

Авторизация пользователей в ЕСИА по новым требованиям ИБ

Елена Новикова
Руководитель продуктового направления

Влада Домлоджанова
Инженер-тестировщик ViPNet EDI

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  **ФЕСТ**

Работа через ЕСИА по новым требованиям



Требуется использование сертифицированных средства криптографической защиты информации (СКЗИ) класса **КСЗ**.

Подключаемая информационная система должна пройти аттестацию по требованиям информационной безопасности (ИБ).

Необходимо реализовать поддержку OpenID Connect с подтверждением соответствия требованиям ФСБ (пройти оценку влияния на СКЗИ).

Канал взаимодействия с тестовой ЕСИА должен быть защищен по протоколу TLS, а с промышленной ЕСИА — с использованием СКЗИ класса КСЗ

Как стать участником ЕСИА





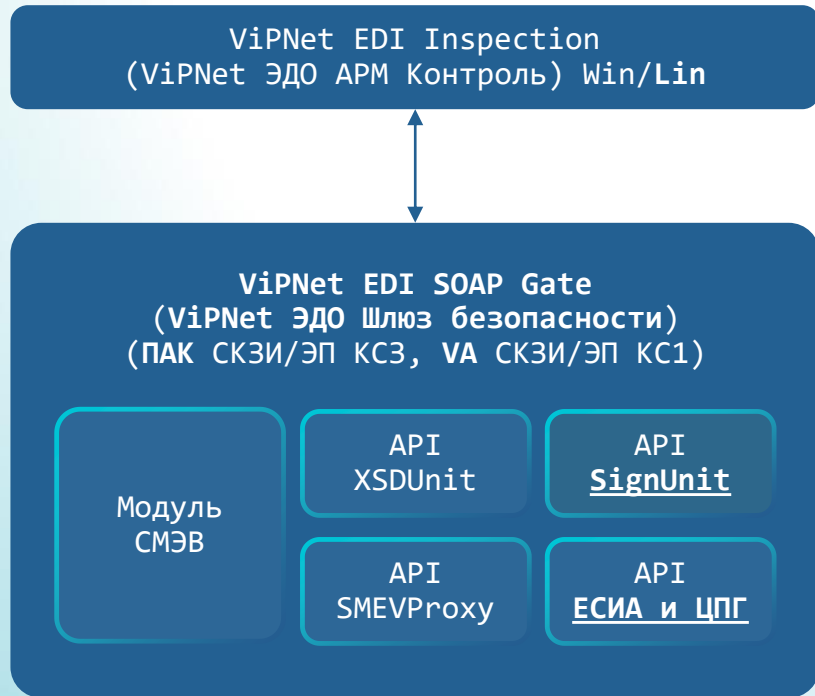
ПАК ViPNet EDI Soap Gate

Криптошлюз для работы
с ЕСИА и ЦПГ



- Соответствует требованиям «Регламента информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства» версии 2.47+ и «Методическим рекомендациям по использованию ЕСИА» версии 3.48+
- Авторизация и аутентификация пользователей в ЕСИА с помощью протокола авторизации OAuth 2.0 и расширения OpenID Connect
- Построение защищенного канала связи с использованием протокола TLS ГОСТ
- Заверение данных ЭП определенного формата и ее проверка, включая проверку действительности сертификата ключа проверки электронной подписи, списка аннулированных сертификатов и цепочки сертификатов
- Формирование, заверение и проверка ЭП хэша данных
- Получение информации о владельцах ЭП и наличии в хранилищах сертификатов и CRL
- Соответствует требованиям ФСБ России к СКЗИ и ЭП по классу КСЗ и КС1

Состав ViPNet EDI 3.6

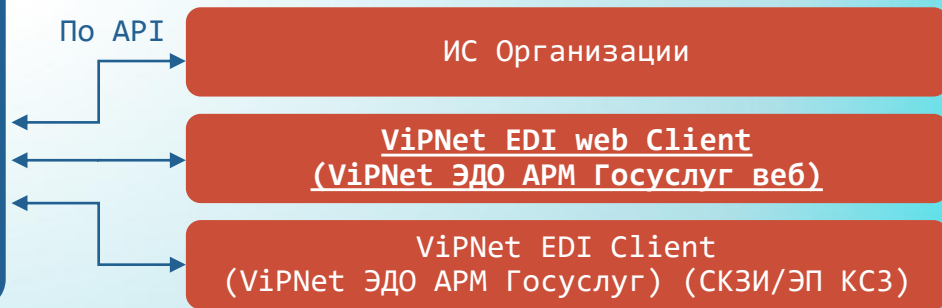


ViPNet EDI Soap Gate (ПАК/VA)*

Лицензии расширения (модули для работы):

- Работа со СМЭВ3: XSDUnit (REST API)
- Работа со СМЭВ3: SMEVProxy (SOAP API)
- Сервис подписи: SignUnit
- Авторизация в ЕСИА
- Получение данных из ЕСИА
- Получение данных из ЦПГ

**лицензии расширения к ViPNet EDI Soap Gate опциональны*



API для взаимодействия с ЕСИА и ЦПГ

Возможность авторизовать пользователя через ЕСИА

Запросить у пользователя доступ к персональным данным, получить ПД пользователя из ЕСИА

Авторизация пользователя через ЕСИА для получения данных пользователя из ЦПГ

Запрос в ЕСИА данные о самозанятых пользователях, организациях пользователя, категориях организации пользователя и список участников организации пользователя

Для интеграции предоставляется Справочник разработчика с описанием методов API



Аутентификация и авторизация через ЕСИА

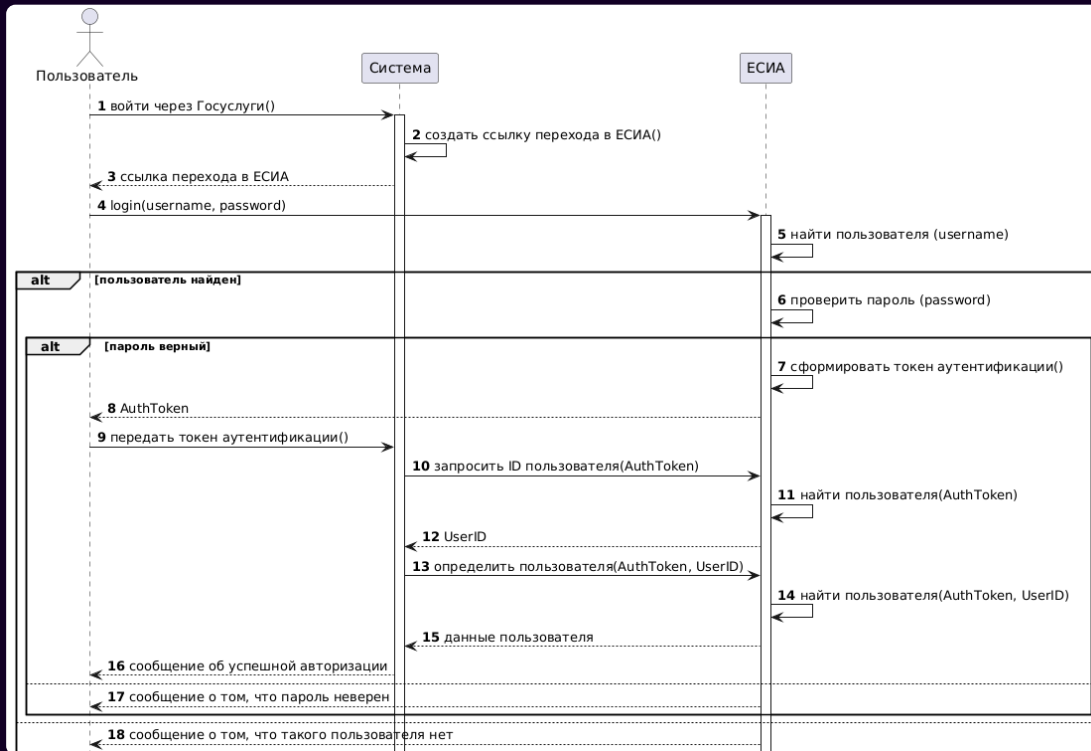


Диаграмма взаимодействия с ЕСИА через ViPNet EDI Soap Gate

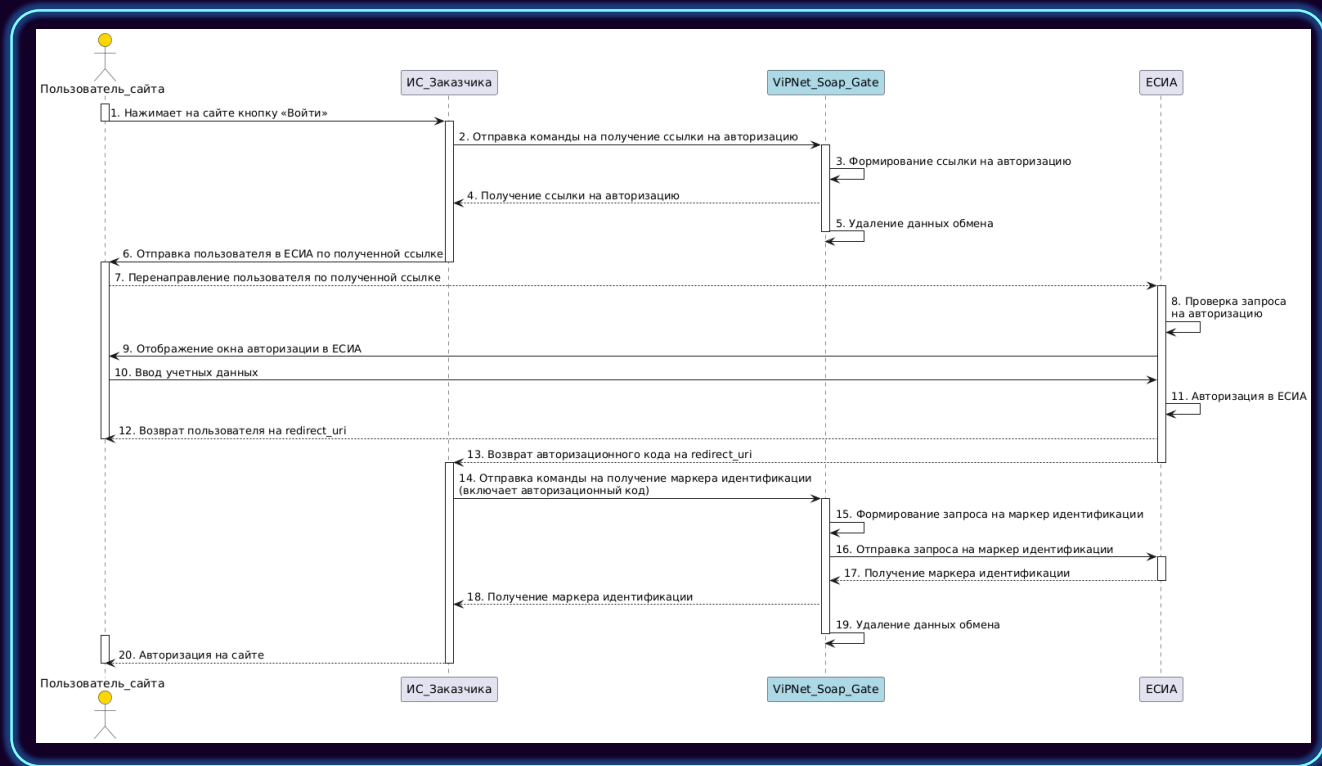
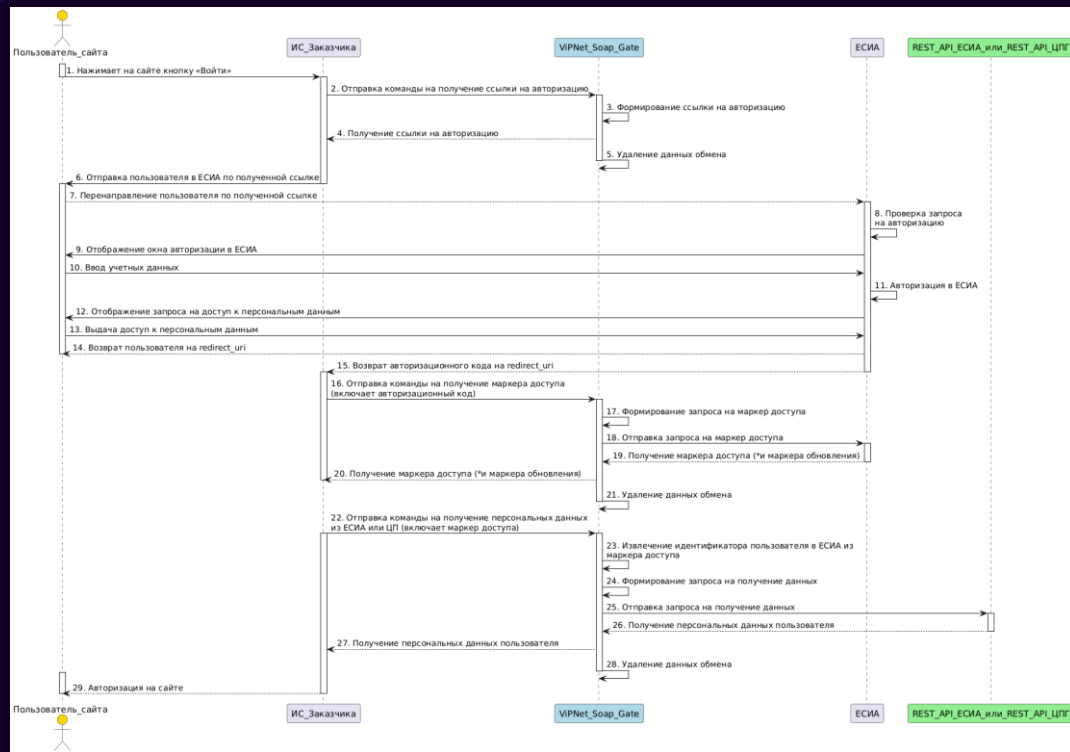


Диаграмма интеграции с ЕСИА с запросом ПД в ЕСИА/ЦПГ



1. ИС с помощью методов для взаимодействия с ЕСИА или ЦПГ отправляет в VipNet ЭДО Шлюз безопасности запрос на получение ПД пользователя или его организации, в котором содержится маркер доступа.
2. VipNet ЭДО Шлюз безопасности формирует запрос на получение данных пользователя из ЕСИА или ЦПГ и отправляет запрос в REST API ЕСИА или в REST API Цифрового профиля.
3. ЕСИА осуществляет проверку запроса и отправляет в ответе запрашиваемые ПД пользователя.
4. VipNet ЭДО Шлюз безопасности получает ответ, который содержит запрашиваемые ПД пользователя, и передает их в ИС

Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate 3.6



Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate 3.6

Шаг 1. Провести организационные мероприятия для подключения ИС к ЕСИА и настроить ViPNet ЭДО Шлюз безопасности.

Шаг 2. Необходимо загрузить сертификаты для подписи запросов в ЕСИА и ЦПГ и установки безопасного соединения по TLS между ViPNet ЭДО Шлюз безопасности и ЕСИА.

- ✓ *создайте запрос на сертификат в формате P10 и загрузите полученный в Удостоверяющем центре сертификат в ViPNet EDI Inspection 3 (ViPNet ЭДО АРМ Контроль 3)*

Шаг 3. Создание и настройка полномочий УЗ ИС в ViPNet EDI Inspection 3 (ViPNet ЭДО АРМ Контроль 3).

Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate 3.6

Шаг 4. Аутентификация ИС через сервис Auth. Предназначен для управления сессией при подключении к API ViPNet ЭДО Шлюз безопасности 3.

Для вызова методов Модуля необходимо получить токен авторизации на основе логина и пароля учетной записи ИС.

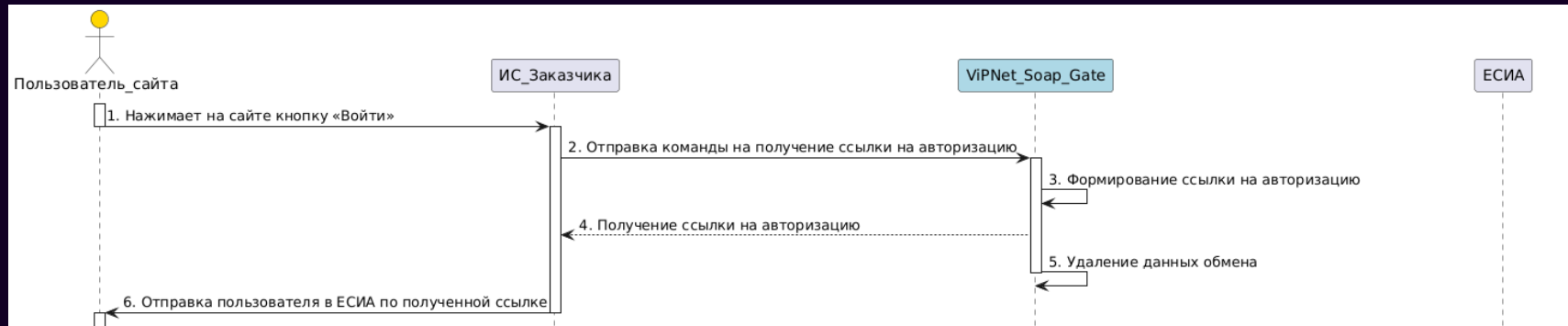
- ✓ *Чтобы получить временный токен авторизации, отправим запрос с ИС на ViPNet EDI Soap Gate. В заголовке запроса укажем логин и пароль учетной записи. Логин и пароль указываются по технологии HTTP Basic access authentication в кодировке base64.*

В теле ответа возвращается временный токен (JWT). При обращении к сервисам необходимо указывать токен в заголовке запроса в виде:
Authorization: Bearer [токен].

Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate 3.6

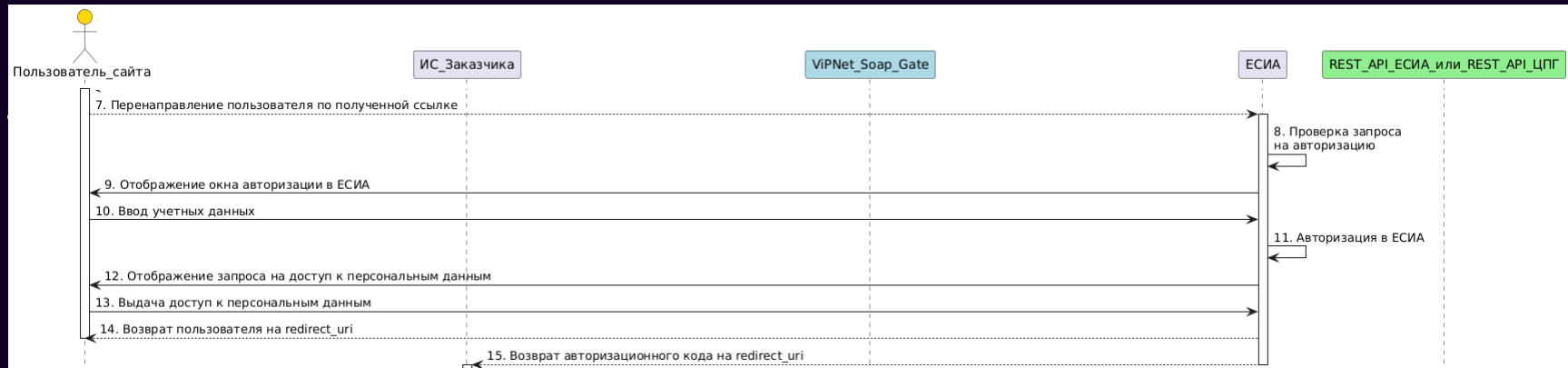
Шаг 5. Авторизация в ЕСИА. Метод getAuthUrl.

Пользователь выбирает на сайте функцию авторизации с помощью ЕСИА. ИС отправляет запрос в SG для получения ссылки на авторизацию в ЕСИА. SG формирует ссылку на авторизацию в ЕСИА и передает ее ИС. ИС организации направляет пользователя по полученной от SG ссылке.



Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate 3.6

Шаг 6. Получение согласия от ФЛ на получение ПДн. После проверки ЕСИА корректности ссылки и отображения страницы аутентификации пользователь вводит учетные данные, проходит авторизацию в ЕСИА и предоставляет доступ к своим ПДн. ЕСИА перенаправляет пользователя на сайт, адрес которого указан в ссылке на авторизацию в параметре `redirect_uri`, и передает ИС авторизационный код (code).



Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate 3.6

Шаг 7. Получение маркера доступа для доступа к ПДн ФЛ.

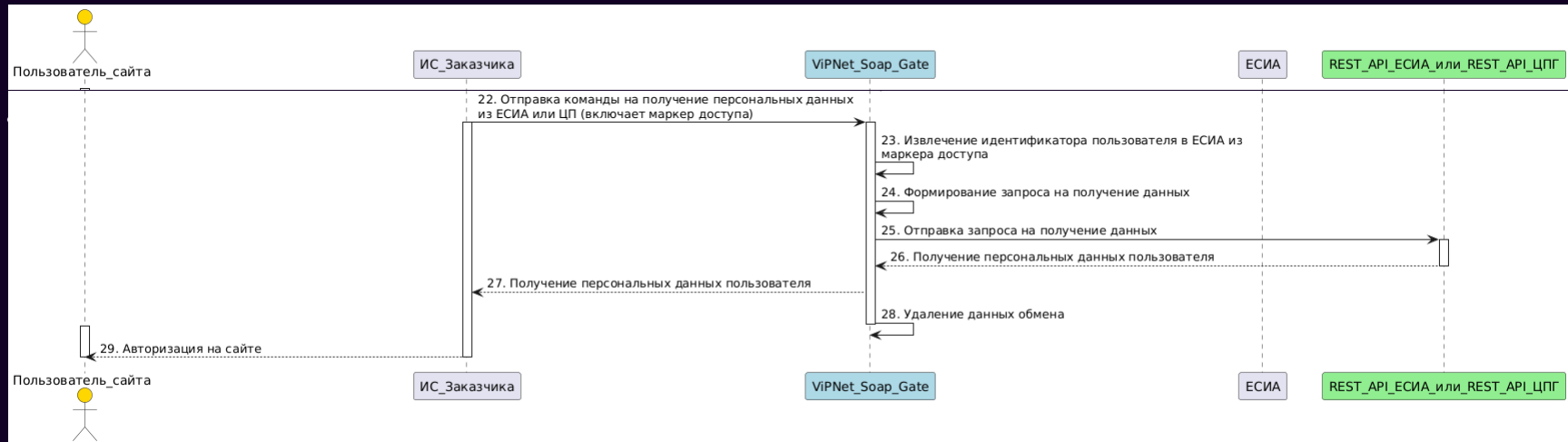
ИС отправляет в SG запрос на получение маркера доступа (access_token).

SG отправляет запрос в ЕСИА на получение маркера доступа и после получения отправляет его в ИС.

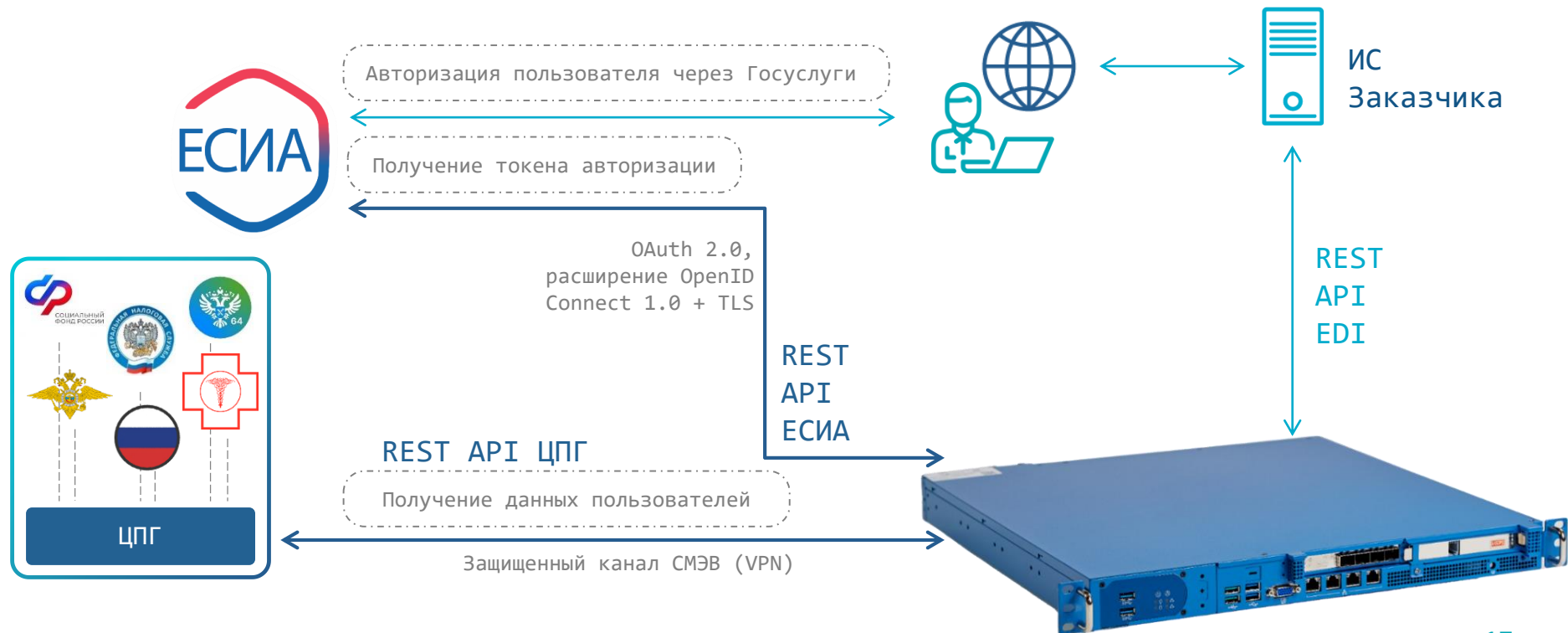


Шаг 8. Получение ПДн из ЕСИА

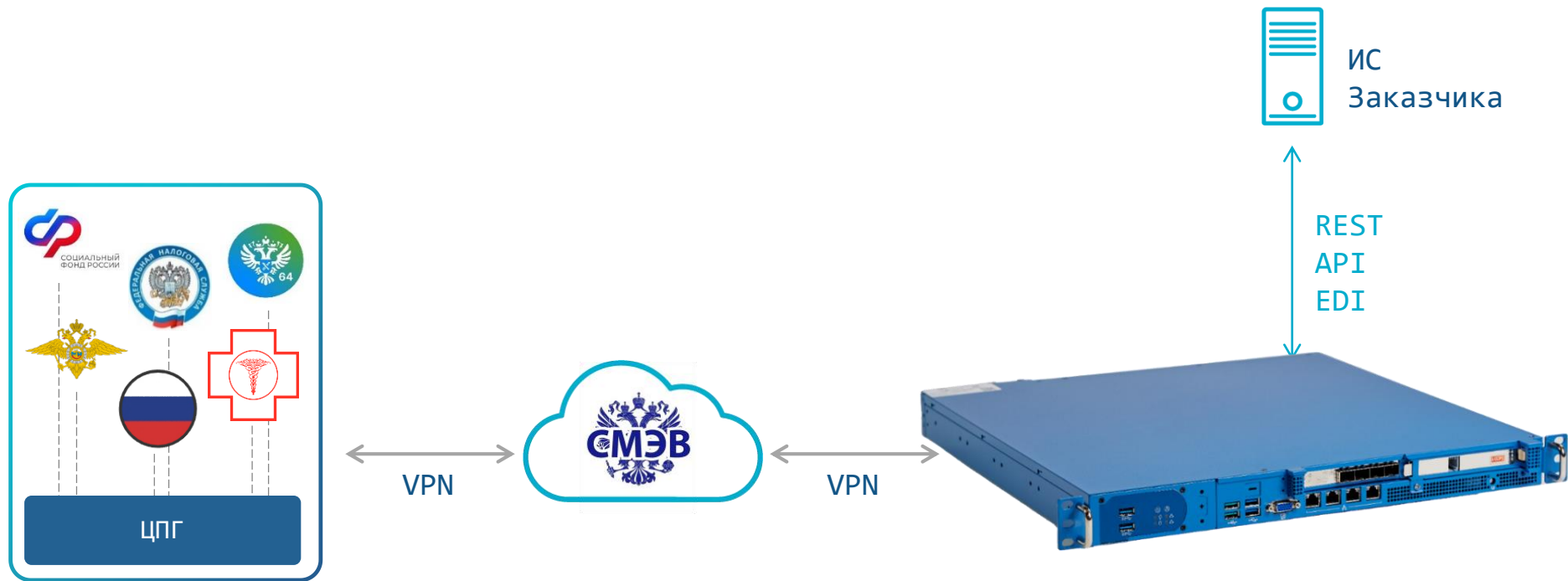
ИС отправляет в SG запрос на получение ПД пользователя или его организации, в котором содержится маркер доступа (access_token). SG извлекает идентификатор пользователя в ЕСИА из маркера доступа (access_token), формирует GET-запрос на получение данных пользователя из ЕСИА и отправляет запрос в REST API ЕСИА. ЕСИА осуществляет проверку запроса и отправляет в ответе запрашиваемые ПД пользователя. SG получает ответ, который содержит запрашиваемые ПД пользователя, и передает их в ИС.



Интеграция с ЦПГ с помощью ViPNet EDI (online-режим)



Интеграция с ЦПГ с помощью ViPNet EDI (offline-режим)



ТЕХНО infotecs Фест

Елена Новикова

Руководитель продуктового направления

Влада Домлоджанова

Инженер-тестировщик ViPNet EDI



NBJ НАЦИОНАЛЬНЫЙ
БАНКОВСКИЙ ЖУРНАЛ



РУТОКЕН
БЮРО АНАЛИТИКИ



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



PR integ

АТБ
ЭЛЕКТРОНИКА

infotecs
{-cademy}

m≡rlion



Подписывайтесь
на наши соцсети,
там много интересного

