Trip Report - Identity North 2016

June 15 and 16, Toronto, Ontario, Canada
Prepared by Kenneth Dagg

Day 1 - Presentations

Introduction

Senior executives in DIACC Board are recognizing, and able to discuss, issues related to identity. This is a significant change over the last 5 years.

Building Canada's Digital Future was prepared as a follow on to the Payments System Review. Both highlight and recognize that identity is key to economic growth.

DIACC is becoming recognized in Canada as a nonpartisan forum where people can come together to discuss and solve problems. Hope to build upon this to become a nonpartisan influencer with regulators.

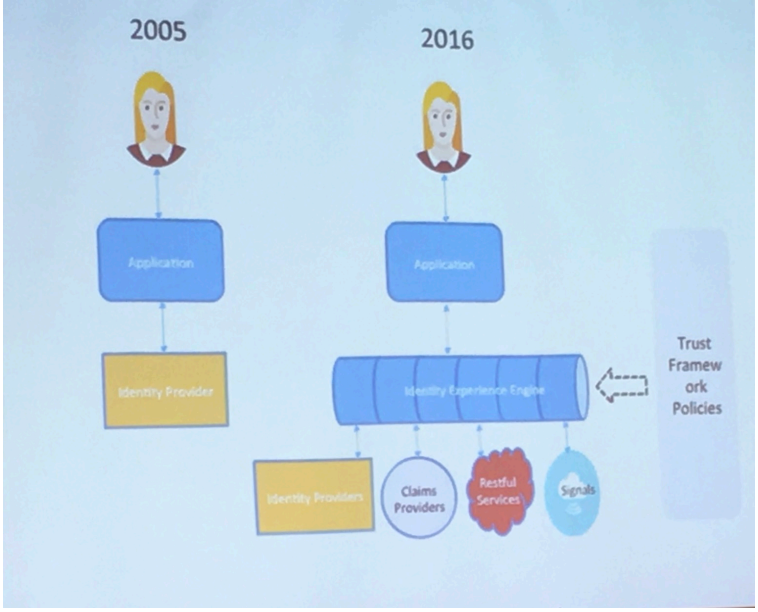
Canada is unique with its values of privacy and user centricity as well as being a federation of provinces. The later enables a faster understanding and appreciation of the challenges associated with federation.

Kim Cameron

The Internet was created without an identity infrastructure. There is no way to know who you're really interacting with on the Internet. Laws of Identity were developed because people were doing things that were privacy invasive.

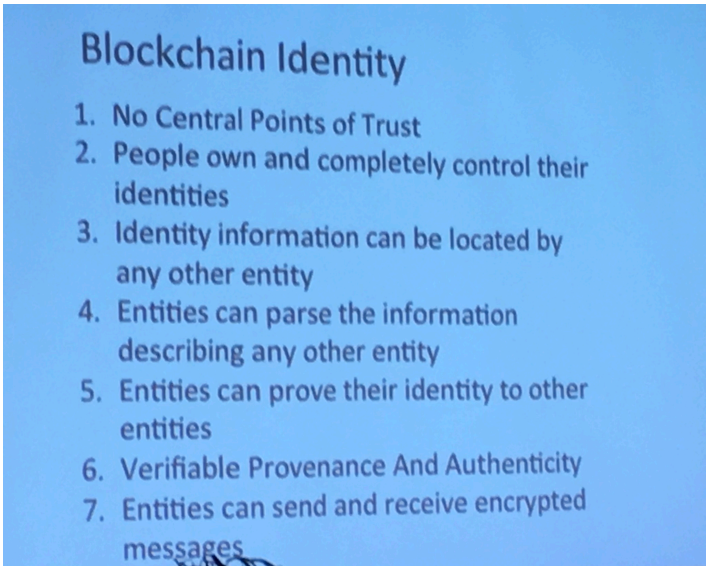
Ten years afterwards the following were identified as what was missed from the Laws of Identity:

- Asymmetry of power between Relying Parties, Identity Providers and Users. The Relying Party is actually the APPLICATION that does something for a User. That is, APPLICATIONs have the power as they use the identity. The question is, how do we get applications to use Identity (is legislation applicable here)? APPLICATIONs need multiple options. That is, APPLICATIONs don't want to rely on a single source of identity. It should be noted that a Relying Party (an organization) has multiple APPLICATIONs.
- The urgent need for professionalization in the application identity management. Attackers are fully professionalized. Organizations need to share details of attacks in order to understand. Requires that the "not invented here" syndrome be left behind. Organizations are becoming aware of the issue and the cost/pain of not doing it.
- There is need for a fourth identity component acting on behalf of the application - the "identity experience engine". goes beyond individual domains.
- Trust frameworks are where things are going- IdPs, claim providers, restful services, signals, trust framework policies --- 2005 2016 picture ---



- The requirement for component operators that are independent of content to enhance privacy.

Freight trains that need to be handled:
- emergence of the cloud (applications in cloud are tenants). The cloud provides compliant automation and trust across tenants that are in the cloud including the possible use for identity authentication. Provides reduced cost of operations but the concentration is potentially bad but also good (eg, less surfaces to attack, cloud operators are motivated to make it safe in order to survive). The fear of dependency drives commitment to standards.
- blockchain --- Blockchain Identity picture --- (NOTE: read Don Tapscott's book)



Identity in Canada

DIACC role is to position Canada in the global digital economy

CPC: looking to expand digital channels. It has the base assets. Important to CPC executives to reduce fraud, process integration and smooth customer experience. Flex delivery is example -

people have to register and therefore integrate into supplier web sites. Trust framework is essential for federation.

PWC: Customer experience is a key for organizations growth especially in digital. Perfect storm is happening with customer expectations. There is more value in collaborative environment but are others certified as being safe? Trust framework is a means to an end.

Notarus: Digital identification needed to authenticate transactions or to sign documents so that they are legally binding (informed him of the blockchain and smart contracts discussion group)

DIACC unique in public/private sector collaboration. Need global interoperability and frictionless customer experience

Proof of Residency proof of concept is underway. Used a collaborative approach which made for open and unconstrained discussion. It is built on the first proof of concept. Next step is to need to involve a potential user to pilot the solution.

International Update

Deb Mathews just announced as digital government minister in the Province of Ontario.

Morpho: Provides mobile payments as well as issues identity documents and payment cards: driver licenses for 42 states and 4 provinces. Now switching to digital space. It is leveraging its epayments experience.

NIST: technology standards and proof of concepts,

ENCAP: 20 minutes to incorporate a company in Norway online. The conversation has shifted to economic value rather than technology.

Kantara: Interacting with government is based on citizen trust of government. In some larger countries citizens have less trust.

Government run systems will solve government problems. In Norway the system was started by banks and government said "it is good enough for us."

In the US public sector funding of pilots has allowed for failure without too much consequence - but most have had some success.

Government has a inherent need to validate identity. They are in the identity business and need to recognize and embrace that fact.

Financial and payments industry could lead the identity space.

Without standards and privacy it won't happen.

Every country needs to work within its cultural milieu. There is an economic value to doing it right. There is faster innovation because identity service exists and doesn't have to be reinvented.

Digital identity is not the end goal. Digital processes are the thing/issue that needs to be fixed. Digital identity is the first step to large innovation opportunities.

Data usage. Regulatory solutions need to be developed that solve for 80% and then "beat the rest with a stick" to get compliance. Data usage has to be respected. There is a need to overcome data usage economy. The issue for users is that the application makes demands for information and they must give consent if they want the service - forced consent with no real choice.

Trend Analysis: Recent Developments in Identity

DIACC video - Digital Identity Card!!!! Privacy Enhancing===Privacy Respecting

Everyone wants a digital transformation but everyone still relies on paper based signatures for legal documents.

Over the last decade 15,000 trusted digital identities created for professionals but everyone required face-to-face verification. Millions of two-factor authentications every year - cannot transfer property in Quebec with one. Millions of authentic documents signed ever year. A major requirement, to satisfy legal requirements, is to be able to open a digital authentic document in 75 to 100 years.

The market enablers for online identity are 1) access to authoritative data sources and 2) secure authentication for the mass consumer market

Enstream is developing a new cloud based service to 26 million Canadian mobile subscribers. Service provides mobile number verification, name and address matching, account type and status, location, and change notification. This is a live service.

Mobile Connect service based on emerging global standard for mobile based federated authentication. Provides a simple, secure alternative to passwords and/or two-factor authentication. Uses device based secure credentials. Extensible to authorization, consent and digital signing services.

Trends from 2Keys: Blockchain, quantum computing (breaks asymptotic cryptography), governance: have to start thinking of clients, governance: board level discussions of impact of cyber requires cyber expertise at the C-level, cyber system admin expertise, IOT

Read Dark Reading article by Jackson Shaw from Dell.

Dr. Ann Cavoukian

There are truths about privacy which dispel current myths:
- Privacy is equal to personal control not secrecy.
- Privacy and functionality can coexist
- Privacy is essential to freedom.
- Privacy is a necessary condition for societal prosperity and well being.

- Surveillance is the antithesis of privacy
- Privacy by design is proactive prevention of privacy breaches. Rather than a trade off model it promotes a win-win model. Need to change the paradigm from zero-sum to a positive-sum model.
- The costs of breaches: class action lawsuits, damage to one's brand, and the loss of consumer trust and confidence.
- European Union General Data Protection Regulation based upon privacy by design, data protection by design and privacy as the default.

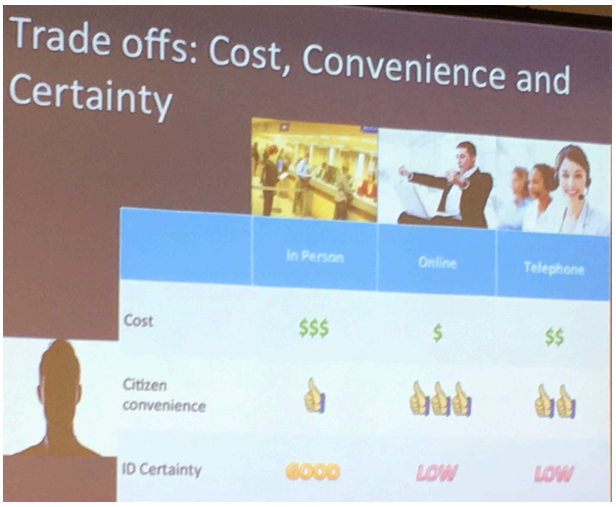
Thoughts on Applying Privacy by Design

Privacy has to be considered (privacy by design) by executives during product conceptual design as well as all other phase of product/service design and implementation.

Other Ways of Providing Privacy by Design - Privacy in Practice

Privacy and Security are two of the key enablers of online adoption. Care has to be taken that IdPs do not become points of surveillance in what users do. They have to collect just enough information and ensure minimal, if any, tracking.

However, the trade offs between cost, convenience and certainty are challenging Trade-Offs Picture



Next issue is frictionless customer experience - the third leg to privacy and security.

800-63 is exploring a Privacy Assurance Level.

Consumers want convenience but also want control, privacy and security.

Privacy question - have you looked at the potential harms that are caused because of the collection of PII.

Day 2 - Unconference

Group C1 - Trust Frameworks

Identity federation is equated to trust framework by many people.

TRUST FRAMEWORK DEFINITION: Rules and tools that help organize come into a community (business, legal and technical) that are agreed to by all participants.

In Canada the Information Management Steering Committee (public sector cross jurisdictional group) has been developing non technical standards. These are being folded into DIACC Trust Framework.

There are different trust frameworks now because organizations are working in their own silos.

VALUE OF TRUST FRAMEWORKS: Enable digital identity mashups.

A trust framework is contextual. DIACC is building a Canada wide trust framework (large context).

The DIACC trust framework does not specify technology or how to do things. It specifies what has to be accomplished.

A trust framework is a capability that enables digital society to work. It is not an end unto itself.

The major issue is how to force or encourage adoption - it will require a major systemic change to how things are done as well as expectations.

There are current trust frameworks in place. The stock market is a symmetric trust framework (trust is both ways). Credit cards are an asymmetric trust framework (trust is one way). SecureKey Concierge is a hybrid trust framework (asymmetric trust on both sides). A trust framework allows transactions to happen.

End points have to be managed with strict criteria

Components: Signin (agnostic to technology, has to meet criteria), verified person (are you a real person) in a context - a government verified and other contexts,

Government to government summit in Ottawa in November to discuss how to coordinate

Canada first but think globally - Canada is a federation therefore well placed over other jurisdictions to understand federated identity

Liability model needs to be teased a part - provided parties are doing what they said they were going to do - RP has to assume the risk - liability is a shared model

Question: what in encourages someone to adopt a trust framework

Session A2 - What's stopping organizations from outsourcing their authentication

- Organization providing authentication service is not from your jurisdiction - issue is what loopholes exist and how to stop them (US patriot act)

- Pieces aren't all there today

- Delegation of authentication to a 3rd party makes people nervous- decision making process

- IDAM in an organization is a vertical stack and poking a hole in that stack to allow third party to do something is a perceived to be a technical nightmare

- Login cost is perceived to be higher than doing it in house - higher risk transactions are thought to need in house solution. But do organizations really understand the cost of doing it house?

- Need criteria that ensure that service is doing the right thing

Note: Connect Europe Facility - have covered entire business / legal / technology aspects

Session A3 - unknown title

Norway experience

45 government departments offering 800 services - government services are more efficient, government processes are simpler, makes businesses more efficient because they spend less time on doing things government requires

Each bank tried to solve their own identity problem, then banks got together to solve the problem once, then platform was opened to government. Government tried to do their own service but came to the conclusion that it did not make sense.

For each Identity assertion their is a cost ... But as a non profit right now ... But savings far outweigh cost

Finland

Started with banks at .30€ per citizen authentication. 3m€ per year. Cost savings to government around 250m€. Tax authority did the study.

Banks don't want to do it anymore. eID, SIM card, bankid can be used. SIM card is stepping up (LOA4) - SIM card has PKI cert. Government stands behind it. Consumer charged 2€/month or .06€/transaction.

Personal data ecosystem landscape

Consumers keep their data in a personal data bank. Their verified claims.

Discussion

- Operations cost of infrastructure (toll road or common road) + cost of converting to digital service
- Question about why taxpayers should pay for organizations that use their Identity service (ie, hotel benefits from reduced risk of identity verified by provincial driver's license)
- Telcos charge for authentication
- Attributes are being sent and charged for. eSignatures are also charged for.