

Work Summary – Identity Management

Problem Statement

In the absence of a harmonized approach to digital identity, Canadian jurisdictions are pursuing different digital identity solutions at different paces with no cross jurisdictional services to anchor the approach. This may compromise the ease of use for residents across jurisdictions in the future. This work stream identifies the different components of identity management on the national stage and the key decisions needed on each component to advance identity management in Canada.

Digital Identity management is a quickly-evolving field that is of public policy interest because of what a secure digital identity enables. Broadly, secure digital identities can allow Canadians to carry out high-value transactions online, in a more economically efficient and convenient environment. Secure digital identity can reduce identity theft and improve public safety and public confidence by making it more difficult to use identities fraudulently.

With respect to the narrower context of government operations -- secure digital identities can improve access to government services, regardless of a user's location, that would normally require them to appear in-person.

In order to do this, Canadian jurisdictions and actors in the identity management space need to agree to adopt common standards for how different jurisdictions handle different components of identity management and different levels of confidence in the veracity of that information. Doing so will:

- facilitate a seamless, convenient user experience across jurisdictions;
- improve security by enabling real time validation of identity attributes across jurisdictions;
- ensure that, even as jurisdictions work at different paces, we are all working towards a common understanding of identity management;
- provide the foundation for uniform service levels online to residents of Canada no matter where a resident is located; and
- realize operational efficiencies in our use of taxpayer dollars – by allowing residents who can/prefer to use online channels to do so rather than requiring they use more costly phone and in-person channels.

The private sector already leverages technology to allow users to carry out a high volume of low-value, low level of assurance identity transactions. Canadians expect to be able to interact with government services similarly. This work stream will parse out the work and effort needed to enable Canada's residents to do the same, but for high value services requiring high level of assurance in the identities of the requestors.

Without a harmonized approach, there is a risk that the digital identity vacuum will be filled with disparate approaches to digital identity management. When jurisdictions work at different speeds, it means significantly greater investment may be required to achieve interoperability among jurisdictions in the future. If we can agree to a framework for our approach, we can all work within that framework at our own paces and be

responsive to the unique needs of our constituents while ensuring that we are working towards a common vision.

Priority Project Lead	Ian Bailey & Jackie Stankey	
Priority Project Partners	<ul style="list-style-type: none"> • Identity Management Subcommittee (and Working Group) • Canada's Digital Interchange (and Identity Linkages Project) • Identity Management Pilot Opportunities Working Group • Digital Identity and Authentication Council of Canada 	
Resource requirements	Pending decision from Joint Council meeting in October 2017	
Timeline	Pending decision from Joint Council meeting in October 2017	
Objective(s)	<p>We require direction from Joint Council on:</p> <ul style="list-style-type: none"> • Public Policy & Governance • Communication/Collaboration • Approach to Technology • Pilots 	<p>To achieve: Accelerated movement on identity management across Canada. Specifically, we require:</p> <ol style="list-style-type: none"> 1. Clarity of approach <ol style="list-style-type: none"> a. A defined governance process for how different groups in this space will work together (public policy & governance) b. Common understanding of identity concepts and common language (communication) c. Common standards (Pan-Canadian Trust Framework) d. Understanding of resources available to do this work (commitment to leveraging pilots and approaches to technology) e. Understanding of the requirements of services in the future (technology)
Forward-looking activities (out of scope of this work stream, for future consideration)	<ul style="list-style-type: none"> • Sustaining the roadmap: Determine how to ensure information is relevant and sustainable. • Identify and leverage existing User Journeys to explain how these complex processes and concepts are experienced by residents • Continue to work on a "tell us once" approach 	

	<ul style="list-style-type: none"> Public consultation on digital identity – “What are the biggest pain points for Canadians?” (Aligns with client centred services work stream)
Links/ Dependencies	<ul style="list-style-type: none"> Digital strategy & Client Centred Services
Risks	<ul style="list-style-type: none"> Anytime we are working to change the ways in which one’s identity is collected, used or disclosed, there may be privacy risks. Similarly, fraud and identity theft implications need to be accounted for. Public perception, Communications – both are difficult when working with complex topics that are sensitive and highly personal. Current uncertainty about governance processes poses a significant risk to those jurisdictions that are leading in Identity Management. These jurisdictions require that the PCTF standards be tested and ratified, so that advancements can continue with the knowledge that the framework is stable. Creating path dependency in a field that is rapidly evolving and ensuring that the public sector’s approach is current to what technology people use. If one of the outcomes of increased digital presence is fewer in-person interactions, there may be adverse impacts for residents that rely on in-person who lack digital literacy, as well as those employed in this field. For example, one of the unintended outcomes of increased automation is <u>fewer middle income jobs</u> and a <u>hollowing out of the middle class</u>. There may also be perception risks associated with this trend. Digital identity is not the cause of this trend, but it may contribute to it. If we are aware of the adverse outcomes of this type of work, we can proactively consider mitigation strategies.
Expected Outcomes	<ol style="list-style-type: none"> Shared public policy position and defined governance structures and processes for the completion of the PCTF standards. This work lays the foundations for a “tell us once” seamless user experience with any level of government no matter where they reside or are located at the time of their interaction. Collaboration between jurisdictions to prove out concepts and how we work together. National identity management roadmap and support structures to sustain the roadmap and focus energies.
Tools to Measure Results	<ul style="list-style-type: none"> Outcomes of a pilot with small number of jurisdictions - what the outcomes can tell us about a larger approach and do the outcomes indicate the approach would be scalable? Testing frameworks and standards with existing approaches in jurisdictions (Alpha testing)
Deliverables Pending Key Decision points of JC	<p>Key Components to Accelerate Identity Management in Canada</p> <ol style="list-style-type: none"> Established public policy position and governance processes for decisions on identity management in Canada.

2. Communication Package: Toolkit/Playbook
3. Process and medium established to leverage technology learnings
4. Process and medium established to leverage lessons learned through pilots.

Reporting Plan

- TBD – pending Joint Council decision at October 2017 meeting.

- **Status/Frequency/
Audience**
-