ИНТЕГРАЦИЯ МИС С ЦИСЗ

Порядок действий

Команда МИС должна интегрироваться с ЦИСЗ (ПИБ) согласно следующим рекомендациям:

1. Разработать функционал для авторизации и аутентификации клиентского приложения (МИС).
2. Выбрать предполагаемую схему аутентификации в зависимости от типа клиентского приложения:
    a. Для API МИС аутентификация производится по схеме Client Credentials Grant;
    b. Для веб-приложений аутентификация производится по схеме по схеме Authorization Code Grant with PKCE.
3. Зарегистрировать МИС у разработчиков ЦИСЗ:
    a. Заявку на авторизацию МИС с ЦИСЗ необходимо направлять в электронную почту (shdm@agsr.by).
        i. В заявке нужно указать информацию об организации, об используемой МИС и желаемую схему интеграции.
    b. Получить от разработчиков ЦИСЗ следующие параметры для аутентификации:
        1. Realm (term, iehr, ppa, и других);
        2. Client ID;
        3. Client Secret.
4. Протестировать МИС **приложенными Postman коллекциями**.
    a. В случае интеграции API МИС (по схеме Client Credentials) используется приложенный файл «МИС Client Credentials.postman_collection.json».
    b. В случае интеграции веб-приложений (по схеме Authorization Code Grant with PKCE) используется приложенный файл «МИС Authorization Code with PKCE.postman_collection.json».

Авторизация клиентского приложения Client Credentials

Авторизация клиентского приложения должна быть с использованием схемы Client Credentials Grant протокола Open Authorization 2.0. Диаграмма последовательности процесса аутентификации и авторизации с использованием схемы Client Credentials Grant представлено ниже (см. Приложение 1, рисунок 1).

Предусловие: клиентское приложение запрашивает токен у ЦИСЗ (ПИБ).

Допущение: нет лимита на количество попыток авторизации с помощью схемы Client Credentials Grant.

Актеры систем: Клиентские приложения (МИС), ЦИСЗ (ПИБ).

Триггер: клиентское приложение (МИС) пытается пройти авторизацию в ЦИСЗ.

Основной сценарий (Таблица 1):

Таблица 1

ШАГ	ДЕЙСТВИЕ
1	Клиентское приложение (МИС) вызывает метод POST/token, передает в нем значения параметров Client ID & Client Secret в ЦИСЗ (ПИБ)

ШАГ	ДЕЙСТВИЕ
2	ЦИСЗ (ПИБ) проводит валидацию Client ID & Client Secret
3	ЦИСЗ (ПИБ) проводит аутентификацию и авторизацию клиентского приложения
4	ЦИСЗ (ПИБ) передает клиентскому приложению access_token (ЦИСЗ)
5	Авторизации клиентского приложения выполнена

Постусловие: ЦИСЗ (ПИБ) обеспечена авторизация клиентского приложения с помощью схемы Client Credentials Grant.

Схема аутентификации и авторизации пользователя Authorization code with PKCE

Аутентификация и авторизация пользователя-медицинского работника должна быть с использованием схемы Authorization code with PKCE протокола Open Authorization 2.0.

Диаграмма последовательности процесса аутентификации и авторизации с использованием схемы Authorization code with PKCE представлено ниже (см. Приложение 1, рисунок 2).

Предусловие: для обеспечения аутентификации и авторизации в ЦИСЗ пользователей-медицинских работников способом ЕС ИФЮЛ с использованием схемы Authorization code with PKCE необходимо выполнение следующих требований.

Взаимодействие с ЕС ИФЮЛ

Для взаимодействия с ЕС ИФЮЛ на стороне Клиентского приложения должен быть установлен Комплекс программных средств прикладной системы (КПСИС), включающий:

- Модуль поддержки OpenID connect;
- Сервис контроля целостности;
- Сервис выработки ЭЦП;
- Сервис проверки ЭЦП;
- Сервис предварительного шифрования;
- Терминал;
- Программный TLS-сервер;
- Сервис генерации личного ключа и запроса на выпуск СОК;
- API, реализующий спецификацию по OAuth 2.0.

На стороне Пользователя-медицинского работника должны быть установлены программы и устройства в следующих сочетаниях:

а) для авторизации с помощью идентификационной карты (ID-карта):

- клиентская программа BY.БФИД.10244-01;
- ID-карта;
- универсальный считыватель.

б) для авторизации на ПЭВМ (операционная система Windows) с помощью носителя (USB-устройства):

- клиентская программа BY.БФИД.10244-01;
- программа криптопровайдера (NTCrypto БФИД.10186-01 или Avest CSP BIGN РБ.ЮСКИ.12005-02 «AvPKISetup2.exe»);
- носитель (USB-устройство) с импортированным личным сертификатом ГосСУОК.

Допущение: нет лимита на количество попыток аутентификации и авторизации с помощью схемы Authorization Code Grant with PKCE.

Актеры: Пользователь-медицинский работник, Клиентская программа, Браузер, Клиентские приложения (МИС), ЦИСЗ (ПИБ), Сервер ЕС ИФЮЛ.

Триггер: клиентское приложение (МИС) пытается пройти аутентификацию и авторизацию в ЦИСЗ.

Основной сценарий (Таблица 2):

Таблица 2

ШАГ	**ДЕЙСТВИЕ**
1	Пользователь-медицинский работник жмет кнопку «Вход»
2*	Браузер вызывает метод GET/auth и передает *code_challenge* в ЦИСЗ (ПИБ)
3*	ЦИСЗ (ПИБ) сохраняет *code_challenge*
4	ЦИСЗ (ПИБ) направляет Браузеру страницу выбора метода аутентификации
5	Браузер отображает страницу выбора метода аутентификации Пользователю-медицинскому работнику.
6	Браузер вызывает Клиентское приложение методом GET/login
7	Клиентское приложение возвращает параметры Браузеру
8	Браузер запрашивает у Клиентской программы согласие на предоставление данных пользователя-медицинского работника
9	Клиентская программа запрашивает у Пользователя-медицинского работника согласие на предоставление данных Пользователя-медицинского работника
10	Пользователь-медицинский работник дает согласие Клиентской программе на предоставление своих пользовательских данных
11	Клиентская программа перенаправляет согласие пользователя-медицинского работника в Браузер
12	Браузер перенаправляет Пользователя-медицинского работника на Сервер ЕС ИФЮЛ для прохождения аутентификации
13	Сервер ЕС ИФЮЛ отображает Браузеру страницу аутентификации
14	Браузер отображает Пользователю-медицинскому работнику страницу выбора метода аутентификации
15	Пользователь-медицинский работник передает Серверу ЕС ИФЮЛ данные пользователя-медицинского работника для аутентификации
16	Сервер ЕС ИФЮЛ проверяет корректность ЭЦП переданных пользовательских данных
17	Сервер ЕС ИФЮЛ передает ЦИСЗ (ПИБ) токен ЕС ИФЮЛ
18	ЦИСЗ (ПИБ) производит аутентификацию Пользователя-медицинского работника
19	ЦИСЗ (ПИБ) вызывает Браузер методом GET/callback и передает *authorization_code*
20	Браузер передает Клиентскому приложению authorization_code
21	Клиентское приложение запрашивает ЦИСЗ (ПИБ) методом GET/token и передает *authorization_code & code_verifier*
22	ЦИСЗ (ПИБ) проверяет *authorization_code & code_verifier*
23	ЦИСЗ (ПИБ) передает Клиентскому приложению *id_token* (ЦИСЗ)
24	Клиентское приложение оповещает Браузер о выполненной аутентификации
25	Авторизация пользователя-медицинского работника выполнена

* *code_challenge* : пример можно посмотреть в прилагаемой Postman коллекции.

Альтернативный сценарий (негативный) процесса аутентификации Пользователей-медицинских работников в ЦИСЗ с помощью схемы Authorization Code Grant with PKCE (Таблица 3)

Таблица 3

Шаг	**Действие**
1	Клиентское приложение передает неверный authorization_code & code_verifier
2	ЦИСЗ (ПИБ) производит проверку authorization_code & code_verifier
3	ЦИСЗ (ПИБ) передает информацию в Клиентское приложение о невозможности аутентификации Пользователя-медицинского работника
4	Клиентское приложение передает браузеру информацию о невозможности аутентификации Пользователя-медицинского работника

Шаг	Действие
5	Браузер отображает Пользователю сообщение о невозможности аутентификации
6	Переход к шагу 1 основного сценария.

Постусловие: ЦИСЗ (ПИБ) обеспечена аутентификация и авторизация пользователя-медицинского работника с помощью схемы Authorization code with PKCE

ПРИЛОЖЕНИЕ 1

Схема аутентификации Client Credentials Grant

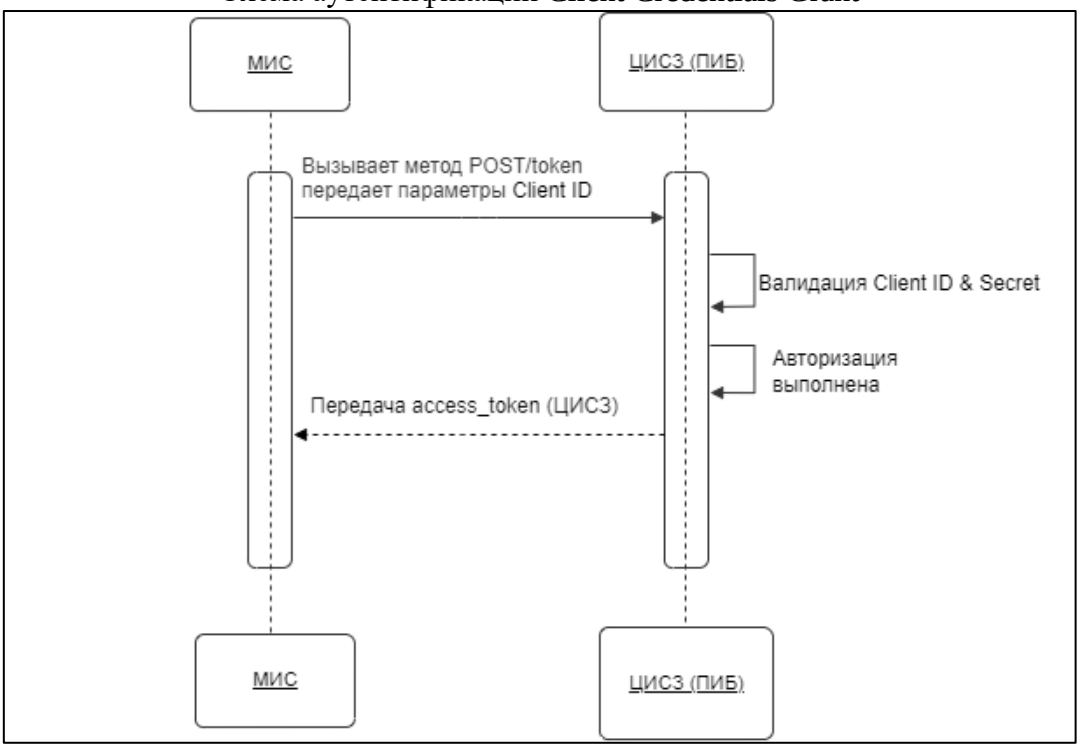

Рисунок 1

Схема аутентификации Authorization code with PKCE

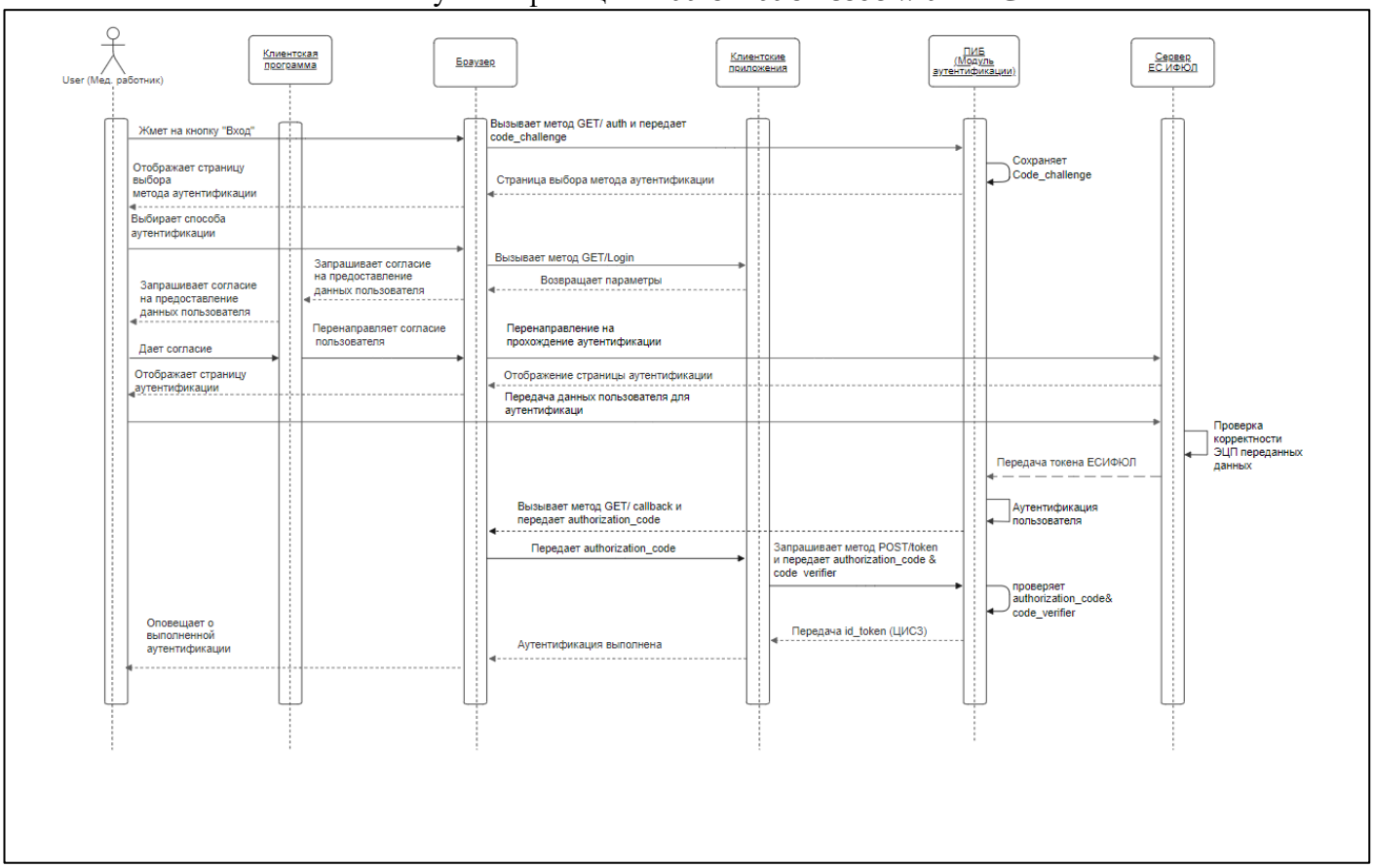

Рисунок 2

ПРИЛОЖЕНИЕ 2

Postman-коллекция для проверки работы по схеме Client Credentials Grant

МИС Client Credentials.postman_collection.json

Postman-коллекция для проверки работы по схеме Authorization Code Grant with PKCE

МИС Authorization Code with PKCE.postman_collection.json