Ключевые понятия

Оглавление

Реалм (realm)
  # Примеры
Клеймы (claims)
  # Клеймы (claims)
  # Примеры
  # Получение доступа к клеймам
  # Таблица клеймов
Уровни авторизации (auth_level)

Реалм (realm)

Механизм объединения пользователей в группы. Механизм реалмов позволяет в рамках одного решения UIDM организовать обслуживание разных категорий пользователей с разными сценариями, источниками данных и приложений. Пользователи в разных реалмах могут иметь одинаковые логин и идентификаторы, при этом они будут являться разными пользователями с точки зрения системы. В частности, для каждого реалма независимо настраиваются:

- источники учетных записей пользователей, в т.ч. со своей атрибутной моделью профиля пользователя
- поддерживаемые способы аутентификации
- сценарии аутентификации
- приложения, в которые выполняет аутентификацию пользователь
- политики авторизации

Примеры

Реалм Customers

- Включает пользователей-физических лиц.
- Данные пользователей хранятся в БД сервера UIDM
- Для пользователей поддерживается вход по логину-паролю, по OTP, через соц.сети
- Сценарии предполагают вход одним из перечисленных способов + опциональный ввод OTP в соответствии с настройками пользователя.
- Пользователи могут выполнять вход в приложения для физических лиц (личный кабинет физического лица, сервисы развлекательного контента)

Реалм B2B

- Включает пользователей, действующих от лица юридических лиц.
- Данные пользователей хранятся в БД сервера UIDM, а также в интегрированных сервисах, где хранятся унаследованные учетные записи.
- Для пользователей поддерживается вход по логину-паролю, по унаследованной учетной записи прикладной платформы, через систему ЕСИА
- Сценарии предполагают вход одним из перечисленных способов + обязательную регистрацию единой учетной записи, если выполнялся вход по унаследованной учетной записи продуктовой платформы.
- Пользователи могут выполнять вход в приложения для юридически лиц (личный кабинет юридического лица при наличии соответствующего уровня пользователя, корпоративные сервисы)

Реалм employee

- Включает пользователей - сотрудников организации.
- Данные пользователей хранятся в Active Directory организации.
- Для пользователей поддерживается вход по доменному логину-паролю, а также через Kerberos
- Сценарии предполагают вход только по доменной учетной записи.
- Пользователи могут выполнять вход только во внутренние приложения организации, размещенные в интрасети.

Клеймы (claims)

Клеймы (claims)

Клейм - это утверждение об аутентифицированном пользователе или его сессии или окружении, в котором он работает.

Клеймы записываются сервером UIDM в токен во время аутентификации и хранятся там до окончания времени жизни токена.

UIDM забирает клеймы из следующих провайдеров:

- сессия предлогина (вебфлоу)
- информация об устройстве пользователя (запоминается информация из первого шага сценария в случае многошаговых сценариев): User-Agent, геолокация, ...
- профиль пользователя, загруженный из RooX IdRepo
- профиль пользователя, загруженный из внешнего IdRepo, если применимо
- профиль пользователя, загруженный из соцсети или IDP, если применимо

Примеры

- идентификатор пользователя
- использованный логин
- время аутентификации
- IP адрес, с которого произошла аутентификация
- номер телефона для OTP
- ФИО

Получение доступа к клеймам

Серверное приложение бизнес-логики может получить клеймы из ответа API /tokeninfo. Некоторые клеймы являются встроенными и отдаются всегда, а некоторые отдаются только при наличии у приложения заданного scope. В таблице ниже указано, какие скоупы требуются для каких клеймов.

Мобильное приложение бизнес-логики может получить клеймы через Mobile SDK (которое внутри в свою очередь получает клеймы из JWT Identity Token).

Таблица клеймов

Таблица 1. Встроенные клеймы, возвращаются вне зависимости от запрошенного и разрешенного scope

Название	Описание	Тип данных	Пример
sub	Идентификатор принципала, уникальное	string с префиксом имени системы	sso____123123123
ext_sub	Идентификатор принципала без префикса (1)	string	123123123
jti	Идентификатор токена доступа	string, uuid	54732921-86cc-49e7-af67-19f61b453ad1
auth_time	Дата и время аутентификации	integer, unixtime	1594634014
authType	Использованный способ аутентификации (2)	string, enum	login_password
roles	Список ролей пользователя (3)	string array	['CUSTOMER','VIP']
auth_level	Уровень аутентификации, значение зависит от настроек и способа	string, но внутри integer	"5"

1. поскольку протокол требует уникальности sub (OIDC 5.7. Claim Stability and Uniqueness), а UIDM обеспечивает уникальность только с префиксом, так как в UIDM могут быть подключены множественные источники учетных записей, то вводится отдельный claim "ext_sub", который разрешается испоьзовать только при уверенности, что в конкретной инсталляции пересечений быть не может
2. login_password, apitokens. Список будет расширен
3. роли пользователя в организации при использовании мультиорганизационной модели сюда не входят

Таблица 2. Клеймы, доступ к которым определяется разрешениями сервиса

Название	Описание	Тип данных	Пример
externalIdpToken	Токен внешней системы, если использовалась внешняя система	string	"xjhl1h1hgdui.1j23loidsd"
preferred_username	Логин пользователя (не идентификатор!)	string	"username1"

name	ФИО пользователя (формат определяется внешней системой)	string	"Иванов Иван Иванович"

Уровни авторизации (auth_level)

Уровень авторизации - числовое значение, определяющее множество операций, доступных защищаемому сервису для выполнения от лица пользователя. Операция защищаемого сервиса может иметь минимальный требуемый уровень авторизации и выполняться только если текущий уровень авторизации пользователя больше или равен минимальной.