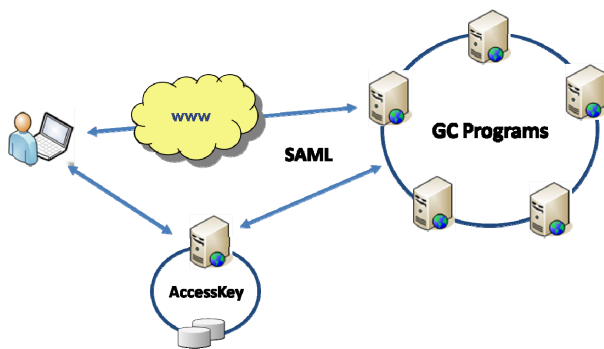


Cyber Authentication Renewal

A well conceived execution strategy

Government of Canada departments and agencies are embracing the evolution of Secure Channel with the Cyber Authentication Renewal program.

If your department is planning or ready to “re-engineer” its existing ePass program, Cistel can complement your effort.



Our team consists of experienced and trained professionals in the area of federated identity and access management, application integration, authentication systems, user data repository integration, and distributed information architectures.

Our services are delivered with a unique combination of people, processes and technology. Our people are highly educated, talented and experienced professionals whom our customers have come to rely on for dependable quality service.

Planning and Execution

Your plan needs to describe how the project will be organized, managed, and accomplished. Cistel personnel can support your transition from ePass to AccessKey by focusing on requirements, design, development, integration, acceptance criteria, reporting procedures, and risks and contingencies.

The Benefits

An execution strategy will allow you to:

- Measure your project performance;
- Map the strategy to your plan;
- Anticipate and manage risks;
- Manage business and technical requirements;
- Comply with standards; and,
- Manage change.

Cyber-Authentication Questions:

- What will be done?
- Who will do the work?
- Why is it being done?
- How much will it cost?
- When will it be completed?
- How does it fit into the overall strategy?

Identity and Access Management with Cistel Security Solutions

SAML 2.0 and AccessKey

The Cyber Authentication Renewal program introduces SAML 2.0 (Secure Assertion Markup Language), a standard XML-based framework for the secure exchange of authentication and authorization information. AccessKey will be the first Credential Provider that will support SAML 2.0. Key milestones for AccessKey:

- Service available May 2010; and,
- GC departments and agencies implementation by December 2010.

Value Proposition

A GC department will be required to evaluate SAML technologies, select a set of vendors, assemble an implementation team, integrate technologies, develop migration procedures, integrate applications, and begin operating and supporting their AccessKey implementation. **Cistel takes the cost and complexity out of your Cyber Authentication Renewal program and allows you to focus on the delivery of your department's electronic services.**



Cistel has developed an **Identity Federation Framework** which is a set of work packages that can be adapted to your needs, whether you are planning or developing your ePass migration strategy.

Federated Identity and Access Management Services

Our customers have come to rely on our deep expertise on IT and consulting services. We can plan and deploy vendor neutral, open standards-based federated security solutions for your department. Solutions include technologies such as:

- SimpleSAMLphp, OpenSSO;
- LDAP, MS AD, OpenLDAP, SQL; and,
- Third party IdM System integration from RSA, Oracle, IBM, Novell, CA and others.

Our expertise in security and privacy standards as well as GC policy compliance issues includes: OASIS, SAML, Liberty, PCI, MITS, GSP / PGS, CLF standards 2.0, and levels of assurance.

Our team of experts provide customers value-added services that rely on our deep knowledge, understanding and experience in Government of Canada security solutions: Secure Channel, MBUN and mapping of SAML assertions and user attributes.

If required, Cistel can also provide 24x7 technical Level-2/Tier-2 support for your federated IdM infrastructure and components. Our technical support services are available via email, web and phone by our highly trained and bilingual SAML security professionals.

For more information, please contact your Cistel Account Manager or email us at: security@cistel.com