



POWERING THE WORLD'S LEADING IDENTITY ECOSYSTEMS

Key Benefits

- ✓ Seamlessly connects services and trusted identity partners
- ✓ Improves online service adoption
- ✓ Ensures minimal data disclosure
- ✓ Enforces trust framework standards
- ✓ Provides transparency and central audit records
- ✓ Supports wide range of business models
- ✓ Enables single point integration to any number of partners

SecureKey bridge.net Exchange enables governments, healthcare and other industries to drive the growth and success of online services by forming trusted identity networks. The Exchange platform acts as a market maker, enabling federation across a wide range of identity and credential partners to enrich online services while making access easier for users. Exchange is designed for high sensitivity services where privacy, security, flexibility and transparency matter most.

Eliminating Friction, Driving Online Success

No one wants another password. In addition to the data storage risks and vulnerabilities, telling customers to create yet-another password drives traffic to the more expensive phone and counter service channels, or to competitors. Exchange gives online services the tools needed to speed sign-up and sign-on processes. By enabling the federation of familiar, trusted credential issuers, authoritative identity services and online services, Exchange makes online services faster and easier to use. Users can choose trusted and familiar credentials, eliminating the barriers of forgotten passwords and the drudgery of enrolling in each new service. Applications can be made rich with user data from third-party sources, delivered on demand without needing every application to become a store of sensitive information.

Privacy by Design

Privacy is a core element of the bridge.net Exchange platform. Exchange eliminates the incidental "information sharing as a byproduct" that is common in systems designed for internal enterprise use. When configured to provide ultimate privacy, Exchange can fully blind each party 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 personal user information and only transports the minimal personal information needed to satisfy the transaction request.

Enforced Trust Framework Compliance

bridge.net Exchange includes tools to enforce compliance with trust frameworks. For example, when configured to deliver identity attributes, Exchange can provide the user with complete control over what personal data will be shared. By including user-driven control at the center of the transaction, the user can see exactly what data the Identity Provider (IdP) has delivered and control which data moves forward into the consuming application. Flexible configuration options allow variations of the attribute approval process to balance control against ease-of-use. In every configuration, attribute approvals become part of the audit record to ensure system transparency.

Similarly, Exchange can present terms of use and record user acceptance of the terms in an auditable record. As terms are updated, Exchange can automatically represent the updated terms.

Minimal Disclosure Management

Within any given community, the attributes available from the various partners may vary greatly. One partner may be able to supply date of birth and address while another can only supply year of birth and the last four digits of a Social Security Number. And for any given request, Exchange ensures that the requesting online service receives only the minimum amount of personal information required to meet the needs. bridge.net Exchange enables communities to manage complex attribute landscapes and ensure minimum data disclosure. For each request, Exchange resolves the request against the business rules and attribute mappings to ensure that the request can be satisfied with the required data while minimizing the attributes disclosed.

Flexible Business Models

bridge.net Exchange provides flexibility to support a wide range of use cases and complex business environments. Attribute mapping enables complex attribute environments to be rationalized and normalized. Configurations can be tailored to enable a wide variety of billing models that can provide a mix of per-transaction and per-attribute-based payment models. As needed, the system can resolve conflicting party interests to exclude partners.

Flexible Presentation

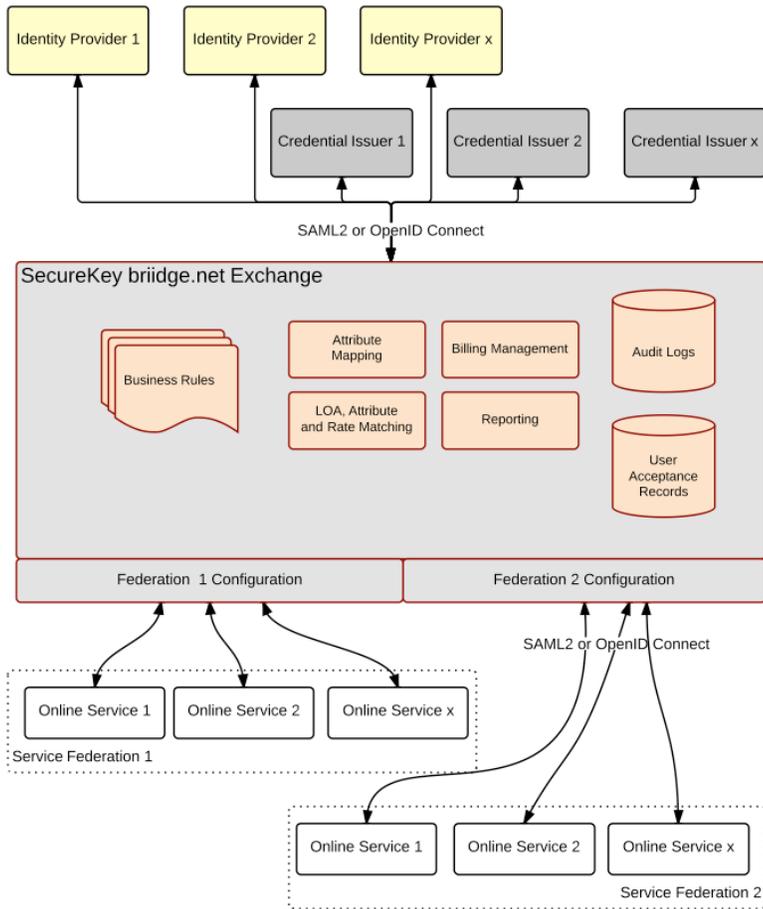
bridge.net Exchange provides flexibility in how the presentation layer is delivered. For each transaction, Exchange discovers which partners can supply the desired Level of Authentication and requested attributes. Each application can choose the how the list of appropriate partners is presented. The list can be delivered within an iFrame, as a consumable service on which applications can build a custom UI or via re-direct to the full-screen selector. Exchange enables seamless user experience by providing flexible control over branding and styling the UI and configure all on-screen languages and wording

LOA Resolution

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

Single Sign On (SSO)

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. Single Sign Out is also provided.



Specifications

Supported Application Integration Protocols	SAML2 OpenID Connect
Supported Credential Integration Protocols	SAML2 OpenID Connect FICAM FPKI (PIV/PIV-I)
Single Sign On / Single Log Out	SOAP Binding Redirect Binding
Credential Selector UIs	Embeddable Selector Standalone Selector JSON data services for custom-building UI
Levels of Assurance	Configurable
SAML Confirmation Methods	Holder of Keys Bearer
Accessibility	WCAG 2.0 Level AA

Sample Use Cases

Government Service Access

Federal governments in USA and Canada have already chosen Exchange as the platform for federating partners to make online services easier to access. Exchange provides the privacy and audit needs that governments demand along with SSO and simple, standards-based integration.

Supply Chain Management

Supply chain portals bring together users from a diverse mix of companies. By federating credentials from across the community, Exchange makes it easier for the community to manage access, off-load credential issuance and ease partner integration. The result is increased convenience for users and greater self-service and delegated management of the credential to the supplier.

Online New Customer Enrolment

For banks, carriers and others looking to reduce the cost of customer acquisition, Exchange can bring together partners to enable online processes for reduced acquisition costs and greater client convenience.

Healthcare

Patient healthcare involves bringing together a variety of professionals spanning hospitals, clinics, pharmacies, governments and other agencies. Exchange provides the strong privacy and data minimization needs that sensitive health information demands.

Commerce

Exchange can be used to eliminate friction in ecommerce and other commerce applications. Credit card brands, for example, can benefit from exchange by enabling users to sign in to merchant sites using their familiar online banking credential. The result is faster checkout for users and greater brand engagement for the card issuer and card brand.

About SecureKey

SecureKey is the identity and authentication provider for organizations that deliver online consumer services. SecureKey eliminates the need to store passwords by securely linking consumer ID to trusted devices, while providing consumers with the choice, control and convenience over how they access the services they want. SecureKey delivers a high-performance, easy-to-use,

strong dynamic authentication platform that reduces the burden, cost, and risks associated with authenticating millions of consumers while also improving the user experience. SecureKey is headquartered in Toronto, with offices in Boston, Washington D.C., and San Francisco. The company is backed by a world-class group of venture and corporate investors.



SecureKey Technologies
36 York Mills Road, Suite 500
Toronto, Ontario M2P 2E9

Toll Free: 1.855.796.3386
www.securekey.com
info@securekey.com