ViPNet EDI: СКЗИ и средство ЭП для легитимной работы с ЕСИА и ЦПГ

Новикова Елена

Хранимые данные

- данные о пользователе (идентификационные данные, данные о транспортных средствах, данные о вхождении в организации и др.)
- данные об организациях (идентификационные данные, данные о сотрудниках)
- данные об ИС (идентификационные данные, данные об организации-владельце)
- данные о согласиях на доступ к сведениям организации для потребителя

Требования законодательства по использованию ЕСИА

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Постановления Правительства Российской Федерации

-№ 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» от 10 июля 2013 ;

-№ 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» от 25 января 2013 г.

-№ 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» от 28 ноября 2011 г.

-**№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г.**

Положение «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утвержденное приказом Минкомсвязи России от 13 апреля 2012 г. № 107

Новые требования безопасности ЕСИА*

- Регламент информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства версии 2.47+
- Методические рекомендации по использованию ЕСИА версии 3.48+

Регламент ЕСИА

- авторизация в ЕСИА (VA КС1)
- авторизация и получение данных (ПАК КС3)

«Критерии принятия решения о корректности выбора СКЗИ, включая средства ЭП, применяемых для организации взаимодействия с ФГИС ЕСИА:

- наличие действующего сертификата ФСБ России у средства ЭП.
- класс средства ЭП не ниже КС3.

Допускается применение средств ЭП, сертифицированных по требованиям ФСБ России по классу не ниже КС1, при взаимодействии с ЕСИА в случае отсутствия необходимости получения каких-либо персональных данных пользователя ЕСИА, проходящего аутентификацию, за исключением идентификатора ЕСИА.

При необходимости получения персональных данных уровень защищенности персональных данных подключаемой системы должен быть УЗ.3 и выше*.»

*В соответствии с Постановлением Правительства РФ от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Необходимые меры для подключения к ЕСИА

- Приобрести и настроить ПАК СКЗИ КСЗ
- Разработать модель угроз, обеспечивающую защищенность ПД в ИС на уровне 3.3 и выше, согласовать ее во ФСТЭК и ФСБ
- Провести аттестацию ИС по требованиям ИБ с привлечением аккредитованной ФСБ России лаборатории. Предварительно разработать всю документацию по ИС
- Пройти процедуру оценки влияния среды функционирования на СКЗИ с привлечением аккредитованной ФСБ России лаборатории
- Провести проверку корректности реализации OpenID Connect с привлечением аккредитованной ФСБ России лаборатории
- Для финансовых организаций подтвердить выполнение 5 положений ЦБ по ИБ

(ПАК КСЗ)

Методические рекомендации ЕСИА

- авторизация в ЕСИА (VA КС1)
- авторизация и получение данных (ПАК КС3)

Приложение Д. Требования по безопасности сервисов ЕСИА, основанных на протоколах Oauth2.0 и OpenId Connect 1.0

3.2. Серверная часть ВИС должна поддерживать возможность взаимодействия с пользователями по протоколу TLS, реализованному с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КС3 на стороне ВИС (сервера) и КС1 на стороне пользователя (клиента). Допускается применение СКЗИ класса КС1 в ВИС в случае отсутствия передачи каких-либо персональных данных из Цифрового Профиля ЕСИА, за исключением идентификатора пользователя ЕСИА, проходящего аутентификацию.

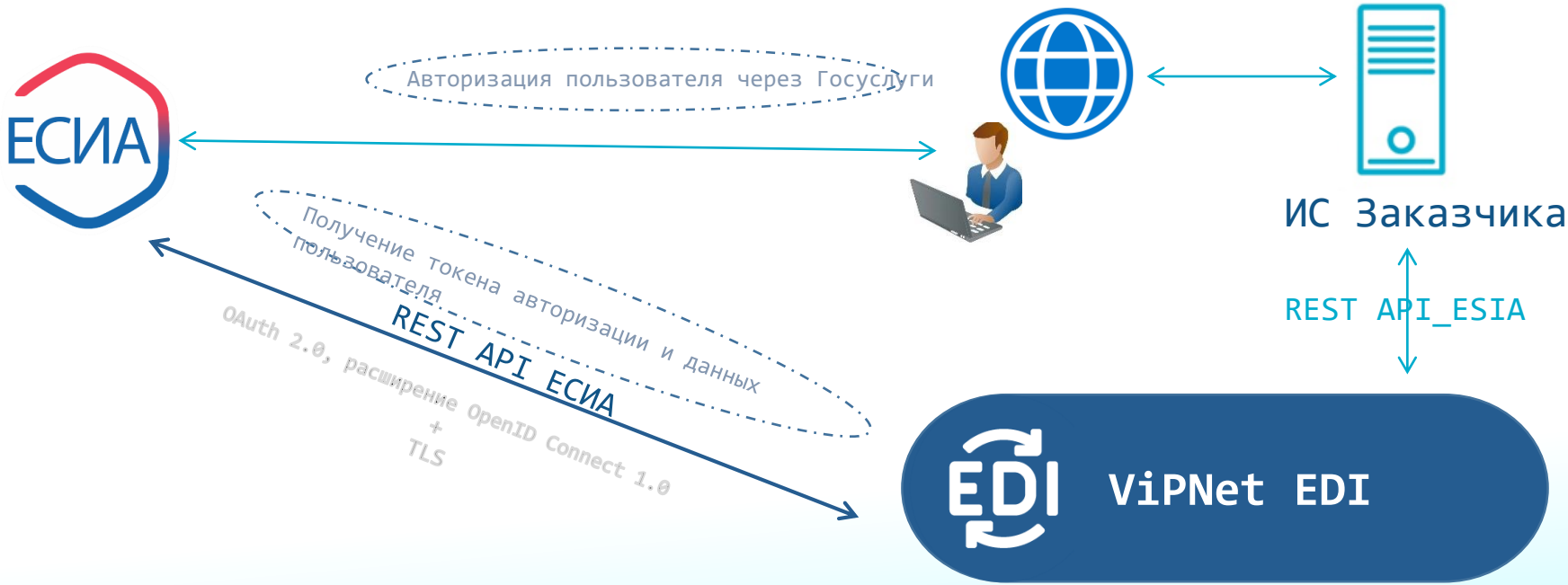
ViPNet EDI Soap Gate

ПАК для обмена электронными сведениями с применением электронной подписи

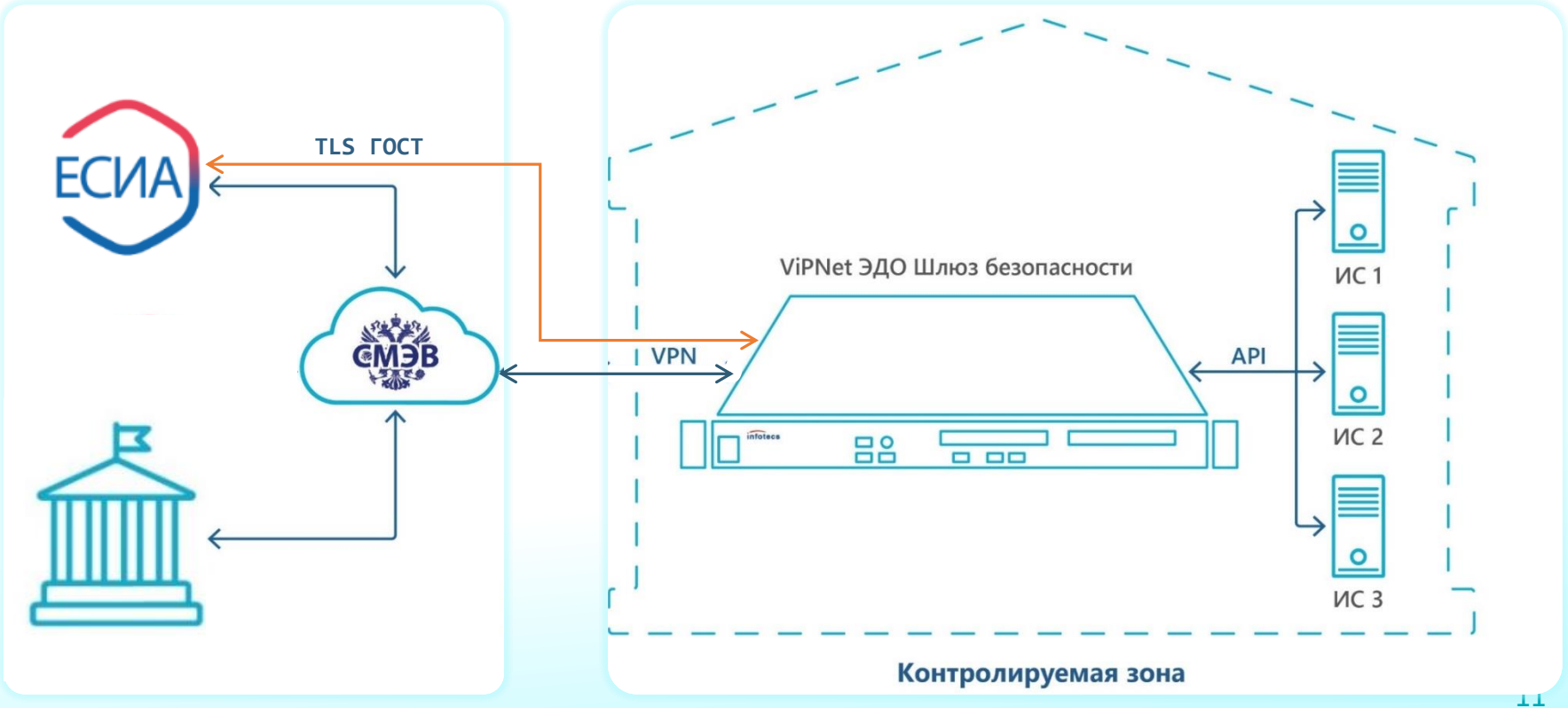
- **ПАК:** СКЗИ и средство ЭП КС3
- **VA:** СКЗИ и средство ЭП КС1
- Авторизация пользователей в ЕСИА и ЦПГ
- Получение данных в СМЭВ, ЕСИА, ЦПГ, ЦПО
- Подпись и проверка подписи ГОСТ
- Построение TLS ГОСТ 1.2, 1.3

ViPNet EDI для ЕСИА

Интеграция с ЕСИА с помощью ViPNet EDI



ViPNet EDI 3.6. Работа со СМЭВ, ЕСИА, ЦПГ и ЦПО

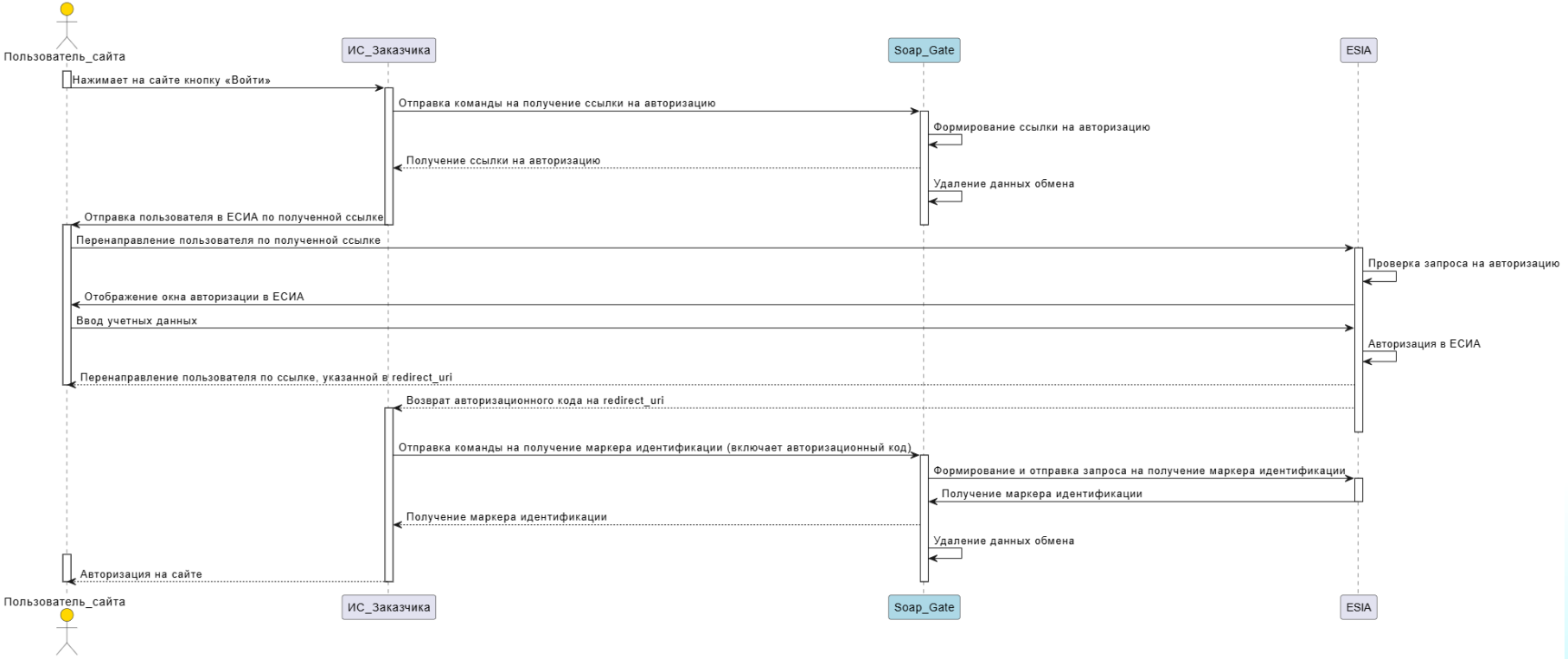


Демонстрация авторизации и получения данных из ЕСИА

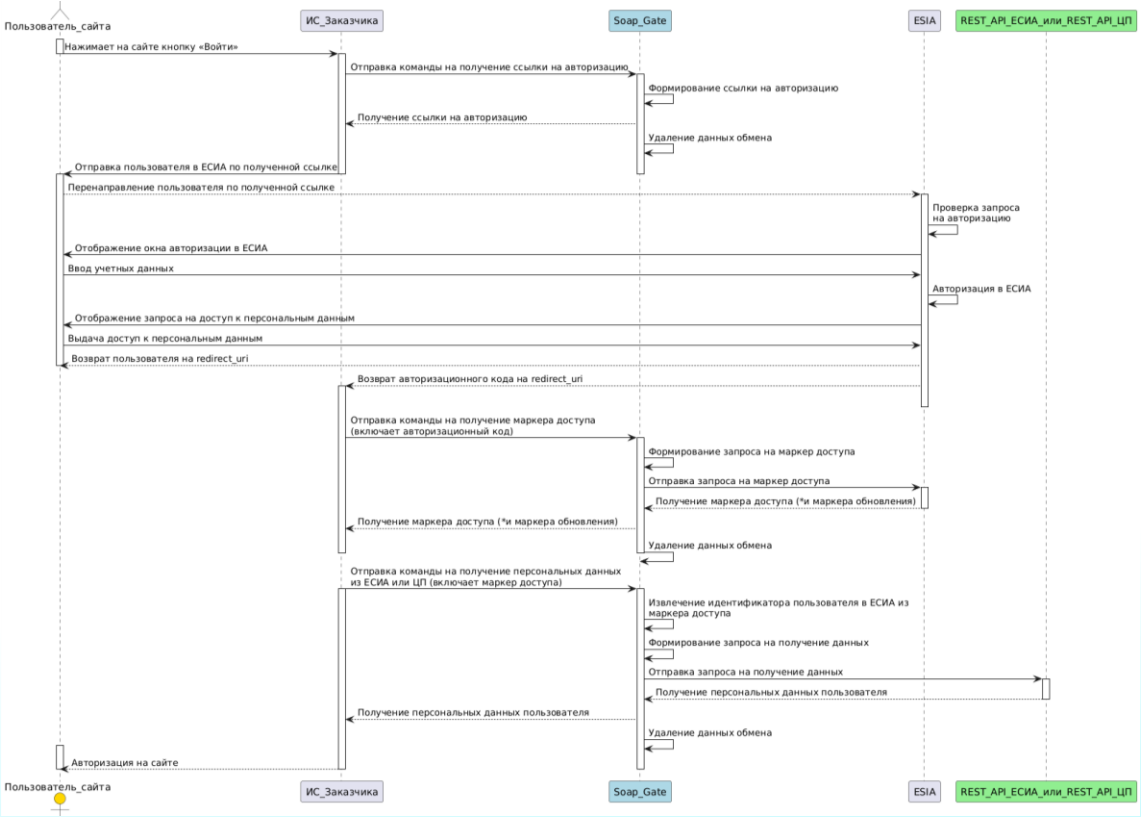
Виды маркеров в ЕСИА

- Маркер идентификации
- Маркер доступа
- Маркер обновления

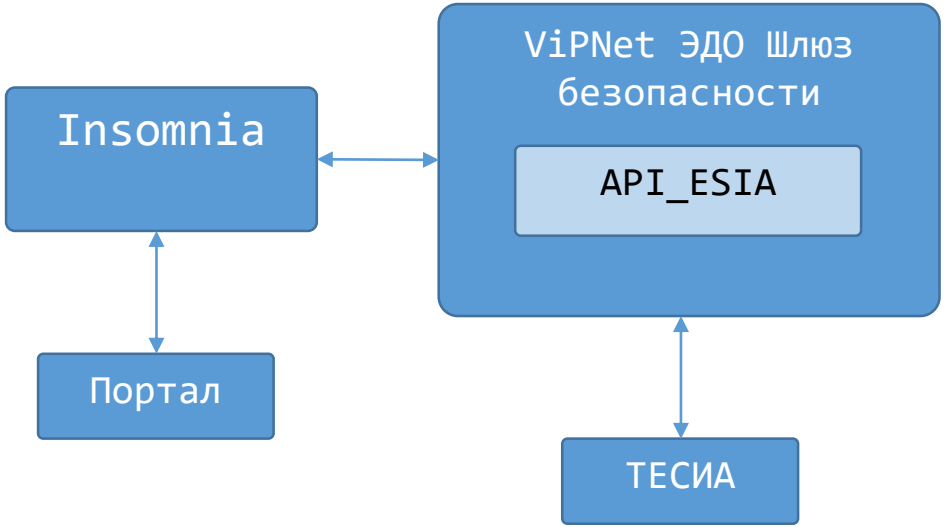
Диаграмма авторизации в ЕСИА



Авторизация в ЕСИА с запросом ПД



Состав стенда



- **ViPNet ЭДО Шлюз безопасности**
- **API_ESIA**
  Отдельный модуль в составе ViPNet ЭДО Шлюз безопасности
- **Тестовый контур ЕСИА**
- **Insomnia (эмулятор ИС организации)**
- **Портал ИС организации**

ViPNet EDI для ЦПГ и ЦПО

ТехноФест infotecs

Цифровые профили: ЦПГ и ЦПО

- актуальные и проверенные сведения о гражданине и организации, содержащиеся в ЕСИА;
- распределенная структура данных, содержащая ссылки на данные, которые формируются по запросу в соответствующих государственных реестрах;
- возможность управления выданными гражданином и организацией цифровыми согласиями на обработку данных, полученных из цифрового профиля с помощью сервиса по управлению согласиями (платформа согласий).

ViPNet EDI Soap Gate

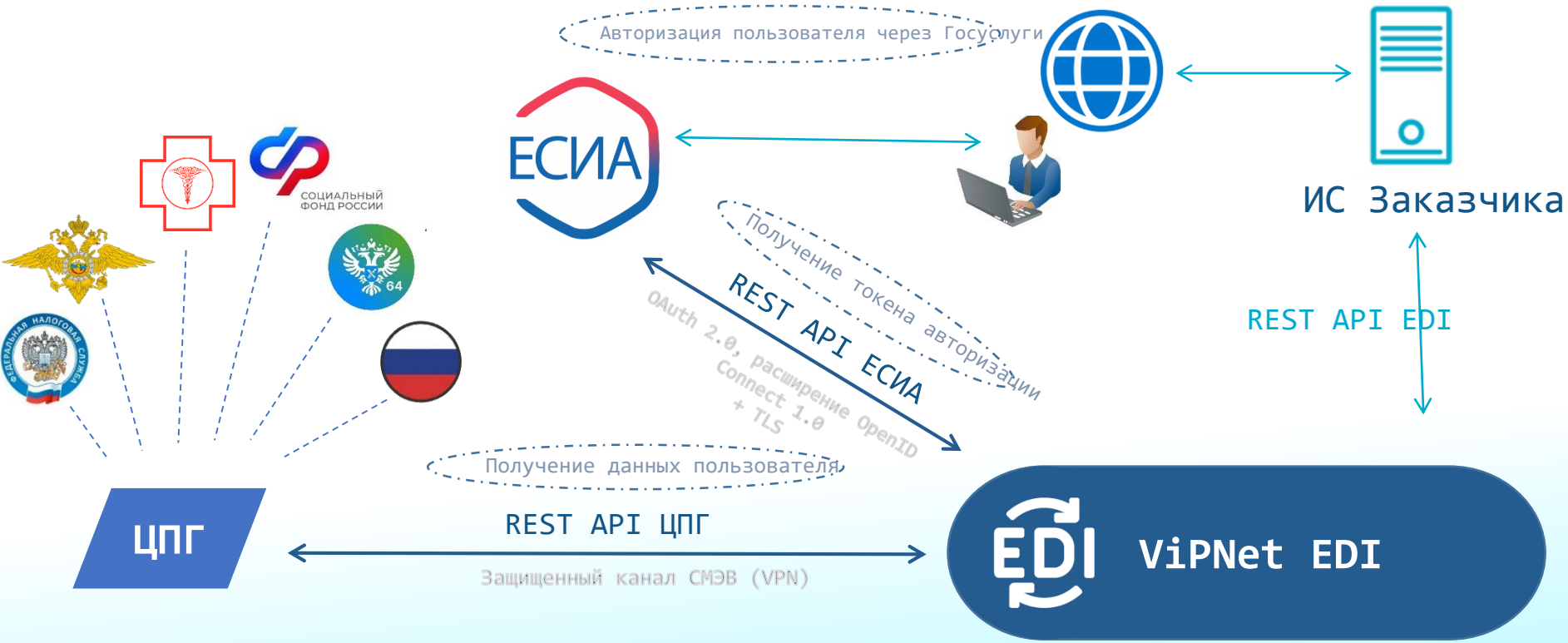
Цифровой Профиль Гражданина

- авторизация в ЕСИА (VA КС1)
- получение данных через СМЭВ (офлайн) (ПАК КС3)
- получение данных через API ЦПГ (онлайн и офлайн) (ПАК КС3)

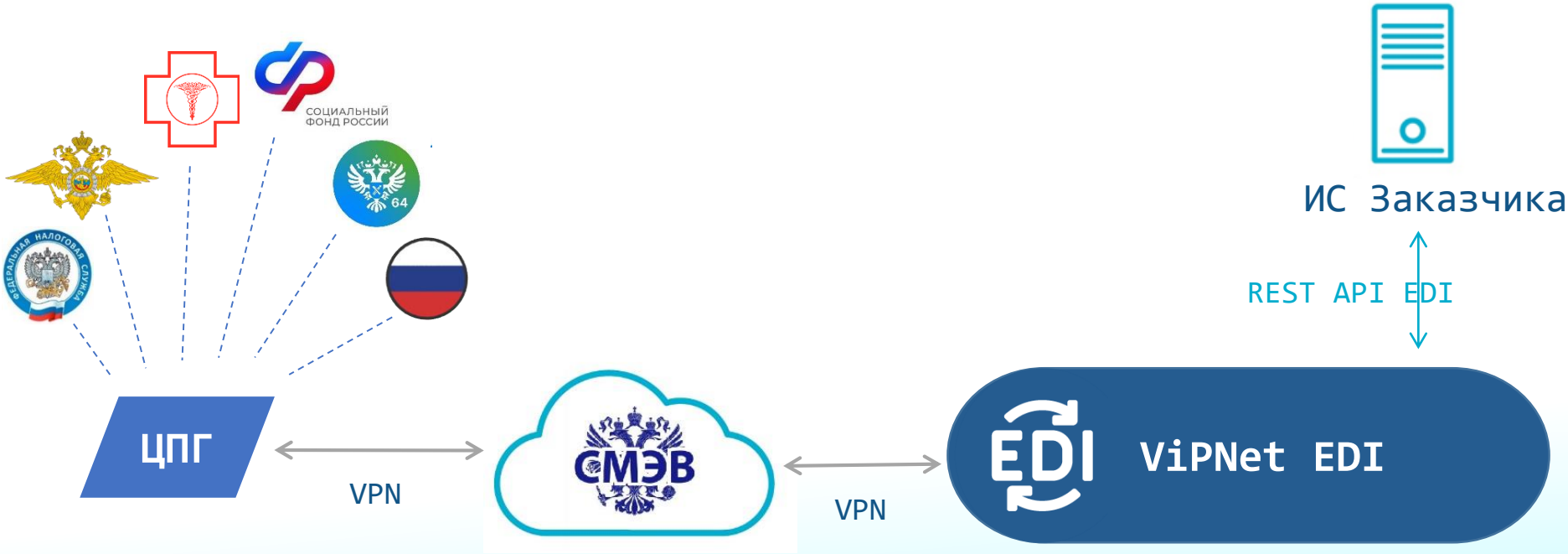
Виды сведений ЦПГ в СМЭВ3

- Запрос согласий пользователя ЕСИА от организации
- Запрос перечня согласий пользователя ЕСИА, выданных организации
- Запрос персональных данных пользователя ЕСИА при наличии его согласия
- Отправка в организацию уведомления о событии платформы согласий ЕСИА
- Извещение подписанных информационных систем об изменениях в учётных записях пользователей ЕСИА

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



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



ViPNet EDI Soap Gate

Цифровой Профиль Организации

- получение данных через СМЭВ

Виды сведений ЦПО в СМЭВ3

- Запрос согласий на получение данных организаций и индивидуальных предпринимателей, зарегистрированных в ЕСИА
- Извещение подписанных информационных систем о событиях платформы согласий бизнеса
- Предоставление данных организаций и индивидуальных предпринимателей, зарегистрированных в ЕСИА, при наличии согласия на получение данных
- Извещение подписанных информационных систем о событиях платформы согласий бизнеса

Преимущества ViPNet EDI

Соответствует требованиям регулятора за счет применения сертифицированных СКЗИ и средств ЭП по классу КС3

Подходит для внедрения в рамках программы импортозамещения

Не требует знаний, опыта работы с протоколами СМЭВ3, отслеживания изменений в СМЭВ

Обеспечивает уровень защищенности обрабатываемой информации по классу КС3

Автоматизирует процесс запроса и предоставления сведений из БД государственных органов

Взаимодействие с ЕСИА по протоколу OpenID Connect в соответствии с Регламентом 2.47

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного