Станция управления заказами

Переход на общий механизм аутентификации для обращения к API СУЗ

Содержание

1 Общие сведения

Контроллер API СУЗ аутентифицирует клиентов с помощью так называемого клиентского токена, отправляемого клиентом в заголовке HTTP-запроса. Маркер безопасности (ClientToken) передаётся в заголовке HTTP в параметре «clientToken».

Получение клиентского токена доступно посредством:

1) Регистрации в пользовательском интерфейсе СУЗ клиентского устройства (системы) и получения статичного токена (см. раздел 2). Впоследствии данный механизм перестанет поддерживаться.

2) Обращения к методам единой аутентификации (см. раздел 3).

2 Текущий механизм получения токена

Текущий механизм получения токена включает в себя:

– регистрацию в пользовательском интерфейсе СУЗ клиентского устройства (системы), которое будет взаимодействовать посредством API СУЗ;

– на основе данных клиентского устройства (системы) СУЗ генерирует уникальный маркер безопасности (клиентский токен);

– токен отображается в пользовательском интерфейсе СУЗ.

Сгенерированный маркер безопасности является статичным, т.е. срок, в течение которого токен можно использовать для запросов к API СУЗ (время жизни), не ограничен и маркер безопасности может быть отозван только самим пользователем.

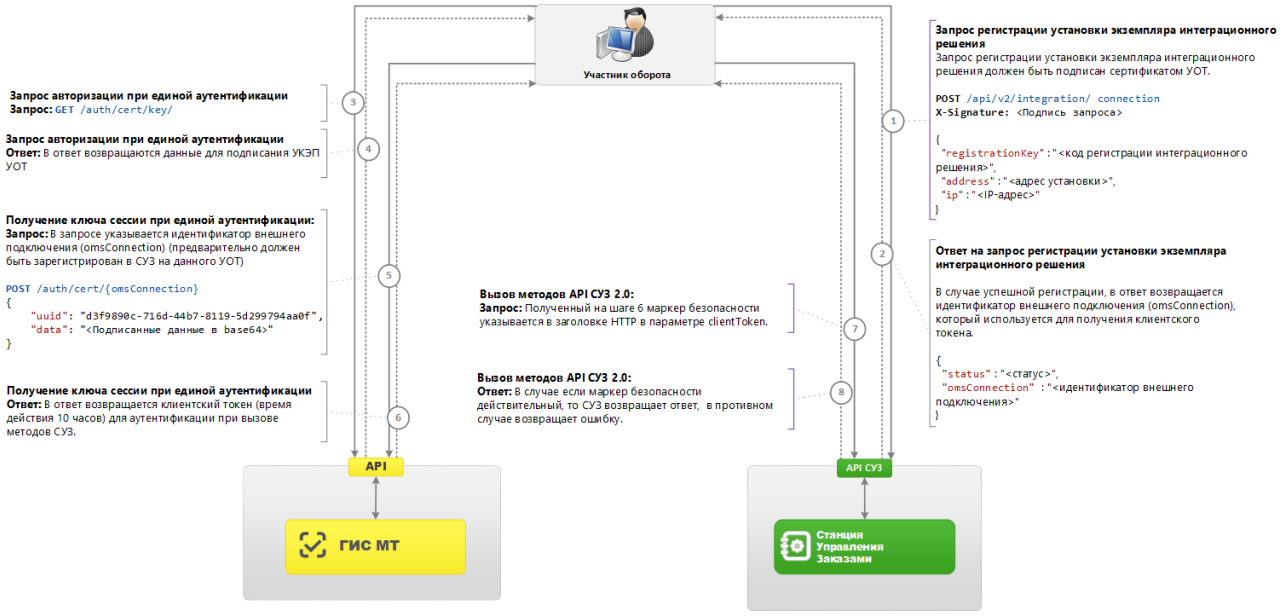
Таким образом, в случае кражи маркера безопасности злоумышленником, он сможет с его помощью направлять запросы в СУЗ неограниченно долго.

В целях повышения безопасности информационного взаимодействия начинается переход на механизм получения клиентского токена, указанный в раздел 3.

3 Целевой механизм получения токена

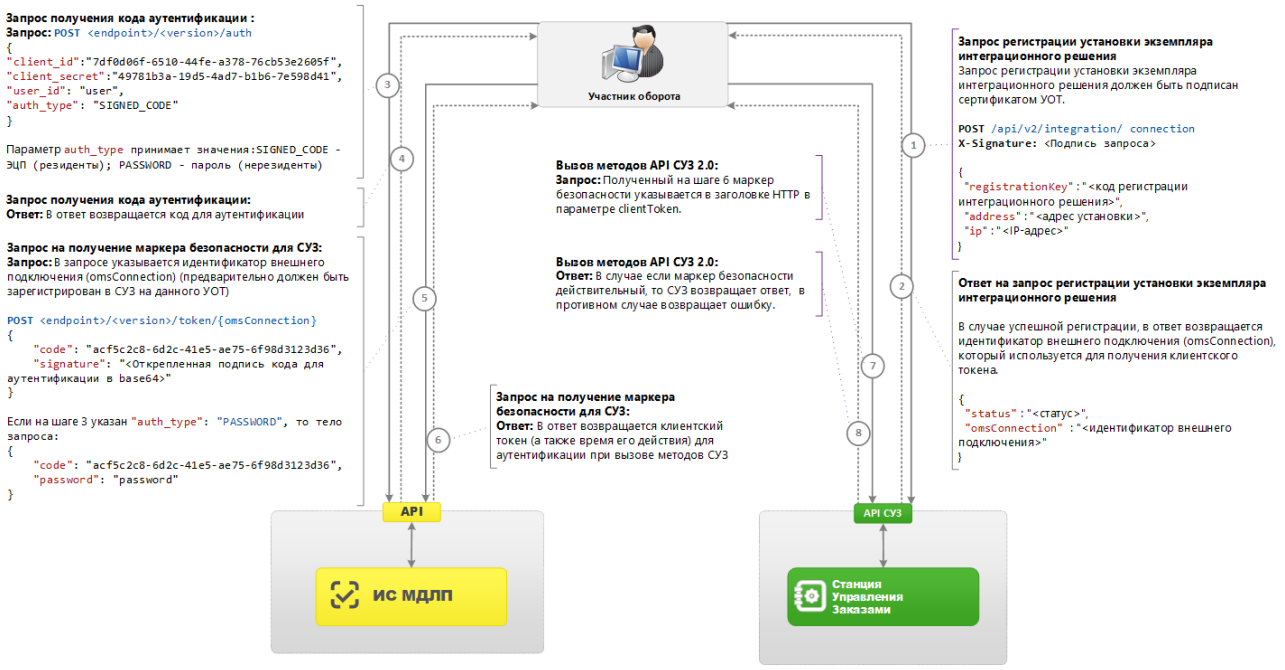
Целевым механизмом получения токена является получение токена посредством обращения к методам единой аутентификации ГИС МТ и ИС МДЛП (для УОТ с товарной группой «Лекарственные препараты для медицинского применения»).

Получение клиентского токена посредством обращения к методам единой аутентификации ГИС МТ и ИС МДЛП отображают Рисунок 1 и Рисунок 2, соответственно.



Общая схема получения клиентского токена API СУЗ посредством методов единой аутентификации ГИС МТ

Рисунок 1



Общая схема получения клиентского токена API СУЗ посредством методов единой аутентификации ИС МДЛП

Рисунок 2

Общая схема получения клиентского токена API СУЗ посредством методов единой аутентификации включает в себя:

– регистрацию в СУЗ установки интеграционного решения, которое будет использоваться для информационного взаимодействия с СУЗ [1, 2]. Для регистрации установки интеграционного решения в СУЗ предусмотрено соответствующее API. Запрос

регистрации установки экземпляра интеграционного решения должен быть подписан сертификатом УОТ. Каждой зарегистрированной установке интеграционного решения присваивается уникальный идентификатор внешнего подключения (omsConnection), который используется на шаге [5] для получения токена.

Доступна регистрация только интеграционных решений, которые прошли проверку на соответствие требованиям для информационного взаимодействия с СУЗ. Учет проверенных решений ведется Оператором и доступен для просмотра в СУЗ.

– получение клиентского токена посредством методов единой аутентификации API ГИС МТ и API ИС МДЛП [3-6]. При этом время действия клиентского токена, полученного посредством ГИС МТ – 10 часов, а полученного посредством ИС МДЛП – указывается в ответе при предоставлении токена.

– запрос данных в API СУЗ с использованием полученного клиентского токена [7, 8] (также как и раньше передаётся в заголовке HTTP в параметре «clientToken»). После истечения времени действия клиентского токена процедура его получения повторяется [3-6].

Примечание: после успешного обращения к API СУЗ с помощью клиентского токена, полученного посредством методов единой аутентификации, использование клиентских токенов, полученных посредством механизма, описанного в разделе 2, становится недоступным.