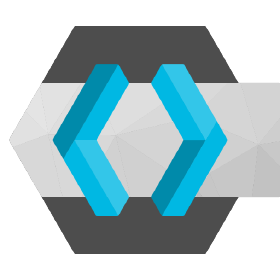
|  |
| --- |
| KeyCloak |
| Billy Hofland  DB03  2023/2024 |



Research Report

Research Report

Research Report

Research Report



Table of contents

[Introduction 3](#_Toc156598708)

[Problem description 3](#_Toc156598709)

[Main question: 3](#_Toc156598710)

[Sub-questions: 3](#_Toc156598711)

[Results 5](#_Toc156598712)

[Sub-question 1: 5](#_Toc156598713)

[Sub-question 2: 7](#_Toc156598714)

[Sub-question 3: 9](#_Toc156598715)

[Sub-question 4: 11](#_Toc156598716)

[Resolution 13](#_Toc156598717)

[References 14](#_Toc156598718)

[Version history 15](#_Toc156598719)

# Introduction

## Problem description

Users need to create and remember different credentials for each service associated with TeamVas, my online education platform. Because my application offers different services with multiple accounts this leads to a rather annoying experience and often results in forgotten passwords or the usage of overly simplistic, insecure passwords. Furthermore, without a centralized system, it’s difficult to track user activities and preferences across different services.

## Main question:

Which IAM best aligns with the specific needs, user management, and the demand for a centralized system in an online education platform?

## ­Sub-questions:

1. How does KeyCloak function inside of IAM?
2. Literature study: By looking at the different sources, information about KeyCloak can be found regarding the IAM system.
3. Document analysis: Examining the official KeyCloak documentation reveals its role and function within Identity and Access Management (IAM).
4. How can KeyCloak be integrated with the specific needs and features of an online education platform?
5. Community Research: By searching for various forums and user created posts, The most active community can be found for all the popular IAMs.
6. Observation: By looking at what other people are using and how they are customizing their IAM, and whether this could be a good fit for an online education platform.

1. How does KeyCloak accommodate the unique roles and access levels required in an online education platform, and how does KeyCloak support SSO for multiple applications?
2. Best good and bad practices: From looking at other high-quality projects, I can find out how they managed to successfully implement all needed features of KeyCloak into their application.
3. Prototyping: Creating a prototype helps in understanding the availability of security features that KeyCloak has to offer.
4. Which OWASP risks are covered by KeyCloak, and which do still exist after implementing KeyCloak?
5. Document analysis: By reviewing the official documentation of KeyCloak, I can determine what risks are covered by KeyCloak.
6. SWOT analysis: By conducting a SWOT analysis for KeyCloak, identify the strengths, weakness, opportunities, and threats.

# Results

## Sub-question 1:

**How does KeyCloak function inside of IAM?**

IAM stands for Identity and access management, it is used to control critical information about user access within the organization. Systems used for IAM include but are not limited to single sign-on systems and two-factor authentication. Single Sign-On (SSO) allows users to access multiple applications and services with a single set of credentials. This reduces the number of attack surfaces as there is fewer passwords for potential breach. IAM systems can also be useful for the ability to securely store identity and profile data. (Gittlen, 2021)

KeyCloak is an open-source tool for IAM, it supports Single Sign-On as well as support for different protocols such as OAuth. The system can be distributed in 3 ways including Docker. The importance of KeyCloak is automating the process of authentication in addition to being logged in on several applications and resources of the network. This would be beneficial for an online education platform since it is based on multiple functionalities that require a user to be logged in before using them. (Żyliński, 2021)

The extra security that KeyCloak offers is MFA (multi-factor authentication) also referred to as two-factor authentication, it gives extra security to the sign-in process by requiring the user to provide an additional form of identification. This could something like a PIN or passcode, generated by an external device. MFA is very important in an application since it reduces the security login risks by a lot. (Kinzer, 2021)

**How does KeyCloak secure applications/services?**

KeyCloak functions within Identity and Access Management (IAM) by offering a comprehensive solution for securing web applications and RESTful web services. KeyCloak operates as a single sign-on (SSO) solution, meaning it centralizes the authentication process across multiple applications. This not only simplifies user access but also enhances security, as applications do not directly handle login forms, user authentication, or user data storage. (Red Hat Software, 2023)

KeyCloak is built on standard protocols such as OpenID Connect, OAuth 2.0, and SAML 2.0, ensuring compatibility and secure integration with a variety of applications and services. This versatility allows KeyCloak to function as a bridge between different authentication systems, including social logins and identity brokering with external OpenID Connect or SAML 2.0 Identity Providers. (Red Hat Software, 2023)

Furthermore, KeyCloaks extensibility is a significant advantage. It offers various Service Provider Interfaces (SPIs) for customizing different aspects of the server, like authentication flows and user providers. It also comes with client adapters for a wide range of platforms, enhancing its adaptability in different environments. (Red Hat Software, 2023)

## Sub-question 2:

**How can KeyCloak be integrated with the specific needs and features of an online education platform?**

A screenshot of a computer

Description automatically generated

*Source 1: Reddit survey about using identity providers* [*https://www.reddit.com/r/devops/comments/16tmdat/does\_anyone\_here\_use\_keycloak\_as\_their\_main\_idp/*](https://www.reddit.com/r/devops/comments/16tmdat/does_anyone_here_use_keycloak_as_their_main_idp/)

In this reddit survey KeyCloak was voted as most popular IDP, the reactions under this survey provided a good oversight of why KeyCloak can fit the specific needs and features of an online education platform. From looking at the comments I’ve found that KeyCloak has an excellent SLA, this stands for service level agreements and is a promise from the supplier of how much the uptime is for a service. For KeyCloak this is 99,9%+, this is rather useful for an online education platform since downtime could have negative effect on the learning path of a student.

**How can KeyCloak be customized to fit the theme of an online education platform?**  
KeyCloak allows users to make custom login screens and a custom User Interfaces to fit the theme of their web application. A starter project has been made by the community named KeyCloakify (Köbler, 2023) (<https://github.com/keycloakify/keycloakify-starter>) . In this GitHub project users can customize their KeyCloak experience. This includes but is not limited to customized layout, colour schemes, sign in screens and typography. (Garrone, 2024)

For an online education platform, this GitHub repository could be customized to enhance the user authentication experience by matching the platform's branding and user interface. This could involve customizing the login, registration, and account management pages to align with the educational platform's design. Specific educational tools or recourses could also be integrated directly within the Keycloak authentication flow for a great user experience.

## Sub-question 3:

**How does KeyCloak accommodate the unique roles and access levels required in an online education platform, and how does KeyCloak support SSO for multiple applications?**

Niko Köbler, a recognized expert in KeyCloak, has contributed significantly to the community by creating a comprehensive YouTube series focused on integrating Single Sign-On (SSO) in applications using KeyCloak, specifically for developers working with React. This series is particularly valuable as it offers a deep dive into the practical aspects of implementing SSO in modern web applications, a critical feature for enhancing user experience and security. (Köbler, 2023)  
  
Aswell as these YouTube tutorials, Niko Köbler has developed and shared a GitHub repository that serves as a practical example or a template for implementing SSO using KeyCloak in ReactJS applications. This repository is not just a codebase but a learning resource, demonstrating best practices, efficient coding techniques, and how to overcome common challenges encountered during the integration process (<https://github.com/dasniko/keycloak-reactjs-demo>).

**Prototype for SSO and role-based access control in KeyCloak:**

To furthermore establish the positive need of KeyCloak in an application, a prototype was built. This prototype featured Single Sign On, role-based access control and an endpoint protected backend. The prototype was created in ASP.net C#, with the framework ReactJS. KeyCloak V23.0.3 ran in docker as an external service providing security to the prototype. Authenticated Endpoints were tested using Postman and 2 separate roles were created upon testing the role-based access control.

A screen shot of a computer program

Description automatically generated

*Source 2: Using KeyCloak for authenticated routes.*

A screen shot of a computer code

Description automatically generated

*Source 3: Initializing KeyCloak in React application.* A black background with white text

Description automatically generated

A black background with white text

Description automatically generated

*Source 4: Authenticating endpoints using KeyCloak in C# ASP.net.*

This prototype was eventually used in the main application. Where it was expended to both frontends that were used and more users/endpoints were authenticated.

## Sub-question 4:

**What is OWASP?**

OWASP is an international organization that focuses on web application security. The OWASP top 10 are the most critical risks involved in web development. These are updated in real time and include but are not limited to Injection, broken authentication, and sensitive data exposure. OWASP also provides recourses, tools, and best practices to assist in mitigating these risks. This includes guidelines for secure coding and official documentation further explanations.

**What are the top 3 OWASP risks (2023) that KeyCloak covers?**

The far most popular OWASP risk is broken object level authorization, this occurs to APIs who do not verify whether clients should have access to the data they are requesting. KeyCloak combats broken object level authorization by having role-based access control, this assigns roles to users and grants permission to these users.

The second most popular OWASP risk is broken authentication, this risk results in attackers gaining access to compromised passwords, keys, or session tokens. KeyCloak prevents this using multi-factor authentication as well as including protocols such as OpenID Connect and SAML 2.0, which allow for securely authenticated users and services.

The third most popular OWASP risk is broken object property level authorization, this differs from the most popular risk because this OWASP goes deeper, specifically to the properties of an object. An attacker attempts to find breaches inside of the properties of an object, changing information about a user for example or try to find undocumented API endpoints that relate to an object’s properties. KeyCloak makes sure API endpoints are secured and can only be reached by authorized users.

**SWOT analysis**

**Strengths:**

KeyCloak provides features for access management, including Single Sign-On and Multi factor authentication. More however it can provide a customizable user interface, which could be applied to an online education platform.

**Weaknesses:**

KeyCloak’s deployment and setup process can be difficult, especially if you do not wish to use Docker. KeyCloak can be resource-intensive, requiring significant server resources for optimal performance. This might be challenging with limited IT infrastructure.

**Opportunities:**

Because of increasing awareness around data security and privacy, IAM solutions like KeyCloak are on the rise. This trend presents an opportunity for KeyCloak to expand its user base.

**Threats:**

The fast pace of technological development in the cybersecurity and IAM fields means that KeyCloak needs to continually evolve to stay relevant. Another huge thread would be vulnerabilities within KeyCloak. Any significant security breach could damage KeyCloak’s reputation and user trust.

|  |  |  |
| --- | --- | --- |
| KeyCloak | Positive | Negative |
| Intern | KeyCloak provides features for access management. | KeyCloak’s deployment and setup process can be difficult. |
| Extern | IAM solutions like KeyCloak are on the rise. | The fast development in IAM systems requires KeyCloak to stay updated |

# Resolution

**Conclusion**:  
As a result of this research report, the final conclusion is that KeyCloak would be the best IAM system for an online education platform. Because the needed customization is flexible and offers a great user experience. Aswell as the easy integration of Single sign on, which is needed for the multiple frontends that TeamVas uses. In an environment where student security and privacy are required, KeyCloak offers a safe environment for all students/teachers and prevents the application from getting exploited.

**Recommendation**:

Based on the findings of this research report, it is recommended that each online education platform adopts KeyCloak as its Identity and Access Management (IAM) solution for their application. KeyCloak's flexibility in customization aligns perfectly with the unique requirements of an educational environment, allowing for a tailored user experience that can reflect the brand and functional needs of the platform.

# References

Garrone, J. (2024, 1 17). *keycloakify-starter*. Retrieved from GitHub: https://github.com/keycloakify/keycloakify-starter

Gittlen, S. (2021, August). *What is identy and access management*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Kinzer, K. (2021, Septembre 14). *The intersection of IAM and MFA*. Retrieved from Jumpcloud: https://jumpcloud.com/blog/the-intersection-of-identity-and-access-management-iam-and-multi-factor-authentication-mfa

Köbler, N. (2023, 11). *KeyCloak Demo*. Retrieved from GitHub: https://github.com/dasniko/keycloak-reactjs-demo

Red Hat Software. (2023). *Securing applications and services using KeyCloak*. Retrieved from keycloak.org: https://www.keycloak.org/docs/latest/securing\_apps/index.html

Żyliński, B. (2021, Octobre 11). *What Keycloak Is and What It Does*. Retrieved from DZone: https://dzone.com/articles/what-is-keycloak-and-when-it-may-help-you

# Version history

|  |  |
| --- | --- |
| **When?** | **What?** |
| 30/11/2023 | Initial setup of Main/Sub questions, problem description |
| 5/12/2023 | Sub question 1 finished, research on OWASP |
| 13/12/2023 | Start on sub question 4, Keycloak and OWASP |
| 21/12/2023 | Research based on official KeyCloak documentation |
| 27/12/2023 | Sub question 2/3 finished |
| 02/01/2024 | Resolution + References |