# Идентификация устройств

Оглавление



## # Общее описание

Идентификация устройств используется для повышения уровня безопасности входа в тот или иной сервис.

При правильной реализации аутентификация устройства может обеспечить надежную защиту от таких распространенных векторов атак, как

- социальная инженерия,
- использование скомпрометированных учетных данных,
- перехват сессии,
- использование скомпрометированного устройства.

В RooX UIDM обеспечены следующие возможности:

- сбор идентификатора устройства ("device id") при входе,
- передача device id в сервис, в который осуществляется вход,
- просмотр списка и параметров активных сессий,
- просмотр истории входов и завершение активных сессий,
- уведомления пользователей о необычных входах, например, с незнакомого ранее устройства.

## # Сценарии

### Сбор и передача в сервисы информации об устройстве device id в сервисы

В момент начала сессии сервер генерирует новый идентификатор устройства и проставляет его в cookie. В дальнейшем, сервер будет анализировать значение данной cookie, а при её отсутствии - генерировать новый идентификатор.

Чтобы исключить возможность подделки deviceId, клиентское приложение должно выполнять подпись атрибута `nonce`, полученного от сервера в ходе выполнения сценария, своим закрытым ключом. Клиент должен сгенерировать пару ключей, например, с помощью Web Cryptography API в браузере. Публичный ключ далее будет

передан UIDM. Клиент сохраняет оба ключа локально, доступным для него способом, например в indexedDb в случае браузера.

После успешной аутентификации deviceId передаётся в ответ на запрос токена доступа (/access token), в клеймах токена доступа.

По переданному значению deviceId интегрированные с UIDM приложениям могут получит информацию о параметрах устройства с использованием API «Получение параметров устройства».

## Сценарий работы клиента UIDM (браузера, мобильного приложения)

Для всех сценариев UIDM, где в результате будет выдан токен доступа (access token), в атрибутах которого необходим идентификатор устройства (deviceId) клиент UIDM должен действовать согласно описаниям в API аутентификации и Интеграция с RooX UIDM по OAuth2.

### Порядок работы клиента в сценариях аутентификации

1. На старте сценария в ответ на первый запрос (POST или GET) сервер UIDM вместе с execution вернет поле `_device_nonce`, которое содержит случайный набор символов.
2. Клиент подписывает полученное значение nonce с помощью приватного ключа и в следующем запросе вместе с данными формы аутентификации отправляет следующие параметры:

| Параметр | Описание |
|---|---|
| `_device_public_key` | Публичный ключ |
| `_device_signature` | подписанный `nonce` |
| `_device_id` и (или) cookie с именем `RX_DEVICE_ID` | идентификатор устройства. Передается, если пользователь ранее выполнял вход с этого устройства. Если в запросе присутствуют и параметр `_device_id`, и cookie `RX_DEVICE_ID`, то приоритет имеет параметр `_device_id` |

3. Если запрос не содержит cookie с именем `RX_DEVICE_ID` либо параметр запроса `_device_id`, то сервер создает и сохраняет в базу данных новый объект `Device`, содержащий новый `deviceId` и полученный от клиента публичный ключ.
4. Если в запросе есть cookie с именем `RX_DEVICE_ID` либо параметр запроса `_device_id`, то сервер находит соответствующую запись устройства в базе и использует публичный ключ из этой записи, а присланный в запросе публичный ключ игнорируется.
5. Если сервер не сможет проверить подпись с помощью публичного ключа, связанного с этим `deviceId`, сервер вернет в сценарии ошибку HTTP status 400.
6. По результатам аутентификации сервер добавит в токен доступа claim с именем `deviceId`, значение которого будет содержать сохраненный идентификатор устройства. Также будет добавлено дополнительно поле `device_id` в ответ сервера после успешной аутентификации вместе с полями access_token, refresh_token и т.д.

# # Спецификация API

## API «Получение параметров устройства»

ВАЖНО

Для вызова API поддерживается ТОЛЬКО способ авторизации по системному токену!

Запрос

```
GET /sso/api/deviceList?deviceId={deviceId}&size={size}&page={page}
```

Таблица 1. Описание параметров запроса

| Параметр | Описание | Комментарий |
|---|---|---|
| `{deviceId}` | идентификатор устройства | |
| `{size}` | размер "страницы" ответа | Сервер разбивает ответ на страницы по `{size}` записей в каждой и возвращает страницу, указанную под номером `{page}` |
| `{page}` | номер запрошенной "страницы" ответа | Нумерация страниц с 0. |

### Успешный ответ

Успешный ответ будет содержать JSON со следующим набором атрибутов.

| Параметр | Описание |
|---|---|
| id | Уникальный идентификатор |
| deviceId | Уникальный идентификатор устройства |
| userAgentDeviceType | Тип устройства: PC, tablet |
| userAgentDeviceBrand | Производитель устройства |
| userAgentDeviceModel | Модель устройства |
| userAgentOSFamily | Семейство ОС |
| userAgentOSNameVersion | Имя с версией ОС |
| userAgentBrowserType | Тип браузера: mobile app, desktop browser, mobile browser |
| userAgentBrowserFamily | Семейство браузеров |
| userAgentBrowserNameVersion | Имя браузера с версией |
| userAgent | Имя и версия браузера в привязке к пользователю на |

| | |
|---|---|
| | момент его последнего входа |
| lastAuthenticationTs | Дата и время последней аутентификации |
| principalId | Ссылка на Principal - владельца устройства |
| geoIPCountry | Страна, определенная по технологии GeoIP |
| geoIPRegionId | Идентификатор региона, определенного по технологии GeoIP |
| geoIPRegionNameNat | Имя региона, определенного по технологии GeoIP |
| geoIPCityId | Идентификатор города, определенного по технологии GeoIP |
| geoIPCityNameNat | Имя города, определенного по технологии GeoIP |
| last | указывает, что текущая страница в ответе является последней |
| totalPages | количество страниц доступных для просмотра |
| totalElements | общее количество сессий доступных для просмотра |
| first | указывает, что текущая страница в ответе первая |
| size | размер страницы |
| number | номер текущей страницы, начинается с 0 |

## API запроса всех устройств пользователя

ВАЖНО

Для вызова API поддерживается авторизация по системному либо клиентскому токену

Запрос

```
GET /sso/api/principalDevice?principalId={principalId}&size={size}&page={page}
```

Таблица 2. Описание параметров запроса

| Параметр | Описание | Комментарий |
| --- | --- | --- |
| `{principalId}` | идентификатор учетной записи пользователя | При авторизации запроса с использованием пользовательского токена можно использовать значение `@me` для определения пользователя по данным токена доступа. |
| `{size}` | размер "страницы" ответа | Сервер разбивает ответ на страницы по `{size}` записей в каждой и возвращает страницу, указанную под номером `{page}` |
| `{page}` | номер запрошенной "страницы" ответа | Нумерация страниц с 0. |

Успешный ответ

Успешный ответ будет содержать JSON со следующим набором атрибутов.

| Параметр | Описание |
| --- | --- |
| id | Уникальный идентификатор данной записи |
| deviceId | Уникальный идентификатор устройства |
| userAgentDeviceType | Тип устройства: PC, tablet |
| userAgentDeviceBrand | Производитель устройства |
| userAgentDeviceModel | Модель устройства |
| userAgentOSFamily | Семейство ОС |
| userAgentOSNameVersion | Имя с версией ОС |
| userAgentBrowserType | Тип браузера: mobile app, desktop browser, mobile browser |
| userAgentBrowserFamily | Семейство браузеров |
| userAgentBrowserNameVersion | Имя браузера с версией |
| userAgent | Имя и версия браузера в привязке к пользователю на момент его последнего входа |
| lastAuthenticationTs | Дата и время последней аутентификации |
| principalId | Ссылка на Principal - владельца устройства |

| | |
|---|---|
| principalId | Ссылка на Principal - владельца устройства |
| geoIPCountry | Страна, определенная по технологии GeoIP |
| geoIPRegionId | Идентификатор региона, определенного по технологии GeoIP |
| geoIPRegionNameNat | Имя региона, определенного по технологии GeoIP |
| geoIPCityId | Идентификатор города, определенного по технологии GeoIP |
| geoIPCityNameNat | Имя города, определенного по технологии GeoIP |
| last | указывает, что текущая страница в ответе является последней |
| totalPages | количество страниц доступных для ocbпросмотра |
| totalElements | общее количество сессий доступных для просмотра |
| first | указывает, что текущая страница в ответе первая |
| size | размер страницы |
| number | номер текущей страницы, начинается с 0 |

## # Настройка функциональности

```
# описание: Название cookie, в которой будет сохраняться идентификатор устройства
# тип данных: строка
# единицы измерения: нет
# ограничения: валидное имя http cookie
com.rooxteam.sso.device_id.cookie.name=RX_DEVICE_ID

# описание: Время жизни куки с deviceId
# тип данных: целое число
# единицы измерения: секунды
# значение по умолчанию: 30 * 86400 секунд (30 суток)
com.rooxteam.sso.device_id.cookie.expiration_time_seconds=2592000.

# описание: Флаг для плавного запуска функциональности. Определяет реакцию UIDM на ошибки проверки подписи.
#           При значении `false` UIDM выполняет проверку подписи клиента и завершает сценарий ошибкой.
#           При значении `true` UIDM игнорирует ряд ошибок проверки подписи.
# тип данных: булевское значение
# значение по умолчанию: false
com.rooxteam.sso.legacy_device.enabled=false
```

Для уведомления пользователя о входе с нового устройства необходимо выполнить настройки подсистемы уведомления пользователей для категории `auth.on.new.device`