Province of Ontario Market Consultation Package - Digital Identity

Kantara Response to Questionnaire
November 2020

This response is submitted by Kantara Initiative.

Kantara's response is from two points of view. The first is based on the core competencies it has developed over the past decade and offers to the Identity Marketplace. The second is based on the experience its Subject Matter Experts have gained from their involvement with the Global Identity Marketplace as either consultants, identity assurance service providers, or product suppliers.

We invite the Ontario team to continue to keep Kantara apprised of its progress. We further suggest a call-in during which we could explore further how Kantara might support the development of an assessment/certification component of the Province's Digital Identity Ecosystem programme.

Intro

1. 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)
   Kantara Response: Kantara is the leading global consortium whose mission is to grow and fulfill the market for trustworthy use of identity and personal data. To fulfill this mission Kantara operates an independent third-party conformity assessment program for the digital identity and personal data ecosystems as well as providing real-world innovation through its development of specifications, such as UMA 2.0, Consent Receipt, applied research and development, its Identity Assurance (Trust) Framework (IAF). Kantara, through the work being done in its newly formed Privacy & Identity Protection in mobile

Driving Licence ecosystems Discussion Group (DGPImDL), also undertakes to explore new areas of study. This group will be producing a report intended to enrich and inform the broader community that will create, deploy, administer, and use mobile Driving Licences on issues concerning privacy and information protection. More information is available at https://kantarainitiative.org/trustoperations/
or contact us at staff@KantaraInitiative.org.

Our interest in offering this submission is to help the Province of Ontario to keep in mind, during the development of its Digital Identity Ecosystem, the importance of providing assurance as to the conformity of all parties involved in the requirements the Province has established for its Digital Identity Ecosystem, and how that assurance can be reliably delivered by proven means.

Kantara is therefore interested in working alongside the Province at key points in the development of their ecosystem to provide a supporting assurance process. The Kantara assurance process is based on the experience of over a decade's operations and on the skills and understanding of our own subject-matter experts, some of whom have contributed to this response.

Ecosystem & Offering

2. How could partnership between the public and private sector be arranged to support the development of the DI ecosystem in Ontario? Government-led? Private sector-led? Consortium? Federated alliance of institutions? As a utility?
   Kantara Response: In Kantara's opinion, the partnership should have Public Sector oversight and governance, with Private Sector delivery. This type of model is used in the Financial Sector where the Public Sector regulates the Private Sector banks, companies involved in securities, and insurance companies. Additionally, the transition Government Ministries will need to make from existing contracts to new contracts that reflect the new requirements involved with Digital Identities and the Wallet will take time.

3. What is the minimal role or involvement by government to establish a stable ecosystem environment, while promoting inclusivity, innovation and private sector involvement? 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?

Kantara Response: Kantara's opinion, based on observations of the marketplace, is that the Public Sector must provide the authoritative sources upon which a system can be built, providing access to at least those requirements that it places on the Private Sector, e.g. checking entitlement to work.

4. What benefits could be realized through public and private sector collaboration? What models of public-private collaboration have you observed in other jurisdictions that Ontario could adopt as a model? Are there specific partnership models that should be avoided and why?
   Kantara Response: The State of New Jersey has a model, but there are others in the Netherlands, Malta, and Italy. Scotland is also actively searching for a new model. In the case of New Zealand, it collaborated with New Zealand Post to leverage its branch network in its early days to undertake in-person identity proofing. New Zealand's RealMe digital identity system uses similar architecture to the Canadian Federal Government's GCKey (being derived from the same source). It is a low assurance login/authentication self attested service where one can upgrade to an Identity Account (architecturally called late binding). 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. It is Kantara's observation that the typical starting position is that the Public Sector focus is on identification and the industry on authentication. Key to these models is active Public Sector oversight and governance to ensure operations remain in the best interest of Ontarians.

5. What attributes/features should a digital identities for individuals or businesses include (apart from basic authentication of name, date of birth, registration date, biometric, address). In other words, what other attributes or offerings should be included and why? (i.e. digital signature)
   Kantara Response: Kantara has no opinion beyond attributes should not be shared without transparency and user consent (either direct or by law).

6. The long-term vision of the government is to issue verifiable credentials to digital wallets that comply with recognized frameworks and standards such as PCTF and W3C verifiable credentials. Recognizing this and other related standards are still under development, how can government progress towards the verifiable credentials model while delivering on its commitment to launch a digital wallet to the public by the end of 2021?

Kantara Response: In Kantara’s opinion if Ontarians already have a wallet, why do they need another, government-provided, one? The provision of credentials and the transition to using them is an enormous project in itself. That being said, Kantara understands that the Province will need a process by which they can approve that an externally provided wallet meets the Province’s requirements. Kantara can assist with this process.

7. What is the best approach in this timeframe to ensure we deliver on this commitment? What role can your organization play in helping us deliver?
   Kantara Response: in Kantara’s opinion this is a very tight and unprecedented timescale for design, development, approval, testing and certification. Kantara can assist with ensuring that the necessary independent evaluation of services, as well as products, is practical.

8. What should be done to drive active user participation, engagement and adoption of digital identity in Ontario?
   Kantara Response: In Kantara’s opinion, if the digital services are easy to use and provide tangible benefits and convenience to Ontarians, they will want to use them without being pressured into using them.

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

10. How can unintended consequences of having digital IDs (e.g. social exclusion, tracing, furthering inequality, profiling) be prevented?
    Kantara Response: In Kantara’s opinion ensuring that requirements to interact with the Digital Wallet include appropriate security considerations and then ensuring, through an operational assurance process, that all participants (i.e., IDP, RP, Identity Network, infrastructure provider, technology provider, other) comply with those requirements will mitigate, though not eliminate, these unintended consequences.

11. 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?
    Kantara Response: In Kantara’s opinion ensuring that privacy requirements to interact with the Digital Wallet are included and then ensuring, through an operational assurance process, that all participants (i.e., IDP, RP, Identity Network, infrastructure provider, technology provider, other) comply with those requirements will mitigate, though not eliminate, the

privacy concerns associated with the handling of sensitive user data. Kantara’s newly formed Privacy & Identity Protection in mobile Driving License ecosystems Discussion Group (DGPImDL) is working in this area.

12. Once the ecosystem is launched, how could it be matured across public and private sector? What can the government create the conditions for inclusion, competition, innovation, private sector investment and participation in the creation of a financially viable digital identity ecosystem?
    Kantara Response: In Kantara’s opinion, relevant policies and legislation governing the use of Digital Identities and the Wallet will need to be developed, or updated if anything appropriate currently exists. Additionally, once the Wallet is launched, the order of what the Province wants to have in the Wallet will need to be determined based on appropriate business cases that are based on the benefits Ontarians will derive from their inclusion. Kantara also recommends that the Province implement relevant operational assurance processes that ensure that all participants (i.e., IDP, RP, Identity Network, infrastructure provider, technology provider, other) comply with the requirements they have established in order to mitigate, though not eliminate, unintended consequences. Kantara can assist the Province with ensuring that the necessary independent evaluation of services, as well as products,are in place.

13. 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?
    Kantara Response: As recommended in its response to question 2, the ecosystem should have active and visible Public Sector oversight and governance with Private Sector delivery. This type of model is used in the Financial Sector where the Public Sector regulates the Private Sector banks, companies involved in securities, and insurance companies.

14. What legal, policy or regulatory changes should be considered to support effective governance and growth of the digital identity ecosystem?
    Kantara Response: Kantara’s opinion, based on observations of the marketplace, regulations should be put in place to deal with liability if something goes wrong (e.g., someone is not who they claim to be). The Commonwealth of Virginia has recently implemented such legislation. The 2008 Crosby report (United Kingdom government) identified the need for both an ombudsman and a repair process.

15. What could the core guiding principles of the governance framework be?

Kantara Response: Kantara recommends that Ontario look to the Pan Canadian Trust Framework (PCTF) for guidance in identifying core operating principles.

16. What could the key operating standards of the ecosystem be?
    Kantara Response: Kantara recommends that Ontario look to the Pan Canadian Trust Framework (PCTF) for guidance in identifying key operating standards.

17. How would be liability be shared among ecosystem participants?
    Kantara Response: See response to question 14.

Technology & Operations

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

19. How would you address difficulties in accessing digital identity services for marginalized Ontarians, who may not have immediate access to a digital device or infrastructure (e.g. high-speed internet)?
    Kantara Response: In Kantara's opinion digital is not synonymous with online. For the most part, those without digital devices will not be needing digital services. Additionally, the digital services should be so good that people want to use them without being pressured into using them by charging lower fees. That being said, Kantara recognizes that the Province wants to provide the ability to digitally register for services which are not delivered digitally. This challenge is being addressed by governments around the world and has not been solved beyond providing access, as the Province is currently doing, to computers in public spaces (e.g., Public libraries) or kiosks.

20. What is your perspective on how to mitigate other technology and operations related risks such as resource gaps, implementation delays, cost-overruns, technology changes over time, technology failure, misuse, device/IP/identity spoofing, bots?
    Kantara Response: In Kantara's opinion, strong programme and project management, especially management of scope, will mitigate, though not eliminate, these risks.

Funding Model & Ownership

21. 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?
    Kantara Response: In Kantara's opinion, based on observations of the marketplace, the funding / business model must take a cost/benefit focus. That is, no charges should be considered without identifying tangible real benefits to the party that will have to pay the charge. For example, individuals are willing to pay for a Driver's Licence because it gives them the privilege of being able to drive. Individuals, for example, are unlikely to be willing to pay for the ability to pay their taxes online.

22. What are the risks associated with your recommendation? How those could be mitigated?Benefits & Monetization
    Kantara Response: In Kantara's opinion the perception of urgency could undermine the development of standards using established processes.

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

Wrap-Up

24. Have you observed any case studies in other jurisdictions that have made significant progress in implementing a digital ID ecosystem? What has worked well and what are some of the key lessons learned?
    Kantara Response: In Kantara's opinion, based on observations of several jurisdictions in the marketplace that have implemented or are planning to implement solutions, is to not only concentrate on lessons learned from success but to also look at why initiatives have failed. In many cases, more can be learned from failure than success. Many have taken far longer than expected: the European Union initiative started in 2005 is now operating but primarily in the Public Sector, and the United Kingdom 2011 plans for an operational system by 2013 have not yet delivered a sustainable system.

25. We have identified some potential risks associated with a digital identity enabled ecosystem –based on the list provided, are there additional risk categories or key risks that have not been addressed? Please share your perspective on mitigating the risks that haven’t been discussed so far.
    Kantara Response: There is mention of variable trust levels with the suggestion that there may be a lack of education. In Kantara’s opinion education needs to be in ways that are relevant to Ontarians. That is, it needs to be non-technical and directed at simplifying the decisions Ontarians have to make. Kantara has recognized that there is little evidence that user trust is based on trustworthiness. gov.uk IDPs show that branding and relevance is demonstrably more important. Kantara also believes that the Province needs to consider a multi-level model for the Private Sector participants when there are multiple parties and no central funding.

26. Is there anything else you would like to share about the approach to developing a digital identity ecosystem?
    Kantara Response: Kantara notes that none of the use case examples given are from the Private Sector, and that the benefits to the user are not offered in measurable terms. Whilst leaving scope for future innovation, relying on it to deliver or to justify a project, adds risk.