Corporate Privacy Impact Assessment for Keycloak

Part 1 – General

PIA Drafter:	Cole Lance		
Email:	Cole.Lance@gov.bc.ca	Phone:	778-698-5837
Program Manager:	Todd Wilson		
Email:	Todd.wilson@gov.bc.ca	Phone:	250-217-5639

1. Description of the Initiative

The OCIO – BC Developers' Exchange and DevOps branch has facilitated a development community contribution to the tools and capabilities associated with Single Sign On in our Kubernetes Container Platform environment. The tool chosen by the BC Government Application Development Community, Red Hat Single Sign-On (RH-SSO), is based on the Keycloak open source project and enables developers to secure your web and mobile applications by providing Web and Mobile single sign-on (SSO) capabilities based on popular standards such as SAML 2.0, OpenID Connect and OAuth 2.0. The RH-SSO server can act as a SAML or OpenID Connect-based Identity Provider, mediating with enterprise user directory or 3rd-party SSO provider for identity information and applications via standards-based tokens. **BC Developers' Exchange and DevOps branch will maintain current technical and service information to support program areas with accurate Keycloak onboarding**.

Features

Authentication Server

Acts as a standalone SAML or OpenID Connect-based Identity Provider.

User Federation

Certified with LDAP servers and Microsoft Active Directory as sources for user information.

Identity Brokering

Integrates with 3rd-party Identity Providers including leading social networks as identity source.

REST APIs and Administration GUI

Specify user federation, role mapping, and client applications with Administration GUI and REST APIs.

2. Scope of this PIA

IN SCOPE:

Single-Sign On **REST APIs, Administration GUI** and **Identity brokering** aspects of Keycloak are within the scope of this PIA. This PIA is intended as a corporate solution for all Ministries to use Keycloak as it pertains to the approved identity providers and information management assessed below. Any program area intending to use Keycloak must ensure that the PIA on the program contains which

approved identity provider is being used, which data elements from that provider are being used and how they are being used in the new program. Identity providers are approved by the BC Developers' Exchange and DevOps branch.

Identity Providers Include:

- BC Gov IDIR
- BCeID (Basic, Business, Personal)
- GitHub.com
- Linkedin.com
- Google.com

OUT OF SCOPE:

The Authentication Server is out of scope and Production use by client applications is strongly discouraged. There are some cases in dev/test environments where it makes business sense for client applications to leverage the Keycloak Authentication Server. This use should be detailed in the client application's PIA.

User Federation is out of scope. A client application may leverage user federation features, and this should be detailed in the client application's PIA.

3. Related Privacy Impact Assessments

CITZ19024 – BC Registry Services Keycloak

Because this PIA is limited in scope to the platform service aspect of Keycloak each client application use of Keycloak must include a detailed description of their specific use case of the identity provider.

4. Elements of Information or Data

Each Identity Provider has slightly different data objects as part of their authentication responses. At a minimum a Security Token is returned to Keycloak and record of successful login is created and cashed with an auto generated Global User Identifier (GUID), Token and Token Expiry.

* = must be made public by user at login time

ID Provider	Data Elements
BC Gov IDIR (Not personal information)	User Identifier Display Name Email Address
BCeID Basic	User ID Name Email Address
BCeID Business	User ID Name Email Address Business Identifier Business Legal Name
BCeID Personal	User ID Name Email Address
GitHub.com	User ID Name* Profile Picture* Email Address*
LinkedIn.com	User ID First Name* Last Name* Profile Picture*
Google.com	User ID Full Name* Image URL* Email Address*

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

All Data is stored within Canada, in the BC Gov Kamloops Data centre.

6. Data-linking Initiative

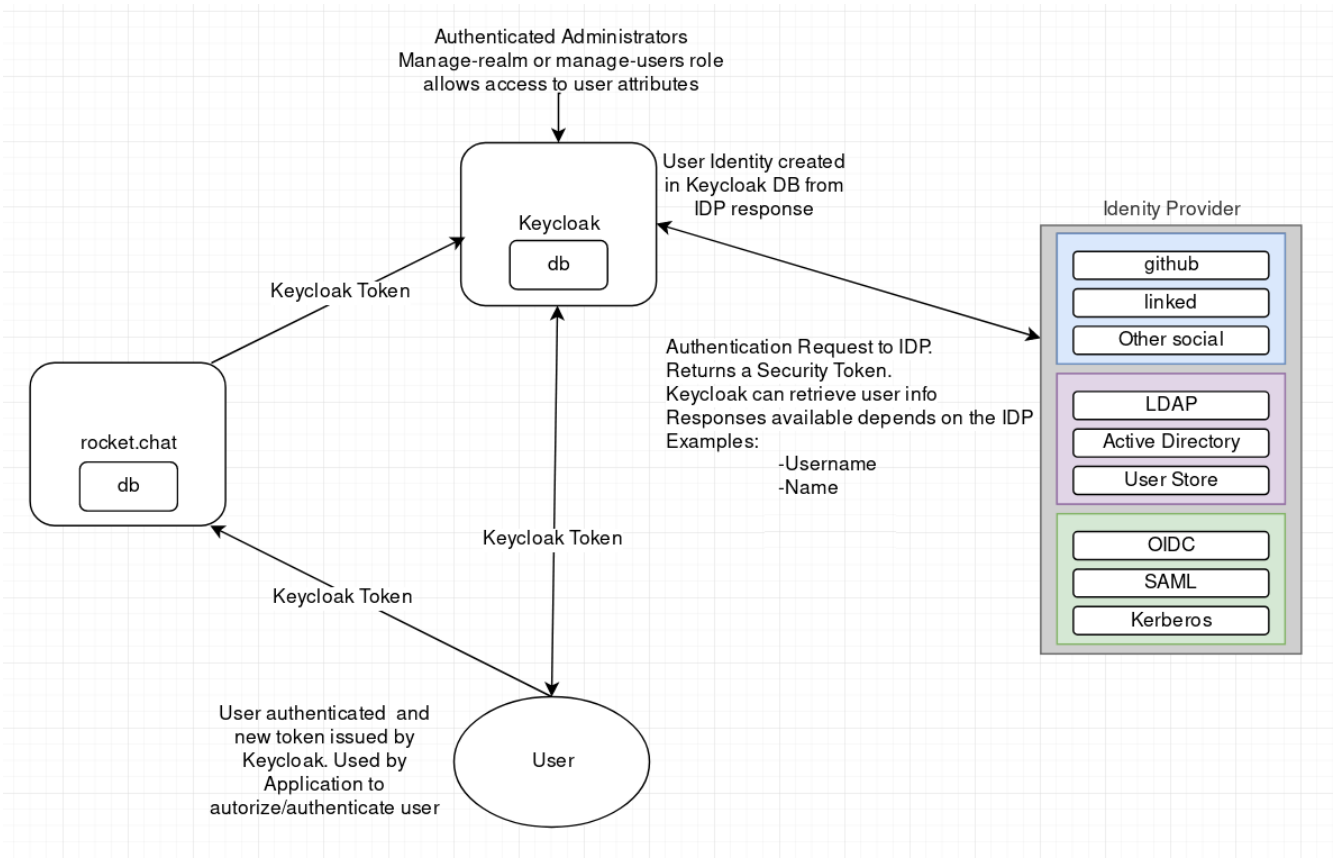
The use of Keycloak is not a data-linking initiative as defined in FOIPPA.

7. Common or Integrated Program or Activity

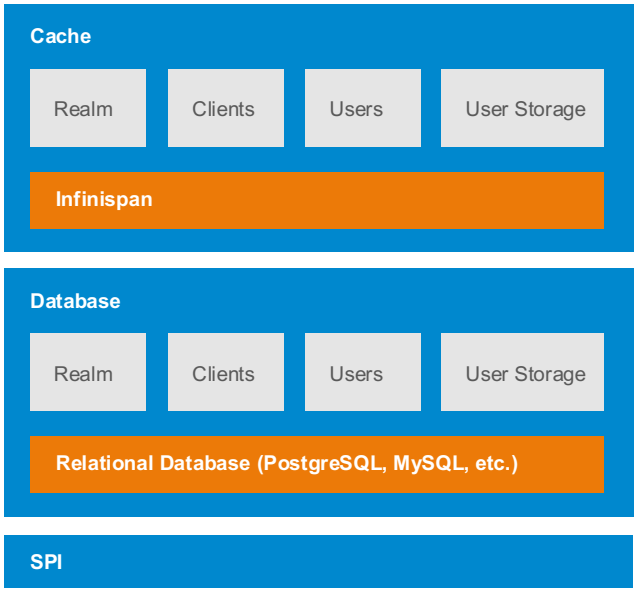
The use of Keycloak is not a common or integrated program or activity.

8. Personal Information Flow Diagram and/or Personal Information Flow Table

This example Personal Information Flow Diagram demonstrates a typical client application use case for Keycloak – in this case the User is connecting to Rocket.Chat client app via Keycloak REST APIs and the Administration GUI view is also included.



A Keycloak realm is a logical grouping of policies and linkages between an Identity Provider and a Client Application. Realms are hierarchical and, as part of the platform service, each Identity Provider connection is made available to client applications as a stand-alone realm. By default, the Identity Provider data is cached in storage and federation of data is only done at the client application realm level.



Keycloak has two types of caches. One type of cache sits in front of the database to decrease load on the DB and to increase overall response times by keeping data in memory. Realm, client, role, and user metadata is kept in this type of cache. This cache is a local cache. Local caches do not use replication even if you are in the cluster with more Keycloak servers. Instead, they only keep copies locally and if the entry is updated an invalidation message is sent to the rest of the cluster and the entry is evicted. There is separate replicated cache which task is to send the invalidation messages to the whole cluster about what entries should be evicted from local caches. This greatly reduces network traffic, makes things efficient, and avoids transmitting sensitive metadata over the wire.

The second type of cache handles managing user sessions, offline tokens, and keeping track of login failures so that the server can detect password phishing and other attacks. The data held in these caches is temporary, in memory only, but is possibly replicated across the cluster.

There are multiple different caches configured for Keycloak. There is a realm cache that holds information about secured applications, general security data, and configuration options. There is also a user cache that contains user metadata. Both caches default to a maximum of 10000 entries or 1 hour lifespan and use a least recently used eviction strategy. Each of them is also tied to an object revisions cache that controls eviction in a clustered setup. This cache is created implicitly and has twice the configured size.

There are also separate caches for user sessions, offline tokens, and login failures. These caches are unbounded.

Personal Information Flow Table – BCeID			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*User attempts to log in to application. A Relaying Party (RP = Rocket.Chat) requires a user to be authenticated, and redirects to Keycloak as an Identity Provider (IdP)*	*No PI*	*N/A*
2.	*Keycloak acts as a RP and starts an authentication request with (example) SiteMinder (IdP).*	*No PI*	*N/A*
3.	*Identity provider (E.g.: SiteMinder CLP) authenticates user. This is completed through the user logging into their account with the IdP.*	*Collection* *Use*	*26(c)* *32(a)*
4.	*IdP forwards valid security token and user information to Keycloak.*	*Use*	*Section 32(a)*
5.	*User is authenticated on the application with Keycloak token. Record of successful login is created and cashed with an auto generated Global User Identifier (GUID), Token and Token Expiry.* *If user attempts to authenticate again before token expires, Keycloak will authenticate the user and log them into the application again. If the token has expired, Keycloak will start another authentication request with the IdP.*	*Disclosure (Out of Scope)*	*N/A*
6.	Clients will have the option of a profile feature. This feature will combine tokens into a single profile using a common data element. If a client realm has profiling enabled, multiple identity providers can be cross-referenced to a single client user profile. Generally this is done through email and is only at the client level not platform. Specific program PIAs will address this feature is it's deemed relevant.	*Out of Scope*	*N/A*

Personal Information Flow Table – GitHub/LinkedIn/Google			
Description/Purpose		**Type**	**FOIPPA Authority**
1.	*User attempts to log in to application. A Relaying Party (RP = Rocket.Chat) requires a user to be authenticated, and redirects to Keycloak as an Identity Provider (IdP)*	*No PI*	*N/A*
2.	*Keycloak acts as a RP and starts an authentication request with (example) SiteMinder (IdP).*	*No PI*	*N/A*
3.	*Identity provider (E.g.: SiteMinder CLP) authenticates user. This is completed through the user logging into their account with the IdP.*	*Out of Scope*	*N/A*
4.	*IdP forwards valid security token (GUID – Non Personal Information) to Keycloak.*	*No PI*	*N/A*
5.	*User is authenticated on the application with Keycloak token. Record of successful login is created and cashed with an auto generated Global User Identifier (GUID), Token and Token Expiry.*	*No PI*	*N/A*
6.	*If user attempts to authenticate again before token expires, Keycloak will authenticate the user and log them into the application again. If the token has expired, Keycloak will start another authentication request with the IdP.*	*No PI*	*N/A*
7.	*Application may request user information from Keycloak. Keycloak will forward this request to the IdP.*	*No PI*	*N/A*
8.	*Based on the pre-set permissions, the IdP will forward user information to Keycloak. GitHub, Linkedin, and Google users must set their permissions to public in order to share any user information with Keycloak and the requesting application. Keycloak receives user information*	*Collection*	*26(c)* *27(1)(a)(i)*

	and creates or updates a record of the user information in cache.		
9.	*Keycloak forwards the user information to the original requesting application**. This disclosure of user information will be addressed in the application specific PIA.***	*Out of Scope (Disclosure)*	*N/A*
10.	*The client application MAY store a copy of the user information (username, first name, last name, e-mail) in their client specific realm (would be detailed in it's own PIA)*	*Out of Scope*	*N/A*

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Identity Provider could falsify authorization for collection and disclosure on behalf of user. (Google, GitHub, Linkedin)*	*Keycloak forwards user to Identity Provider at point of original authorization. User is able to set permissions with Identity Provider at that time.* *Identity Provider takes on serious legal risks by falsifying authorizations for disclosure.*	*Low*	*High*
2.	*Keycloak information management process or security changes*	*OCIO will periodically review Keycloak to ensure it remains a compliant and safe application for government use.* *Ministry users can contact Privacy.helpline@gov.bc.ca or Pathfinder@gov.bc.ca to raise process changes that need to be reflected in the CPIA*	*Low*	*High*

3.	*Program area uses a new identity provider that is not assessed under this PIA*	*Corporate PIA appendix will identify the approved identity providers. The developer hub will contain a link which gives program areas direct instructions on the approved identity providers and how to appropriately incorporate Keycloak.* https://developer.gov.bc.ca/Authentication-and-Authorization/BC-Government-SSO-Service-Definition	*Low*	*Med*

10. Collection Notice

This collection notice must appear as part of any application using Keycloak:

Your user information (*List user information elements*) is collected by the BC Government under Section 26(c) of *The Freedom of Information and Protection of Privacy Act* and will be used for securing applications and services, Single Sign-On and Identity Brokering. Should you have any questions about the collection of this personal information please contact **<< contact person or position, telephone contact number, and mailing address>>.**

Part 3 – Security of Personal Information

11. **Please describe the physical security measures related to the initiative (if applicable).**

BC Gov Data Centre in Kamloops adheres to BC Gov Security Policy in relation to physical security.

12. Please describe the technical security measures related to the initiative (if applicable).

Use of government firewalls, document encryption, or user access profiles assigned on a need-to-know basis, protected by government authentication

13. Does your branch rely on security policies other than the Information Security Policy?

No.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Role-based access.

Administrators: Full Access
Client Administrators: Client Specific Realm

15. Please describe how you track who has access to the personal information.

Keycloak provides a rich set of auditing capabilities. Every single login action is recorded and stored in the database and reviewed in the Admin Console. All admin actions are also recorded and reviewed. There is also a Listener SPI with which plugins can listen for these events and perform some action. Built-in listeners include a simple log file and the ability to send an email if an event occurs.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

Information is always updated/synchronized upon logon.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No.

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

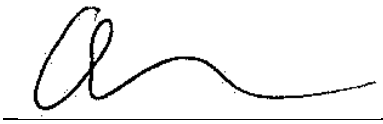
No.

22. Will a personal information bank (PIB) result from this initiative?

Yes, however, the PIBs will be addressed in program specific PIAs that utilize Keycloak.

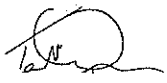
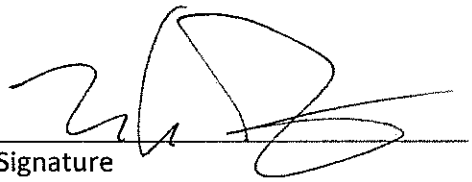
Part 6 – PCT Comments and Signatures

Any program area intending to use Keycloak must ensure that the PIA on the program contains which approved identity provider is being used, which data elements from that provider are being used and how they are being used in the new program. Please see the appendix for more detailed information.

Quinn Fletcher		January 8, 2020
Director, Operations and Privacy Management Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Corporate Privacy Impact Assessment for Keycloak

Part 7 – Program Area Signatures

Todd Wilson		2020-01-22
Program Manager OCIO Technology Solutions Ministry of Citizens' Services	Signature	Date
Hayden Lansdell		2020-02-24
Assistant Deputy Minister Digital Platforms and Data Division Ministry of Citizens' Services	Signature	Date

Corporate Privacy Impact Assessment for Keycloak

Appendix A – Keycloak

What is Keycloak?

This BC Government **Single Sign-On (SSO)** service, based on the Open Source Keycloak (aka Red Hat SSO) product, provides an industry standard (OIDC) and enterprise-policy compliant means of implementing authentication and authorization within applications that is also simple for development teams to provision, utilize and manage. This service is offered to BC Government development teams building cloud native web or mobile applications. Teams wishing to use this service should connect with the Enterprise DevOps Team to discuss their needs and ensure alignment prior to making a request.

Approved Identity Providers

Keycloak must only be used with these specific approved identity providers:

Approved BC Government Identity Providers	BC Gov IDIR and BCeID (Basic, Business, Personal).
Approved Third Party Identity Providers	GitHub, Linked In, and Google

Ministries seeking to use alternative identity providers should contact the Enterprise DevOps Team at Pathfinder@gov.bc.ca. **Any use of an alternative identity provider will need to be assessed in the application or project PIA.**

My Project is Using Keycloak, Now What?

The Privacy Impact Assessment (PIA) for the application or project using Keycloak will need to address some specific Keycloak details. This requirement originates from the Corporate Keycloak PIA. Here is a list of details that should be included in the application or project PIA which uses Keycloak.

Detail	Explanation
1. Identity Provider	Only approved identity providers can be used with Keycloak
2. Data Elements	Each Identity Provider has slightly different data objects as part of their authentication responses. Part of the different data objects contains user information which may contain personal information and will be to be assessed in the PIA.
3. Disclosure	User information that is personal information may be disclosed to the application using Keycloak. This disclosure needs to be assessed in the PIA.

4. Collection Notice	Ensure your application or project PIA includes the required collection notice as found in the Corporate Keycloak PIA – question 10.
5. Personal Information Bank (PIB)	Any personal information that is stored and searchable by a personal identifier needs to be recorded as a PIB. This includes any user information that is personal information.

For more information on Single Sing-On (SSO) service and Keycloak, please visit: https://developer.gov.bc.ca/Authentication-and-Authorization/BC-Government-SSO-Service-Definition

For more information on The Keycloak Corporate Privacy Impact Assessment, please visit <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments/corporate>, contact your Ministry Privacy Officer, or call or email the Privacy and Access Helpline at 250-356-1851 or privacy.helpline@gov.bc.ca