**Keycloak** - это решение для единого входа (Single Sign-On) для веб-приложений и RESTful веб-сервисов. Оно предоставляет пользовательские интерфейсы для входа, регистрации, администрирования и управления учетными записями, а также может использоваться в качестве платформы интеграции для подключения к существующим серверам LDAP и Active Directory.

Keycloak предоставляет следующие функции:

* Единый вход (Single-Sign On) и выход (Single-Sign Out) для браузерных приложений.
* Поддержка OpenID Connect, OAuth 2.0 и SAML.
* Аутентификация с внешними поставщиками идентификации, такими как Facebook и Google.
* Адаптеры клиентов, которые делают очень простой интеграцию с Keycloak.

Keycloak также предоставляет средства для создания разрешений для защищенных ресурсов и областей, ассоциирования этих разрешений с политиками авторизации и принятия решений об авторизации в ваших приложениях и сервисах.

**Процесс идентификации, аутентификации и авторизации с помощью Keycloak** может выглядеть следующим образом:

1. Пользователь пытается получить доступ к защищенному ресурсу, например, к странице веб-приложения.

2. Веб-приложение перенаправляет пользователя на страницу входа Keycloak.

3. Пользователь вводит свои учетные данные (логин и пароль).

4. Keycloak проверяет учетные данные пользователя и, если они верны, создает токен доступа.

5. Токен доступа содержит информацию о пользователе, его ролях и правах доступа.

6. Веб-приложение использует токен доступа для проверки прав доступа пользователя к защищенным ресурсам.

7. Если пользователь имеет права доступа к ресурсу, то он получает доступ к нему.

**Назначение основных разделов Keycloack:**

1. Realms – сферы или области. Область управляет набором пользователей, учетных данных, ролей и групп. Пользователь принадлежит к области и входит в нее. Области изолированы друг от друга и могут управлять и аутентифицировать только тех пользователей, которых они контролируют.
2. Clients (клиенты) – это объекты, которые могут запрашивать Keycloak для аутентификации пользователя. Чаще всего клиентами являются приложения и службы, которые хотят использовать Keycloak для обеспечения собственной безопасности и предоставления решения для единого входа. Клиентами также могут быть организации, которые просто хотят запросить идентификационную информацию или токен доступа, чтобы они могли безопасно вызывать другие службы в сети, защищенные с помощью Keycloak.
3. Users (пользователи) – это организации, которые могут входить в вашу систему. У них могут быть атрибуты, связанные с ними самими, такие как электронная почта, имя пользователя, адрес, номер телефона и день рождения. Им может быть назначено членство в группе и им могут быть назначены определенные роли. Вы создаете пользователей в области, в которой вы собираетесь размещать приложения, необходимые этим пользователям.
4. Role (роли) – определяют тип или категорию пользователя. Admin, user, manager и employee – это все характерные роли, которые могут существовать в организации. Приложения часто назначают доступ и разрешения определенным ролям, а не отдельным пользователям, поскольку работа с пользователями может быть слишком мелкой и сложной в управлении.
5. Groups (группы) – управляют группами пользователей. Атрибуты могут быть определены для группы. Вы также можете сопоставить роли с группой. Пользователи, которые становятся членами группы, наследуют атрибуты и сопоставления ролей, определенные группой.
6. Authentication Flows (потоки аутентификации) – это рабочие потоки, которые пользователь должен выполнять при взаимодействии с определенными аспектами системы. Поток входа в систему может определять, какие типы учетных данных требуются. Процесс регистрации определяет, какую информацию профиля пользователь должен ввести и нужно ли использовать что-то вроде reCAPTCHA для фильтрации ботов. Процесс сброса учетных данных определяет, какие действия должен выполнить пользователь, прежде чем он сможет сбросить свой пароль.
7. User federation provider – Keycloak может хранить пользователей и управлять ими. Часто в компаниях уже есть службы LDAP или Active Directory, которые хранят информацию о пользователях и учетных данных. Вы можете использовать Keycloak для проверки учетных данных из этих внешних хранилищ и извлечения идентификационной информации.
8. Identity provider federation – Keycloak можно настроить для делегирования аутентификации одному или нескольким IDPL. Вход в социальную сеть через Facebook или Google+ является примером федерации поставщиков удостоверений. Вы также можете подключить Keycloak для делегирования аутентификации любому другому OpenID Connect или SAML 2.0 IDP.

**Пример**

Для примера рассмотрим, как Keycloak может использоваться для идентификации, аутентификации и авторизации пользователей на сайте Gmail.com.

1. Идентификация: пользователь вводит свой email на странице входа в Gmail.com.   
Gmail.com отправляет запрос на сервер Keycloak для проверки, существует ли пользователь с таким email в системе.

2. Аутентификация: если пользователь существует, Keycloak отправляет на почту пользователя ссылку для подтверждения входа. Пользователь переходит по ссылке и вводит свой пароль. Keycloak проверяет правильность пароля и, если он верен, выдает токен аутентификации.

3. Авторизация: Gmail.com отправляет запрос на сервер Keycloak с токеном аутентификации для проверки прав доступа пользователя к ресурсам сайта. Keycloak проверяет права доступа пользователя и, если они соответствуют требованиям, выдает токен авторизации.

4. Пользователь получает доступ к своей почте на сайте Gmail.com.