



Presentation by Catherine Johnston to Cardware 08: Securing ID

Good morning. In terms of your identity and the things you carry in your wallet, what do you think of? Do you view your debit card as something that identifies you as the only authorized user of the funds in your bank account?

Do you see your health card as something that shouldn't be used by someone else to get government paid health care?

That is likely the case, but neither card is technically an identity card.

When it comes to identity management, terminology has been a problem. Identifying who we are and identifying our rights and privileges are often intermixed. When we separate the two, certain things become easier. For example, not everyone we deal with on a daily basis needs to have information that identifies us, but they may need information on what we are entitled to do and they likely need the related transaction data.

A financial institution needs to be able to identify us when we open an account, but after that they only need to identify our rights related to credit, debit and other banking functions.

Passport Canada needs to identify us when we apply for a passport, but once that is done, they should only be concerned with our travel transactions.

A critical question that should be asked is whether each program needs its own copy of a client's identity documents or related electronic data, or are the purposes served if they have access to them. Are we safer when there are fewer copies and the access process is secure? Most people would argue that this is the case.

Governments around the world are tackling the challenges of identity management made more complex by globalization and data connectivity.

ACT Canada and our government strategic leadership team started an environmental scan of e-id projects earlier this year and we have found that Canada has fallen behind many other countries. On a positive note, the projects we have implemented, such as the Transport Canada card that you will hear

about this afternoon, have been very successful, but they are few and far between.

I believe that we are struggling with the complexities of working across organizations and across jurisdictions.

We know how to handle Identification, Verification, and Authorization for transactions and we know how to protect data, but sharing policies and processes is difficult in the absence of a national identity management strategy. For the past eight years, speakers have talked about the imminent completion of such a policy.

For those of you here today, you are at the forefront of identity management. Over the past sixty days, we have spoken with over 700 of your peers who work in ministries that deal with the public. They were selected because their work is in the area of policy, security, privacy or service delivery. Fewer than 40 felt that identity management had anything to do with their job, but many changed their minds after we explained why we felt it did. Let me give you one example. After a forest fire or flood, when victims arrive without ID and need help to replace it and need interim aid, and officials on site need to mitigate the risk of fraud, does this not entail identity management?

So this is our first challenge. In the face of dwindling resources, increasing identity fraud and the lack of a national policy that bridges organizations and jurisdictions, each of us must question what we can do and let me suggest that there is a lot that can be done by individuals.

Canadian civil servants did phenomenal work on the ICAO travel standards. Their ability to facilitate differences, rather than insisting on compromise, was inspiring. Individuals also made a significant difference in the US where a hand full of civil servants formed the IAB, the Interagency Advisory Board. This unfunded, unofficial group is now more than 300 strong. They have ascertained the extent of their initial operating capability (IOC) to issue Federal interoperable credentials. They determine next steps, share agency results and address issues. They meet monthly and next month they will meet, as they do each year, at a conference like this in Washington. Individuals do make a difference.

You may ask, when we've had identity systems in place for a long time, what is driving us to change them? There are five key drivers and they bring their own challenges

- Growth in data theft, fraud or compromise: a serious problem when so much identity information is stored electronically. In the payment card industry standards have been developed to tackle this problem. We might consider how much of that work could be leveraged for use by government

- ❑ Use of outdated technology – the world is moving away from magnetic stripe technology because it is not tamper or counterfeit resistant enough to protect valuable information. Adding to the challenge of identity management are all the form factors and technologies now moving into the market.
- ❑ Drive to increase services and promote e-commerce and e-government. This requires us to provide ID that is portable. Today you cannot know what computer, smart phone or other device a customer may want to use to be connected.
- ❑ Need to contain budgets
- ❑ Desire to protect reputations

These drivers are the same in many organizations throughout the public and private sectors. You may already know that the financial institutions in Canada are upgrading the technology on your credit and debit cards. This is because they also faced many of the problems we have today with identity management and fraud.

Fraud migrates, so as the banks move forward and reduce the ability of organized crime to make money from counterfeit payment cards, we will see an increase in other frauds. Organized crime already counterfeits government ID, as well as credit and debit cards. This requires us to upgrade government issued cards or run the risk of increased counterfeiting. If we are considering new cards to identify people or their rights and privileges, for any government purpose, we need to ensure that they are counterfeit and tamper resistant to withstand the attacks by criminals and others.

That brings us to the next challenge. There is no shortage of standards and technology in the area of identity management. Selecting each piece and integrating them into a complete application that meets the requirements of privacy, security, portability and other objectives, without sacrificing any one of them is a tough, but not impossible challenge.

We must view identity systems from the perspective of protecting personal data, from the moment it is collected, whether that is electronically or on a paper form, through every single point from where it can be accessed, until its final disposition. This is hard to do in silo'd organizations and even harder to do when multiple organizations or jurisdictions are involved.

That leads to yet another challenge – speaking for Canadians in matters of International identity management.

So in these challenging times in government, what do we need to do?

I would suggest:

- Identify the champions who will drive this forward
- Get personally involved
- Attract all the right participants and that means a broad group of stakeholders. We need to look outside of our own sectors to see how others are solving similar problems. Other sectors and industry experts can provide valuable information
- Work together to stay true to the mandate of identity management
- *Make decisions that matter to Canadians*

I know something about every person in this room, so I don't say this lightly. I believe you can make a difference.

So to conclude, everything we would want to do as Canadians to securely manage identities **can be done**. This can be seen in programs in other countries. As we move forward we must approach each program as a fully integrated system so that we can ensure that not only each part is sufficiently secure and privacy protective, but that the program as a whole meets the same standards.

ACT Canada and our members can help. We will support you in the drive to implement solutions for the benefit of all Canadians and we thank you for the work you do.