

Canadian Government Secure Channel Digital Signing with Luna HSMs

Governments worldwide are moving their processes online to offer citizens improved service levels and much more efficient use of tax dollars. Today's communication technologies provide efficient and secure ways of transacting government business online, with low delivery costs. Canada has one of the most advanced electronic government infrastructures in the world, and has realized a major e-government initiative that changes the way services are delivered to Canadians.

Business Challenge

The Canadian government created an online network known as the "Secure Channel" that enabled Canadian citizens to perform a wide variety of online transactions with the government — from paying taxes to applying for benefits for starting businesses — with assurances that all transactions will remain private and secure. Canada's vision was to have an electronic government that enabled Canadian citizens to conduct any government transaction by computer — including wireless devices — from anywhere and at any time. The Canadian government also required a solution that would keep track of individuals' entitlements and the ability to verify that transactions have taken place. For Canada, the Government Online initiative represents the country's largest technology undertaking to date.

Benefits

- Secures online procurement
- Boosts efficiency
- Increases access

Solution

- Thales Luna Hardware Security Modules (HSMs)

The primary goals for such an ambitious project included:

- Bringing related services together, across organizational boundaries into groupings meaningful to Canadians citizens
- Simplifying access by reaching Canadians where they live and where they work
- Accelerating the pace at which electronic commerce is introduced for government services.

Goals for the technology selected:

- Standards-based to ensure interoperability
- Capable of handling the growing volumes of electronic traffic
- Highly secure to provide a trusted environment for Canadian citizens

The nation's expanding online government services required a means to carry out secure, identifiable, verifiable transactions.

The Solution

"The Secure Channel" is designed to allow Canadian citizens and businesses to access a wide range of different government services electronically. Key components of the solution include an IP network, authentication, a services directory, and web based access interfaces.

As part of the authentication component, a Public Key Infrastructure (PKI) was established to provide citizens with digital identities so that they would be able to supply strong online identification when they deal with government officials via the Internet. The Canadian government has hired a consortium of companies including Bell Nexxia, CGI, Entrust and Thales to provide critical pieces of the security infrastructure.



The security solution is required to issue digital identities to participants in the form of digital certificates, which are electronic files that contain identity information about Canadian citizens. The government centrally issues certificates and each certificate is digitally signed with a private root-signing key owned by the Canadian government that proves the certificate's authenticity. These certificates are analogous to digital passports that must be presented when using online government services via the Secure Channel. Since the government root-signing key proves the authenticity of every issued certificate to potentially millions of citizens, it is of critical importance that this key is carefully protected.

Thales Hardware Security Modules (HSMs) were selected and deployed throughout the Secure Channel system to control and protect the copies of the government root signing keys. Thales products were chosen because they meet the Government of Canada's stringent standards and specifications for hardware security by being validated to FIPS (Federal Information Processing Standards) and Common Criteria standards. Thales products are in widespread use throughout the Canadian government and in many others around the globe.

The Benefits

Among other benefits, the digital certificates issued throughout the Secure Channel will enable secure online procurement, boosting efficiency and increasing access. For example, the \$8 billion the government spends in procurement annually will increasingly be spent via online transactions. Different parts of the government have also improved access to information in a secure manner, in order to better serve the public.

Canada now boasts a central government web portal (www.canada.gc.ca) through which citizens can get information and services from federal, provincial and local government agencies. Because Thales HSMs underpin the issuance of trusted digital certificates, users can be fully confident that their sensitive personal data is protected as they fill out forms and access services. Citizens are able to securely conduct other sensitive activities such as filing tax returns, renewing passports and checking employment records all online.

Conclusion

In recent consulting studies, Canada has been identified as the world's e-government leader. Through the use of advanced technologies like hardware-secured digital identities, the Secure Channel project is bringing enhanced online security to millions of citizens and businesses throughout Canada. Secure Channel is helping transform the way Canadians access and use government services by providing secure access to key government services and information anytime and from nearly anywhere.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.