Авторизация запросов

Общая информация об HTTP авторизации по ссылке.

Авторизация запросов происходит двумя способами

Базовая авторизация - Basic(rfc7617)

В базовой HTTP-авторизации запрос содержит поле заголовка(Headers) формы Authorization: Basic <credentials>, где credentials это кодировка в base64 имени пользователя и пароля соединенные двоеточием.

Данные для авторизации будут выдаваться отдельно.

Авторизация по токену - Bearer(rfc6750)

Авторизация происходит с помощью JWT токена(rfc7519).

В токене содержится информация о пациенте, под которым происходит запрос, например запись на прием. Формат используемых токенов указан в разделе Заголовки запроса описания метода.

Формирование токена происходит в центральном сервисе авторизации, который проверяет наличие пациента в Мастер Индексе Пациентов(МИП).

Токены

Схема использования токена при интеграции:
1. Пациент использует авторизацию на портале 2др.
2. Сервисы 2др производят поиск пациента в МИП(Мастер индексе пациентов)
3. При нахождении формируется токен(Внутри сервисов 2др)
4. Сформированный токен прикладывается ко всем запросам записи на прием. В том числе получение, создание и отмена записей.
5. Сторонняя МИС принимает запрос и анализирует токен, проверяя его подпись(ключ будет передан) и наличие пациента у себя в системе.
6. При положительном результате проверки производятся необходимые валидации записи на прием и создается запись, а ее идентификатор возвращается сервису 2др.
7. При отрицательном результате возвращается сообщение об ошибке/сообщении валидации, причем желательно в формате стандартного ответа сервера и с HTTP кодом 400.

- Токен пациента - PatientToken