TRUST FRAMEWORK – SECUREKEY CONCIERGE IN CANADA

SK-UN117

Table of Contents

1. Executive Summary

This document summarizes the Trust Framework of the SecureKey Concierge™ service operated by SecureKey Technologies Inc. in Canada. It is publically available to support SecureKey's commitment to openness and transparency with respect to its consumer identity and authentication services.

The SecureKey Concierge service is a cloud-based, Relying Party (RP) and Credential Provider (CP) neutral, online authentication service that enhances the security of online authentication transactions between Users and RPs through a network of trusted CPs.

As with any identity ecosystem, the SecureKey Concierge Trust Framework incorporates the use of particular technology and standards, identifies roles and responsibilities of each participant, formalizes participation through contractual relationships and has a governance structure in place to ensure ecosystem development and enhancement.

The Trust Framework herein outlines the Business, Privacy, Legal and Technical aspects of SecureKey Concierge:

- The Business section provides an overview of the service from a participant connectivity and logical communication flow point of view, as well as defines the ecosystem roles and responsibilities.
- The Privacy section outlines the privacy aspects of SecureKey and its SecureKey Concierge service, including SecureKey's Privacy by Design Ambassador status, a description of the anonymous identifiers used within SecureKey Concierge and how these identifiers are used to enable the service's Triple-blind privacy model.
- The Legal section reviews the contractual arrangements and discusses the limited liability allocation among the ecosystem parties. This section summarizes the SecureKey Concierge Terms and Conditions and Privacy Notice and Policy that are available to the User for review and acceptance. In addition, the Legal section describes the ownership aspects of both User personal information and service activity data.
- The Technical section details the technical aspects of the SecureKey Concierge service including the authentication Levels of Assurance and protocols supported, the certificate governance structure, the community nature of the cloud service and summarizes the technical integration aspects of the onboarding process. It is worth noting that SecureKey Concierge does not currently offer user identity information as part of the service, however, there is market interest for consumer identity services so the groundwork to support identity services in future is being made now.

2. Business

This section descries the Business layer of the SecureKey Concierge Trust Framework.

2.1 Platform Overview

The SecureKey Concierge™ service operated in Canada by SecureKey (herein, SecureKey Concierge) is a cloud-based, Relying Party (RP) and Credential Provider (CP) agnostic, online authentication service that enhances the security of online authentication transactions between Users and RPs through a network of CPs. SecureKey Concierge is a multi-tenant (i.e., multi-Customer) service that enables a User to leverage pre-existing authentication credentials created by the User with a third party CP for login to online service(s) offered by an RP.

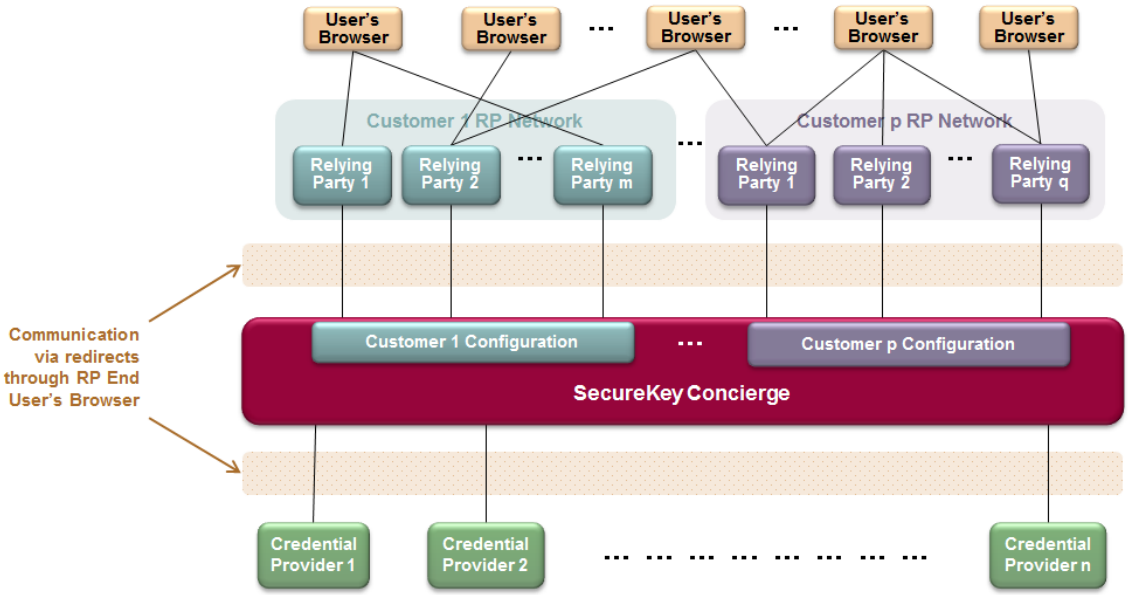
SecureKey's briidge.net Exchange™ platform (sometimes referred to in this document as the Platform) forms the basis of SecureKey Concierge and enables the connection point between RPs and CPs that:

1. Alleviates the need for RPs to connect to multiple CPs (and vice versa), as well as
2. Abstracts the specific User credentials being used for strong authentication to the RP online services.

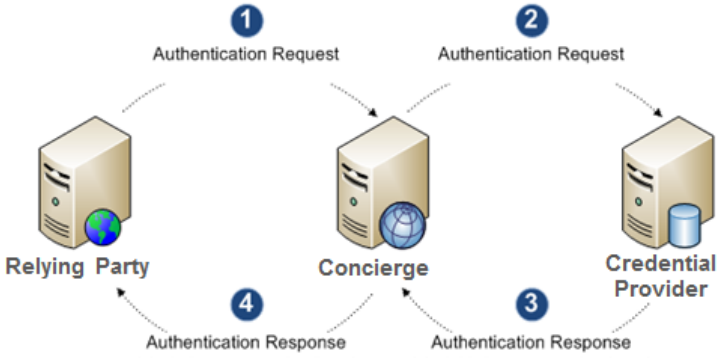
The Platform supports a variety of configurations including Single Sign-On capabilities across a federated group of RP online services, shared terms and conditions and levels of assurance required by each RP offering online services. The policy on which features are configured for a specific group of RPs is decided by the government or corporate sponsor (the Customer) of that group of RPs. The group of RPs for a specific Customer is thus referred to as the Customer RP Network.

Customer RP Networks could include, for example, Federal Government Department / Agency online services, multiple online services across business lines of a single Enterprise, online services for a set of industries as part of an industry association, or simply a grouping of Relying Parties who wish to utilize the SecureKey Concierge service under the Trust Framework established by SecureKey, as summarized in this document.

The general view of connectivity within the SecureKey Concierge service is shown in the diagram below:



The following diagram illustrates the logical communication between the entities:



The authentication process involves indirectly passing authentication messages between entities as the User interacts directly with each entity:

1. RP receives request from the User to sign-on. RP creates an authentication request and passes it to SecureKey Concierge.
2. SecureKey Concierge processes the request and presents a list of CPs to the User. The authentication request is passed to the selected CP.
3. CP receives request and presents the User with sign-on page. The CP authenticates the credentials submitted by the User, creates an authentication response and passes it to SecureKey Concierge.
4. SecureKey Concierge processes the response, creates an authentication response and passes it to the RP.

The RP can then choose to grant the User access to the RP service based on the response.

2.2 Roles & Responsibilities

2.2.1 Technology Provider

As the technology provider of the SecureKey Concierge service, SecureKey is responsible for the development and distribution of the briidge.net Exchange™ platform and for ensuring the Platform is developed using coding best practices for quality and security. SecureKey is responsible for ensuring the Platform conforms to all certifications claimed by SecureKey or required by SecureKey's Customers, such as FICAM compliance for its SAML and OpenID implementations. In addition, SecureKey is responsible for ensuring the Platform is designed and built to support service operational information security requirements and/or certifications required by SecureKey and/or its Customers.

2.2.2 Service Owner & Operator

As the party operating the SecureKey Concierge service in Canada, SecureKey is responsible for negotiating contracts with CPs and with each Customer, conducting audits and completing certification processes on the SecureKey Concierge service, maintaining operational information security in compliance with requirements defined by SecureKey and Customer policies, and ensuring compliance with all Customer contractual obligations.

2.2.3 Customer

The SecureKey Concierge Customer is responsible for contractual agreements with RPs and defining the configuration of the Customer RP Network, including which CPs are approved providers of credentials for use by Users wishing to access online services offered by RPs within the Customer RP Network.

2.2.4 Relying Parties

RPs are responsible for complying with their contractual obligations with the Customer overseeing the Customer RP Network and performing technical integration to the SecureKey Concierge service. Each RP is also responsible for all interactions with a User wishing to access the online service offered by such RP, including all terms and conditions applicable to the relationship between the User and the RP.

2.2.5 Credential Provider

CPs are responsible for complying with their contractual obligations with SecureKey and performing technical integration to the SecureKey Concierge service. Each CP is also responsible for all credential–related interactions with individuals wishing to access online services offered by the RPs, including credential creation, storage and use, and all applicable terms and conditions.

2.2.6 User

Users are required to accept the SecureKey Concierge terms and conditions in order to utilize the service to access an RP site. Each User will be responsible for compliance with the existing terms and conditions that s/he agreed to with the CP that provides the User's credentials, and is also responsible for accepting and complying with the terms and conditions applicable to the online service(s) provided to such User by each applicable RP.

2.2.7 SecureKey Concierge Steering Committee (Governance)

SecureKey, together with other participants in the SecureKey Concierge service (e.g., CPs, RPs), has established a Steering Committee to generally monitor the progress and results of their mutual activities in furtherance of the development and operation of the ecosystem. In particular, the Steering Committee focuses on business, operational and technical issues of mutual concern to the participants, such as usage trends, system performance, security risks, technology evolution, industry standards, marketing and communication efforts, regulatory matters and government relations. The Steering Committee functions as an information-sharing and advisory body for the benefit of the entire ecosystem and consists of one (1) nominee from each party, with meetings typically held on a quarterly basis.

3. Privacy

This section descries the Privacy aspects of SecureKey and its SecureKey Concierge service.

3.1 *Privacy By Design* Ambassador Status

In November 2012, SecureKey joined an exclusive group of privacy thought-leaders committed to ensuring the ongoing protection of personal information by following the Principles of *Privacy by Design*.

Privacy by Design (PbD) is a concept that was developed in 1990's by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. It has since grown into a tangible and functioning reality, with a robust framework of principles and implementation guidelines. Many public and private sector organizations have adopted the principles of PbD, representing diverse fields, from specific technologies or organizational practices, to entire information ecosystems and architectures.[1]

The objectives of Privacy by Design's 7 Foundational Principles are:

1. Proactive not Reactive
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality
5. End-to-End Security
6. Visibility and Transparency
7. Respect for User Privacy

SecureKey developed, deployed and continues to operate SecureKey Concierge according to the PbD foundation principles.

3.2 Anonymous Identifiers

As alluded to in the Business section above, briidge.net Exchange is effectively an authentication hub between RPs and CPs. Of utmost importance in the development of the underlying Platform was privacy. This is evidenced by the sole use of anonymous identifiers within the Platform to provide the authentication hub capabilities. The Platform incorporates the use of two (2) fundamental anonymous identifiers:

- Meaningless But Unique Identifiers (MBUNs)
- Persistent Anonymous Identifiers (PAIs) of two types:
    - Internal Persistent Anonymous Identifiers (iPAIs)
    - RP-specific Persistent Anonymous Identifiers (rpPAIs)

Meaningless But Unique Identifiers (MBUNs)
Each authentication response from a CP includes a value that represents the User associated with the credential used in an authentication attempt. This value is persistent for a single User credential and is a meaningless but unique identifier (an MBUN).

[1] http://securekey.com/press-releases/securekey-designated-as-a-privacy-by-design-pbd-organizational-ambassador/

Persistent Anonymous Identifiers (PAIs)
The Platform generates persistent anonymous identifiers (PAIs) to add privacy enhancing capabilities within the system. The MBUNs received from CPs in the authentication responses are mapped (within the Platform) to internal PAIs (iPAIs), which are in turn mapped to RP-specific PAI (rpPAI) values. These rpPAI values are what get passed to the RPs in authentication responses returned to the RP from SecureKey Concierge. As a result, the identifier used to represent an individual in the authentication response received by RPs from SecureKey Concierge does not provide any personally identifiable information about the User, nor does it identify the CP selected by the User for the authentication transaction.

A single iPAI value in the Platform may include mappings to multiple rpPAI values associated with multiple RPs. rpPAI values are never shared across RPs, and thus knowledge of the rpPAI for one RP would not reveal the User's rpPAI sent to any other RP.

3.3 Triple-blind Capability

The SecureKey Concierge service has a triple-blind privacy model in that:

- RPs are blind to the User's selected CP
- CPs are blind to the RP the User is attempting to access
- SecureKey has no access to a User's personally identifiable information

Blinding the CP to the RP comes as a result of the nature of SecureKey Concierge as an authentication hub. When SecureKey Concierge receives an authentication request message from an RP, it first validates the authentication request, and then generates a new authentication request to be sent to the CP selected by the User. Although SecureKey Concierge internally maintains the correlation between the original request from the RP and the corresponding request to the CP, no RP-related information is contained in the authentication request that is submitted to the CP. The EntityID contained in the authentication request submitted to the CP is that of SecureKey Concierge and not the originally requesting RP. As such, the CP has no exposure to which RP made the request.

On the blinding of the CP from the RP, once the User elects to login to an RP online service with a SecureKey Concierge Sign-In Partner, the User is redirected to a SecureKey Concierge screen (or widget) for CP selection. Thus the RP is not aware which CP the User selects from among the available options. And similar to the blinding noted above, SecureKey Concierge validates the CP authentication response message and then generates a new authentication response to be returned to the RP. SecureKey Concierge uses its MBUN → iPAI → rpPAI database mapping to send the appropriate rpPAI in the authentication response back to the RP. Thus neither the MBUN nor any other CP-related information is contained in the authentication response submitted to the RP, and, as such, the RP has no exposure to which CP the User authenticated with.

The SecureKey Concierge service in Canada does not collect, use, store, transmit or otherwise process any personally identifiable information about the Users in the operation of the authentication hub. As such, SecureKey remains blind to a User's PII, completing the triple-blind nature of the service.

4. Legal

This section describes the Legal layer of the SecureKey Concierge Trust Framework.

4.1 Contracting Arrangements

The SecureKey Concierge Trust Framework consists of the following contractual relationships:

- A Credential Provider Agreement between SecureKey and each CP under which the CP agrees to provide User authentication, as evidenced by the provision to SecureKey of an MBUN sent to SecureKey in its capacity as the authentication hub of the SecureKey Concierge service;
- A Sponsor Agreement between the Customer overseeing or sponsoring a particular Customer RP Network and SecureKey under which the SecureKey Concierge service acts as an authentication hub in order to facilitate access to the applicable RP websites or services by Users who have been authenticated in accordance with the specified Level(s) of Authorization; and
- The Service Terms and Conditions and the Privacy Terms governing each User's use of the SecureKey Concierge service.

Each User will also be bound by: (a) the existing contractual arrangements between such User and his or her CP which address among other things, the issuance, use and protection of the User's credentials (such as username, password, card number or other information used), and (b) the website or other service terms and conditions that the User accepts as a precondition to access a particular RP online service and/or to perform a particular online function.

There is no contractual relationship between any CP, on one hand, and the Customer (or any RP), on the other hand.

4.2 Limited Liability Allocated Among the Parties

SecureKey Concierge operates under the model of properly apportioned and limited liability. Provided that an authenticating CP adheres to existing legal and industry standards, established and proven protocols, processes and contractual obligations for the creation, storage and validation of an individual's credentials and the required Level of Assurance and other specific obligations contained in its contract with SecureKey, such CP shall generally be exempt from liability. A CP's failure to comply with its specific obligations contained in the Credential Provider Agreement resulting in damages suffered by SecureKey could result in the CP incurring damages up to the amounts specified in such Agreement. In addition, a CP may incur liability for damages beyond such amount to the extent it is subsequently determined to have acted fraudulently, violated applicable laws, breached its confidentiality obligations, or otherwise acted in a negligent manner.

The SecureKey Concierge service operated by SecureKey acts as a hub between the CP and the RP seeking to authenticate a User's credentials. Within the SecureKey Concierge Trust Framework, it is understood that SecureKey, in its capacity as the authentication hub, receives an MBUN that is generated by a CP once the User has been authenticated by the CP. The SecureKey Concierge service in turn generates an rpPAI that is conveyed to the RP in satisfaction of the Level of Assurance specified by such RP where the User wishes to complete an online transaction or receive services from the RP. SecureKey's role is simply to facilitate secure and private access to RP websites chosen by Users in adherence to the Level of Assurance chosen by such RP in reliance on credential authentication of a User by his or her chosen CP. SecureKey's obligations (and any resulting potential liability for failing to meet its specific obligations to a CP, a User and the Customer overseeing the Customer RP Network) will be capped at the dollar amounts specified in the applicable contracts that SecureKey has with each of these Trust Framework participants.

As such, provided SecureKey has complied with its specific obligations to each CP, the Customer and each User, SecureKey will not incur liability or be responsible for any damages suffered by a participant beyond the amounts specified in the applicable Agreement. If, however, SecureKey is subsequently determined to have acted fraudulently or negligently, violated applicable laws or a third party's intellectual property rights or otherwise breached its confidentiality obligations, it may incur liability to third parties beyond the dollar amounts specified in the various Agreements.

4.3 Service Terms and Conditions

Each User wishing to use the SecureKey Concierge service (which is distinct from the User's relationship with its chosen CP and the User's interaction with an RP) is presented the terms and conditions that apply to his or her use of the SecureKey Concierge service. By using the SecureKey Concierge service, a User agrees to be bound by such terms and conditions.

Summary of Terms and Conditions

The terms and conditions that govern the User's use of the SecureKey Concierge service are presented to each User on the CP selector page. The terms and conditions[2] contain a description of the SecureKey Concierge service, confirm that the SecureKey Concierge service is provided on 'as is' and 'as available' basis with no performance warranties, and clearly state that the User of the SecureKey Concierge service is responsible for his or her credentials (such as username, password, card number or other information used) in connection with use of the SecureKey Concierge service. Consistent with the User's existing relationship with the chosen CP, the terms and conditions instruct the User to notify the CP if the User suspects any unauthorized access to his or her credentials.

The terms and conditions also clearly state that SecureKey does not collect any personal information in the operation of the SecureKey Concierge service, and further clarify that any collection of personal information by a CP or a desired RP website is done in accordance with such parties' applicable agreements and privacy policies.

As is common with similar online service offerings, the terms and conditions also clearly state that the User is responsible for the use of his or her credentials in order to utilize the SecureKey Concierge service, and releases each of SecureKey, the CP, the Customer overseeing the Customer RP Network in question and each of the RP websites the User wishes to access after being authenticated using the SecureKey Concierge service.

4.4 Privacy Notice & Policy

Each User wishing to use the SecureKey Concierge service is presented with SecureKey's Privacy Notice[3] on the CP selector page as part of the authentication process. The terms within the Privacy Notice explain:

- The nature of the SecureKey Concierge service;
- That no personal identifying information is collected in the operation of the SecureKey Concierge service;

[2] *https://services.securekeyconcierge.com/cbs/nav/tc-cg-eng*

[3] *https://services.securekeyconcierge.com/cbs/nav/priv-conf-eng*

- The information relating to a User that is used within the SecureKey Concierge service, namely:
  - Anonymous identifiers (that is, MBUNs and PAIs);
  - Anonymous session identifiers;
  - The User's language preference; and
  - The User's Internet Protocol (IP) address;
- The manner in which the information relating to a User may be utilized by SecureKey; and
- The specific situations where SecureKey is permitted to disclose the information relating to a User (e.g., to a government body as part of an investigation, in response to a court order, subpoena or other lawful judicial process or as may be otherwise required under applicable law).

To ensure that potential users of the SecureKey Concierge service have an opportunity to review the Privacy terms and to expressly indicate acceptance of the Privacy Terms, each User is required to click "Accept and Continue" in order to continue the authentication process.

SecureKey also maintains a Privacy Policy[4] which can be easily located on SecureKey's website. This Privacy Policy explains the concept of Personal information, confirms that the Policy adopts principles articulated in the Canadian Standards Association's Model Code for the protection of Personal Information, and references the requirements of the Personal Information Protection and Electronic Documents Act (PIPED). In addition, the Privacy Policy offers guidelines on SecureKey's collection, storage, use, disclosure and retention of Personal Information, and provides examples of Personal Information that may be collected by SecureKey.

4.5 Personal Information Ownership

When a User wants to obtain online services or perform a desired function on a RP website, the SecureKey Concierge Trust Framework clearly delineates the relationship between the User and his or her chosen CP from the relationship between the User and the RP in question. Any personal (and/or personally identifiable) information of a User that is created or utilized by the CP in the process of authenticating the identity of the User continues to be subject to the existing contractual arrangements between the CP and the User. Similarly, the applicable website terms of use and/or other contracting terms implemented by the RP website or service and accepted by the User will specify the ownership and permitted use of that individual's personal (and/or personally identifiable) information.

4.6 Activity Data Ownership

During the authentication event for a User to login to an RP online service using their CP via the SecureKey Concierge authentication hub, there are three entities with access to activity data: the RP, SecureKey (in its operation of the SecureKey Concierge service) and the CP.

The RP has ownership of the User's activity on their website. This includes, for example, User requests to access the RP's online service(s), the User's selection of SecureKey Concierge for Sign-in and all User activity following the redirect back to the RP site when SecureKey Concierge sends the authentication response.

SecureKey has ownership of the activity data when the user is redirected to SecureKey Concierge (both from the RP for the authentication request and from the CP for the authentication response. Activity data on SecureKey Concierge includes, for example, which RP made the request, which CP was selected by the User, acceptance (or decline) of terms and conditions, review of terms and conditions and/or privacy notice, MBUN to iPAI and rpPAI mappings, etc.

[4] *http://securekey.com/privacy/*

Similarly, the CP has ownership of the User's activity on their website. This includes, for example, which account is being used for the authentication service, password resets within the authentication flow, if an authentication attempt is successful or not, etc.

SecureKey performs network monitoring for the purposes of threat detection and alerting, to identify capacity issues, etc. SecureKey does not, however, monetize the User activity data it receives.

5. Technical

This section descries the Technical layer of the SecureKey Concierge Trust Framework.

5.1 Levels of Assurance

SecureKey Concierge has adopted Levels of Assurance as specified in the User Authentication Guidance for IT Systems document (ITSG-31) issued under the authority of the Chief, Communications Security Establishment Canada (CSEC). ITSG-31 references the U.S. National Institute of Standards and Technology Special Publication (SP 800-63): Electronic Authentication Guideline.

ITSG-31 Summary Table					
Strength of Mechanism	**Design Requirement Categories**	**Robustness Levels**			
		Level 1	**Level 2**	**Level 3**	**Level 4**
	Authentication Factors	At least one factor required	At least one factor required	At least two factors required	At least two factors required
	Authentication Tokens	At least one of: - something the user knows[1] - something the user has[2] - Something the user is or does[3]	At least one of: - something the user knows[1] - something the user has[2] - Something the user is or does[4]	At least two of (based on different factors): - something the user knows[1] - something the user has[2] - Something the user is or does[5]	The following are required (and may be combined with other tokens): - Hardware crypto token (with activation data) - One of: - Password (subject to password rules); or - Biometric token
	Threat Mitigation (as applicable to environment)	Mitigation against: - On-line password guessing - Replay	Mitigation against: - On-line password guessing - Replay - Eavesdropping - Session hijacking	Mitigation against: - On-line password guessing - Replay - Eavesdropping - Session hijacking - Verifier impersonation / phishing - Man-in-the-middle	Mitigation against: - On-line password guessing - Replay - Eavesdropping - Session hijacking - Verifier impersonation / phishing - Man-in-the-middle
	Cryptographic Module Validation (as applicable to environment)	No minimum cryptographic module validation requirements	No minimum cryptographic module validation requirements	FIPS 140-2 Level 1, augmented with Level 2 for identity-based user authentication (hardware or software)	FIPS 140-2 Level 1, augmented with Level 3 for physical security (hardware only)

ITSG-31 Summary Table					
Security Assurance		SAL 1: applicable where only some confidence in correct operation is required given the low value or sensitivity of the transactions involved and minor threat environment	SAL 2: applicable where a low to moderate level of assured security is required	SAL 3: applicable where a moderate level of assured security is required	SAL 4: applicable in those circumstances in which a moderate to high level of assured security in conventional products is required, and where developers or users are prepared to incur additional security-specific engineering costs
		[1] Password (subject to password rules) / Pre-registered secret token [2] Look-up secret token (printed) / Look-up secret token (electronic) / Soft crypto token (with activation data) / Out-of-band secret token / One-time password token / Hardware crypto token (with activation data) [3] Biometric token [4] Biometric token (to be used only in conjunction with a non-biometric token) [5] Biometric token (to be used only as activation data for another authentication token)			

5.2 Protocol Support

SecureKey's briidge.net™ Exchange platform currently supports the following open-standard data formats/protocols for exchanging authentication and authorization data: SAML, OpenID and OpenID Connect.

Many aspects of the general SecureKey Concierge Trust Framework have been adopted from the Cyber Authentication Technology Solutions Interface Architecture and Specification Version 2.0 Deployment Profile (CATS V2). CATS V2 was developed and published by the Government of Canada Treasury Board Secretariat. It is based on the SAML 2.0 suite of specifications and the profile of SAML 2.0 referred to as the "Kantara Initiative eGovernment Implementation Profile of SAML2, version 2.0 (eGov 2.0)".

The following is a sample of elements from CATS v2 that were adopted in Canada for the SecureKey Concierge Trust Framework:

Requirements in CATS V2

- Language passing using a common domain language cookie
- Level of Assurance as specified in ITSG-31 (as specified in Section 5.1 above)
- Algorithms used must be CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC (ITSA-11E)
- <entityID> values must be agreed upon by the entity and the GCCFGB

Extract of CATS V2 General Requirements

- Level of Assurance request specified using the "exact" compare operator
- Authentication responses must be returned regardless of success or failure of the User authentication
- IDP discovery must be implemented
- Notification of credential revocation by IDPs
- Persistent name format; and NOT support for transient format
- HTTP-redirect binding; and NOT support for other bindings
- Authentication responses must contain at most a single assertion

Key CATS V2 Support Requirements

- Back-channel single logout
- Credential revocation via back-channel requests using the using the SAML Name Identifier Management Protocol (and Profile)
- Level of Assurance as explicitly required

CATS V2 Attribute Requirements

- <AttributeStatement> element required for mandatory attribute: ca:gc:cyberauthentication:basic:specVer = “2.0” for CATS V2

5.3 Certificate Governance Structure

SecureKey Concierge uses digital certificates for authentication request and response encryption and signing, as well as for transport security: TLS communication between the RPs and SecureKey Concierge and between CPs and SecureKey Concierge – all via the User’s Browser. Certificates used for authentication message encryption and signature validation are distributed via metadata files

SecureKey utilizes DigiCert Certificate Authority (CA) for its transport security server certificate(s) for the TLS communication between SecureKey Concierge and CPs. CPs are responsible for their own TLS server side certificates, but typically such certificates are issued from commercially available CAs.

SecureKey also utilizes the DigiCert CA for its encryption and signature validation certificates that are included as part of its metadata file that is exchanged with CPs.

On the RP-SecureKey Concierge communication side, the Customer may dictate which CA must be used to provide the transport and authentication message security. If that is the case, SecureKey will obtain TLS certificate(s), as well as encryption and signature validation certificates (to be included in the metadata file to be exchanged with that Customer’s RP Network) from the Customer-specified CA.Otherwise, SecureKey will utilize DigiCert CA for the certificates on the RP-SecureKey Concierge interface as well.

5.4 Community Cloud Service

SecureKey Concierge is a community cloud service. That is, SecureKey Concierge is a cloud service that is available only to authorized entities: CPs that have an established contract with SecureKey as Credential Providers and RPs that are part of a Customer RP Network, where the Customer has an established contract with SecureKey. From a technical point of view, this community trust is established through an onboarding process of metadata exchange and database configuration.

In order for an authentication request to be accepted and actioned by SecureKey Concierge, the signature on the request is validated. To do this, SecureKey Concierge checks its database for an RP EntityID matching that provided in the authentication response. If the EntiryID exists in its database, SecureKey Concierge will obtain (from its database) the signature validation certificate contained in the metadata file associated with that EntityID and will validate the signature on the authentication request. Assuming it is valid, SecureKey Concierge deems this message to be received from a valid entity in the community and will allow the authentication process to continue by presenting the User with CP options. If the EntityID does not match any EntityID in the SecureKey Concierge database, the authentication message will not be further processed for authentication.

Similarly, SecureKey Concierge validates the signature on authentication responses from CPs by accessing the CP signature validation certificate from the metadata file associated with this CP’s EntityID noted in the authentication response. If the EntityID from the authentication response is not in the database, this authentication response is deemed invalid and is not further processed for authentication.

As a result, any entity that has not undergone a metadata exchange and production onboarding process to the SecureKey Concierge service will not be able to utilize the service.

5.5 Technical Integration

The onboarding process for RPs and CPs follows a similar generic set of activities.

Phase 1 – Initiation

In this preliminary phase the integration process, plan and technical requirements are reviewed and confirmed. An SFTP account is set up for secure file sharing between the Technology Provider and the CP or RP. The integration guide/documentation is shared with the CP or RP and technical support is provided to ensure integration requirements are clarified. The integration plan with partner is aligned with the Customer's overall service enablement plans.

Phase 2 – Partner preparation

This phase refers to the activities related to RP/CP federation service preparation and configuring RP/CP systems for trusted interoperability based on Customer federation requirements. For the RP this phase involves the creation of a SAML service or configuration of an existing SAML service to generate the metadata files required to support the partnership. For the CP this involves the activities required to support the authentication request and provide the response as per Customer requirements.

Phase 3 – Integration

Following the RP/CP metadata preparation based on SAML CATS v2 and validation by the Technology Provider, the initial onboarding process begins. This process involves the sharing of metadata and key exchange in a secure, auditable process. The RP or CP partnership is set up on the SecureKey Concierge service test environment.

Phase 4 – Testing

There are three general phases to testing. Integration Testing: this phase involves testing each component of the overall interface; System Integration (End-to-End) Testing: this phase involves testing the authentication process from end to end; Customer Acceptance Testing: Final acceptance testing is done in this phase, and involves authenticating with RPs/CPs as appropriate during the execution of test cases.

Phase 5 – Approval

Upon the completion of the testing phase and successful execution of the required test cases and Customer use cases the partnership can be approved for promotion to production.

Phase 6 – General Availability

Formal production onboarding procedures are followed to promote the partnerships into production. RP and CP services are made available to Users.

Specific activities related to RP/CP onboarding are outlined in the detailed SecureKey Concierge integration guides. The following highlights some of the additional tasks relative to RPs and CPs.

5.5.1 CP Integration

Additional activities for CP onboarding:

1. SAML request handling and MBUN generation requirement
2. Digital Certificate preparation for Production
3. CP to provide CP login page for SecureKey Concierge authentications
4. Customer branding and SecureKey Concierge CP login page requirements: logos, alternate names etc.
5. User support channel modification as required

5.5.2 RP Integration

Specific additional activities for RP onboarding:

1. Digital Certificate preparation for Production as per Customer CA requirements
2. CP selector mode decision
3. SAML response PAI handling and first time user account binding
4. User support channel modification as required

5.6 Attributes

Although not discussed above, the briidge.net Exchange platform has the capability for CPs to send and RPs to consume User attributes. However, no CPs onboarded to the SecureKey Concierge service in Canada are currently capable of sending attributes, and no current Customers are requiring attributes. As such, attribute flow from CP to RP is not currently in service in SecureKey Concierge in Canada. If that does change in the future, the SecureKey Concierge Trust Framework would be updated to reflect this new capability.