

The Digital ID and Authentication Council of Canada (DIACC) is a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation in the global digital economy.

For more information on the DIACC, our members, our mandate and our governance, please visit www.diacc.ca.

[Tip of the Hat](#)

This newsletter featured contributions from:

- **Kenneth Dagg**, Independent consultant in the identity space
- **Timothy Reiniger**, Consults on cybersecurity and information privacy policy with FutureLaw, LLC

[US News: Virginia enacts Digital Identity Law](#)

The Commonwealth of Virginia has become the first common law jurisdiction to enact a digital identity management law. The law aims to facilitate electronic commerce by arming citizens with an affordable means of strong multi-factor authentication by which to fight cybercriminals and identity thieves in the online environment.

Reflecting the overall decentralized and market-based approach of the United States government as set forth in the National Strategy for Trusted Identities in Cyberspace, the law enables and incentivizes market choices for citizens to obtain trusted digital identities for use in e-commerce, social media, and e-government services. Virginia's model rejects a centralized database approach in favor of citizen-controlled identity.

At the United Nations Commission on International Trade (UNCITRAL) Commission meeting this month in Vienna, the governments of Austria, Belgium, France, Italy and Poland, joined by the American Bar Association Identity Management Legal Issues Task Force, proposed that UNCTRAL begin formal work in identity management and trust services. The proposal was well received with work slated to start as early as 2016.

Citing the 2014 European Regulation on electronic identification and trust services, the 2015 Virginia law, and a host of ongoing public and private sector initiatives, UNICTRAL will be asked to consider developing model legislation along the lines of previous such efforts around electronic commerce and electronic signatures.



[DIACC listed as a key accomplishment in Digital Canada 150 - 2.0](#)

We continue to see the DIACC gaining visibility/profile. Most recently, in its update to the Digital Canada 150 policy (Digital Canada 150v2, July 15th, 2015), the Canadian Government listed continuing to work with the DIACC as a key accomplishment.

Protecting Canadians - 2nd pillar of Digital Canada 150 (2.0):

"Furthered the development of a digital identity policy framework for Canada by continuing to work with the Digital ID & Authentication Council of Canada—a not-for-profit coalition of public and private sector leaders committed to developing a Canadian digital identity

framework—to enable Canada’s full and secure participation in the global digital economy.”

"The Digital ID and Authentication Council of Canada has been proud to work closely with Minister Moore, Industry Canada, and the Government of Canada to allow Canadians and our businesses and governments to continue to be global leaders in the newly emerging digital economy."

To access the complete report go to:

English: Digital Canada 150 (2.0) <https://goo.gl/jjU6kh>

French: Digital Canada 150 (2.0) <https://goo.gl/a9KBJO>

[Around the World Update: A Digital Single Market Strategy for Europe](#)

On May 6, 2015, coincidental with the DIACC releasing the Building Canada's Digital Future strategy, the European Commission published **A Digital Single Market Strategy for Europe**: <http://goo.gl/vTmDVb>. The strategy identifies 16 initiatives that are to be delivered by the end of 2016 that when completed could contribute as much as €415 billion per year to Europe's economy, create jobs and transform its public services.

Similar to the strategy published by the DIACC, this strategy is about transforming European society and ensuring that it can face a digital future. The European strategy defines a Digital Single Market as one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. To realize this vision the strategy proposes activities in three pillars:

Better access for consumers and businesses to online goods and services across Europe – the Commission will work towards the rapid removal of key differences between the online and offline worlds (e.g., 28 different national consumer protection and contract laws) to break down barriers to cross-border online activity.

Creating the right conditions for digital networks and services to flourish – the Commission will work towards



At a minimum, the online economy will need methods to deal with legal cross-border recognition issues posed by the use of digital identities now being issued under statutory authority in civil law and common law jurisdictions. Last week in Washington, D.C., the United Department of State conducted a public hearing on the proposal with speakers from the EC, the ABA, and Virginia.

A comprehensive study of identity system participant risks and potential liabilities by the American Bar Association's Identity Management Legal Issues Task Force has revealed the existence of significant legal barriers to the creation of a digital identity credential market. First, there is a lack of a common legal framework. Second, liability allocation is unpredictable. As a result, risks associated with the commercial digital identity credential are currently treated as uninsurable.

The Virginia law resolves this uncertainty by providing a legal foundation for identity trust frameworks as an approach to implementing federated identity along the lines of that which is afforded in other industries such as credit cards. Identity trust frameworks represent a decentralized and flexible source of information governance and policy rules with respect to implementing digital identity for the private and public sectors. The law is not designed to remove liability, but rather to make liability predictable and manageable for digital identity credential providers.

Enabling the development of an digital identity policy through identity trust frameworks has several advantages over a centralised model in that it: 1) helps to avoid cross-jurisdictional authority and choice of law challenges, 2) provides greater flexibility and customization to suit the wide variety of network and participant situations, 3) enables greater ease in adapting information policies to rapidly changing technology, and 3) is easier to enforce against rule violators.

implementing high-speed, secure and trustworthy infrastructures and content services, supported by the appropriate regulatory conditions for innovation, investment, fair competition and a level playing field.



Maximising the growth potential of the European Digital Economy – the Commission will work towards investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.

*By **Kenneth Dagg** - an independent consultant in the identity space. Ken, a former employee of the Government of Canada and part of their Cyber Authentication Initiative, is currently chair of the Kantara Initiative Identity Assurance Working Group. Ken can be reached at KENDAGGTBS@GMAIL.COM*

Events

- Identity Management Europe, Amsterdam | Sept 17
<http://goo.gl/D3z31A>

- Global Identity Summit, Tampa, Florida | Sept 21-24
<http://goo.gl/2q6ea3>

- Privacy. Security. Risk. 2015, Las Vegas | Sept 29-Oct 1
<https://goo.gl/PHfe89>

Join the DIACC

Interested in playing a part of shaping Canada's digital future? Join the DIACC. For information on how you can participate please contact membership@diacc.ca.

By promoting a citizen-focused strategy of making available strong multifactor means by citizens can prove their identities online, the Virginia law represents a new direction in overall cybersecurity strategy that will supplement the current enterprise and network focus.

The law builds on Virginia's extensive digital legal framework for e-commerce and related trust services, including the first cybernotary statute (online notarization using two-way audio video means) in the United States.

And Virginia already has a large commercial base of digital identity-related companies such as CertiPath (for the defense industry), Exostar, and the Kantara Initiative (for the healthcare industry).

Article reference: Virginia digital identity law takes centre stage: <http://goo.gl/Yqvmc4>

*By **Timothy Reiniger** - Timothy consults on cybersecurity and information privacy policy with FutureLaw, LLC in Richmond, Virginia including service as Special Advisor on Digital Identity to the Commonwealth of Virginia. Timothy can be reached at treiniger@futurelaw.net*

READ MORE:

- Virginia first state to enact digital identity law
<http://goo.gl/ApsbNm>
- New Virginia Digital identity law Strengthens Consumer protection
<https://goo.gl/DpYKVT>
- Virginia House Bill 1562/Senate Bill 814
<http://tinyurl.com/no42bcl>

Jobs

Are you looking to fill a position? Submit your requirements to newsletter@diacc.ca and we will be sure to post a link to your job posting on our website.

Newsletter

Would you like to see a particular topic covered or have a corporate success story to share. Submit your suggestions or story to newsletter@diacc.ca.

Follow us

[@digitalcdns](https://twitter.com/digitalcdns)

newsletter@diacc.ca

www.diacc.ca