CyberRes

Flash Point Paper

Designing Identity Integration Across Intergovernmental Agencies

As Canada's public sectors push themselves to raise both the efficiency level and the quality of their service as a leading digital government, a vital component of that evolution is how to ensure citizens can identify and receive a mix of services that is appropriate for them, and at the same time comply with security and privacy mandates. These challenges are further exacerbated by the reality that these agencies are, to an extent, decentralized. Here is some perspective and suggestions for solving those challenges.

Intergovernmental Security and Identity

Whether pursued in a coordinated fashion or driven as internal initiatives, government agencies across Canada continue to grapple with integrating and leveraging resources spanning across agencies. The sphere of potential collaboration needs that the agencies do and will continue to have spans beyond their level of governments; i.e., municipalities need access to provincial and territorial information stores and all of them interacting with federal services. Whether these agencies are blending, amalgamating, or fusing their digital information and services, the integration and security requirements are quite lofty:

- Beyond the integrations themselves, from an identity perspective, how do you ensure that citizens can identify and access the set of services they are entitled to receive? As each agency defines its strategy and reviews its options, they will be working with different budgets and skills levels.
- How do you meet privacy mandates, both from the citizen side as well as those working in both the public and private sectors behind the curtain enabling services? These mandates include potentially complex auditing and attestation requirements. Think of the different budgets and skills level each agency has to achieve this.

While the bulk of Canada's public sectors remain decentralized, citizens expect their interactions with them to be singular or contiguous. Whether it's for backend automation behind an online service or through a mobile app, identity information needs to be invoked on behalf of that interacting citizen.

IdM Rules of Engagement

Despite Canada's decentralized public sector agencies, the need to deliver a continuous experience to their citizens will require some model of identity management (IdM) infrastructure, as will the need to secure their privacy. Canada's privacy mandate[1] protects against accidental or intentional disclosure from unauthorized access or unauthorized modifications. Both of these objectives require resources to be secured by an identity management environment.

Agency IdM Options

Since governance plays such an essential role in each agency's ability to comply with these mandates, a review of a few options may be helpful. In their paper defining governance archetypes[2], the MIT Sloan

Defining integration criteria is among the more complex exercises that loosely coupled agencies need to work through:

- How are citizen accessed resources affected by policies and mandates?
- How consistent are each agency's on-boarding processes?
- For collaboration and delivery of shared services, are their identity models compatible?

NetIQ

1. https://priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/
2. Peter Weill, Jeanne W. Ross. IT Governance. Harvard Business School Press, 2004. 57-63

School Center for Information Systems Research described the options. Below are short summaries of the three closest archetype options.

MONARCHY

Is a top/down model where public sector executives make IdM decisions that direct the entire organization of agencies. This model is often executed in the form of specialized committees which make decisions as a group. Even though this is a top/down approach, representatives from affected agencies are typically represented to share their concerns and potentially unique challenges. The advantage of this model is that it's easier for the decision makers to remain focused on the citizen's experience across all agencies.

FEUDAL COOPERATION

A feudal model is one in which each agency retains their own primary decision-making body but is open to negotiating terms for interactions with other agencies as they choose. As applied to IdM or governance decisions they are still in control on how they interpret and apply mandates to their organization, as well as the citizen experience is interacting with them.

INDEPENDENT

In this model, there is no cooperation, no rules of engagement, or coordinating efforts between intergovernmental agencies. The result is that citizens are forced to manage their interaction with each public-facing agency independently.

Model Implications

Regardless of whatever approach is settled on to define the rules of engagement between agencies, two types of interactions need to be defined.

IDENTITIES ACROSS AGENCIES

A key set of IdM rules of engagement that need to be negotiated across agencies include:

- When a user (citizen, public sector worker or partner) moves to a different identity store, such as a province, or spans across multiples of them?
- Does it get copied or moved?
- Who is ultimately responsible for the administration of it?
- Do any of these processes expose an agency to a scenario that falls out of compliance?

INTEGRATION / SYNCHRONIZATION

Whatever the IdM rules of engagement are agreed to for the identities themselves, there will likely be integration or synchronization requirements. While there will likely be a list of concrete requirements, at a higher level, each agency will need a design an interface that can:

- Securely publish identity information beyond their agency to others
- Control who can consume specific identity information
- Perform identity-related audits

Summary

As identity and security architects design their interagency integrations, a few highlights of what we discussed:

- The Privacy Act and PIPEDA continues to play a significant role in each agency's identity management strategy.
- Agencies need to settle on a set of IdM rules of engagement as identities span across them.
- As citizens' access requirements evolve and policies change, plan on IdM playing an expanded role in delivering personalized services securely.

Contact us at
CyberRes.com

About NetIQ

NetIQ provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage at **www.cyberres.com/netiq** to learn more.

Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is part of CyberRes, a Micro Focus line of business.

CyberRes
A Micro Focus Line of Business