IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

TD West Tower | 100 Wellington Street West
Suite 1910, PO Box 173 | Toronto, ON M5K 1H6

416.364.2754 | www.iiac.ca

www.iiac.ca

Ontario Digital Service (TBS) & Infrastructure Ontario
Market Consultation on **Enterprise Digital Identity Program**

CATEGORY: INTRO

Briefly describe your organization's experience with digital identity in Canada and/or globally. What role do you see your organization playing in a digital identity ecosystem? (i.e. IDP, RP, Identity Network, infrastructure provider, technology provider, other)

The Investment Industry Association of Canada ("IIAC") is the professional association for Canada's securities industry. Our membership is comprised of approximately 120 regulated investment dealers employing 40,000 individuals. Our members provide various wealth management, capital raising, advisory and securities trading services to retail and corporate clients. Collectively our members administer approximately $3 trillion in client assets.

Our organization's experience with digital identity has been very limited thus far. However, we realize the opportunities that a digital identity ecosystem can bring to our members and our industry. We do not see our organization as playing a direct role in a digital identity ecosystem, however, our members would have direct involvement most likely as Relying Parties ("RP"). The IIAC would work closely with our member firms to raise awareness and increase adoption of digital identities within the securities industry.

CATEGORY: ECOSYSTEM & OFFERING

How could partnership between the public and private sector be arranged to support the development of the DI ecosystem in Ontario? What parts (if any) of the DI ecosystem do you feel must be lead, managed, owned by government in the interest of the public good?

The IIAC believes the best approach forward for developing a Digital Identity ("DI") Ecosystem in Ontario would be one that is government lead but which also includes strong participation from the private sector.

The government must establish the guiding principles for the DI Ecosystem which will be the basis for evaluating any product/service/technology offering that is to be part of the ecosystem. We believe these guiding principles are in the interest of the public good. Only with such clear direction from government can the private sector then identify the appropriate DI use cases and begin the necessary planning, investment, and development. We also believe adoption of the DI Ecosystem among Ontarians will accelerate if they know that this is an initiative being fully supported by the provincial government. Lastly, we believe that implementation of a DI Ecosystem will, in some cases, require changes to existing legislation or regulations and the Ontario government can play a pivotal role facilitating those changes without which DI adoption will ground to a standstill.

What benefits could be realized through public and private sector collaboration?

The public/private partnership above has several potential benefits. Canadian's will stand to benefit most from a DI Ecosystem when service delivery efficiencies are maximized. It is imperative, therefore, that all government and private sector use cases be identified and evaluated against the guiding principles. We believe the government is best placed to identify which public services are well suited for the DI ecosystem. Conversely, the private sector will be best placed to identify which of their current service offerings can, and should, embrace DI adoption.

Collaboration between the public and private sector will also be necessary to address several of the risks/challenges that are outlined through out the other sections of this consultation ie. privacy, adoption, security, etc.

What attributes/features should a digital identity for individuals or businesses include?

In addition to basic authentication of name, date of birth, registration date and address we believe it would be very helpful if a digital signature was also included as part of the DI attributes as it would broaden the application of the DI ecosystem. Specifically, client/customer signatures remain a common requirement across various public and private sector services. For example, in our industry client signatures are

required as part of the new account onboarding process. Current industry efforts to transition away from wet-signatures and towards signatures in electronic form would be propelled forward with the inclusion of digital signatures as part of the DI attributes.

Another attribute worthy of very careful consideration is Social Insurance Number (S.I.N). We recognize that there will be increased sensitivities surrounding S.I.N. information forming part of the individuals DI and those sensitivities must be weighted carefully against the additional uses cases that would be opened by its inclusion in the customer's digital wallet. Account openings at Financial Institutions, tax reporting, applications for government services, etc. would all potentially benefit from this added digital attribute. Ontarians may be receptive to its inclusion only if they were confident in the privacy and security of the DI framework.

What role can your organization play in helping us deliver?

Our organization can play an important role in raising awareness of the DI framework and encourage its adoption among our 120 member organizations. Some of the mediums we could use to achieve this can include conferences, webinars, roundtables, direct mailing to members etc. We can also work with our members and their service providers to identify practical use cases within Canada's securities/brokerage industry.

Because our industry is heavily regulated, we suspect adoption of a DI framework would entail significant regulatory and legislative changes in order for our members to change the way they currently do things. Our organization can play a role in facilitating meetings and discussions with industry regulators and work towards the necessary rule changes that would allow our industry to transition to the DI ecosystem.

What should be done to drive active user participation, engagement and adoption of digital identity in Ontario?

Active user participation and adoption of digital identity in Ontario will be predicated on ensuring users have sufficient confidence that their DI will be used solely in the manner they authorize and that sufficient safeguards are in place to protect the confidentiality of the DI. Offering consumers greater control of their data also provides them with a deeper understanding of how it is being used. Any framework perceived to be susceptible to fraud or misuse would face challenges with its adoption.

Ontarians may also feel uncomfortable in sharing their private data with public and private institutions, when the benefits of doing so remain unclear. It is imperative, therefore, that efforts are made to raise the public awareness of the benefits of DI. Transparency will also be very important in achieving acceptance as it will ensure customers/end users are fully informed of their rights and responsibilities regarding the transfer, possession, and use of their digital identity.

Promoting confidence in the DI framework needs to be a joint responsibility of the both the public and private sector.

What are the highest priority use cases for your organization and/or industry/sector that would benefit from the use of digital identities?

The highest priority use case for the securities industry would likely center around the client on-boarding process. DI's can potentially add significant efficiencies to the current account opening process at our member firms. DI could also help our members meet their compliance responsibilities in various areas such as Anti-Money Laundering, Know-Your-Client obligations, and Canadian and Foreign Tax Reporting. The DI could also serve to replace other forms of client identifiers currently in use within the industry.

How could the digital identity ecosystem be structured to protect data and privacy, build trust and reduce identity fraud? How can privacy concerns associated with the handling of sensitive user data be mitigated?

Institutions, both public and private, utilizing the DI framework would be expected to take necessary steps to mitigate the risk of a data breach —a process that would likely require significant time to implement. Encryption technology will be important in making sure sensitive information is protected when it is in transmission or storage. Artificial Intelligence (AI) technology can also play a role in identifying suspicious activity and advances in automated threat responses will also help safeguard the ecosystem.

Additionally, many private firms have developed in recent years 'cyber incident response plans' to deal with cyber threats. Similar type of planning would need to be considered in relation to securing the DI ecosystem.

Offering consumers greater control of their data will provide them with a deeper understanding of how their data is being used which in turn will help address some of their privacy concerns.

CATEGORY: GOVERNANCE AND AUTHORITY

How should responsibilities for different parts of the Digital ID ecosystem must be delineated? What do you envision the role of Public Sector and Private Sector to be in the overall governance model? Do you see benefit in having the Province provide oversight for the ecosystem?

Responsibilities for different parts of the Digital ID ecosystem can be delineated in multiple ways. The Province should play a leading role in achieving consensus on the attributes of the digital identity as well as establishing the guiding principles that will govern the Digital ID

ecosystem. Ultimate day-to-day oversight should be based on who is storing the DI or who is delivering the service that utilizes the digital ID or who ultimately has the relationship with the end-user.

Given the potential size and scope of the Digital ID ecosystem it would be impractical for the Province to provide complete oversight for the ecosystem. Where the Province can and should have oversight are the use of Digital ID's within the public sector. The use of Digital ID's within the private sector should be the responsibility of industry to consume and safeguard the DI. There may be an important role for government or regulatory bodies in reassuring consumers on the authenticity of services or apps requesting their digital identity.

There will be some instances where some shared public/private oversight may be necessary. For example, the Ontario Securities Commission (an agent of the Ontario government) may have some oversight on when and where the use of DI will be permissible within the securities industry/capital markets.

What legal, policy or regulatory changes should be considered to support effective governance and growth of the digital identity ecosystem?

A shifting data-privacy regulation environment may make companies unwilling to invest in programs and services that utilize DI, when the way they can access consumer data is subject to constant change or uncertainty. Ontario's data privacy regulation (ie. Freedom of Information and Protection of Privacy Act) should be harmonized to the extent possible with federal legislation to eliminate duplicative or contradictory requirements on the private sector.

CATEGORY: TECHNOLOGY AND OPERATIONS

What are the necessary foundational pieces of the ecosystem that can be stood up / enabled now while standards continue to mature and evolve?

Communication between a range of parties from across the ecosystem will be fundamental to the DI ecosystem's foundation. We are witnessing Open APIs (application programming interfaces) and VPNs (virtual private networks) driving collaboration and communication between and within the private sector to create other secure ecosystems for the end consumer. We believe this must continue for the successful implementation of the DI ecosystem.

CATEGORY: FUNDING MODEL AND OWNERSHIP

How should a digital identity ecosystem be funded? Who should be responsible for capital and operating costs? Any insights from financing a multi-entity ecosystem in the past, that may also have included public and private sector stakeholders? Should any parts of the DI ecosystem be owned and managed by the government, in the public interest/good?

Ideally, the DI ecosystem should be self-funded through revenues generated through the potential new use cases. 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. We view this similar to other current ecosystem initiatives that are in their early stages such as application of Blockchain and Open Banking.

We also believe there is an onus on the Ontario government to ensure that their use of DI in any government programs/services are also financially viable without the need for a back-stop from Ontario taxpayers. Business case requirements should be established by the Ontario government to help with its decisioning. Government services that are perceived to be in the public-good may warrant special consideration.

CATEGORY: BENEFITS AND MONETIZATION

What are the opportunities for monetization in the ecosystem for various participants to support its overall longer term sustain ability (e.g., business to business, business to government or vice versa, end user fees, data related services)?

The private sector business opportunities for the DI ecosystem can be far reaching. Not only can the use of DI potentially generate new services and revenue streams for firms but it can also help increase current efficiencies thereby reducing industry costs. Within our industry we see the greatest opportunities stemming from business to consumer application. We also envisage business to government application within our industry (eg. tax reporting to the Canada Revenue Agency)