Overview

It's a known fact that people naturally resist change and often prefer using the same methods and practices that they have always used. The more familiar individuals are with a process, the more convenient it typically is. People use the Internet on a daily basis to find information, do their banking and pay their bills and, since 2004, they have been able to interact with the Government of Canada online as well. So when the Government of Canada sought to extend its online services, they wanted to ensure an easy-to-use solution that was client-centric and that would be convenient for clients to use.

The goal of the government's Cyber Authentication Renewal Initiative, was to implement a scalable, non-proprietary credential service that would offer client choice, reduce costs and continue to provide secure online services to Canadians. The solution also needed to allow clients to use a single-sign on for multiple services and be adaptable to evolving technologies.

GOVERNMENT OF CANADA

Case Study

The challenge

When individuals regularly use an account, they tend to remember the login details. However, many government services are accessed only a few times a year, which may lead to clients forgetting their passwords. Additionally, the average person possess a 130 userids and passwords, so remembering all of them can be difficult, and may lead to password fatigue - over 66% of users forget passwords for sites they don't visit regularly.[1]

While the Government of Canada offers over 80 services online, clients typically don't access them on a daily basis. The government looked for a solution that would provide a choice of credentials that clients already possessed and used on a regular basis. They also wanted to ensure that clients could access multiple services with a single sign-on event. Respecting privacy was of paramount concern as well.

The solution

A key consideration in the government's competitive process for a new online authentication solution was that the proposal had to include a significant number of active user credentials - user names and passwords that were already being used on a regular basis from trusted online services. This would enable secure access to services and would reach a large volume of clients. After a competitive RFP process, SecureKey's

1. A Forrester Consulting Thought Leadership Paper Commissioned By SecureKey Technologies, To Increase Security and User Trust, Embrace a Federated Consumer Identity Model, November 2013

SECURE KEY

proposal was selected. The SecureKey solution included participation from several tier one Canadian banks. The solution would enable online banking customers to sign in to government services using their established banking credentials as the authentication method.

SecureKey initially partnered with three of the largest financial institutions in Canada; BMO Financial Group, Scotiabank and TD Bank Group, to create the SecureKey Concierge solution. Since the successful implementation in 2012, Caisses Populaire Acadiennes, Caisses Populaire, CHOICE REWARDS MasterCard (CUETS), DesJardins, Royal Bank of Canada and Tangerine have also become credential service providers.

SecureKey Concierge operates under a "bring your own credentials" (BYOC) service that enables users to sign into government services via their familiar online banking sign in process. This minimizes the challenge of forgotten, little-used passwords and also reduces the number of passwords that users have to remember. The platform provides a simple and familiar process and eliminates the operational burden of password management. Throughout, privacy is respected. Financial institutions do not know which government services are being accessed and government services do not know anything about the user's banking information – not even which bank the user has used. With SecureKey Concierge employing trusted credentials, the Government of Canada can off er Canadians and individuals and businesses a convenient choice in how they interact with online services.

The outcome

Seamlessly, over 80 diff erent government services were integrated with SecureKey Concierge. The original systems already used the security assertion markup language (SAML) standard, and SecureKey Concierge's SAML2 protocols enabled a straightforward connection between the numerous platforms. The initiative launched on time and on budget, and its popularity has been growing since with over 4 million users.

The system was designed with simplicity in mind. It was recognized that there might be some difficulty withfirst time use. For that reason, SecureKey ensured that help was made available at every step of the sign-in process, to anyone in need of assistance. SecureKey Concierge's discovery process has created an intuitive login process that has been enhanced since its initial implementation and the overall reception has been very positive.

SecureKey Concierge enabled choice and convenience for online users, freeing them from needing yet another credential and another password. At the same time, the Government Canada realized its goals of operational effi ciency, online security and client privacy through an approach that leverages a private sector investment in authentication technology.

About SecureKey

SecureKey is a leading identity and authentication provider that simplifies consumer access to online services and applications. SecureKey's next generation privacy-enhancing identity and authentication network enables consumers to conveniently assert identity information from trusted providers, like banks, telcos and governments, and help them connect to critical online services using a digital credential they already have and trust.

SECURE KEY