

Cross-Jurisdictional Authentication and Authorization Working Group

Terms of Reference

Background

Governments across Canada face a number of complex challenges in supporting primary or core businesses of government while promoting service delivery transformation through the use of new technologies. Electronic service delivery requires some rethinking of traditional approaches to ID authentication and authorization (IA&A). In addition, because citizens are demanding seamless service from all levels of government, there is an urgent need to find ways to recognize and accept electronic credentials across jurisdictions and so leverage the various registration and authentication infrastructures that already exist.

At Lac Carling VII and PSCIOC and PSSDC meetings held in Saint Sauveur, Québec in May 2003 the governments of Ontario and Canada presented an overview of an identity authentication and authorization framework for service delivery that is generic and transferable. This “Chain of Trust” framework was intended to provide the underpinnings for further discussions on the components of IA&A systems, the goal being the development of a standard that all jurisdictions could use to simplify the work to build cross-jurisdictional IA&A systems and to provide a consistent, coherent client experience. It was agreed that a Working Group needs to be established to develop common cross-jurisdictional language to describe the components and related levels of trust for Identity Authentication and Authorization systems and to test the utility of this common language in at least one business sector function at the federal, provincial and municipal level. It was also agreed that the Working Group should recommend an on-going governance structure for the standard.

Objective

The ultimate objective is to have Identity Authentication and Authorization standards that facilitate seamless, cross-jurisdictional electronic service delivery and leverage each jurisdiction’s IT infrastructure. Standards will be maintained by a permanent governance body.

As an interim step towards the long term goals, the Working Group will develop IA&A guidelines, demonstrate the application of the guidelines in a pilot, and develop options and recommendations for establishing the permanent governance body.

Guiding Principles

- Consistent/coherent client experience
- Cross-jurisdictional

- Transparent
- Customer-focussed
- Cost-effective
- Respectful of policy, legal framework of each jurisdiction
- Technology neutral

Membership

The Working Group will be chaired by Ontario and will include representatives from all interested Provinces, Territories, Municipalities and the Federal government. The Working Group will liaise with other PSCIOC/PSSDC committees as appropriate, such as the National CIO Subcommittee on Information Protection and the PSSDC Privacy Committee.

Membership must be approved by the candidate's representative on the PSCIOC or PSSDC. Individual members of the Working Group are responsible for communicating and soliciting views from their respective organizations.

The Chair may also invite representatives of selected organizations to participate such as self-governance professions (Law Societies, Colleges of Doctors and Surgeons) and financial institutions. Such organizations may wish to provide input to the development of IA&A standards because they will be users or deliver some components of broad-based IA&A systems.

Meetings, for the most part "virtual", will take place every two to four weeks at the call of the Chair.

Deliverables

The Working Group will :

1. Develop guidelines containing a common set of definitions and vocabulary for identity authentication and authorization processes for inter-jurisdiction application, including trust levels related to each component of the Trust Chain;
2. Conduct research, review short term opportunities for action and identify suitable candidates for a pilot project to test the first two elements of the trust chain (identification and authentication) at an high enough level of assurance to:
 - demonstrate quick win opportunities
 - demonstrate a "no wrong door" approach
 - confirm the capacity of the network to transport information
 - address cross-jurisdictional relationships and the authority of one jurisdiction to react appropriately to another jurisdiction;

3. Initiate, implement and evaluate the pilot project.
4. Develop recommendations with respect to next steps, including an on-going governance structure and the role of Third Parties

A detailed work plan will be developed and tabled with the PSCIOC and PSSDC.

Timeframe

The Working Group Terms of Reference/work plan submitted for approval to the PSCIOC and PSSDC in **September 2003**.

An interim report made to the joint meeting of the PSCIOC and PSSDC in **February 2004**.

A presentation shall be made to Lac Carling VIII in **May 2004** about the Working Group, reviewing progress and proposing next steps.

Operating Protocols

The objective should be to achieve consensus agreement on decisions and recommendations by the Working Group. In the absence of consensus, dissenting views should be noted for consideration by the governance body and other interested parties.

The Chair must ensure that the work of the Working Group complements other related policy development processes such as the Federal/Provincial/Territorial Council in Identity in Canada and the Canadian Council of Motor Transport Administrators (CCMTA). Development of IA&A guidelines must also take into account existing, related standards such as the ISO 17799 Code of Practice for information security management.

Secretariat

The Office of the Ontario Corporate Chief Strategist (OCCS) will act as the secretariat for the Working Group. Wherever possible, the Working Group will leverage existing processes and infrastructures.

The Chair will rely upon the PSCIOC-PSSDC Secretariat to communicate with the members of those councils.