

# Сервис авторизации и проверки доступа

## Общее описание

|                    |                |
|--------------------|----------------|
| Индекс             | Shield.Int-GD  |
| Конфиденциальность | Публичный - L0 |
| Ревизия            | 1.0            |
| Статус             | Согласован     |

## Содержание

|   |    |
|---|----|
| 1. Введение .....   | 3  |
| 1.1. Назначение .....   | 3  |
| 2. Термины и сокращения .....   | 4  |
| 3. Описание системы .....   | 6  |
| 3.1. Общее описание .....   | 6  |
| 3.2. Архитектура .....  | 6  |
| 3.2.1. Компоненты системы .....   | 7  |
| 3.2.2. Взаимодействие компонентов .....   | 9  |
| 4. Сценарии работы Shield .....   | 11 |
| 4.1.1. Сценарий создания аккаунта .....   | 11 |
| 4.1.2. Сценарий авторизации аккаунта .....  | 11 |
| 4.1.3. Сценарий проверки доступа к целевому сервису с проверкой авторизации ..... | 11 |

# 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,<br>Сокращение | Определение, Расшифровка  |
|-----------------------|---|
| Термин,<br>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.   |
| Нотификация           | Оповещение одного сервиса другим о возникновении какого-либо события.   |
| Пользователь          | Человек, использующий приложение или браузер для авторизации в Shield.  |
| Субъект авторизации   | Сущность (человек или другой сервис), обращающаяся к Shield для регистрации или выдачи токена.  |
| СМС                   | Сервис мобильных сообщений, SMS.  |
| Токен                 | Выдается пользователю после успешной авторизации и являются 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.  |
| ConfigManager         | Условное наименование DRE Config Manager. Сервис хранения списка операторов, конфигурационных данных операторов, конфигураций STB и текстов пользовательских сообщений.   |
| Device                | Устройство, см. Контроллер.   |
| DRM                   | Сокращенное наименование продукта "Система управления цифровыми правами DREPLUS (DRM DREPLUS)", предназначенного для защиты контента, передаваемого по сети Internet, от нелегального копирования и распространения, а также для управления правами доступа пользователей к контенту. |
| Shield                | Сервис авторизации и проверки доступа.  |
| SMHCloud              | Условное наименование сервиса облачного управления DREHOME&TV.  |

|         |  |
|---------|--|
| Okydrom | Условное наименование сервиса DRE Guaranteed Delivery System (DRE Garant). |
| JWT     | JSON Web Token.  |

## 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.
- создание и удаление аккаунта в DRM;
- создание и удаление домена в DRM;
- создание контроллера в DRM;
- добавление и удаление контроллера из домена в DRM;
- получение из ConfigManager параметров конфигурации, а также набора текстов, символьных и числовых кодов для различных операторов, типов приложений, источников и языков;
- нотификацию BSS об операциях с аккаунтами, контроллерами и доменами.

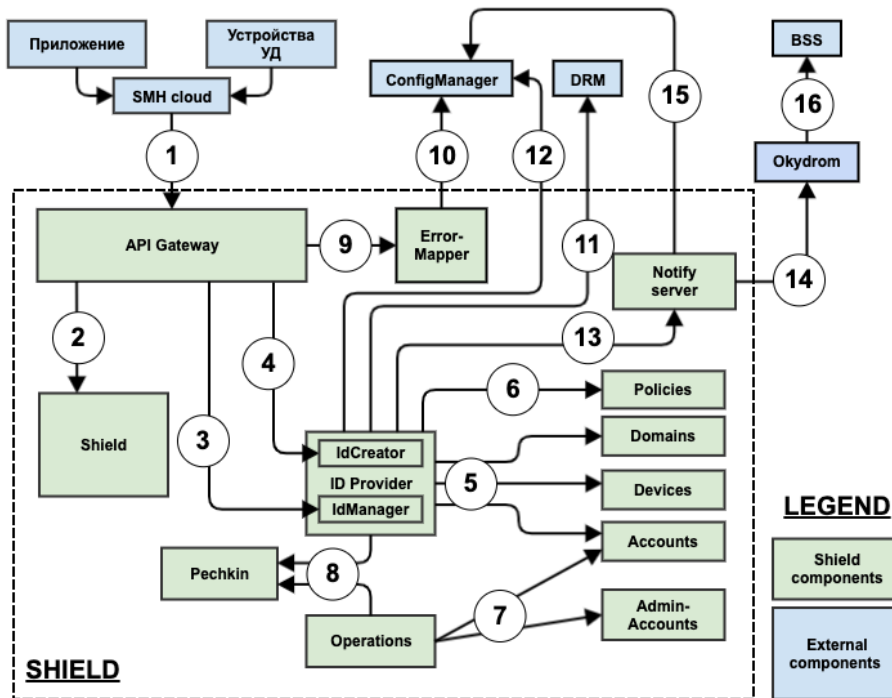
#### 2. Shield использует следующие виды авторизации:

- 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. Единая точка входа для маппинга ошибок.
- 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.
- Error-Mapper - обеспечивает настройку маппирования кодов и текстов ошибок, возвращаемых из API Gateway.
- Notify server - сервис, обеспечивающий направление в Okudrom запросов по созданию задач о нотификации BSS об операциях с аккаунтами, доменами и контроллерами в Shield.

#### 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.
- ConfigManager - хранение списка операторов, конфигурационных данных операторов, конфигураций STB и текстов пользовательских сообщений.
- DRM - сервис управления правами доступа пользователей к ресурсам.
- Okudrom - сервис, реализующий отложенную нотификацию стороннего REST сервера о наступлении заданного события.
- BSS - компонент информационных систем оператора, выполняет подключение необходимых услуг для абонентов, домохозяйств и оборудования.



### 3.2.2. Взаимодействие компонентов

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

| №  | Клиент<br>(инициатор)     | Сервер<br>(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<br>/IdManager        | Запрос на управление аккаунтами, доменами и устройствами (разрешен только при наличии токена доступа с правом на запрашиваемую операцию). |
| 4  | API Gateway               | ID Provider<br>/IdCreator        | Запрос на создание аккаунтов и устройств УД.  |
| 5  | ID Provider               | Accounts<br>/Devices<br>/Domains | Создание и управление аккаунтами, контроллерами и доменами УД.  |
| 6  | ID Provider               | Policies                         | Проверка прав доступа субъектов авторизации.  |
| 7  | Operations                | Accounts<br>/Admin-<br>Accounts  | Создание, просмотр, редактирование, бан и удаление аккаунтов.   |
| 8  | Operations/ID<br>provider | Pechkin                          | Запрос отправки кода активации аккаунта и одноразового кода для входа в аккаунт.  |
| 9  | API Gateway               | Error-Mapper                     | Маппинг ошибки, вернувшейся из внутренних сервисов без текста, получение текста пользовательского сообщения, возвращаемого Shield.        |
| 10 | Error-Mapper              | ConfigManager                    | Получение набора текстов, символьных и числовых кодов для различных операторов, типов приложений, источников и языков.                    |
| 11 | ID Provider               | DRM                              | Создание или удаление аккаунтов и доменов, создание контроллеров, добавление или удаление контроллеров из доменов.                        |
| 12 | ID Provider               | ConfigManager                    | Получение параметров конфигурации (URL DRM, наличие монетизации).   |
| 13 | ID Provider               | Notify server                    | Создание уведомлений для BSS об операциях с аккаунтами, доменами и контроллерами в Shield.  |
| 14 | Notify server             | Okydrom                          | Проверка параметров запроса, типа и тела уведомления, направление в Okydrom запросов по созданию задачи о уведомлении.                    |
| 15 | Notify server             | ConfigManager                    | Получение тела уведомления и настроек Okydrom.  |

|    |         |     |   |
|----|---------|-----|---|
| 16 | Okydrom | BSS | Нотификация BSS об операциях с аккаунтами, доменами и контроллерами в Shield. |
|----|---------|-----|---|

## 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", 2019-2024

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