PLATFORM V
SBER

PLATFORM V IAM SE

Управление аутентификацией и авторизацией пользователей бизнес-приложений. Набор инструментов для управления доступом к информационным ресурсам IAM (Identity & Access Management). Проверяет права доступа на вызовы API и совершение действий сервисом платформы.

Используется для реализации технологий аутентификации и авторизации в приложениях. Обеспечивает удобное и безопасное подключение защищаемых приложений к провайдеру в соответствии с отраслевыми стандартами — OpenID Connect, Oauth 2.0, SCIM 2.0.

Пример использования

Управление политиками и временем жизни пользовательских сессий в рамках технологии SSO

Состоит из трех взаимно интегрированных сервисов

Keycloak SE — провайдер идентификации, основанный на open source версии Keycloak

OCA — сервис авторизации для реализации централизованной точки принятия решений о возможности доступа на основе политик по ABAC-модели

IAM Proxy — реверсивный proxy-сервер, упрощающий аутентификацию и авторизацию

Импортозамещение

Разработан с использованием проверенных open source решений: Keycloak, OPA, Nginx, Spring, Quarqus, PostgreSQL, OpenResty, React. Включен в Реестр российского программного обеспечения (запись в реестре от 05.09.2022 №14757). Может использоваться как альтернатива продуктам западных поставщиков.

Преимущества

- Разделение инфраструктурных и прикладных механизмов
- Поддержка различных авторизационных движков, в том числе OPA
- Принятие авторизационных решений в runtime
- Возможность настройки гранулированной ABAC-/RBAC-модели авторизации
- Многоплоскостное представление структуры привилегий
- Поддержка индустриальных протоколов аутентификации и авторизации — OpenID Connect, OAUTH

Функциональность

Каждый компонент Platform V IAM SE может использоваться как в рамках единого сценария, так и в качестве самостоятельного инструмента

Функции Keycloak SE

- Управление Realm — сущностями, клиентами, пользователями, ролями и шаблонами клиентов/области (scope), согласиями (Required Actions)
- Аутентификация, настройка сценариев аутентификации и подключение аутентификаторов
- Авторизация и настройка политик авторизации и парольных политик
- Поддержка внешних хранилищ LDAP / AD Provider, Kerberos Provider, SSSD / Free IPA

Функции OCA — сервиса авторизации

- Механизмы Role-based access control (RBAC)
- Механизмы Attribute-based access control (ABAC), включая язык политик — XAML
- Функции Policy Decision Point (PDP), включая клиентскую библиотеку и sidecar
- Функции Policy Administration Point (PAP), включая Rest API и административный UI
- Функции Policy Enforcement Point (PEP), включая клиентскую библиотеку и sidecar

Функции IAM Proxy

Аутентификация пользователя при доступе к приложению, в том числе:

- Взаимодействие с внешним провайдером аутентификации по OpenID Connect
- Поддержка custom IdP
- Передача проверенной информации о пользователе внутренним приложениям в удобном виде: JWT, http headers, custom

Функции авторизации, включая:

- Авторизацию доступа к защищаемым приложениям по ролям
- Дополнительный слой авторизации на основе URL(RBAC) и атрибутов запросов
- Кэширование авторизационных политик и др.

Модель поставки

Индивидуально по модели on-premise

PLATFORM V

platformv.sbertech.ru platformv@sberbank.ru +7 495 547-99-80