

Сервис авторизации и проверки доступа

Общее описание

Индекс	2004-Shield.Int-GD
Секретность	Публичный - L0
Ревизия	1.0
Статус	Согласован
Подразделение	ДПРСУД
Компания	GS Labs

Содержание

1. Введение	3
1.1. Назначение	3
2. Термины и сокращения	4
3. Описание системы	5
3.1. Общее описание	5
3.2. Архитектура	5
3.2.1. Компоненты системы	5
3.2.2. Взаимодействие компонентов	7
4. Сценарии работы Shield	8
4.1.1. Сценарий создания аккаунта	8
4.1.2. Сценарий авторизации аккаунта	8
4.1.3. Сценарий проверки доступа к целевому сервису с проверкой авторизации	8

1. Введение

1.1. Назначение

Документ содержит общее описание **Сервиса авторизации и проверки доступа** (далее в документе используется условное наименование данного сервиса - **Shield**) и предназначен для широкого круга специалистов.

2. Термины и сокращения

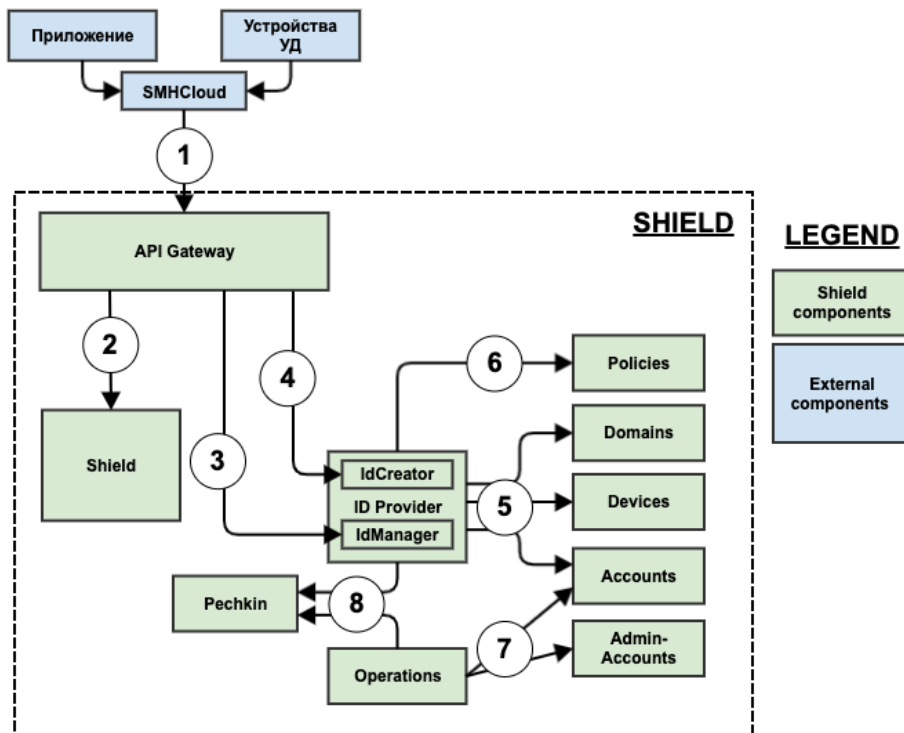
Термин, Сокращение	Определение, Расшифровка
Авторизация	Процесс проверки субъекта авторизации на доступ к определенным ресурсам или действиям.
Аутентификация	Процесс проверки подлинности данных субъекта авторизации.
БД	База данных.
Домен	Логическая группа, объединяющая контроллеры и аккаунты.
Контроллер	Программно-аппаратный комплекс, непосредственно управляющий устройствами и принимающий сигналы от датчиков умного дома.
Пользователь	Человек, использующий приложение или браузер для авторизации в Shield.
Сервис облачного управления DREHOME&TV	Продукт GS Labs, представляющий собой сервис для удаленного управления контроллерами умного дома.
Субъект авторизации	Сущность (человек или другой сервис), обращающаяся к Shield для регистрации или выдачи токена.
СМС	Сервис мобильных сообщений, SMS.
Токен	Выдаётся пользователю после успешной авторизации и является ключом для доступа к целевому сервису.
УД	Умный Дом.
Целевой сервис	Сервис, к которому пользователь запрашивает авторизацию у сервера Shield.
BSS	ИС Оператора - Информационные системы Оператора.
Device	Устройство, см. Контроллер.
DRM	Digital rights management - управление цифровыми ограничениями, а также технические средства защиты авторских прав.
Shield	Сервис авторизации и проверки доступа.
JWT	JSON Web Token.
SMHCloud	См. Сервис облачного управления DREHOME&TV

3. Описание системы

3.1. Общее описание

1. Shield обеспечивает:
 - работу с внутренним (интегрированным в Shield) провайдером, содержащим список аккаунтов, доменов, контроллеров и политик;
 - авторизацию пользователя во внутреннем провайдере с выдачей персонального токена доступа к необходимому ресурсу;
 - проверку токена у внутреннего провайдера.
2. Shield использует следующие виды авторизации:
 - Base - выдача токена или предоставление ресурса происходит на основании введенных пользователем данных:
 - логин и пароль;
 - логин и проверочный код;
 - логин и СМС код.
 - Beager - предоставление пользователю доступа к ресурсам с помощью уже выданного токена.
3. Для обеспечения безопасности Shield использует:
 - токены формата JWT с алгоритмом шифрования HMAC с использованием SHA-256 (HS256);
 - ограничение на количество попыток отправки одноразового пароля или кода регистрации по СМС.

3.2. Архитектура



3.2.1. Компоненты системы

Внутренние компоненты продукта Shield:

- API Gateway - сервис роутинга запросов, проксирует API от всех внешних подсистем нужному Provider.
- Компонент Shield - отвечает за прием запросов на авторизацию и выдачу ответов пользователям (предназначен для получения, хранения, валидации и отзыва токенов доступа - токена доступа к аккаунту и токена доступа к устройству). Имеет отдельную БД Redis - хранилище токенов и кэшируемой информации.
- ID Provider - осуществляет проверку данных для авторизации и формирует ответ. Данный сервис является обёрткой для работы с сервисами Accounts, Domains, Devices для пользователей Умного Дома (УД). Имеет отдельные БД: PostgreSQL - выполняет роль хранилища данных сервиса, Redis - хранилище токенов и кэшируемой информации.
Сервис логически можно разделить на два компонента:
 - IdCreator - создание аккаунтов и устройств УД.
 - IdManager - управление аккаунтами, доменами и устройствами УД (для выполнения операции требуется токен авторизации).
- Accounts, Devices, Domains:
 - Accounts - предназначен для управления учетными записями пользователей УД.
 - Devices - предназначен для управления устройствами пользователей УД.
 - Domains - предназначен для объединения нескольких аккаунтов в один домен и привязки устройств УД к домену.
 - Каждый из этих сервисов имеет отдельную БД в СУБД PostgreSQL.
- Policies - предназначен для управления правами доступа пользователей к ресурсам. Сервис имеет две функции: публикация прав доступа к ресурсу (выдача субъекту авторизации прав на управление ресурсами) и проверка прав доступа к ресурсу. Права доступа хранятся в key-value хранилище etcd.
- Operations - предназначен для управления аккаунтами пользователей. Разделяются два вида аккаунтов - customers и admins. Аккаунтами customers считаются аккаунты, заведенные в сервисе Accounts. Аккаунтами admins считаются аккаунты, заведенные в сервисе Admin-Accounts.
 - operations-ui - пользовательский интерфейс для управления customers и admins. Взаимодействие осуществляется посредством web-browser.
- Pechkin - микросервис уведомлений. Рассылает СМС и Email уведомления пользователям.

Внешние компоненты:

- SMHCloud - сервис, обеспечивающий возможность удаленного управления устройствами умного дома (УД).
- Устройства УД - исполняющие/контролирующие/управляющие устройства. Выполняют команды пользователя, SMHCloud или других устройств.
- Приложение - приложение УД для удаленного доступа к компонентам УД.

3.2.2. Взаимодействие компонентов

Взаимодействие компонентов на схеме обозначено цифрами, описание сведено в таблицу:

№	Клиент (инициатор)	Сервер (получатель)	Цель взаимодействия
1	SMHCloud	API Gateway	Авторизация пользователя, регистрация устройств, управление аккаунтами, доменами, устройствами.
2	API Gateway	Shield	Получение, обновление и проверка токенов доступа и обновления.
3	API Gateway	ID Provider /IdManager	Запрос на управление аккаунтами, доменами и устройствами (разрешен только при наличии токена доступа с правом на запрашиваемую операцию).
4	API Gateway	ID Provider /IdCreator	Запрос на создание аккаунтов и устройств УД.
5	ID Provider	Accounts /Devices /Domains	Создание и управление аккаунтами, контроллерами и доменами УД.
6	ID Provider	Policies	Проверка прав доступа субъектов авторизации.
7	Operations	Accounts /Admin- Accounts	Создание, редактирование, блокирование и удаление аккаунтов.
8	Operations/ID provider	Pechkin	Запрос отправки кода активации аккаунта и одноразового кода для входа в аккаунт.

4. Сценарии работы Shield

В данном разделе приведены примеры некоторых типовых пользовательских вариантов сценариев (основные потоки) с использованием продукта Shield. Описание всех возможных вариантов сценариев выходит за рамки данного документа.

4.1.1. Сценарий создания аккаунта

1. Пользователь инициирует в приложении регистрацию аккаунта.
2. Пользователь вводит номер телефона/email и запрашивает регистрацию аккаунта.
3. Запрос на создание аккаунта отправляется на API Gateway, который проксирует запрос в сервис ID Provider (в структуру IdCreator).
4. ID Provider обращается в сервис Accounts для создания учетной записи с заданными параметрами.
5. Сервис Accounts создает в своей БД аккаунт с переданными регистрационными данными.
6. ID Provider сообщает в сервис нотификации Pechkin о выполнении записи аккаунта и Pechkin высылает пользователю нотификацию с кодом подтверждения.
7. Пользователь вводит код для активации аккаунта - мобильное приложение отправляет компонент API Gateway логин аккаунта и код активации.
8. API Gateway обращается к сервису ID Provider для верификации данных в сервисе Account: существование логина и валидность кода активации для данного логина.
9. Аккаунт активирован и можно в него войти.

4.1.2. Сценарий авторизации аккаунта

1. Пользователь инициирует в приложении вход по паролю.
2. Пользователь вводит логин и пароль и запрашивает вход по логину и паролю.
3. На основе данных аутентификации формируется запрос в API Gateway на получение токена авторизации. API Gateway проксирует запрос на компонент Shield.
4. Компонент Shield обращается к ID Provider для сверки (верификации) аутентификационных данных.
5. ID Provider обращается к соответствующему сервису для сверки аутентификационных данных.
 - a. Для устройств - devices
 - b. Для учётных записей - accounts
6. ID Provider отвечает компоненту Shield информацией о пользователе.
7. Компонент Shield выпускает токен доступа для этого аккаунта, сохраняет его в кеш-память (в дальнейшем, при инициации пользователем каких-либо действий (например, выслать приглашение или добавить устройство), этот токен будет передаваться с запросом).
8. Аккаунт становится авторизованным.

4.1.3. Сценарий проверки доступа к целевому сервису с проверкой авторизации

1. Авторизовавшись, пользователь на мобильном приложении инициирует запрос на выполнение действия.
2. Мобильное приложение обращается к API Gateway с запросом на выполнение целевого действия в сервисе, передавая полученный ранее токен доступа.
3. API Gateway получает запрос и обращается к компоненту Shield для валидации токена.
4. Компонент Shield осуществляет проверку токена (существование токена, проверка его срока действия).
5. Компонент Shield отвечает информацией APIGateway о распознанном субъекте авторизации.
6. API Gateway добавляет в заголовок запроса информацию о субъекте авторизации. Формируется целевой запрос.

7. API Gateway отправляет запрос на ID-provider (ID Manager) для проверки в сервисе Policies права субъекта авторизации на выполнение того или иного действия.
8. ID Provider обращается в соответствующий сервис (Accounts, Domains или Devices) для выполнения действия.
9. По выполнению действия ID Provider передает в API Gateway информацию о результате выполнения действия, API Gateway передает данные в мобильное приложение.

© ООО "Цифра", 2019-2022

Документация "Сервис авторизации и проверки доступа. Общее описание" является объектом авторского права. Воспроизведение всего произведения или любой его части воспрещается без письменного разрешения правообладателя.