Назначение подсистемы управление пользователями

Требования:

- Возможность подключения к существующим системам (Active Directory)
- Ролевая модель
- Возможность ограничивать доступ к определенным объектам системы для определенных ролей.

Функции ядра по работе с пользователями

- Аутентификация
- Проверка прав
- Личный кабинет
- Коммуникация пользователей (чат)
- Подписка на события

Процесс работы сервиса:
Пользователи логинятся в систему с помощью средств сервиса (сервис может предоставлять свою страницу логина), проходят аутентификацию, авторизацию.
В результате клиент получает стандартизированный JWT токен, с помощью которого обращается к функционалу ядра.

Ядру предлагается оставить две функции:

- Проверка прав (на основе переданных в токене ролей)
- Личный кабинет (т.к. встроенный в сервис кабинет может не иметь необходимых возможностей)

Реализация - open source сервис Keycloak (https://www.keycloak.org).
Аутентификация, авторизация, управление пользователями - это довольно стандартный функционал.

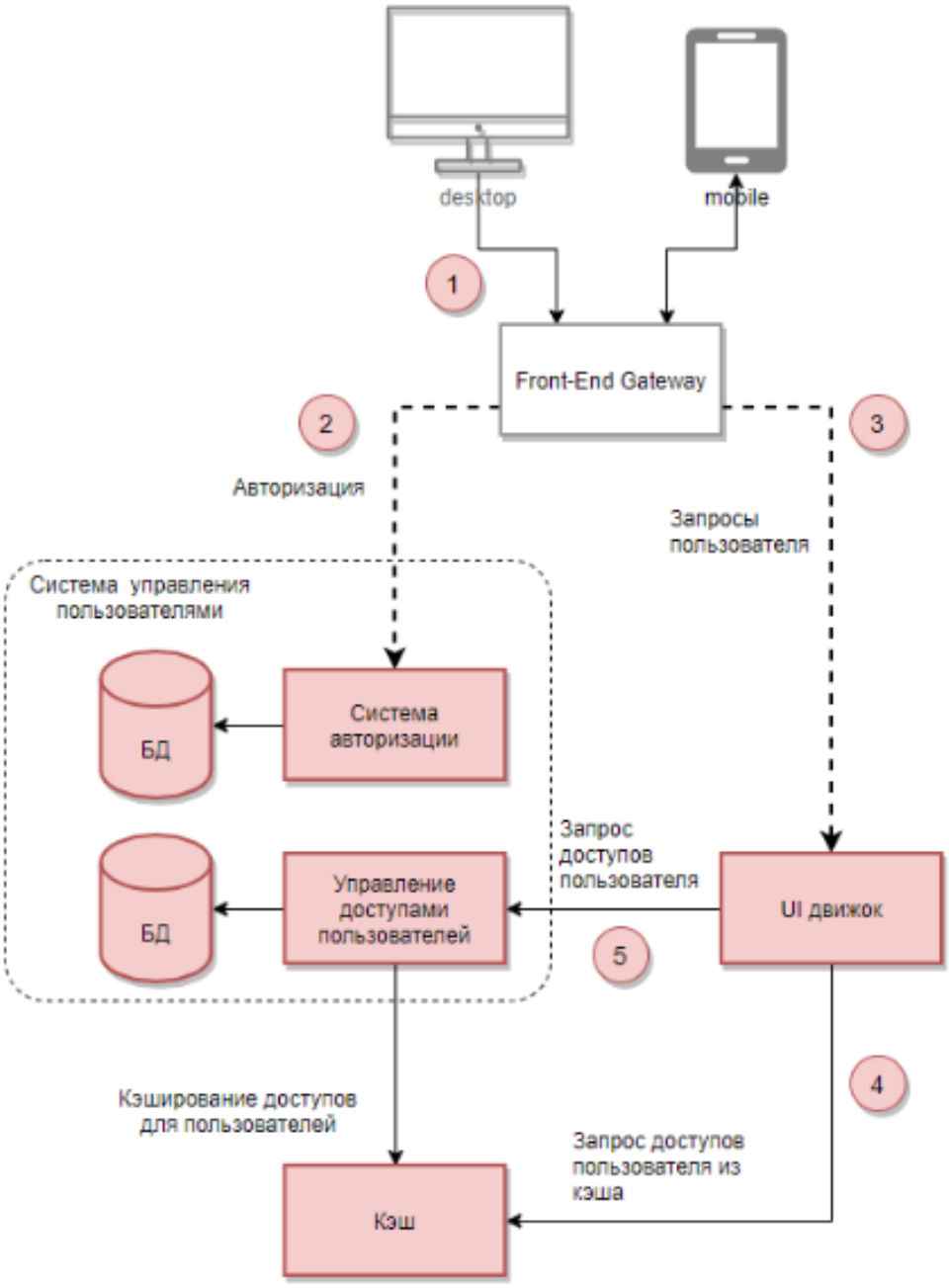
Keycloak известный поддерживаемый проект, имеет большую гибкость, поддерживает много стандартов, обладает следующими преимуществами:

- умеет работать с Active Directory, LDAP (умеет синхронизирует пользователей)
- поддерживает стандарты OAuth2.0, OpenID, SAML
- имеет встроенную систему управления пользователями (добавление, удаление, редактирование)
- имеет систему управления ролями
- имеет систему управления группами пользователей
- поддержка тем и кастомизации интерфейса
- поддержка двухфакторной аутентификации
- встроенный экран логина и функции смены пароля, восстановления пароля
- личный кабинет пользователя (ограничен по функционалу)

- поставляется с встроенной базой, однако может работать с базой ядра (Oracle, Ms SQL, My SQL, PostgreSQL)

Обработка запросов пользователя

1. Пользователь запрашивает страницу
2. Front End gateway проверяет наличие JWT токена и при его отсутствии перенаправляет на систему авторизации.
3. Получив токен, пользователь перенаправляется на UI движок для получения необходимого интерфейса.
4. UI движок пытается получить из кэша данные о разрешениях конкретного пользователя по его роли, полученной из JWT токена.
5. При отсутствии данных в кэше UI движок делает запрос в систему управления разрешениями ролей. И выдает результат пользователю.



[5.11.1. Видение]