

Joint Councils DIACC Liaising Status Report

Digital ID & Authentication Council of Canada
September 2016



Connecting Canadians to each other and
the world through digital ID innovation.

DIACC Highlights (1)

- Complete - Letter of Intent to collaborate with the Joint Councils of Canada, specifically in the scope of the Identity Management Sub-Committee (IMSC) to develop components of the Pan-Canadian Trust Framework.
- Complete – Letter of Intent with Kantara Initiative to focus on multilateral cross-recognition use cases for trusted identity services
- Complete – Memorandum of Understanding with Rutgers University, Command, Control, and Interoperability for Advanced Data Analytics (CCICADA) to identify opportunities for digital identity services applied research in a cross-border application context. Proposals must be based upon DIACC 10 Principles for a Canadian Digital Identity Ecosystem

DIACC Highlights (2)

- Complete – Published [Proof of Concept #2](#) focused on On-line Proof of Residency.

“By putting the client at the centre of the proof of residency, the DIACC was able to focus on developing an online proof of residency framework that is privacy enhancing, secure, transparent, robust and efficient. This would open up many online opportunities where technological capabilities were once a limiting factor.

The focus on Privacy by Design is key to the framework. By putting the client, and more specifically the client’s privacy, at the centre of the framework, control is in the hands of the client. The client initiates any requests. No information is requested or shared without the express and clearly informed consent of the client.”

DIACC Highlights (3)

- Complete – Published [Pan-Canadian Trust Framework Overview, A Collaborative Approach...](#)

“Canada’s full participation in the digital transformation and global digital economy depends on developing reliable, secure, scalable, privacy-enhancing, and convenient solutions for digital identity. Made-for-Canada solutions reflect and incorporate Canadian principles, business interests, technical models and, demonstrate compliance with Canadian regulations. Made-for-Canada solutions also enable paths to safe and secure cross-border transactions and service delivery.

The Canadian digital identity ecosystem must be trustworthy, reliable, and enable an individual to securely manage access to their personal information and services. These elements are central principles that underpin made-for-Canada solutions. Canadians expect their digital identification infrastructure to operate with transparency ensuring fairness for all. Furthermore, Canadians expect clear and meaningful notice about why and how their information may be collected and disclosed.

Key Highlights (4)

- SecureID News – [Canadian Council Aims for Trusted Identities](#)
- Global identity Summit – Moderator of Identity Proofing and Validation workshop
- Membership – Canadian businesses continue to join the DIACC, however more international and non-Canadian businesses and organizations are becoming members.
 - Interest in Canada as a strategic market
 - Export of Canadian Innovations (personal data protection etc)
 - Connect Canadian collaborative knowledge to global community.

Innovative Initiatives...



1. Collaborate, Create and Publish a Pan-Canadian Trust Framework:

Building upon the work being done by current leaders of the public and private sector, the DIACC is working together with the public sector, to develop and launch a unified Trust Framework that contains the standards and protocols - along with the business, legal and operational policies- that will enable digital identification transformation in Canada.

The main objectives of the Trust Framework are to deliver a standard for digital identity assurance and to create an environment that would support a platform for participants to transact with and trust each other in a robust, secure, scalable and privacy-enhancing way.

2. Develop A Certification Process And Trustmark:

Building on the Trust Framework, a certification will be developed to deploy the Framework in a consistent and credible manner. A licensing protocol and trustmark logo and will also be developed to represent the Canadian standards and controls that ensure the integrity and security of Digital Identification-enabled transactions (a national federated model for digital ID).

3. Diversify the DIACC Funding Model:

While the DIACC is dependent upon membership fees to support its work, the Board and Executive team are focused on developing a mid and long term funding model that will ultimately be self-sustaining.

In the long-term, the vision is to become financially self-sustaining through grants, memberships, certification fees, the/licensing of the Trustmark registry services.

It could be 3-5 years before this model is in place and generating fees that are sufficient to support the DIACC and it's mandate.

4. Existing and Emerging Market Acceleration:

DIACC calls on members to propose new Proof of Concepts, Innovation White Papers, and Applied Research.

Innovation White Papers – take a forward looking or past perspective view. Communicate industry knowledge to business, legal, and technical audiences. (effort: 1-3 months)

Proof of Concepts – test concepts, fast learning, accelerate findings toward solution viability. Participants are encouraged to develop services as appropriate. To maintain neutrality DIACC never engages in related commercial negotiations. (effort: 3-6 months)

Applied Research – develop concepts for services viable for commercial, government and research application. Opportunity to win grants funding. Proof of Concept model that is supported by Applied Research capabilities. (effort: 6-18 months)

5. Member Engagement:

Global highlights are below. Currently performing a scan of Canadian events. We invite feedback to add or adjust any DIACC hosted event.

- **June** AGM – Big Success. DIACC conducted business followed by a workshop of member presentations. This AGM had the highest attendance to a DAICC member meeting to date. DIACC will continue to invite members of the Joint Councils IMSC to join DIACC member meetings to support the collaboration.
- **June** IdentityNORTH – Big Success. Over 150 in attendance from in Canada and around the world. Recognition awards presented to Canadian leaders Kim Cameron (Microsoft) and Dr. Ann Cavoukian (Ryerson).
- **Sept 19-21, Tampa, FLA** Global Identity Summit – Sharing Canadian perspectives and connecting with global thought leaders with focus upon Identity Proofing and Validation standards and innovations.
- **Oct 4, Montreal, QC** Executive Summit hosted by DIACC and Notarius – An opportunity to connect industry expertise and build community within QC.
- **Nov 2, Ottawa, ON (TBC)** DIACC Member Meeting / Workshop – An opportunity for DIACC members and collaborators to share information.
- **May 2-4, Mountain View, California** – Internet Identity Workshop – Global industry experts connecting to share knowledge and identify opportunities to collaborate.
- **May 9-12, Munich, Germany** – Sharing perspectives and connecting Canadian innovation and knowledge with European leaders of business and industry. Supporting Canada's participation in the global digital economy.



Contributor Highlights...

Who's Who of the 2016/2017 DIACC Board

- President, Joni Brennan, DIACC
- Chair, Dave Nikolejsin, Govt of BC
- Vice Chair, Eros Spadotto, Telus
- Treasurer, Andre Boysen, SecureKey
- Brenda Clark, CIBC
- Susie De Franco, Canada Post
- André Lesage, Desjardins
- Corinne Charette, Industry Canada
- John Messina, Treasury Board Secretariat
- David Nicholl, Govt of Ontario
- John Jacobson, Govt of BC
- Janice Wagner, PwC
- Franklin Garrigues, TD Bank
- Jeffrey Wright, BMO

jbrennan@diacc.ca

Dave.Nikolejsin@gov.bc.ca

Eros.Spadotto@telus.com

Andre.Boysen@securekey.com

Brenda.Clark@cibc.com

susie.defranco@canadapost.postescanada.ca

Andre.Lesage@desjardins.com

Corinne.Charette@ic.gc.ca

John.Messina@tbs-sct.gc.ca

David.Nicholl@ontario.ca

John.Jacobson@gov.bc.ca

Janice.Wagner@ca.pwc.com

Franklin.Garrigues@td.com

jeffrey.wright@bmo.com

Trust Framework Expert Committee

- Formalized committee connecting the knowledge and expertise of DIACC members to develop components of the Pan-Canadian Trust Framework.
- Currently Developing: User Sign-In Component
- 3 Inter-related Scopes
 - Priv2Pub = Private sector delivery of service capabilities to the public sector
 - Priv2Priv = Private sector delivery of service capabilities to the private sector
 - Pub2Pub = Public sector delivery of service capabilities to the public sector
- 4 initial Priv2Pub Minimum Viable Use Cases identified
 - MUC1 - Private Sector Native Credentials at a Level 2 Assurance level to be accepted by Public Sector Relying Parties (MUC #1).
 - MUC2 - MUC1 is elevated to an Assurance Level of 3
 - MUC3 - Private Sector Mobile Authenticator/Credentials at a Level 2 Assurance level to be accepted by Public Sector Relying Parties.
 - MUC4 - MUC3 is elevated to an Assurance Level of 3

Thank you!

jbrennan@diacc.ca