to the state resident, we calculate less than 1.5% of the addressable user base has enrolled. With such low user participation rates, there is a reluctance from relying parties to invest and accept the credential.

Ecosystem & Offering Insights (3 of 4)

9 Minimize identity fragmentation

- ✓ Too many digital identities spread across multiple entities and each managed in isolation make it confusing and cumbersome for end users to use the product
- ✓ Wherever possible, existing data points, attributes and components should be reused rather than recreating / duplicating them

10 Communication channel between ecosystem participants

- ✓ Option to have a private and secure digital communication channel with other participants to exchange additional credentials, verification, or authentication requests. This may simplify frequent interactions between ecosystem participants and may facilitate additional value add use cases, such as the government sending reminders to citizens for upcoming license renewals

11 Control and ownership over the identity

- ✓ The identity holders should be able to recover, access and control identity from different devices or when they replace devices
- ✓ Option to delegate the identity to a trusted third party or proxy to participate in the ecosystem on their behalf with due considerations for accessibility
- ✓ They could also have the flexibility to discard any credentials they have previously accepted, as well as the ability to abolish their digital identity altogether

12 Ensure interoperability as the ecosystem matures across jurisdictions

- ✓ As other jurisdictions implement their own digital identity vision, Ontario may have to consider alternative credentialing standards and model to provide the best experience for Ontarians traveling outside the Province

13 Enable existing communities to provide oversight on credentials

- ✓ Allow communities / regulatory bodies / associations to set required attributes for relevant credentials (e.g., law society for lawyers, Professional Engineers Ontario for P.Eng.)
- ✓ Similarly the overall governance could also be domain-specific to enable specific needs e.g., financial services, health, travel, education, services

Selected Statements

Successful private and public sector collaboration leverage a collaborative framework and problem-centric challenge model. Individual challenges allow organizations to cluster around areas that they can contribute most, while the outcomes of challenges can be shared across collaborative members. These challenges are executed within an overarching public-private governance framework that has oversight and insight into all challenges.

For Estonia, a community of popular public and private sector parties adopted the digital ID worked well for Estonia. This included banks accepting the credential as the only method for users to login and access online banking; online banking is a flagship service and is a significant draw for digital ID enrolment.

For New Zealand, easier for people to enroll and on-board high value service drove adoption after slow uptake in the first two years. Today, almost 20% of New Zealanders have accounts and verified their identity, and there are 22 services across 17 organizations that support RealMe allowing users to access and conduct services online.

Ecosystem & Offering Insights (4 of 4)

14 Awareness and engagement campaigns

- ✓ Some proponents highlighted the importance of social media campaign combined with print, press releases and tv advertising to drive awareness and engagement
- ✓ Further, education of users to the security behind the service that is handling their personal information can provide much needed peace of mind to Ontarians
- ✓ Engaging like minded parties to communicate the value and need of such initiative to their clients encouraging participation
- ✓ Appropriate training needs to individuals and SMEs also need to be considered

15 Opportunity to include unbanked and undocumented

- ✓ Certain municipalities highlighted their respective policies to serve residents that may not have the required documentation and / or may want to access certain services without being asked for proof of status – any future digital identity solution may need to have appropriate considerations for these residents.

16 Ability to display information in easily accessible manner

- ✓ A technology company highlighted the importance of displaying relevant information in simple, large font and symbols that clearly indicate the credential information itself is all that is required; large and bold letter will enable people with vision impairment, or in limited lighting conditions to easily verify information.
- ✓ Further some US state police authorities are keenly interested in an application that may allow them to verify someone's driver's license and vehicle registration without actually leaving the police vehicle

17 Additional design considerations

- ✓ Some research studies indicated the importance of user being in the possession of the device throughout the verification process and knows what information is being requested before sharing
- ✓ There are mixed views on using biometrics – some organizations recommended using biometrics as a starting point and supplementing with administrative identity while other highlighted that biometrics should be optional as it's not needed for every use case
- ✓ Some proponents highlighted the need to be able to verify offline especially in remote parts of the country; physical smart cards could be one such option; further, service terminals as well as Software & Hardware tokens could also be used

Selected Statements

CBN recommends Ontario augment the wallet functionality with additional services that leverages the credentials it stores to facilitate a digital channel; a Wallet+ approach. It is the services that delivers value to the citizen, not the credentials themselves.

Ontario Digital Services announced last year a priority to increase online uptake of ServiceOntario's top 10 transactions. A synergy lies between this priority and the digital identity priority. Bringing the appropriate services into the app can leverage the credentials it stores to make them easier. No typing in drivers licence numbers, or insurance information. With user consent, the information is pulled automatically. Combined with mobile payment, transactions can be done in minimal clicks. Additional services like a chat window, and notifications can bring ServiceOntario into people's homes, authenticating them easily and allowing for the delivery of personalized services. This will bring real effective value to the end user, and drive user adoption, and entice more relying parties.

Governance & Authority

Governance and Authority Insights (1 of 2)

1 Selecting the operating model with clear delineation of responsibilities

✓ The first step would be to select the appropriate operating model of the future. Two prime options would be – Centralized vs Federated

1. **Centralized** – Government is accountable for collecting user attributes, issuing digital credentials and authenticating users. Some respondents highlighted the advantages such as perpetual integrity of a centralized DI model, while partners could be leveraged for to provide inputs, data sources and / or assurance checks. Though, this would put significant onus on the government to set up and manage the service, while mitigating risks related to data breach. The model could be more viable with smaller population such as Estonia with a population of only 1.3 million
2. **Federated** – Multiple accredited identity providers collect, store, and manage attributes / credentials and authenticate users (useful when large network of providers have sufficient capabilities in identity proofing) e.g., Denmark, Finland, Norway, and Sweden have all partnered with banks to run their respective ID programs. This can help in optimizing costs though requires capacity management and appropriate oversight.

   Consider delineating between core offerings that need to be centralized such as issuing Digital ID Token (e.g., driver's license), while private sector can take lead in enabling a multitude of use cases as well as consumer facing technologies such as digital wallet.

   The growing use of consortium based digital identity networks (e.g., V.me) would also fit into this model. The model involves participating organizations to act as IDPs (e.g., leveraging bank credentials), drive consortium policies and standards and service hosts to maintain the network.

   This was highlighted as the most viable model for Ontario by a number of respondents
3. **Decentralized** – The end user is in control of their data or they can choose to delegate control to trusted parties. Traditional trusted IdPs play key governance roles. Decentralized models are designed to be open and interoperable and a verifiable credential model could be added to any participating wallet.

2 Establishing appropriate regulatory framework

✓ The government will have to play a central role in establishing a regularity framework and providing guidance to establish a viable Digital ID ecosystem. Some key regulatory considerations included –

- **Ensuring Interoperability** – Able to seamlessly exchange data with the various systems, devices, databases, and applications that are part of the ecosystem, as well as across other jurisdictions. This may require writing these standards into law.
- **Public engagement** – The government was suggested to own the overall governance, as well as control and access to public assets, though strong public engagement is deemed critical for securing the support and trust of Ontarians. Further, a multi-stakeholder model — including Ontarians and Ontario businesses — would lead to establishing an open and transparent governance committing to continually working to improve governance to align with safer and faster shared outcomes.
- **Legal equivalence** – Legislation ensuring the legal equivalency of Digital ID with existing authentications as well as amending policies that may inhibit use cases across private and public sector. For instance, any in-person requirements or mandate to include original documentation that cannot be shared digitally (e.g. university diplomas) in the process of opening a bank account can immediately discourage Digital ID usage amongst the banks' consumers.
- **Two pieces of ID** – Regulations that currently require verifying two pieces of ID may need to be reviewed in the digital identity world
- **Meeting national and international regulations** – Regulatory constraints and policies to ensure operability across borders. For example, banks in UK has low adoption due to an EU Anti-Money Laundering initiative requiring banks to keep record of how customers were verified
- **Liability model** – agreements are reached on responsibility and accountability between ecosystem participants

Governance and Authority Insights (2 of 2)

3 Clarity on information sharing

- ✓ Appropriate governance on sharing of information including which wallets or applications can hold or share Ontario credentials including defining security standards for these applications.
- ✓ Further, which Relying Parties can request what information also needs to be defined

4 Third / Neutral Party Oversight & Full Public Consultation

- ✓ There is a perspective that independent 3rd party oversight will ensure that government and other relevant stakeholders are using digital ID in the best interests of the person and the public
- ✓ Engaging / funding organizations such as Information and Privacy Commissioner of Ontario (IPCO) as well as performing a full public consultation to understand human rights implications was also recommended

5 Eliminating Systemic Bias

- ✓ Some organizations highlighted intentional steps to eliminate systemic bias whether through collecting broad sociodemographic information or other necessary means
- ✓ A wide variety of barriers needs to be considered including geographic, financial, knowledge, policy-based and access-related
- ✓ Consumer rights into digital transaction (protection against dark patterns [1], standardization of commercial contacts, etc.)

6 Potential liability in case of misuse

- ✓ There is a strong perspective that data should be decentralized and any organization that is participating in the ecosystem should be help responsible for the information they hold with appropriate penalties for misuse
- ✓ Having said that, a clear guidelines on privacy and security to be followed by the participants would be very helpful
- ✓ Further, creating a level playing for SMEs is important to prevent online commercial monopolies

7 Leveraging existing working groups & infrastructure

- ✓ Some organizations suggested Ontario to work with the established working groups that already connect with stakeholders across the industry to drive Digital Identity in Ontario & Canada
- ✓ Proponents also advised to repurpose existing identity stores and UIs to limit development to credential issuance platform and recognition engine

Selected Statements

EU's eIDAS Regulation mandates that organizations delivering public digital services within an EU member state must recognize electronic identification from other EU member states.

In British Columbia, the Identity Assurance Sercices (IAS) provides provincial identity information services that: manage registered identity information of BC residents who receive a BC Services Card; authenticate the BC Services Card when a person chooses to use it; allow a BC Services Card to be represented on a mobile device (mobile card); and provide identity information to government services whether a physical or mobile card was presented for authentication. The IAS includes identity authentication services, processes, infrastructure, applications (web and mobile), platform, web sites, security, data integrations, reporting, and tools.

In Estonia's program, electronic authentication and signatures are legally equivalent to face-to-face identification and handwritten signatures.

[1] A dark pattern is "a user interface that has been carefully crafted to trick users into doing things, such as buying overpriced insurance with their purchase or signing up for recurring bills". They are increasingly common and represent a significant portion of anti-consumer practices online.

Ontario

Technology & Operations

Technology & Operations Insights (1 of 4)

1 Provide an advanced end-user solution such as Wallet+

- ✓ Some providers recommended Ontario develop a Wallet solution that becomes the primary service delivery channel for most of the highly utilized services to Ontarians
- ✓ Augmenting the Wallet with additional services (not just the credentials) may generate more interest from the community.
- ✓ Louisiana's state-sanctioned app 'LAWallet' supported a state-provided service, driver licence renewals, and this capability played a key role in driving four times the user enrollment than Oklahoma, which opted to provide only basic credentials
- ✓ Some proponents also questioned the need of a second wallet if Ontarians already have one, on the other hand, there is also a perspective to differentiate Ontario solution from big tech and advantages of providing a ON-branded wallet to built trust

2 Tiered authentication with more secure checks for higher risk transactions

- ✓ Calibrated and tiered authentication system with more rigorous checks in alignment with risks levels. Example jurisdictions –
  - **New Zealand** – RealMe ID scheme requires only a username and password for many applications (e.g. interactions with city, district, and regional councils) and more secure identity checks for other needs (e.g. replacing driver's license)
  - **Australia** – the degree of access is dependent on the number of identity documents provided by the user

3 Microservices Architecture and leveraging API based services

- ✓ A microservices architecture (MSA), an approach to developing a single application as a suite of small services, each running in its own process and communicating with lightweight mechanisms, was recommended, ensuring that the DI ecosystem can move fast and quickly innovate via small, incremental improvements
- ✓ Participants recommended to start small by launching proof of value / pilots leveraging API based identity validation services using public sector databases that could be easy to integrate with as new offerings are developed

4 Ongoing engagement for continuous improvement and interoperability

- ✓ An ongoing forum for ecosystem engagement to assist with continuous improvements. In addition, creating and maintaining a development sandbox to allow partners to test against ongoing changes (e.g. API changes), and to participate in improvements and innovations, should be considered.
- ✓ Even when a common technical framework is followed, the interpretation and implementation differences may make these solutions to not be as seamlessly interoperable as desired, so having discussions and testing interoperability on a periodic basis could prevent any such challenges in the future

Selected Statements

Bluink surveys have indicated that over 80% of citizens would use a digital identity if it can save time, effort and money

Estonia claims that it has developed an ecosystem where 99% of government services are online making it "one of the most advanced digital societies in the world" according to Wired. The number of queries that go through X-road per month has gone from 63,000 in 2003 to more than 180,000,000 in 2019. The X-road system is now being used around the world by countries including Iceland, Germany and Japan.

Avoid a 'build it and they will come' approach

Technology & Operations Insights (2 of 4)

5

Leverage learning from existing projects built on common standards

- ✓ Selecting components of the technical stack that are built using common standards (e.g., W3C, Decentralized Identity Framework – DIF) would enable the government to leverage existing experience, understanding, and trust in the platform to accelerate implementation and reduce risks
- ✓ Some respondents also shared challenges with VC standards, and highlighted that these are still in early stages of maturity with limited interoperability and not ready for broad deployment

6

Continue to monitor new standards beyond verifiable credentials

- ✓ Keeping an eye on purpose built standards to successfully enable different use cases would enable Ontario to develop a holistic solution
- ✓ Some examples cited included ISO 18013-5 mobile driver's license (mDL) and ICAO backed Digital Travel
- ✓ mDL specifications is written such that other kinds of digital credentials besides Driver Licenses could be supported, such as citizen ID or a health card
- ✓ The Modular Open Source Identity Platform (MOSIP) was also sighted as a good example that embraces the best practices of scalability, security and privacy

7

Appropriate safeguards to protect user's identity

- ✓ A stolen unique identifier (e.g., Health Card number) could be stolen and shouldn't be enough to receive appropriate services
- ✓ There could be links / digital verifications to ensure the presenter himself holds the credential, preventing any bad actors from misusing the information. The concept is known as 'devaluing of information'
- ✓ Services could also be setup to perform a verification of input information ONLY, and not release information to protect privacy (i.e., zero-knowledge proof)

8

Open competition among technology providers

- ✓ Open competition amongst technology providers of all sizes enables innovation, lower prices, increased efficiency, variety of offerings, and user-driven choice. In turn, this enables greater uptake and responsiveness. Ecosystem stewards avoid monopolies wherever possible.
- ✓ Look for solutions with no / limited lock-in on a vendor / platform

Selected Statements

We can envision a model similar in structure to Salesforce's customer relationship management (CRM) software. Under this model, there is a core platform and a supported application developer community that is incentivized to develop and integrate value-added functionality to the core platform through a series of well documented application programming interfaces (APIs) that provide access to the data and functionality of core platform. The core platform itself is tightly governed to ensure its own integrity as well as the integrity of third-party applications. A portion of the revenues generated by third party apps goes back to the core platform for support and continued maintenance and innovation of the core platform itself.

One model that Ontario can look to is from Argentina, where the digital ID roadmap, although led by Digital Services Team, received plenty of input for other stakeholders, both internal and external to government, that were invited to think broadly in the future uses of digital ID.

Technology & Operations Insights (3 of 4)

9

Single identity issuance system across ministries

- ✓ There were suggestions to role out a single digital identity issuance system that can be designed to issue multiple identity credentials on behalf of respective agencies
- ✓ Verification, issuance, and revocation services could be exposed, allowing for all agencies and departments to maintain control and provenance over their respective issued credentials, while leveraging a common infrastructure

10

Take a Minimum Viable Product (MVP) approach

- ✓ Participants recommended to consider an MVP approach while keeping the bigger picture in mind. There could be two options –
  1. Start with a low-assurance, self-asserted identity, followed by upgrading Ontarians ID through a separate process (Alberta model)
  2. Identify people first and issue a high assurance credential up front (BC model)
- ✓ Some proponents also highlighted the risks associated with setting a too ambitious deadline to roll out a mature product
- ✓ Depending on provincial comfort, advance technologies such as AI could be used to identify people based on facial recognition and scans of documents

11

Leverage data analytics to understand authentication behaviour

- ✓ Here is an overview of some of the ways Financial Institutions authenticate a use based on their behaviour –
  - Knowledge-based confirmation
  - behavioural characteristics confirmation
  - Physical possession confirmation
  - Normal frequency of authentication events
  - Normal time of day of authentication events
  - Geographic location the User typically logs in from: city / country
  - IP that the User typically logs in from
  - Increased identity verification requirements established for specific authentication event purposes
- ✓ Telcos provide in addition to owner information, information about the users device, has the SIM changed, where is it, and many other data sets with the users consent while credit bureaus provide history of the consumer, is their fraud on their account, are they credit worthy, and we are integrating now the Known Fraud Exchange

Selected Statements

A "big bang" approach of trying to achieve everything at once – of trying to launch several applications and enable several credentialing authorities and end user verifiers at the same time, is one which poses specific risks to the entire project. It could lead to design flaws that could undermine public confidence in the platform. Ambitious over-engineering could unwittingly introduce bugs or errors into the system; this could end up being unnecessarily costly to the public treasury and embarrassing to the Government of Ontario; and further, it could send confused messages to the public that might prejudice their confidence. Moreover, it may prejudice Ontario's opportunity to fully monetize the system as it grows.

The use of focus groups, hackathons, user testing, consumer surveys, and other sources of feedback loop mechanisms must become part of the regular program cadence

Technology & Operations Insights (4 of 4)

12

Leverage traditional access management standards

- ✓ Ability to authenticate using standards such as OIDC or OAuth2 that could be implemented using a web hook implemented in an SMS message, sent via email or encoded as a QR code on the login page of a web portal prompting consistency in providing the requisite details to the service by means of verifiable proof

13

Mixed perspectives on including mobile number as a key attribute

- ✓ Some respondents advised to consider linking digital identity with mobile numbers as it could be easily verified and generally link to individual account holders; this may also enable linking a digital wallet with a mobile number, allowing for multi-factor authentication for both confirming ownership and transactions
- ✓ While there were also security concerns raised with this approach with increased instances of sim cloning, intercepting SMS and voice calls, etc. The alternate approach could be to use “secure link” rather than a text message as a more secure medium for verification

14

Platform extensibility to enable future use cases

- ✓ Allow for system to be extensible so that scenarios and services can evolve over time and be used by e.g., local / muni governments for voting, transit, 311

15

Prevent duplication of information

- ✓ Refer to other VCs where appropriate preventing data being duplicated in multiple credentials
- ✓ For example, a driving license includes a date of birth (DOB) and so as the birth certificate. So rather than repeating the DOB in driving license it should be linked back to birth certificate VC, if available

16

Consider owning verification gateway

- ✓ There were suggestions to develop a model similar to the one built by Digital Transformation Agency in Australia for verification gateway service: ON establishes and owns a gateway service that allows for verification of ON-issued IDs, biometric verification, fee-based to the province for DI provider
- ✓ At the same time, Ontario may have to consider consuming private sector DI services from certified and accredited providers, enabling a market of providers

Selected Statements

New Zealand is currently undergoing a second generation reset of its programme, with a pro-forma legislation backed Trust Framework. For this, and the Private Sector access to the document verification service which provides Zero Knowledge Proof (ZKP) / Minimal data / yes-no responses to claims made to it by the Private Sector, Service Level Agreement (SLA) oriented contracts were agreed, supported by a high-level third-party ISMS + privacy certification

UK Verify lessons learned: existing private sector solutions may not have been developed with modern approaches to accessibility and inclusion so more expensive afterward to retrofit; calculate and agree to tangible commercial benefits with industry partners upfront

Funding Model & Ownership

Funding Model & Ownership

1

The Government is the sole funder

- ✓ The government provides a Digital ID as a utility and fees are paid per transaction by ecosystem participants. This would be in line with the traditional role of the government in providing foundational government-issued digital issued credentials
- ✓ Further, proponents suggested that government should own / manage verifiers that are part of exposed government services as well as any highly trusted centralized entity in the ecosystem
- ✓ Some edge cases may especially require government support to ensure universal access
- ✓ Consider the role of indigenous government as well in building and maturing the digital identity ecosystem

2

A consortia of public and private sector entities combine funds

- ✓ The government partners with a number of private sector entities who provide the capitol to fund the establishment and maintenance of the Digital ID and ecosystem
- ✓ Alternative consortium funding model options are:
  - ✓ A membership model where each participant's contribution is tailored according to their role / contribution
  - ✓ A proportion-based contribution where the investment is scaled in proportion with a pre-defined driver (e.g. quantifiable revenue return / benefits for each organization)
- ✓ It was recommended to keep the participation open allowing interested parties to join on an ongoing basis
- ✓ Further, rather than defining funding model for the whole ecosystem, define it by network. Some networks funded by data requesters and verifiers (at no cost to residents); others may use mix of funding by gov't, business, resident; others may be built as public infrastructure (so taxpayer is funder). Liability model can help in mitigating any associated risks

3

Technology providers are the funders

- ✓ One or multiple technology providers build and maintain the Digital ID and are paid based on transactions / membership fees
- ✓ Considering the volumes may be low in the nascent stages leading to higher commercial risks for the technology providers, and that may result in significant per transaction fees
- ✓ To reduce prices, a combination of fixed fee and variable fee could be considered where prices per credential decline as volume increases to protect government / payers from high costs when volumes take off

Selected Statements

Digital identity can reduce customer onboarding costs by 90% and reduce payroll fraud by $1.6 Trillion – McKinsey, 2019

515 million adults worldwide opened an account at a financial institution or through a mobile provider between 2014-2017 – World Bank Group, 2019

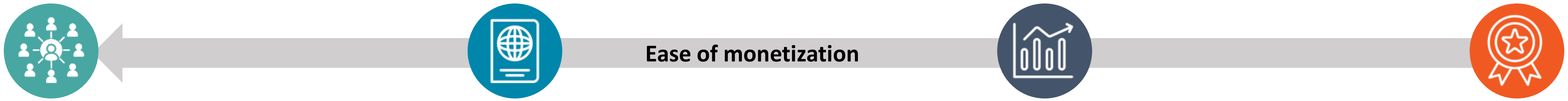
US$150 is the average cost of stolen record containing confidential and sensitive information – IBM, 2019

Enacting user control of data could reduce customer churn by 40% - Gartner, 2019

Private sector should develop and operate DI infrastructure to achieve returns; province can provide initial seed grants (though not a must)

Benefits & Monetization

Benefits & Monetization



	Ecosystem Participants (IdPs & RPs)	Establishing & Retaining Credentials	Analytics & Insights	Global Leader (Consulting)
Description	*Ecosystem participants will have varying levels of transactional complexity and can benefit from the value creation enabled by a Digital ID. Treat the ID like a utility to share cost, security capabilities and information.*	*Both individuals and businesses are required to establish credentials to validate their identity and get access to various services. There are fees associated with these credentials and the model assumes no extra fees for digital credentials.*	*There is an opportunity to provide internal and external organizations to the ecosystem with insights and analytics enabling them to optimize their business. None of this assumes monetizing the data itself.*	*As a leading jurisdiction in Digital Identity ecosystem creation and maintenance, the Government has an opportunity to share learnings and advise other jurisdictions in establishing their own ecosystems.*
Monetization Models	1. Pay an initial fee to become part of the ecosystem and ongoing maintenance fees for access to ecosystem services. 2. A transaction-based fee structure that could be anchored in value-based pricing or a cost-plus strategy	1. Pay an initial fee for establishing a credential and then subsequent fees to renew / retain the credential (e.g. driver's license, transit passes, library card). 2. Subscription fees for access to optional value-add services (e.g. convenience, experience, insights).	1. Exchange of analytics and insights between government bodies to identify service delivery improvements. 2. Exchange of analytics and insights between ecosystem participants to identify service delivery improvements. 3. Exchange of analytics and insights with external organizations to identify service delivery improvements	1. Charge interested jurisdictions for a variety of services and technology associated with digital identity ecosystem creation.
Value to Monetize	Organizations can create transactions to add more value for users which improves the customer experience and increases adoption.	Credentials are essential for access to services, but a more seamless experience saves individuals time and money.	Access to insights are of interest to organizations looking to improve efficiency, save costs, increase revenue, improve customer experience, and reach a broader audience.	There is a growing need for digitizing services and a lever to facilitate user efficiencies and experiences is Digital Identity.

Selected Statements

Private sector firms will be inclined to commit the resources required for developing the ecosystem if they are confident in the potential business implications that the ecosystem offers

Identity providers could set up monetization contracts with relying parties for access to info; governments should not prevent this monetization so long as it's done with user consent – to support longer-term sustainability

Should not aim to generate profits, unless reinvested in utility evolution and DI stakeholders' needs

wallet services should make DI and service interaction easier without overburdening a citizen through expensive 'pay for play' engagement models.

Risks & Mitigation

Risks & Mitigation (1 of 3)

Risks

Security & Privacy

1 Cybersecurity attacks (e.g., unauthorized access to data, leaks of private and confidential information, system disablement)

- ✓ Government should lead, manage and / or own security framework principles of the digital identity ecosystem
- ✓ Decentralized digital identity solution can avoid large data breaches
- ✓ Secure PKI ID Mgmt., Highest levels pf encryption for data in transit and data at rest, encrypted storage
- ✓ Strong controls on Protected B systems and infrastructure that handle any data
- ✓ Mobile security, for example mobile environment detection library, anti-routing, debugging, RASP runtime, obfuscation, secure pin pad;
- ✓ Secure and accurate ID credential provisioning, secure data verification;
- ✓ Use of state-of-the-art cryptography, certified by third parties.
- ✓ Cyber testing and penetration testing of apps and infrastructure of all associated services
- ✓ Encourage relying parties to request identity information on-demand (from digital wallet) rather than collecting large databased on personally identifiable information

2 Privacy violations such as misuse, unauthorized use, manipulation of data credentials, non-compliance with organizations such as FINTRAC, etc.

- ✓ Ensure built-in privacy provisions such as data minimization and proportionality, robust governance / controls, and an established rule of law
- ✓ High-assurance digital ID programs reduce the risk of credential forgery and unauthorized use
- ✓ Use double blind credential sharing architecture between IdP and RP
- ✓ A secure communication channel for bilateral parties to eliminate data exhaust and unnecessary data exposure
- ✓ Ensuring data aggregation is not possible through monitoring or collusion using peer-wise identifiers including policy and protocols to prevent data re-identification
- ✓ Ability on the part of the verifiers to challenge the presenting party to prove they are the subject to whom the credential anchoring the attestation was issued
- ✓ Misuse, device/IP/identity spoofing etc. can be addressed through strong device authentication practices, IP Whitelisting, client-side TLS authentication, and token encryption between Relying Parties and the IdP, as well as liveness detection, geo location and other best practices

Technology & Operations

3 Lack of standardization limits interoperability of ecosystems (e.g., provincial, federal, global) leading to lower overall benefits than expected

- ✓ Leverage technical blueprints provided and standards by some leading organizations such as Trust Over IP (TOIP), W3C and decentralized identity framework (DIF)
- ✓ Consider modular architecture separating the business applications, the wallet, data registry, and communication protocols allowing government to upgrade or replace any component of the technical stack as needed

Risks & Mitigation (2 of 3)

Risks

Technology & Operations

4 Lack of qualified resources to drive implementation and maturity of ecosystem

- ✓ Work with a partner with deployable infrastructure will allow gaps to be identified and mitigated early
- ✓ Consider modular architecture separating the business applications, the wallet, data registry, and communication protocols allowing government to upgrade or replace any component of the technical stack as needed

5 Program implementation and operationalization end up taking much more time and costs than expected

- ✓ Using an iterative, scalable and an MVP-based build approach while prioritizing high-value, low-to-medium complexity use cases will reduce the risk of program delays

6 Technical maturity / digital infrastructure of stakeholder groups (i.e., financial services, telecom) not ready to adopt digital identity at scale

- ✓ Public private partnerships with clear roadmap may enable stakeholder groups to digital their own processes in parallel with digital identity evolution

7 Unpredictable and costly technological failure and human error

- ✓ Working with established partners to prevent technological failure

Inclusion & Adoption

8 Lack of supporting infrastructure (e.g., access to internet, levels of education, marginalized groups) preventing inclusion of all Ontarians

- ✓ Increased support for digital literacy education
- ✓ Increased funding for affordable high-speed internet and / or community ownership of high-speed internet access
- ✓ Ability for the individuals to delegate responsibilities to others may allow certain segment of the population the ability to access services (the guardianship model)
- ✓ Cloud based wallets may enable marginalized Ontarians to interact with the digital ecosystem and make use of the verified credentials from public computers available at libraries or schools
- ✓ Continuing to allow access to services via legacy mechanisms at a much-reduced scale, as digital enablement frees up current service bureaus
- ✓ Ensure that agencies that serve marginalized groups don’t have additional costs

9 Users and institutions are slow / resistant to adopt (e.g., comfort with technology, varied trust levels, low user control / value, crowded DI marketplace,)

- ✓ Human centered design principals and tools are essential to driving enrollment and adoption

Risks & Mitigation (3 of 3)

Risks

Governance

10 Lack of robust and adaptable governance structure leaves the ecosystem open vulnerabilities (e.g. privacy, evolving standards)

- ✓ Government should play an active role early in setting the governance structure as well as standards

Other

11 Inability of the core stakeholder group to agree on the future vision, roadmaps and implementation plans in a timely manner

- ✓ Government should play an active role early in setting the governance structure as well as standards
- ✓ Identity a clear exec sponsor from gov’t and steering committee that’s gov’t-led but includes business, academia, legal, policy, etc.

12 Lengthy policy, regulatory and legislative progress slowing delivery and project timelines

- ✓ Focus on smaller incremental projects that revolve around concrete service delivery scenarios to move faster

13 Competing priorities (e.g., COVID) lead to lack of funding or resource availability

- ✓ Digital Identity may play a vital role in ensuring business continuity in situations such as COVID and should be prioritized accordingly

14 Ministries / programs unable to undertake digital transformation of their services procure / build their own solutions to benefit from digital identity

- ✓ Leverage existing standards, infrastructure and technology and leave actual implementation on private sector

Case Studies

British Columbia – BC Services Card

BC launched the BC Services Card in 2013 as a replacement for both the province's health insurance card and driver's license. Over 4.7 million BC Services Cards are active today.

What Worked Well

1 It is a full service integrated program, involving multiple public and private sector parties to handle identity proofing, card issuance, systems development and operations, help desk, citizen communications, and onboarding of relying parties

2 It has specific authorities in the BC Freedom of Information and Personal Privacy legislation that enable it to collect and share citizen information

3 A privacy-by-design approach, including providing different identifiers for the same citizen to different government programs, has prevented unauthorized cross-linking of citizen information across program areas

4 BC developed and maintains the identity management and authentication systems, including the mobile app, with the support of outside service vendors, and has been able to implement new capabilities relatively quickly

5 Shifting to a mobile-first strategy, where a citizen can download the mobile card, verify their identity by video, and authenticate to a new online service within five minutes.

Key Lessons Learned

1 Services were reluctant to adopt BC Services Card for online use until the entire population had a BC Services Card, which was rolled out over five years as people replaced their Driver's License, and until citizens could get set up for online authentication without a counter visit, which only became possible with the introduction of a verified by video service in 2019

2 The process of directly integrating relying parties is technically easy but is challenging to scale up due to the responsibility, per BCs' privacy office, of the BC Services Card program to ensure each relying party meets security and privacy requirements before signing an information sharing agreement.

3 It is relatively easy to collect and share basic demographic attributes about a citizen. The far greater challenge is in implementing things such as the relationships between people (e.g., parent-child, guardian-child) and consent when it cannot be automatically inferred (e.g., a parent wanting access to the medical records of their teenage child), yet these are key to online services such as access to health records and K-12 school registration.

4 Many program areas that adopt BC Services Card for authentication also serve people who do not have a BC Services Card, either because they are new to BC, live in another part of Canada, or live outside Canada. This requires service areas to provide alternate channels and/or means of authentication

Examples from Estonia, the UK, Australia, Norway and India

An overview of key insights highlighted by Accenture from these jurisdictions

What Worked Well

1. Mandatory physical and digital identification cards which work interchangeably
2. Police and border guard authority rolled out ID card with contactless interface, a QR code, and enhanced security
3. Provision of a single trusted login across all government digital services –users can choose from several companies to verify their identity before accessing the government services
4. Introduced a mobile identification program which enables common transactions such as signing contracts, applying for a loan, placing a bid for housing and purchasing airline tickets
5. Creation of a national digital identification scheme available to all citizens for proof of residence, leveraging biometrics and replacing previous paper-based solutions

Key Lessons Learned

1. Engage and onboard the private and public sector early into the digital identity ecosystem to encourage acceptance and adoption
2. A government-led trust framework is required to provide a set of principles, standards and specifications that support the exchange of information between entities
3. A common vision and set of rules based on trust that form a mutually beneficial partnership to address a common and reoccurring pain point that has frequent user interactions
4. Recommendation for the government to be at the forefront of any ecosystem engagement to establish either themselves as a trust anchor or empower another body at inception
5. The value proposition needs to be strong with incentives for all stakeholder groups within the ecosystem