27.10.2023

Подключение к тестовой среде API онлайн регистрации клиентов

Получение токена доступа

Для работы с API первоначально необходимо получить токен доступа, для этого необходимо выполнить несколько шагов:

1. Создать тестовую учетную запись на https://passport-test.moex.com/registration. Получить MOEX Passport Token, выполнив GET запрос по адресу https://passport-test.moex.com/authenticate, используя Basic аутентификацию с учетными данными пользователя, от имени которого предполагается работа с API. Значение **Moex Passport Token** будет возвращено в cookie MicexPassportCert;

2. Прислать на адрес help@moex.com письмо с заголовком «Тестирование онлайн-регистрации клиентов», в котором указать:
   - Email, который использовался для регистрации в MOEX Passport в п. 1;
   - Идентификатор фирмы, с которой вы работаете на тестовых стендах INET_GATEWAY/INETCUR_GATEWAY (если есть). Если такой фирмы нет, то она будет создана.
   - Желаемый тип сертификата для п. 3 (RSA или ГОСТ)

   В ответном письме будут высланы:
   - Тестовый сертификат пользователя для п. 3;
   - **client_id** и **client_secret** для п. 4;
   - Данные для подключения к тестовым стендам INET_GATEWAY и INETCUR_GATEWAY, если необходимы.

3. **Для ГОСТ-сертификата** и СКЗИ "Валидата CSP" версии 6.0: скачать дистрибутивы можно тут https://www.moex.com/s1292
   - Скачать и установить Дистрибутив АПК Клиент МБ (ПК "Справочник сертификатов", ZCS) соответствующей разрядности (если не установлено/без поддержки компонент TLS, при необходимости добавить считыватель типа «Реестр»). Перезагрузить компьютер.
   - Скачать и установить Дистрибутив СКЗИ "Валидата CSP" соответствующей разрядности (если не установлено). Запустить.
   - Запустить Справочник сертификатов. При первичном запуске необходимо выполнить восстановление из резервной копии. В полученном в п. 2 архиве с тестовым сертификатом в папке Spr находится база локального справочника сертификатов. Эту папку нужно указать в качестве источника резервной копии. Также можно скопировать ее содержимое в каталог профиля C:\Users\<USER>\AppData\Roaming\Validata\zcs\. При следующем запуске указать тестовый сертификат. В дальнейшем при запуске Справочника будет выводиться сообщение с просьбой предоставить носитель с ключом, для этого необходимо выгрузить содержимое папки vdkeys из архива в корневой каталог съемного носителя (виртуальная дискета или USB-флэш накопитель).
   - Для ГОСТ-сертификата необходимо использовать Утилиту командной строки zpki1utl. Утилита командной строки поставляется с ПК "Справочник сертификатов" и располагается по умолчанию в C:\Program Files\Validata\zpki. Пример команды для создания отсоединенной ЭП:

zpki1utl.exe -profile <User> -sign -detached -data <token> -out token.p7d

Для RSA-сертификата: скачать дистрибутивы можно тут https://www.moex.com/s1293

- Скачать и установить Дистрибутив ПКЗИ СЭД МБ (ПК "Справочник сертификатов", RCS) версии не ниже 6.0.

- Запустить Справочник сертификатов. При первичном запуске необходимо выполнить восстановление из резервной копии. В полученном в п. 2 архиве с тестовым сертификатом в папке Spr находится база локального справочника сертификатов. Эту папку нужно указать в качестве источника резервной копии. Также можно скопировать ее содержимое в каталог профиля C:\Users\<USER>\AppData\Roaming\Validata\rcs\. При следующем запуске указать ключ UserOrg.rsa.
- Скачать утилиту Утилита командной строки для использования в СЭД (прямая ссылка http://fs.moex.com/cdp/po/rpkiutlv6.zip). Для RSA необходимо использовать утилиту rpki1utl* соответствующей разрядности. Краткое описание параметров запуска находится в архиве, файлы RunUtil.txt и rpki1utl.txt. Создать отделенную ЭЦП, пример команды:

  rpki1utl.exe -profile <User> -sign -detached -data <token> -out token.p7d

4. Далее полученный токен необходимо закодировать в Base64 с помощью любого инструмента или функции используемого языка программирования. Пример использования стандартной команды в Windows:

   certutil -encode token.p7d token.sig

   Полученный файл подписи не должен содержать переносов строк! Соответственно, для команд, не имеющих параметра для создания файла без переносов (включая приведённый пример с certutils), необходимо их удалить из закодированного в Base64 файла.

5. Выполнить POST запрос по адресу https://sso2.beta.moex.com/auth/realms/SSO/protocol/openid-connect/token, передав следующие параметры (параметры должны передаваться с использованием метода “application/x-www-form-urlencoded”):
   - **grant_type** – password
   - **grant_type_moex** – passport
   - **scope** – запрашиваемые права доступа
   - **client_id** – новый идентификатор приложения
   - **client_secret** – новый ключ безопасности
   - **certificate** - MOEX Passport Token, полученный как в п. 2 предыдущего раздела
   - **algorithm** – значение GOST или RSA, в зависимости от типа подписи, использованной при формировании электронной подписи MOEX Passport Token
   - **signature** – электронная подпись MOEX Passport Token в Base64 кодировке, сформированная в п. 4, в Base64 кодировке

Общий алгоритм двухфакторной аутентификации:

MicexPassportCert = Аутентифицироваться_MOEX_Passport (login, password) ;

Signature = Валидата.создать_ЭЦП (MicexPassportCert , CLIENT_CERTIFICATE);

access_token = HTTP.post (url=https://sso2.beta.moex.com/auth/realms/SSO/protocol/openid-connect/token, параметры= {

grant_type= “password”, grant_type_moex= “passport”, scope “*<scope>*”,

client_id=*Client_id*, client_secret=*Client_secret*,

certificate= **MicexPassportCert**,

algorithm=”GOST”|”RSA”, signature=**Signature**

}

);

Если запрос выполнится успешно, вы получите JSON объект со следующими полями:

- **access_token** – токен доступа, который должен передаваться при каждом вызове API
- **expires_in** – время жизни токена доступа в секундах
- **refresh_expires_in** – время жизни токена обновления в секундах
- **refresh_token** – токен обновления, токен который необходимо использовать при обновлении текущего токена доступа
- **token_type** – всегда имеет значение Bearer
- **not-before-policy** – активна ли политика неиспользования токена ранее установленного времени после выпуска (‘0’ – не активна)
- **session_state** – идентификатор аутентифицированной сессии
- **scope** – полученные права доступа

В случае же, если переданные данные не являются валидными (например, приложение с таким client_id отсутствует, client_secret не соответствует client_id или же переданная электронная подпись не соответствует переданному MOEX Passport токену) результатом будет **HTTP Response Code 403**

Использование токена доступа

Теперь, когда у вас есть токен доступа, все, что вам нужно сделать, это использовать его для подписания запросов, отправленных в API.

Вы делаете это, добавляя следующий заголовок к вашим запросам:

Authorization: Bearer <access_token>

В случае, если используемый Access Token (токен доступа) не является валидным или время его жизни истекло, в ответ вы получите **HTTP Response Code 401**.

При получении ответа с данным кодом ошибки, вы можете повторно запросить токен доступа так, как это описано ранее.

27.10.2023

Описание API Online registration

API строится на принципах RESTful API, используя следующие стандартные HTTP методы и в настоящее время поддерживает две операции:

1. POST https://play-apim.moex.com/client/v1/applications — Отправка заявки на регистрацию клиента(ов). Формат тела запроса соответствует существующему формату файла регистрации клиентов https://www.moex.com/a3361.
   При вызове должен быть указан HTTP заголовок Content-Type со значением application/xml.

   Возможные коды ответа:
   - 202 – заявка успешно зарегистрирована. В HTTP заголовке Location будет содержаться URL, по которому можно будет посмотреть статус обработки заявки на регистрацию
   - 503 – заявка не зарегистрирована, так отправлена в нерабочее время.
   - 429 – превышено допустимое количество запросов. Необходимо повторно отправить запрос через 30 сек.
   - 400 – неверный формат заявки. Конкретное описание ошибки содержится в теле ответного сообщения
   - 500 – прочие ошибки. Конкретное описание ошибки содержится в теле ответного сообщения
2. GET https://play-apim.moex.com/client/v1/applications/{DOC_DATE}/{DOC_NUM} — Получение статуса обработки заявки на регистрацию, где:
   - DOC_DATE – дата формирования заявки на регистрацию клиента
   - DOC_NUM - уникальный учетный номер заявки на регистрацию клиента

   Формат тела ответа соответствует существующему формату ответного файла регистрации клиентов https://www.moex.com/a3361.

Ограничения и доступность на тестовых полигонах

Время доступности API на тестовых стендах – 11:00:00 (MSK) – 16:00:00 (MSK)

Применимо к тестовым контурам: INET_GATEWAY (фондовый рынок), INETCUR_GATEWAY (валютный рынок), T1 (срочный рынок)

Количество допустимых вызовов API – 1 запрос/секунду

Максимальный размер тела запроса – 1 Мб

Системные требования

- При использовании СКЗИ Валидата:
  - Операционная система Windows 7 и новее.
  - В настройках безопасности браузера необходимо отключить протокол tls ver 1.0 и выставить поддержку протокола tls ver 1.1 и/или tls ver 1.2
- Должна устанавливаться telnet-сессия на адреса https://passport-test.moex.com и https://play-apim.moex.com/ на порт 443/tcp
- HTTPS запросы должны быть разрешены в вашей локальной сети.