Жизненные циклы токенов

Оглавление

Жизненный цикл токена
Виды токенов
  # Токен доступа (access token)
  # Токен обновления доступа (refresh token)
  # Токен автоматического входа
  # Токен одноразового доступа (per operation access token)
  # Токен доступа к API (API token)
  # Системный токен доступа
  # Мультиплатформенный токен
  # SSO-токен
Обмен токенов

Термины

Токен

> Жетон (маркер аутентификации), используемый для авторизации действий клиента при запросах к RooX UIDM. Если токен представлен в формате JWT, внутри него содержится информация о лице, запрашивающем авторизацию той или иной операции. Токены могут представлять из себя и текстовую строку-идентификатор (GUID); в этом случае сведения, связанные с токеном, хранятся в RooX UIDM.

Токен доступа (access token)

> Токен, который может использоваться сервисами, интегрированными с RooX UIDM, для авторизации действий, совершаемых от имени пользователя.

Токен обновления доступа (refresh token)

> Токен, который используется для получения нового токена доступа.

Токен автоматического входа

> Токен, который сам по себе не может использоваться для авторизации действий от имени пользователя, но который может быть использован для создания новой аутентификационной сессии без повторного ввода учетных данных пользователя.

Токен одноразового доступа (per operation access token)

> Одноразовый токен доступа, позволяющий выполнить одну заданную операцию с его использованием, которую как правило невозможно выполнить с обычным токеном доступа.

Токен доступа к API (api token)

> Токен доступа, позволяющий выполнять запросы к RooX UIDM API.

Системный токен доступа

> Токен доступа, выдаваемый приложению и позволяющий такому приложению действовать от собственного имени, а не от имени конечного пользователя.

Мультиплатформенный токен

> Токен доступа, заменяющий ввод логина, пароля или одноразового пароля в сценарии аутентификации. Такой токен позволяет выполнять бесшовный переход (без повторной аутентификации) из одного сервиса в другой, или из приложения для мобильного устройства — в Web-приложение, если все сервисы и приложения используют RooX UIDM.

Токены выпускаются (создаются) сервером, передаются клиентам в ответ на запросы авторизации, и содержат необходимую и актуальную информацию для последующей авторизации действий пользователя при помощи такого токена.

Передача (предъявление) токена клиентом в составе запроса к серверу означает, что клиент желает подтвердить своё право на выполнение запрашиваемой операции или обращение к защищаемому ресурсу.

Формат токена

В RooX UIDM используются токены, представленные в двух форматах: GUID (он же opaque) и JWT.

GUID

> Токен представляет из себя уникальный идентификатор в формате GUID. Вся связанная с токеном информация хранится в RooX UIDM.

JSON Web Token (JWT, RFC 7519)

> JWT — формат контейнера для передачи данных. RooX UIDM поддерживает токены формата JWT в двух вариантах: JWS (RFC 7515) и JWE (RFC 7516).
>
> Токен формата JWT (далее — токен) представляет из себя последовательность из трёх (JWS) или пяти (JWE) текстовых строк в формате JSON, каждая из которых закодирована алгоритмом Base64URL, и которые разделены точками.
>
> Вариант токена (JWS или JWE) определяется содержимым заголовка токена (Javascript Object Signing and Encryption, JOSE).
>
> ##### JSON Web Signature (JWS)
>
> > JWS — это токен формата JWT, в котором тело токена не зашифровано, но токен подписан цифровой подписью.
> >
> > Если заголовок токена соответствует формату JWS, то токен состоит из трёх секций:
> >
> > 1. **заголовка** (JOSE Header), в котором содержатся метаданные токена, и указание на криптографические алгоритмы, использованные при его подписании;
> > 2. **тела**, содержащего в себе JSON с набором клеймов — утверждений, которые могут включать в себя информацию о личности пользователя, разрешенных доступах и т. д.;
> > 3. **подписи** (сигнатуры), которая подтверждает, что токен не был изменен (не подделан) и ему можно доверять. При использовании токена перед его использованием или сохранением подпись проверяется **в обязательном порядке.**
> >
> >   Для создания подписи токена берутся закодированные алгоритмом Base64URL заголовок и тело токена, а также «секрет», и подписываются с использованием одного из алгоритмов (RFC 7518), указанных в заголовке токена.
>
> ##### JSON Web Encryption (JWE)

> JWE — это токен формата JWT, в котором тело токена зашифровано.
>
> Если заголовок токена соответствует формату JWE, то токен состоит из пяти секций:
>
> 1. **заголовка**;
> 2. **ключа шифрования**;
> 3. **вектора инициализации**;
> 4. **зашифрованного текста (тела токена)**, который вычисляется с использованием ключа шифрования, вектора инициализации и алгоритма шифрования, определенного в заголовке токена;
> 5. **данных**, которые подтверждают целостность зашифрованных данных.

Содержимое токена

В тело токена могут включаться произвольные данные, необходимые серверу для авторизации тех или иных операций. Такие данные (поля JSON) называются клеймами (claim).

Шифрование токена

Если в соответствии с требованиями содержимое токена должно быть закрыт от третьих лиц, тело JWE-токена шифруется на стороне сервера, и не может быть расшифровано на стороне клиента или третьего лица, не обладающих ключом (секретом). Дополнительные сведения (клеймы) могут быть включены в JWS- или JWE-токен только самим сервером, который при необходимости включения в клеймы токена дополнительных сведений создаёт новый токен с дополнительными данными, подписывает или шифрует его и передаёт запрашивающей стороне.

Жизненный цикл токена

Жизненным циклом токена называется период действительности токена и его пригодности для авторизации действий пользователя.

Жизненный цикл токена начинается от момента его выпуска (создания его сервером и передачи запрашивающей стороне) и заканчивается в момент его аннулирования (истечения срока его действия или отзыва).

Виды токенов

Токен доступа (access token)

Группа

- токены доступа.

Выпускается

- при открытии аутентификационной сессии;
- после использования токена обновления.

Аннулируется

- по истечении срока действия этого токена;
- по истечении срока действия аутентификационной сессии;
- при смене логина или пароля пользователя (аннулируются все токены доступа, кроме того, с использованием которого вызвана операция смены пароля);
- при отзыве токена с использованием API;
- при локальном выходе пользователя (logout);

- при блокировке или удалении учётной записи пользователя.

Таблица 1. Системные события и действительность токена доступа

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск
Выход пользователя (logout)	Аннулирование
Удаление или блокировка учётной записи пользователя	Аннулирование
Смена логина или пароля пользователя	Аннулирование[1]
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	Аннулирование
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	Выпуск
Совершение операции с использованием токена	—
Вызов специального API для получения экземпляра токена	—

Срок действия токена доступа рекомендуется настроить в диапазоне от нескольких минут до часов.

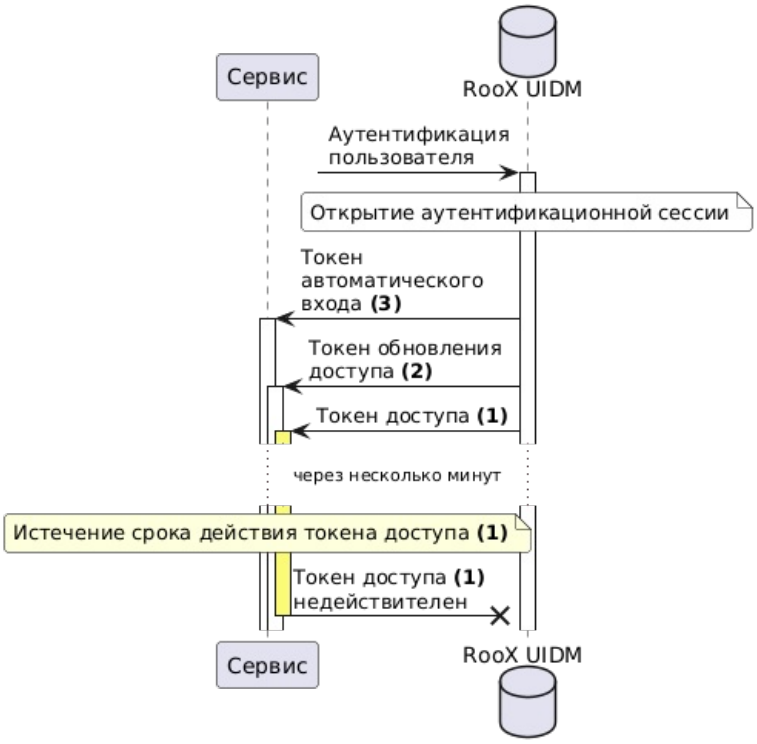

Рисунок 1. Диаграмма действительности токена доступа

Токен обновления доступа (refresh token)

Выпускается

- одновременно с выпуском токена доступа.

Аннулируется

- по истечении срока действия этого токена;
- по истечении срока действия аутентификационной сессии;
- при смене логина или пароля пользователя (аннулируются все токены обновления, кроме того, который выдавался вместе с текущим токеном доступа);
- при отзыве токена с использованием API
- при локальном выходе пользователя (logout);
- при блокировке или удалении учётной записи пользователя.

Таблица 2. Системные события и действительность токена обновления доступа

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск
Выход пользователя (logout)	Аннулирование
Удаление или блокировка учётной записи пользователя	Аннулирование
Смена логина или пароля пользователя	Аннулирование[2]
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	Аннулирование
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	Выпуск
Совершение операции с использованием токена	—
Вызов специального API для получения экземпляра токена	—

Срок действия токена обновления доступа рекомендуется настроить заметно бóльшим, чем время жизни токена доступа. От разницы в настройке времени жизни токена обновления и токена доступа зависит время, в течение которого сервис сможет обновить доступ без выполнения пользователем повторной аутентификации.

Запрос на обновление токена доступа с помощью токена обновления доступа выполняется без дополнительной аутентификации пользователя.

Рисунок 2. Диаграмма действительности токена обновления доступа

Токен автоматического входа

Группа

- токены восстановления сессии.

Выпускается

- при открытии аутентификационной сессии.

Аннулируется

- при отзыве токена с использованием API;
- по истечении срока действия этого токена.

Таблица 3. Системные события и действительность токена автоматического входа

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск
Выход пользователя (logout)	—
Удаление или блокировка учётной записи пользователя	[3]
Смена логина или пароля пользователя	—
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	—
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	Выпуск
Совершение операции с использованием токена	—
Вызов специального API для получения экземпляра токена	—

Токен автоматического входа не сохраняется на сервере RooX UIDM.

Срок действия токена автоматического входа настраивается и может составлять до нескольких месяцев.

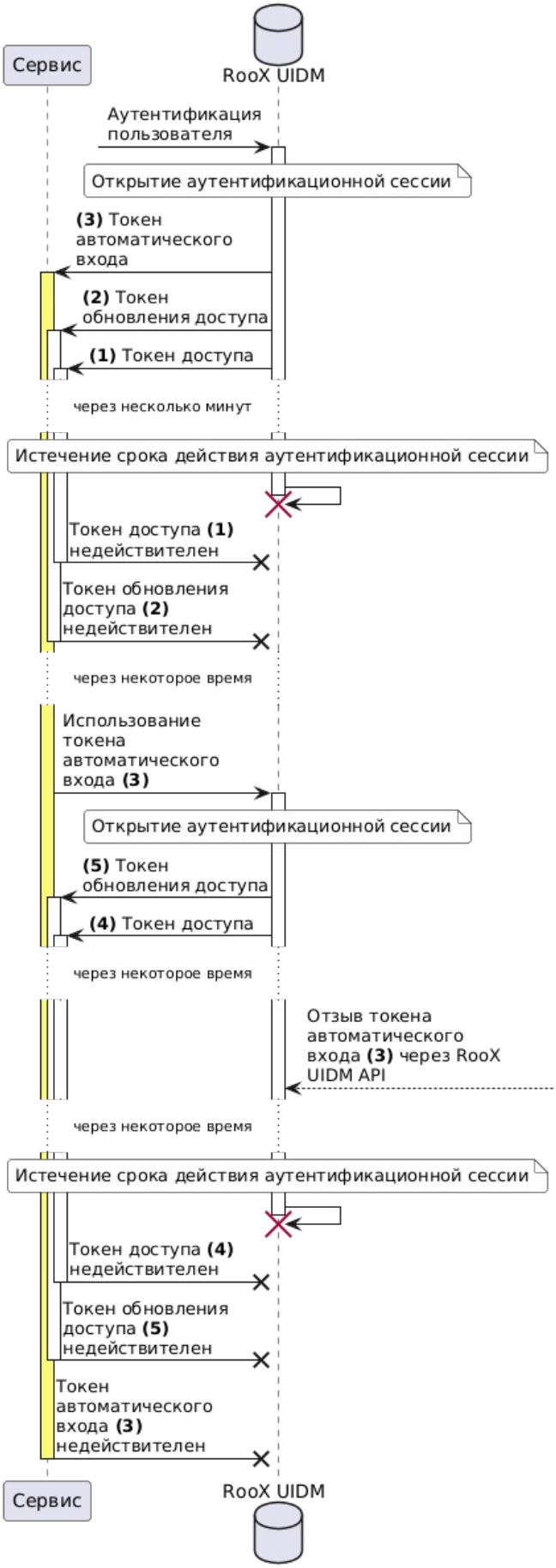

Рисунок 3. Диаграмма действительности токена автоматического входа

Токен одноразового доступа (per operation access token)

Группа

- токены доступа.

Выпускается

- после прохождения пользователем аутентификации способом, установленном для этой операции или для операции с отдельными параметрами.

Аннулируется

- немедленно после совершения операции;
- по истечении срока действия этого токена;
- по истечении срока действия аутентификационной сессии;
- при отзыве токена с использованием API;
- при локальном выходе пользователя (logout);
- при блокировке или удалении учётной записи пользователя.

Таблица 4. Системные события и действительность токена одноразового доступа

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск[4]
Выход пользователя (logout)	Аннулирование
Удаление или блокировка учётной записи пользователя	Аннулирование
Смена логина или пароля пользователя	Аннулирование
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	Аннулирование
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	—
Совершение операции с использованием токена	Аннулирование
Вызов специального API для получения экземпляра токена	—

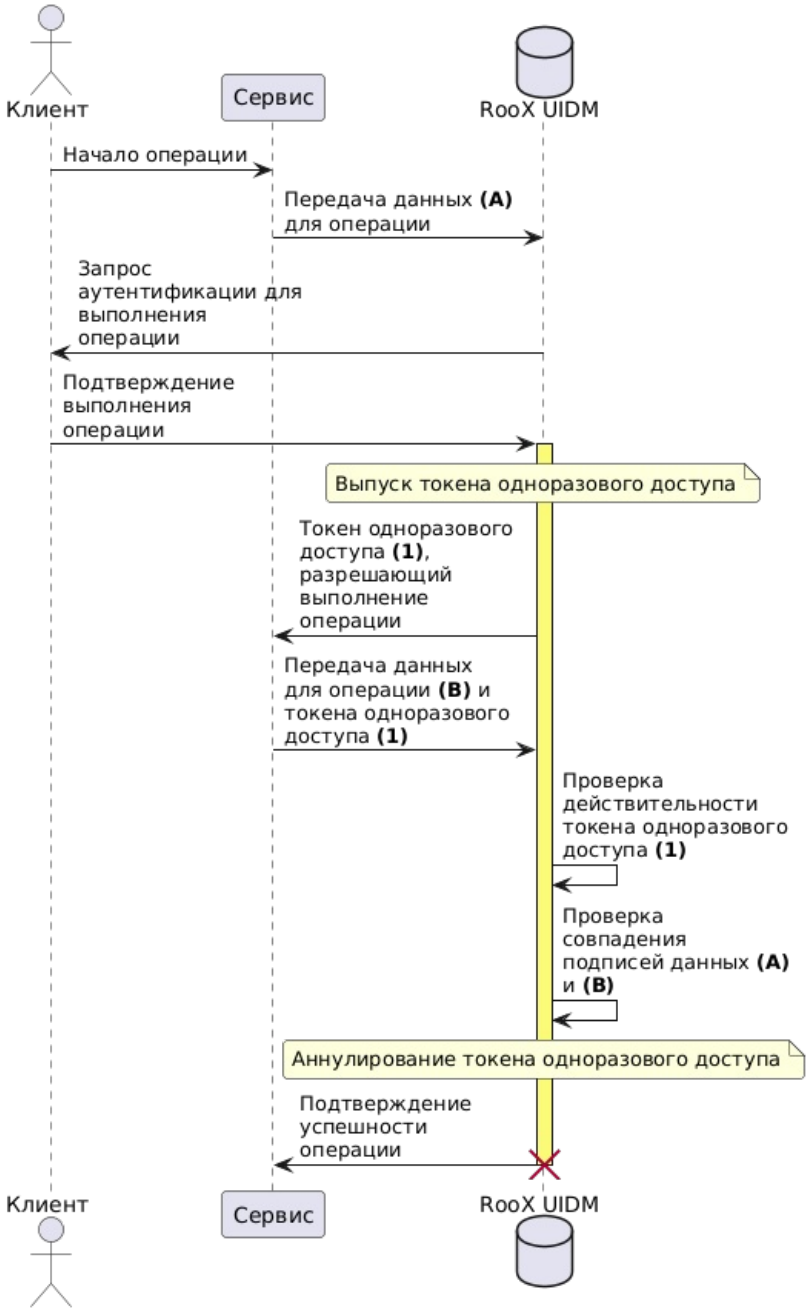

Рисунок 4. Диаграмма действительности токена одноразового доступа

Токен доступа к API (API token)

Группа

- токены доступа.

Выпускается

- при вызове специального RooX UIDM API.

Аннулируется

- при отзыве токена с использованием API;
- по истечении срока действия этого токена.

Таблица 5. Системные события и действительность токена доступ к API

Событие	Статус токена
Открытие аутентификационной сессии	—

Выход пользователя (logout)	—
Удаление или блокировка учётной записи пользователя	—[5]
Смена логина или пароля пользователя	—
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	—
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	—
Совершение операции с использованием токена	—
Вызов специального API для получения экземпляра токена	Выпуск

Системный токен доступа

Группа

- токены доступа.

Выпускается

- по запросу сервиса к RooX UIDM API.

Аннулируется

- по истечении срока действия этого токена;
- при отзыве токена с использованием API.

Таблица 6. Системные события и действительность системного токена

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск
Выход пользователя (logout)	Аннулирование
Удаление или блокировка учётной записи пользователя	Аннулирование
Смена логина или пароля пользователя	—
Истечение срока действия токена	Аннулирование

Истечение срока действия сессии	Аннулирование
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	Выпуск
Совершение операции с использованием токена	—
Вызов специального API для получения экземпляра токена	—

Мультиплатформенный токен

Группа

- сессионные токены.

Выпускается

- при открытии аутентификационной сессии (m2m, AJAX).

Аннулируется

- по истечении срока действия этого токена (срок действия MPT-токена равен сроку действия токена доступа);
- при локальном выходе пользователя (logout);
- при смене логина или пароля пользователя;
- при блокировке или удалении учётной записи пользователя.

Продлевается

- при обновлении токена доступа.

Таблица 7. Системные события и действительность MPT-токена

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск
Выход пользователя (logout)	Аннулирование
Удаление или блокировка учётной записи пользователя	Аннулирование
Смена логина или пароля пользователя	Аннулирование
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	Аннулирование
Отзыв токена с использованием API	Аннулирование

Использование токена обновления —

Совершение операции с использованием токена —

Вызов специального API для получения экземпляра токена —

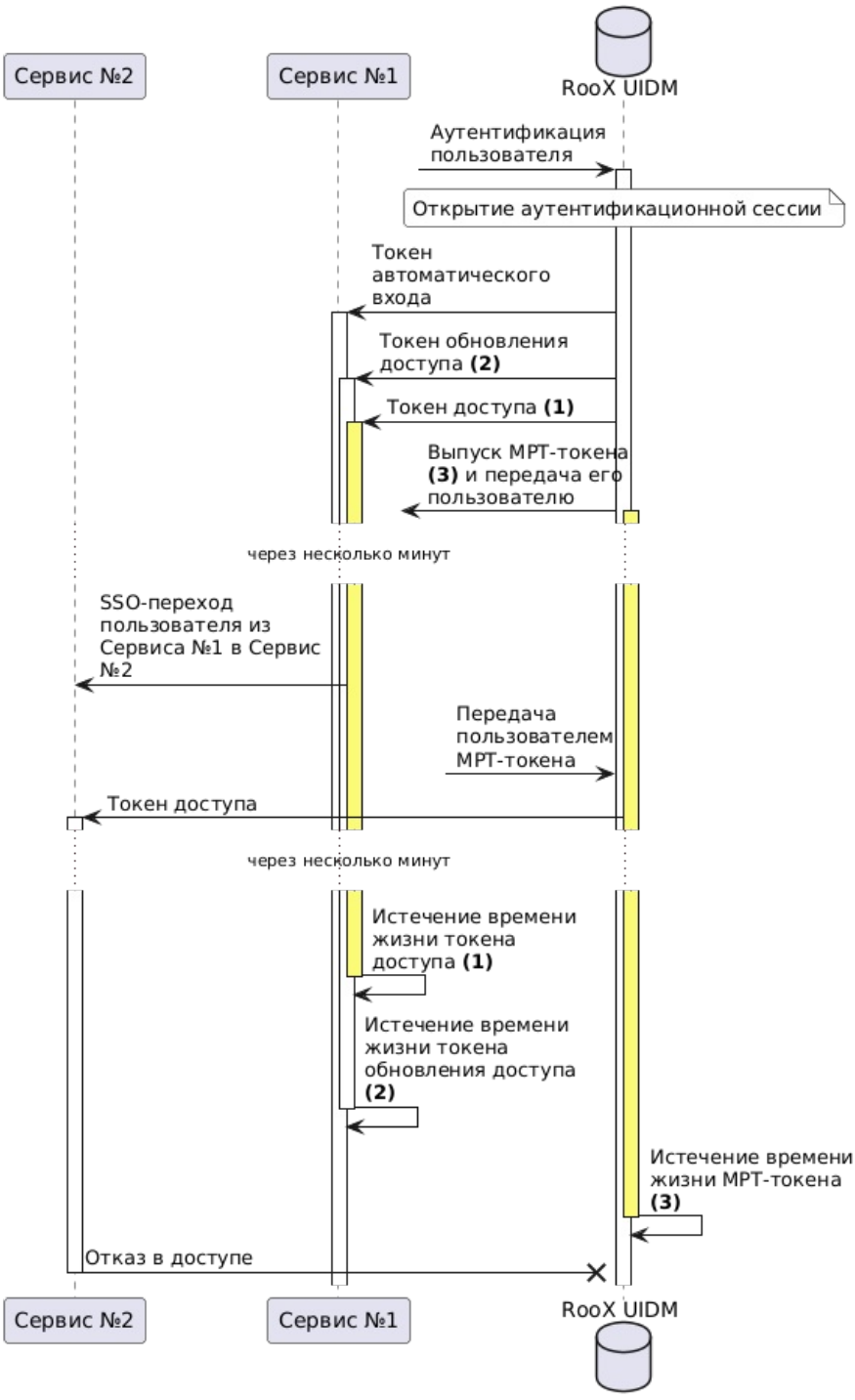

Рисунок 5. Диаграмма действительности MPT-токена

SSO-токен

ПРЕДУПРЕЖДАЕМ

SSO-token является технически устаревшим и будет удалён в будущих версиях RooX UIDM.

Группа

- сессионные токены.

Выпускается

- при открытии аутентификационной сессии (только по login-протоколу).

Аннулируется

- при локальном выходе пользователя (logout);
- при смене логина или пароля пользователя;
- при блокировке или удалении учётной записи пользователя.

Продлевается

- при использовании (выполнении SSO-перехода).

Таблица 8. Системные события и действительность SSO-токена

Событие	Статус токена
Открытие аутентификационной сессии	Выпуск
Выход пользователя (logout)	Аннулирование
Удаление или блокировка учётной записи пользователя	Аннулирование
Смена логина или пароля пользователя	Аннулирование
Истечение срока действия токена	Аннулирование
Истечение срока действия сессии	Аннулирование
Отзыв токена с использованием API	Аннулирование
Использование токена обновления	—
Совершение операции с использованием токена	—
Вызов специального API для получения экземпляра токена	—

Обмен токенов

Механизм обмена токенов (token exchange) позволяет приложению обменять токен доступа с одним набором атрибутов на другой токен доступа с другим набором атрибутов без повторной аутентификации пользователя.

Такой механизм может быть использован в том числе:

- для вызова одним сервисом, использующим RooX UIDM, API другого сервиса, также использующего RooX UIDM;
- для разделения объема полномочий приложения на несколько отдельных токенов доступа и передачи их другим приложениям.

ВАЖНО

Срок действия токена, полученного в результате операции по обмену токена, определяется настройками RooX UIDM и не зависит от срока действия исходного токена.

1. Аннулируются все токены доступа, кроме того, с использованием которого вызвана операция смены пароля.
2. Аннулируются все токены доступа, кроме того, с использованием которого вызвана операция смены пароля.
3. Токен не может быть использован, пока пользователь не будет разблокирован.
4. После прохождения пользователем аутентификации способом, установленным для этой операции или её параметров.
5. Токен доступа к API выдается не пользователю, а по его запросу, поэтому такой токен продолжит действовать даже если запросивший его пользователь был удален или заблокирован.