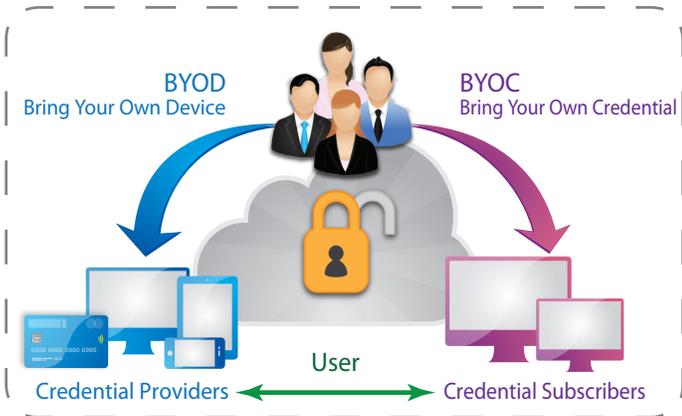


SecureKey bridge.net Exchange combines the convenience of “Bring Your Own Credential” (BYOC) with a privacy-enhancing architecture. Users can sign on to online services using the credential of their choosing without lowering the high bars for security and privacy that government and other highly sensitive services require.



BYOC has arrived

No one wants another password. That’s why social sites are now encouraging users to bring their own credential. Pinterest, Yelp and most social sites now provide “Sign in with Facebook” option that let users bypass new password set up. Users appreciate the convenience, and online sites are happy to remove the sign-up barriers and the liability that comes with storing passwords.

But Sensitive Data Demands More than Social ID

For government services, healthcare and other highly sensitive online applications, enabling BYOC is not easy. Social credential sharing schemes lack the privacy controls that are demanded for sites that manage highly personal information.

What’s needed is a way to combine the convenience of Bring Your Own Credential with strict privacy and security.

A Better User Experience

Exchange makes the Sign up and Sign on processes simpler and easier. Users get to choose a sign in partner that is familiar and comfortable. All partner selection and management options are consolidated within a single user interface.

UI Configuration

Exchange enables each federation to brand and style the UI. Each application within the federation can choose between presenting an embedded credential selector or a standalone selector page.

Privacy by Design

Exchange is designed for privacy. Exchange eliminates the information sharing that happens with other credential sharing solutions. When configured to provide ultimate privacy, each party is blinded from the others. The credential provider never knows what site the user is accessing, and the site never knows which credential provider was used. Exchange itself does not store any or transit any identifying information. A hacker would need to compromise all three parties to piece together the full picture.

Multiple LOAs

Exchange manages the Level of Authentication (LOA) authorities and always presents the sign in partners that meet or exceed the required LOAs. Each CSP is given an authentication level grade during system enrolment, based on an assessment of the Credential Provider’s authentication practices.

User-driven Attribute Sharing

Exchange provides the user with complete control of any attribute exchange requests. Users can control the sharing of each attribute individually.

SecureKey Concierge™ is an implementation of Exchange used by over 120 government agencies in Canada.

Choice of Sign-In Partners

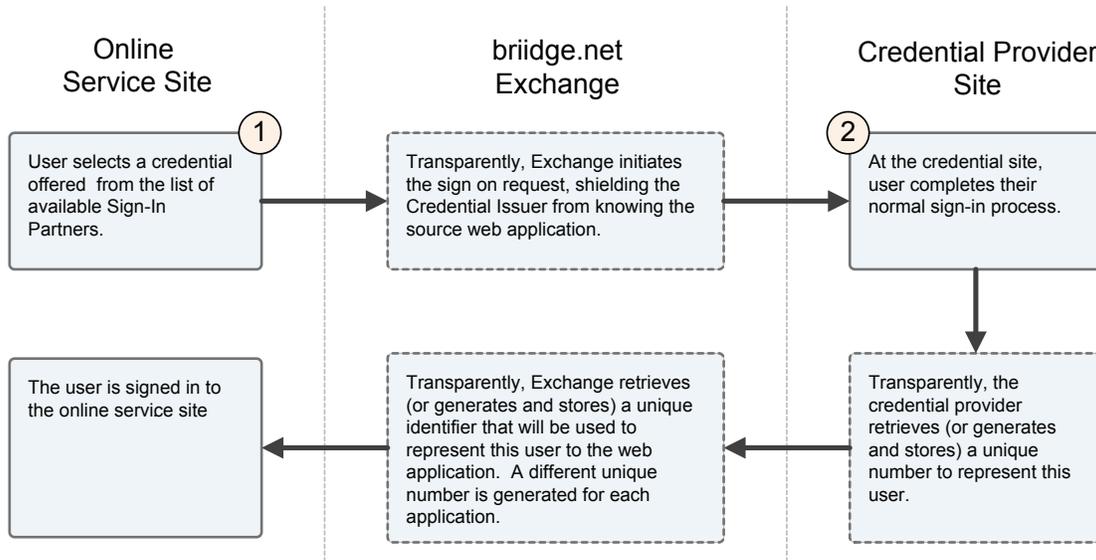
Exchange can provide turn-key access to a wide range of credential issuers supporting various LOAs including PIV credentials. Designed on open standards, Exchanges can accommodate a wide variety of Credential Providers, including Social sign in.

Single Sign On

Organizations with multiple online applications can have all their online applications sharing a single sign on process. After signing in to one online application, a user can then access any of the same organization’s other applications without having to repeat the sign-in process.

The Exchange Sign-In Process

The diagram below provides an overview of the processes that occur when a user signs into your site using Exchange. Steps that the user will see are numbered. The rest are transparent to the user.



Key Benefits

- Better User Experience
- Eliminates Forgotten Passwords
- Eliminates Password Management
- Single Integration providing multiple credentials
- Federated SSO
- Reduced data theft risks
- Strong credential partners
- Enables social without the privacy concerns

Specifications

Supported Application Integration Protocols	SAML2 FICAM/CATS
Supported Credential Integration Protocols	SAML2 FICAM/CATS OpenID 2.0 FICAM FPKI (PIV/PIV-I)
Single Sign On/ Single Log Out	SOAP Binding Redirect Binding
Credential Selector UIs	Embeddable Selector Standalone Selector
Levels of Authentication	Configurable
SAML Confirmation Methods	Holder of Keys Bearer
Accessibility	WCAG 2.0 Level AA

About SecureKey

SecureKey is a global leader in building identity and authentication ecosystems. SecureKey makes it easy to incorporate strong authentication into a wide range of online, mobile and in-person identity and authentication applications for financial services, government, healthcare, converged commerce, and extended enterprises. SecureKey's cloud-based *bridge.net*™ platform combines powerful, device-based security with federated authentication to enhance privacy, create trust, and increase convenience for consumers—using devices and credentials they already have. SecureKey is a Privacy-by-Design (PbD) Ambassador based in Toronto, Canada, with backing from leading technology, payments and mobile network operators.

For more information:

+1 416 477 5625 | info@securekey.com | www.securekey.com

Online Security Made Easy

SecureKey, the SecureKey Logo, *bridge.net*, and the SecureKey App Logo are registered trademarks, trademarks or service marks of SecureKey Technologies Inc. All other product and service names are the trademarks of their respective owners.
©SecureKey Technologies Inc. All rights reserved.

