

Интеграция с ЕСИА, СМЭВ и ЦПГ и аттестация информационной системы – быстро и просто

Елена Новикова
Руководитель продуктового направления

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  ФЕСТ

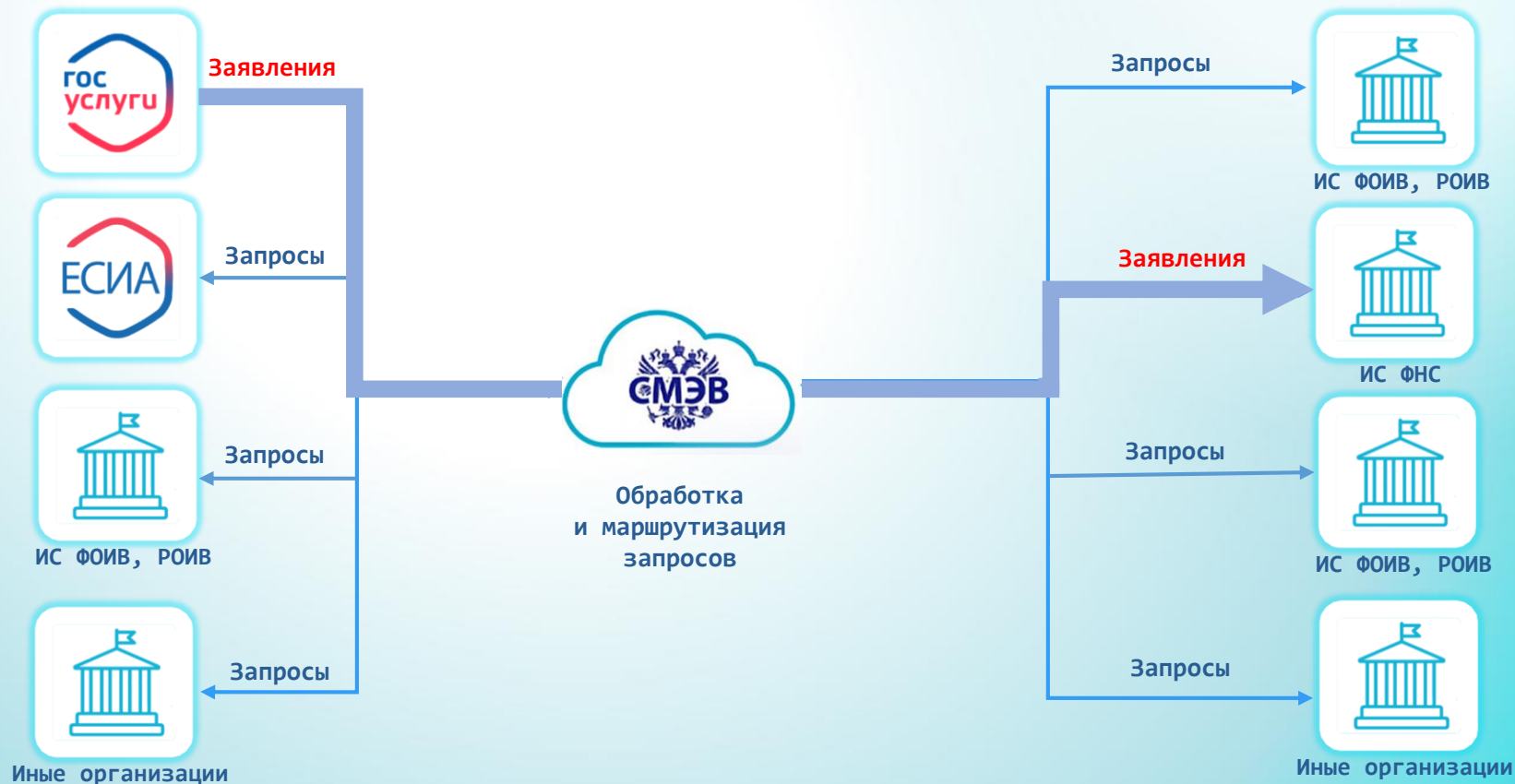
Зачем нужен СМЭВ?



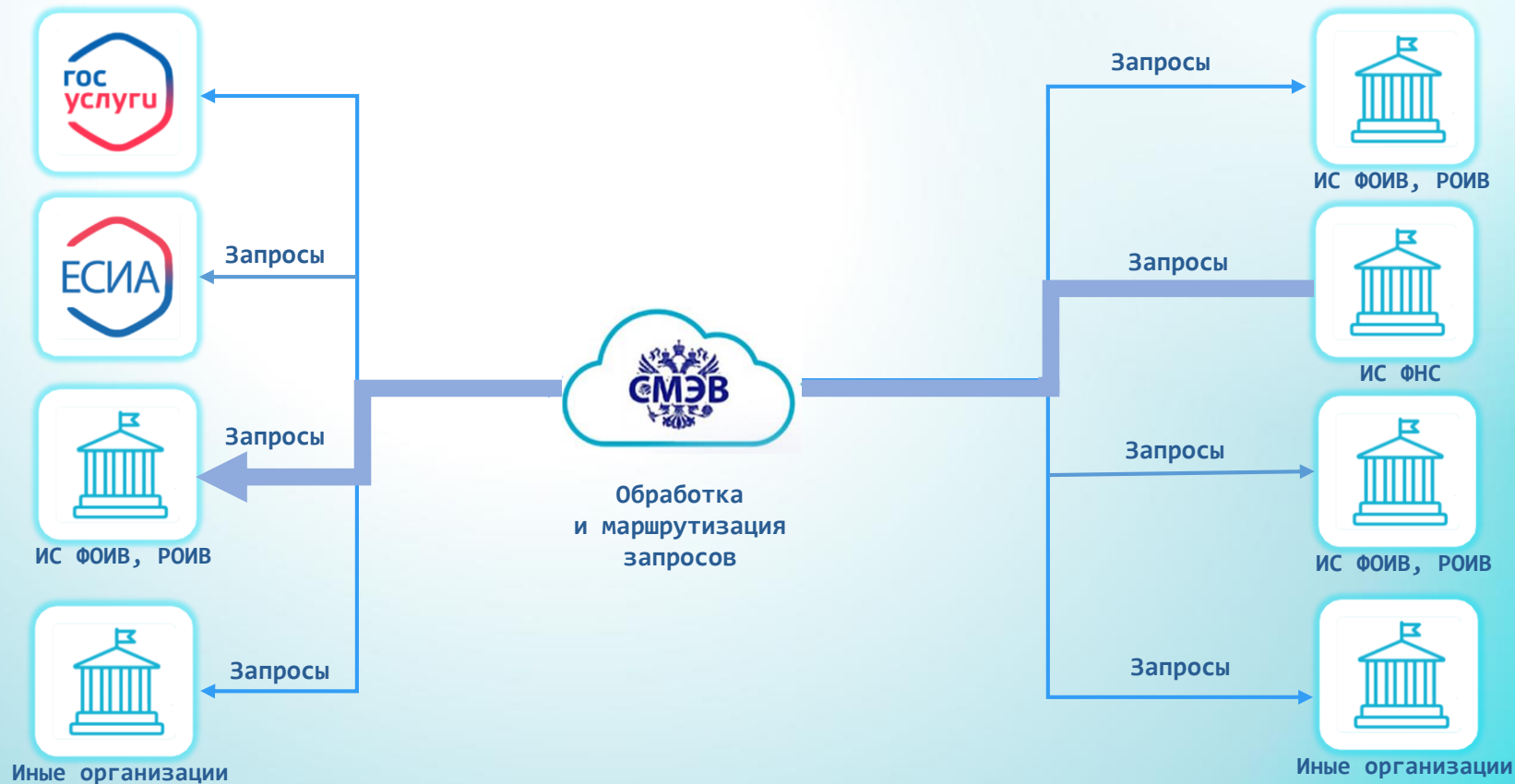
Оказание государственной услуги



Оказание государственной услуги



Оказание государственной услуги



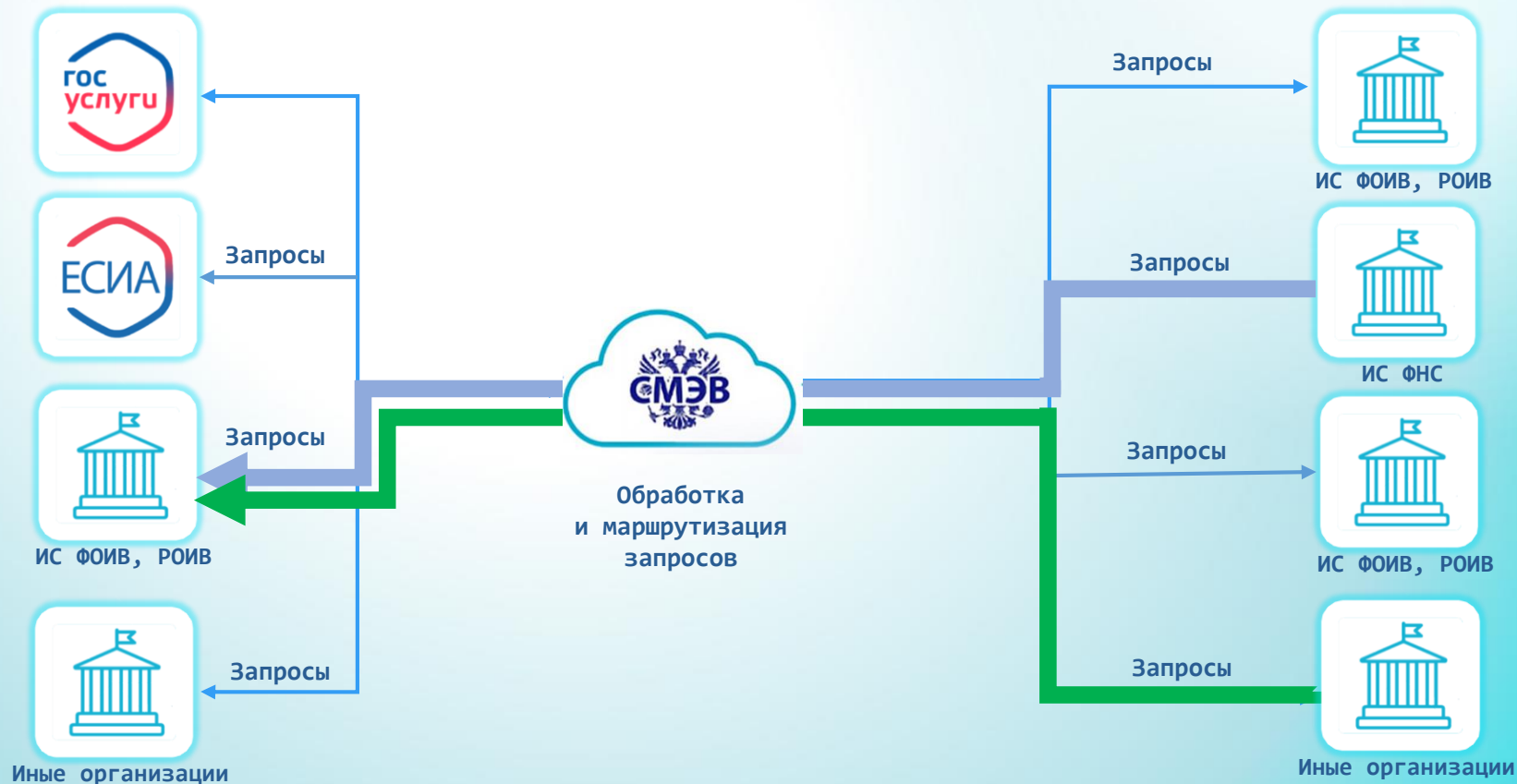
Оказание государственной услуги



Оказание государственной услуги



Межведомственное взаимодействие



Межведомственное взаимодействие

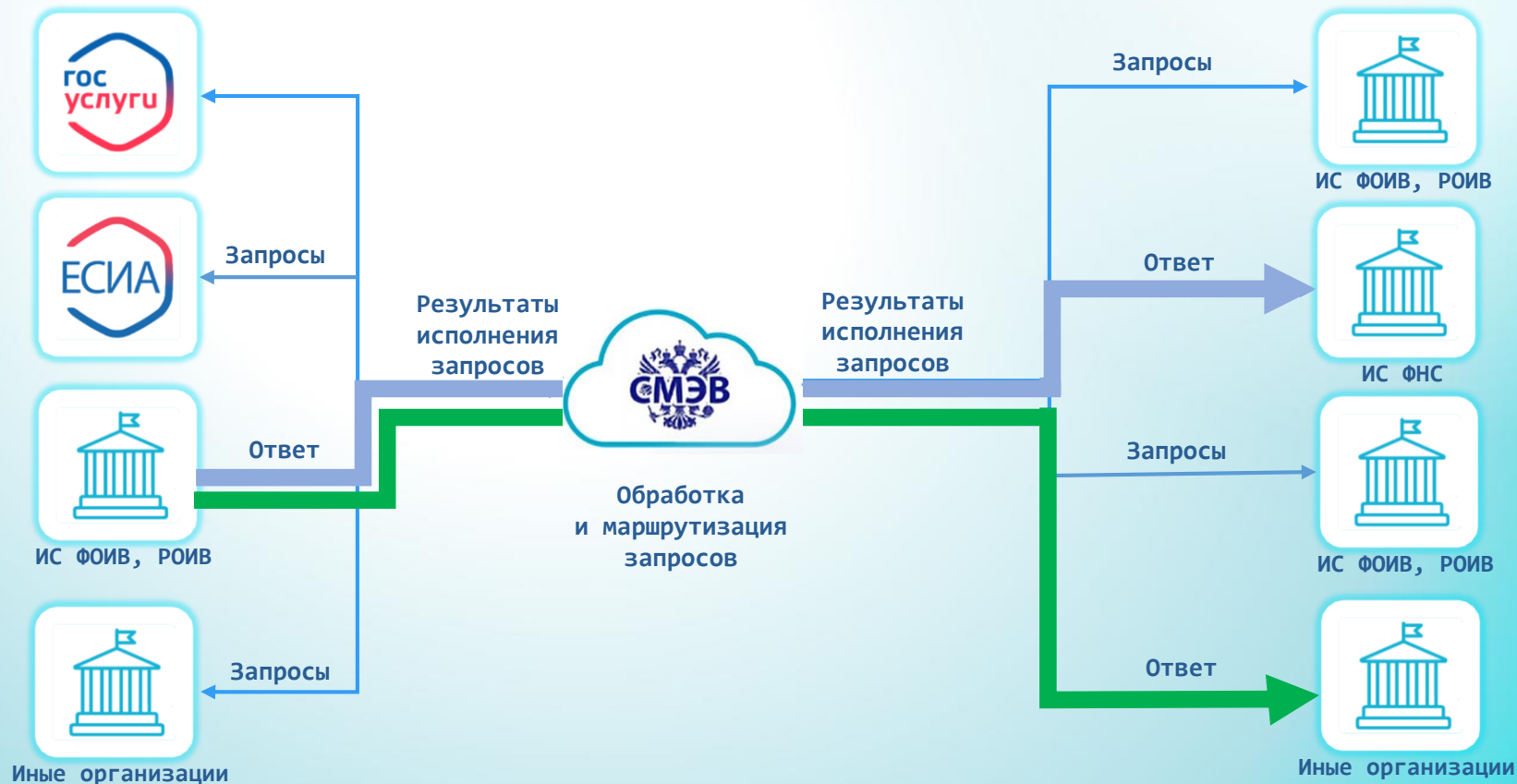
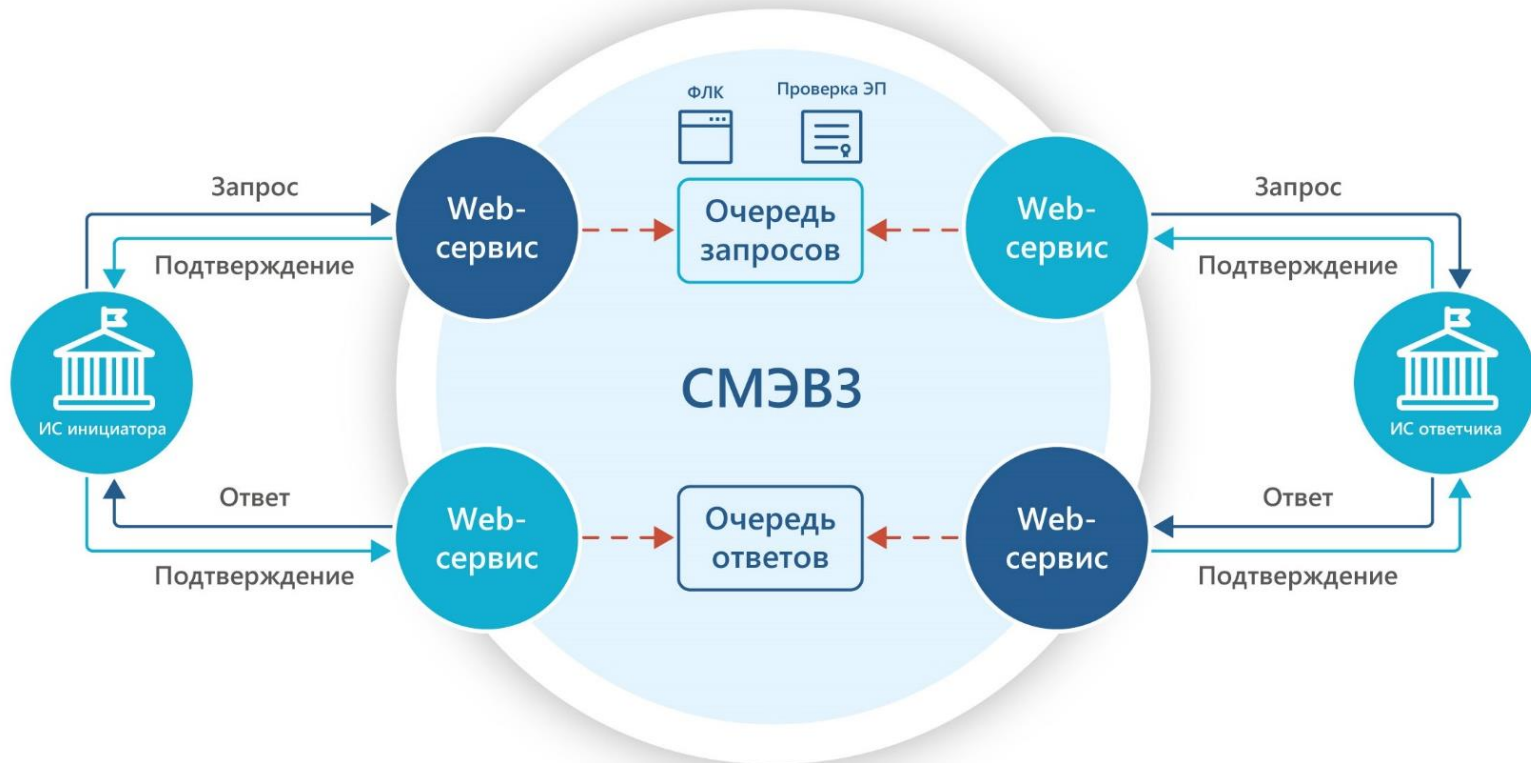
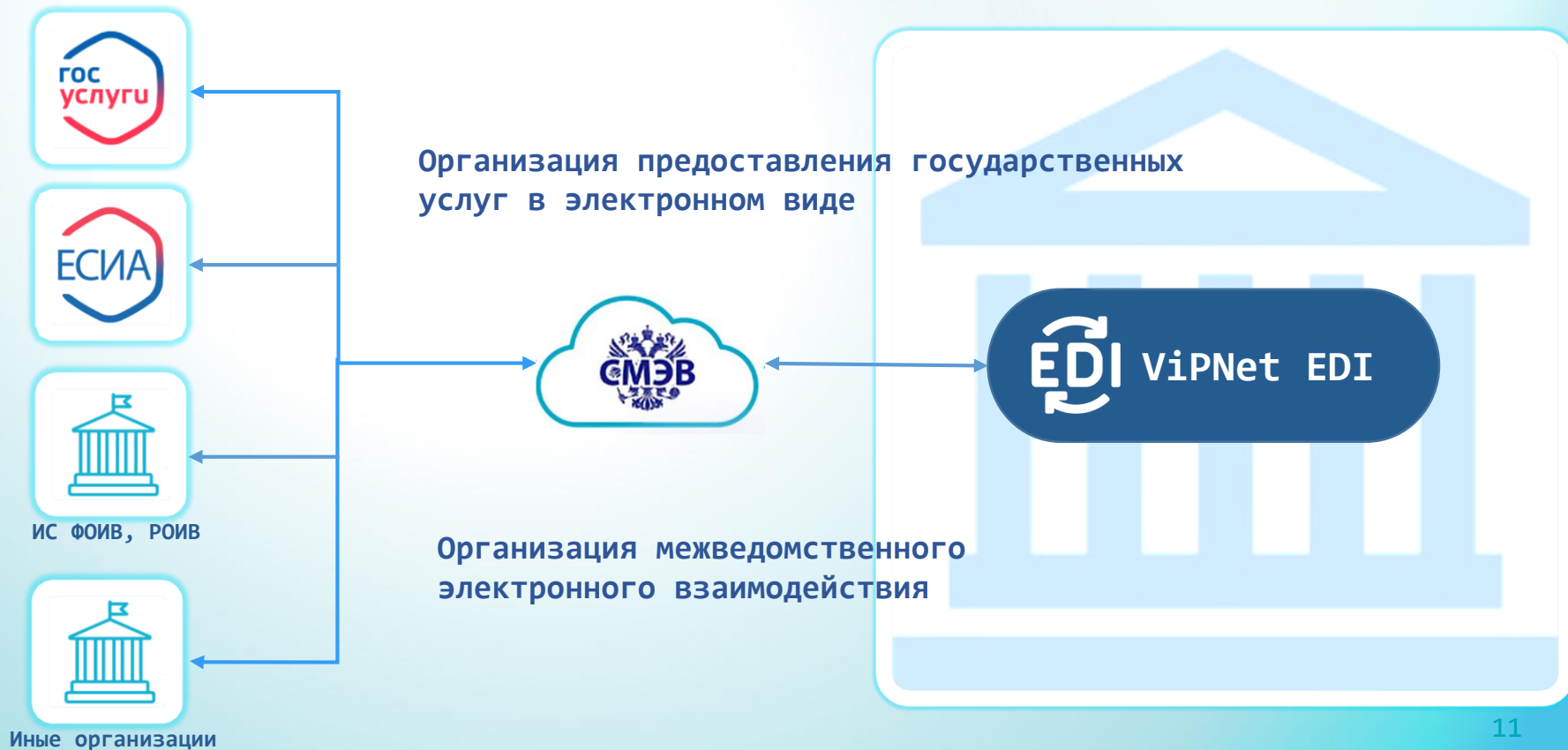


Схема работы СМЭВЗ



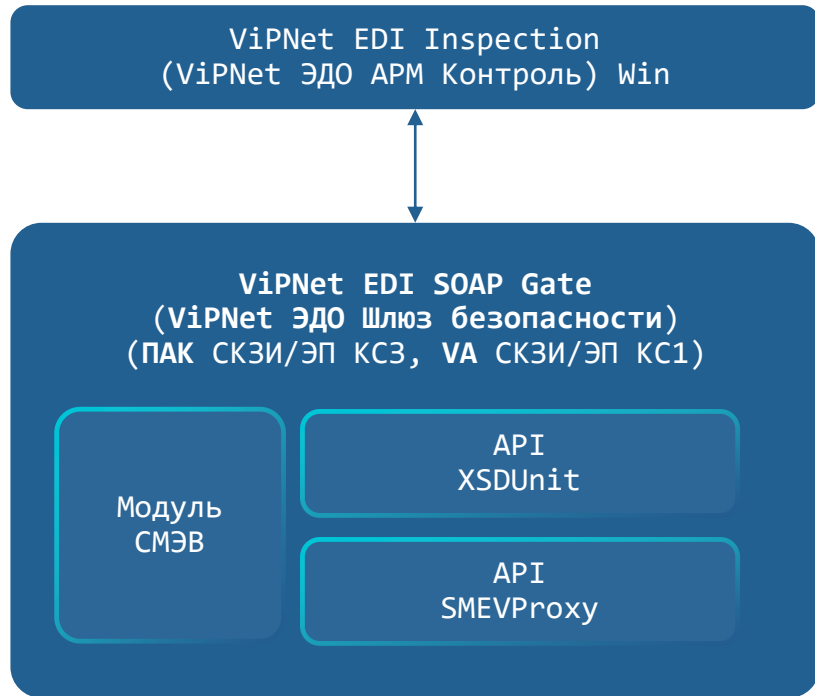
VipNet EDI





- работа с СМЭВЗ, схемы 1.1, .1.2, 1.3
- формирование SOAP-сообщения запроса в формате СМЭВ
- отправка SOAP-сообщения в СМЭВ
- получение ответного SOAP-сообщения из СМЭВ
- подписание SOAP-сообщения запроса ЭП организации (ЭП-ОВ), должностного лица (ЭП-СП)
- работа с файловым хранилищем СМЭВ (FTP для вложений) по S3
- механизм MTOM

Состав ViPNet EDI 3.5



ViPNet EDI Soap Gate (ПАК/VA)*

Лицензии расширения (модули для работы):

- Работа со СМЭВ3: XSDUnit (REST API)
- Работа со СМЭВ3: SMEVProxy (SOAP API)

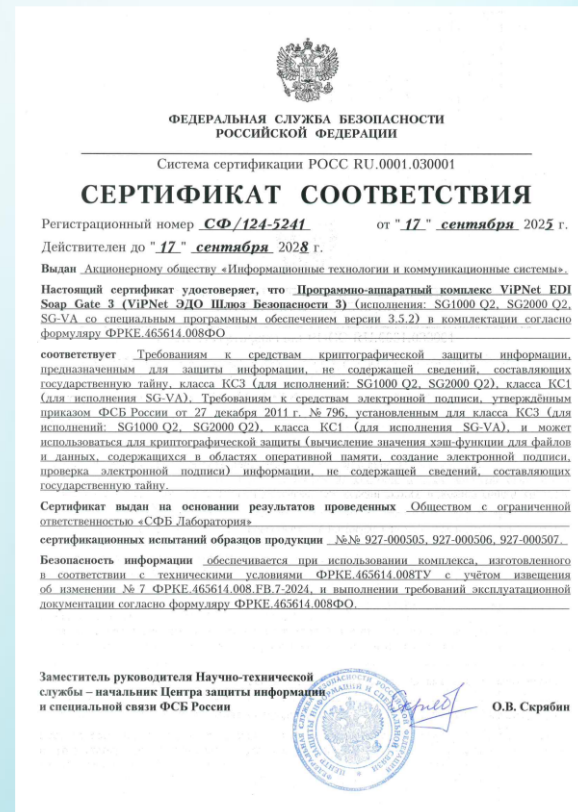
API

ИС Организации

ViPNet EDI Client
(ViPNet ЭДО АРМ Госуслуг) (СКЗИ/ЭП КСЗ)

ViPNet EDI Soap Gate 3.5

- ✓ Исполнение ПАК (СКЗИ и СЭП по классу КС3)
 - ViPNet ЭДО Шлюз безопасности SG1000 Q2
 - ViPNet ЭДО Шлюз безопасности SG2000 Q2
- ✓ Исполнение VA (СКЗИ и СЭП по классу КС1)
 - SG-VA – образ виртуальной машины в формате OVA или QCOW2
- ✓ Зарегистрирован в Едином реестре российских программ для ЭВМ и баз данных № 3276
- ✓ Зарегистрирован в Роспатенте
- ✓ Зарегистрирован в реестре Минпромторга
- ✓ Формирует и проверяет ЭП в соответствии с ГОСТ Р 34.10-2012





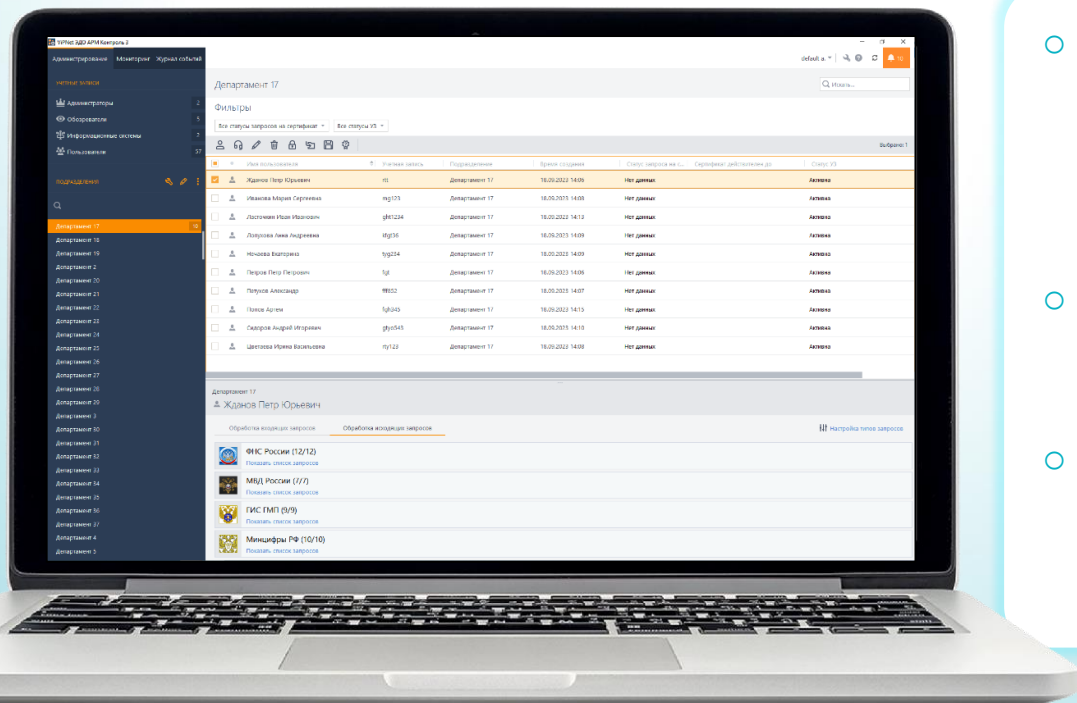
VipNet EDI Soap Gate 3.5

Криптошлюз для обмена
электронными сведениями
по каналам СМЭВ с применением
электронной подписи



- Прием и обработка заявлений на оказание услуг в электронном виде с ЕПГУ
- Формирование электронной подписи для отправляемых запросов и проверка электронной подписи входящих запросов
- Хранение истории запросов и ответов
- Передача вложений через СМЭВ 3.xx с использованием механизма МТОМ и файлового хранилища по протоколу S3
- Возможность создания и отправки запросов в режиме «Широковещательная рассылка»
- 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

ViPNet ЭДО АРМ Контроль- рабочее место администратора ViPNet EDI



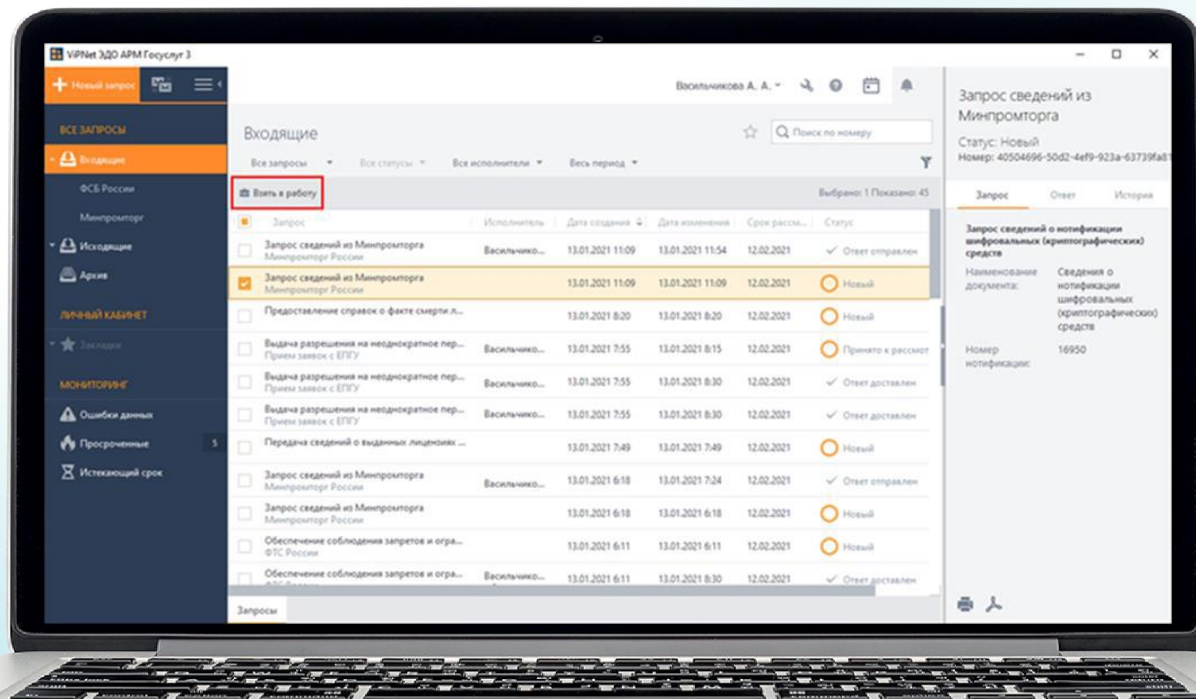
- Администрирование учетных записей пользователей, мониторинг и сбор статистики по запросам и ответам на запросы
- Зарегистрирован в Едином реестре российских программ для ЭВМ и баз данных № 146
- Исполнения:
 - -ОС Win
 - -ОС Lin (в 3.6)

ViPNet ЭДО АРМ Госуслуг- рабочее место пользователя ViPNet EDI

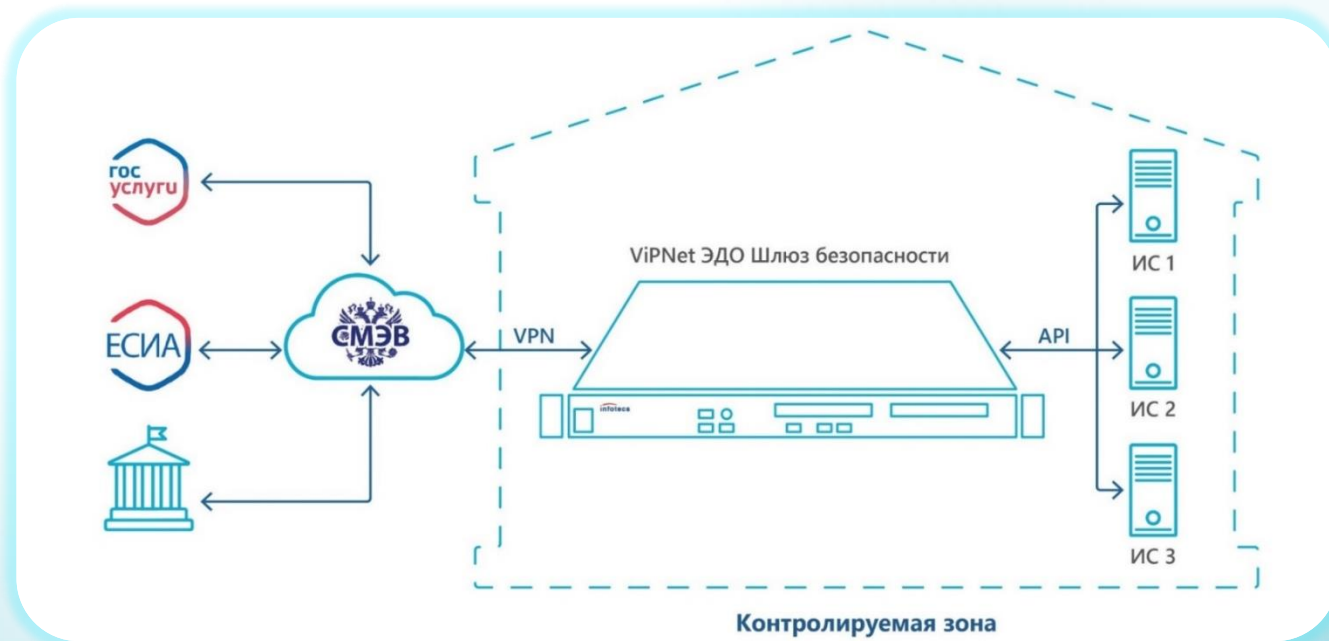
- ✓ принимать и обрабатывать заявления на оказание услуг в электронном виде с ЕПГУ;
- ✓ создавать, редактировать и отправлять запросы различным организациям, а также при необходимости заверять отправляемые запросы электронной подписью;
- ✓ получать доступ к централизованной базе данных, в которой хранятся запросы и ответы на запросы, полученные организацией;
- ✓ проверять электронные подписи на входящих запросах и ответах, что дает возможность работать только с проверенными данными;
- ✓ экспортировать созданные запросы или ответы на запросы в форматы PDF, XML;
- ✓ просматривать историю документооборота за настраиваемый период.



VIPNet ЭДО АРМ Госуслуг - рабочее место пользователя VIPNet EDI

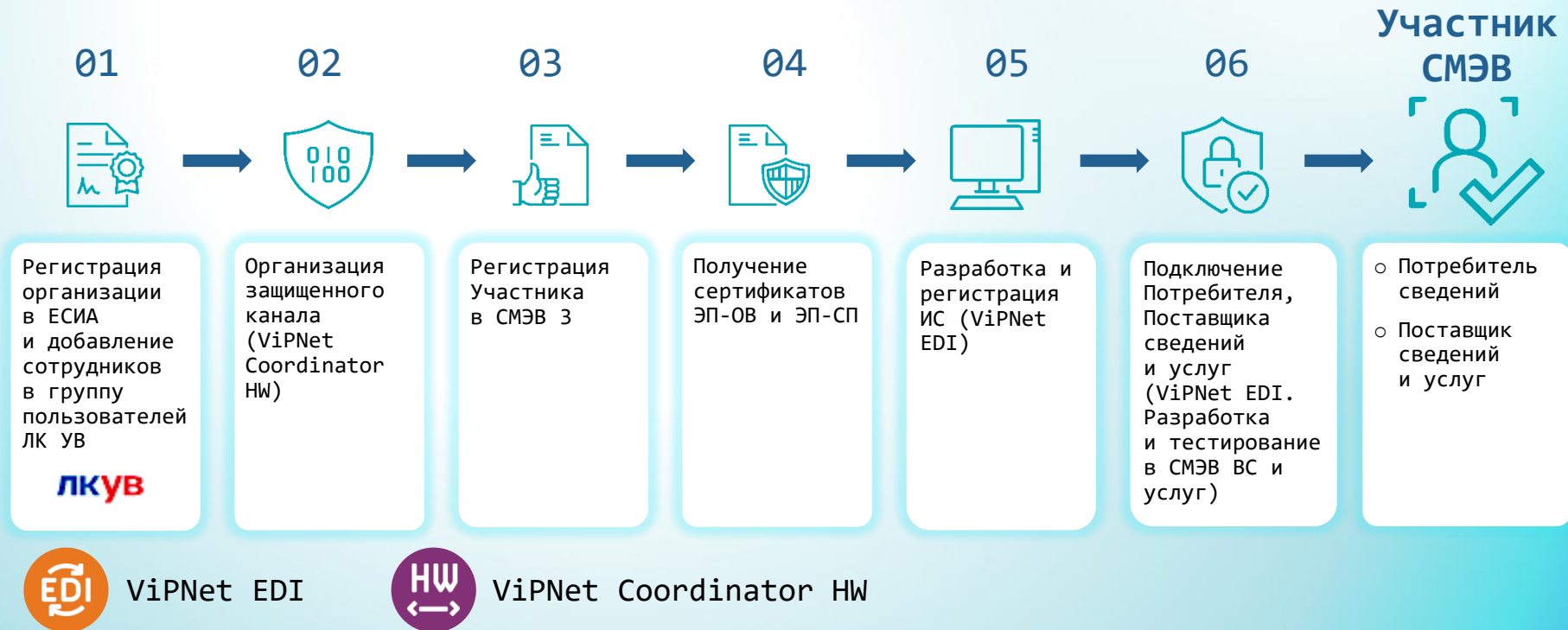


Работа ИС организации со СМЭВ



- Отказоустойчивость (кластеризация)
- Масштабируемость решения (можно несколько ПАК в одну систему объединить)
- Возможность подписи больших вложений (PKCS7)
- Быстрая подпись запросов (XML) до 3500 запросов (1 кб) в сек (4 потока)

Как стать участником СМЭВ*

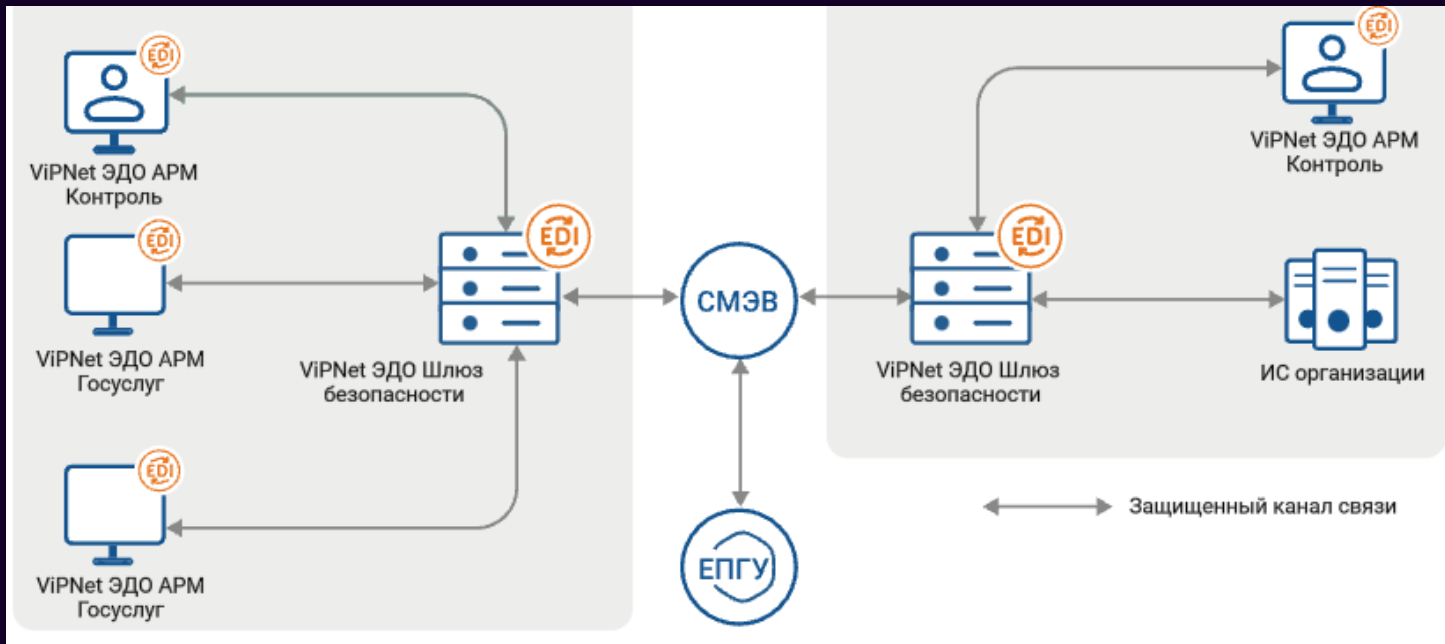


* https://info.gosuslugi.ru/articles/Что_необходимо_для_подключения_к_СМЭВ3/

Сценарии построения систем для работы со СМЭВ и ЕПГУ

Работа с запросами и ответами на запросы с помощью ViPNet ЭДО АРМ Госуслуг

Работа с запросами и ответами на запросы с помощью ИС организации



Интеграция ИС организации с ViPNet EDI Soap Gate для работы со СМЭВ

Сертифицированное решение, которое предоставляет **два** варианта API для быстрой интеграции со СМЭВ

XSDUnit (REST API)

Универсальный модуль для взаимодействия со СМЭВ, где мы сделаем за вас почти всё и даже чуть больше

SMEVProxy (SOAP API)

Прозрачный сервер для общения со СМЭВ, часть задач мы берём на себя

SMEVProxy (SOAP API)



Проксирует запросы в СМЭВ
Ничего не сохраняет

Масштабируемый

Позволяет увеличивать нагрузку
путем установки нескольких
одинаковых серверов

Самостоятельный опрос СМЭВ

Информационная система сама выполняет
каждый шаг в работе со СМЭВ

Для интеграции предоставляется
справочник разработчика с описанием
методов API

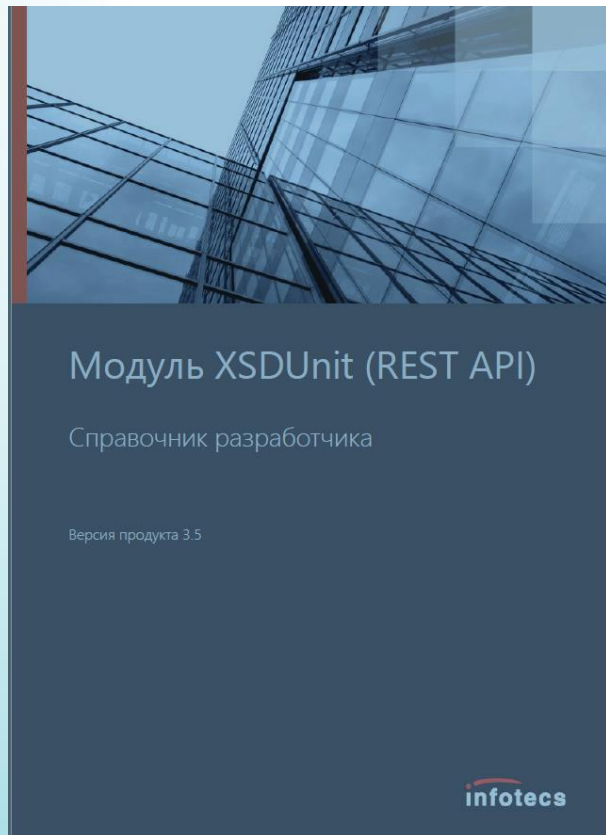
Диаграмма работы ИС УВ напрямую со СМЭВ для Потребителя сведений



Сценарии работы со SMEVProxy



XSDUnit (REST API)



Специально разработан для удобства интеграции

Проверка ФЛК

Сервер проверит данные на соответствие схеме запроса

Хранение информации о запросах

Все запросы хранятся на сервере

Администратор системы может просматривать историю с помощью ViPNet ЭДО АРМ Контроль

Автоматический опрос СМЭВ

Каждый этап работы со СМЭВ мы берем на себя, пользователь получает внутренний статус запроса и ответ на него

Для интеграции предоставляется справочник разработчика с описанием методов API

Виды сведений в СМЭВЗ*



Правила, по которым
формируются
запросы и ответы
(XSD)



Эталоны (XML)



Руководство
пользователя

* <https://lkuv.gosuslugi.ru/paip-portal/#/main>

Диаграмма работы ИС УВ со СМЭВ через XSDUnit



Схема XML-конверта сообщения в СМЭВ3

Для работы со СМЭВ3 информационная система организации должна сформировать конверт для отправки сообщения и загрузить файлы на файловое хранилище СМЭВ

Данные, передаваемые в СМЭВ

Техническая информация о запросе

Бизнес-данные запроса

ЭП-СП



Информация о вложениях

ЭП-ОВ



Загрузка вложений на FTP

Сборка конвертов сообщений с API

SMEVProxy

Данные, передаваемые в СМЭВ

Техническая информация о запросе

Бизнес-данные запроса

Электронная подпись
пользователя



Информация о вложениях

ЭП ОВ



Загрузка вложений на FTP

XSDUnit

Данные, передаваемые в СМЭВ

Техническая информация о запросе

Бизнес-данные запроса

Электронная подпись
пользователя



Информация о вложениях

ЭП ОВ



Загрузка вложений на FTP

*синим выделены блоки, формируемые в ViPNet EDI

Обязательность аттестация ИС для работы со СМЭВ

В соответствии с действующей редакцией документа “Требования к сети передачи данных участников информационного обмена” от 26.04.2024, пункт 4.5 гласит: **“Доступ к СМЭВ предоставляется участникам межведомственного взаимодействия при наличии подтверждения выполнения в информационной системе участника межведомственного взаимодействия предъявленных к ней требований по защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).”**

1

Соответственно, **необходимо аттестовать ИС как автоматизированную систему в соответствии с этими требованиями.** Например, в соответствии правилами аттестации для систем, не содержащих сведения составляющие Гостайну, определенные в приказе ФСТЭК России № 77 от 29.04.21 г.

2

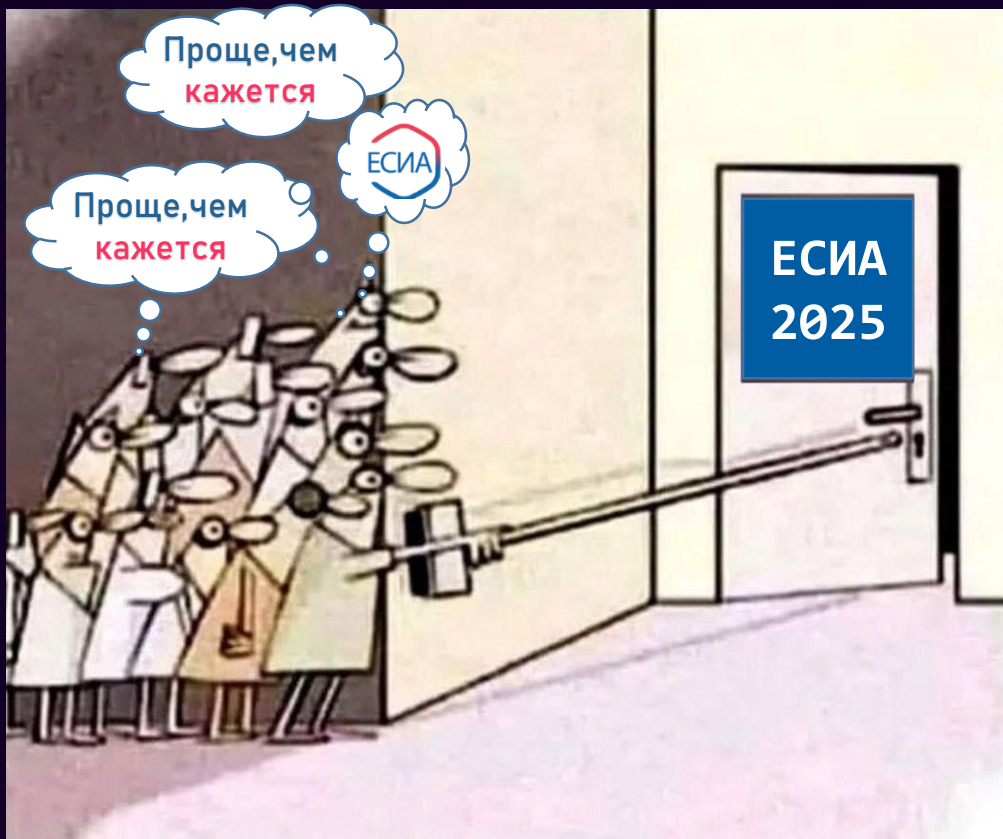
Пункт 1, сноска 1 Приказа 77, гласит: “Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17, с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. N 27 , приказом ФСТЭК России от 28 мая 2019 г. N 106, приказом ФСТЭК России от 27 апреля 2020 г. N 61.”

3

Соответственно аттестация происходит с учётом требований, таких же, какие предъявляются к сертификации в части СЗИ.

4

Немного юмора)



ГОСУСЛУГИ
Проще, чем кажется

ЕСИА

ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

gosuslugi.ru

Новые требования ЕСИА*

с 01.07.2025

для вновь подключаемых ИС

с 01.01.2027

для ранее подключенных ИС

**Приняты Протоколом Президиума Правкомиссии от 18.07.2024 № 26пр утвержден действующий Регламент подключения к Инфраструктуре электронного правительства и Методические рекомендации ЕСИА.*

Регламент подключения к ИЭП 2.47 и Методические рекомендации ЕСИА 3.48 поэтапно вводят новые требования к подключению информационных систем к федеральной инфраструктуре электронного правительства и ЕСИА

1. Требования к используемым средствам СКЗИ
2. Требования к подключаемой информационной системе
3. Требования к реализации взаимодействия с ЕСИА
4. Организационные требования

1. Требования к используемым СКЗИ

Для формирования ЭП должно применяться СКЗИ класса КСЗ

Пункт 9.1 Регламента:

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

- наличие действующего сертификата ФСБ России у средства ЭП (название в соответствии с эксплуатационной документацией (формуляром) на изделие, номер сертификата, его срок действия и класс СКЗИ указываются заявителем);
- класс средства ЭП не ниже КСЗ. ".

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

- **Пункт 9.1 Регламента:** «При организации канала связи до тестовой среды ЕСИА должен применяться канал, защищенный с использованием протокола TLS».
- **Пункт 10.1 Регламента:** «Подключение к промышленной среде ЕСИА допускается только с использованием сертифицированных ФСБ России средств защиты канала связи класса не ниже КСЗ».

2. Требования к ИС организации

Защищенность ИС должна быть уровня УЗ.3+

Пункт 9.1 Регламента: «При необходимости получения персональных данных уровень защищенности персональных данных подключаемой системы должен быть УЗ.3 и выше».

Канал работы ИС с ЕСИА и с пользователями должен быть защищен с использованием СКЗИ класса КСЗ

Пункт Д1.6 МР: «Все каналы связи на участке взаимодействия «ЕСИА-ВИС», выходящие за пределы контролируемых зон участников взаимодействия, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, удовлетворяющих установленным требованиям к средствам криптографической защиты информации класса не ниже КСЗ».

Серверная часть ВИС должна поддерживать возможность взаимодействия с пользователями по протоколу TLS, реализованному с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КСЗ на стороне ВИС (сервера) и КС1 на стороне пользователя (клиента)".

Используемые в ИС СЗИ должны быть уровня доверия 5+

Пункт Д1.5 МР: «Все используемые средства защиты информации должны быть сертифицированы ФСТЭК России и соответствовать уровню доверия не ниже 5 или должны быть сертифицированы ФСБ России».

ИС должна быть аттестована по требованиям ИБ

Пункт 10.1 Регламента: «Решение о подключении ИС к промышленной среде ЕСИА принимается Минцифры России, в том числе, на основании следующих сведений:

сведения об оценке эффективности реализованных мер по обеспечению безопасности информации подключаемой информационной системы, осуществленной в порядке, установленном законодательством Российской Федерации, и проведенной с привлечением организации, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации".

3. Требования к интеграции с ЕСИА

Реализация интеграции с ЕСИА должна пройти оценку влияния на СКЗИ

Пункт 10.1 Регламента: «В случае выбора заявителем варианта реализации подсистемы идентификации, аутентификации OpenID Connect с использованием собственного технического решения <...> заявитель должен провести процедуру оценки влияния на СКЗИ, применяемое в составе технического решения, согласно требованиям (или положениям) эксплуатационной документации на СКЗИ с привлечением испытательных лабораторий, аккредитованных ФСБ России, в соответствии с требованиями действующего законодательства».

Реализация OpenID Connect должна быть согласована с Минцифры и проверена на корректность реализации в ФСБ России

Пункт 10.1 Регламента: «Техническое задание на создание такого технического решения в части реализации протокола OpenID Connect при взаимодействии с ЕСИА должно быть согласовано Минцифры России».

Пункт Д1.3 МР: «Реализуемый в собственном техническом решении протокол на базе OpenID Connect 1.0 и OAuth2.0, должен соответствовать описанию и схемам, приведенным в Приложение Б (за исключением разделов, рекомендованных к выводу из эксплуатации). Безопасность реализации протокола должна быть подтверждена в установленном порядке в соответствии с действующими нормативно-правовыми актами».

4. Обязательность аттестации ИС организации для работы с ЕСИА

В соответствии с действующей редакцией документа “РЕГЛАМЕНТ ЕДИНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ” версия 2.47, раздел “Обозначения и сокращения” содержит следующую информация: “Шлюзовой модуль (API Gateway) Компонент, обеспечивающий взаимодействие ИС коммерческой организации с ЕСИА и ЕПГУ, прошедший сертификационные исследования по требованиям информационной безопасности ФСТЭК России в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 03.04.2018 № 55”

Соответственно, необходимо сертифицировать ИС в соответствии с этими требованиями.

Так как в ИС применяется средства контейнеризации, то необходимо привести системное окружение в соответствие с требованиями приказа №118 ФСТЭК России, информационных сообщений ФСТЭК России от 10 января 2025 г. № 240_24_39 и от 13 января 2025 года № 240_24_38.

Данные работы необходимо завершить в 2025 году.

В случае неисполнения данных требований, появляется риск отключения от ЕСИА в соответствии с нормами содержащимися в указанных документах. Например пункт 2, раздела I. Права и обязанности участника информационного взаимодействия, документа “Права и обязанности участника информационного взаимодействия” гласит: “Участник осознает, что нарушение требований и условий, содержащихся в настоящем разделе, повлечет отключение от сервисов и интерфейсов ЕСИА;”



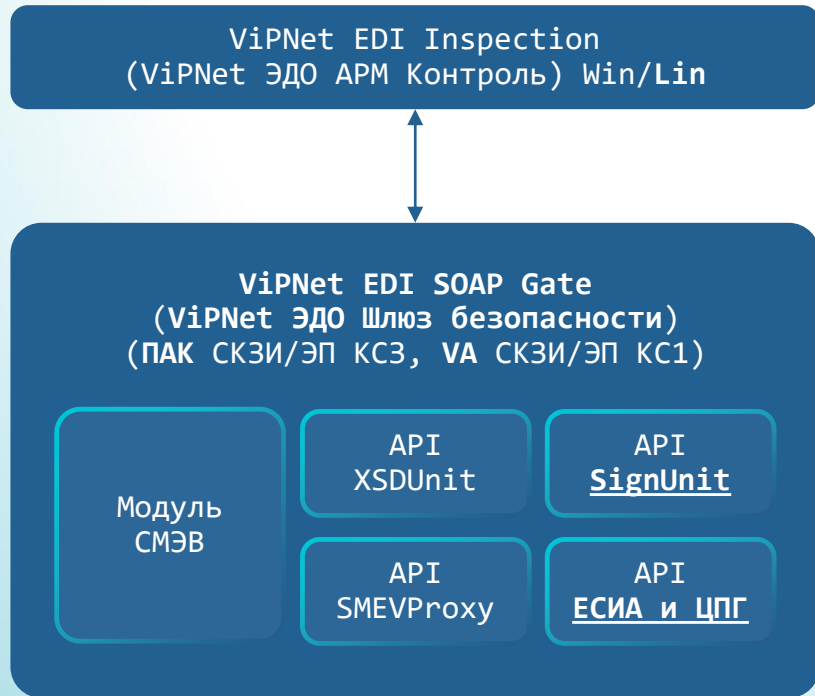
ПАК ViPNet EDI Soap Gate 3.6 (AI)

Криптошлюз для работы
с СМЭВ, ЕПГУ, 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

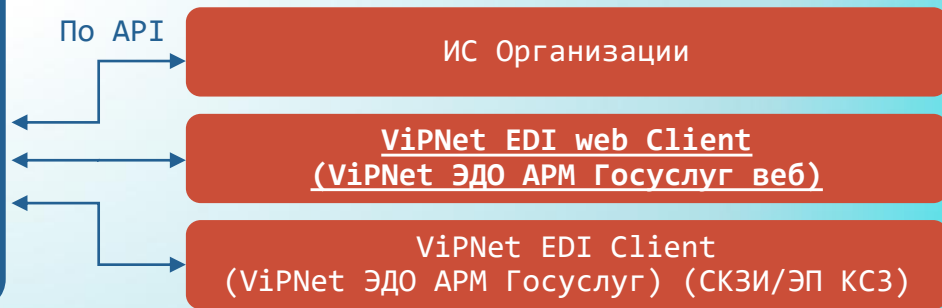


ViPNet EDI Soap Gate (ПАК/VA)*

Лицензии расширения (модули для работы):

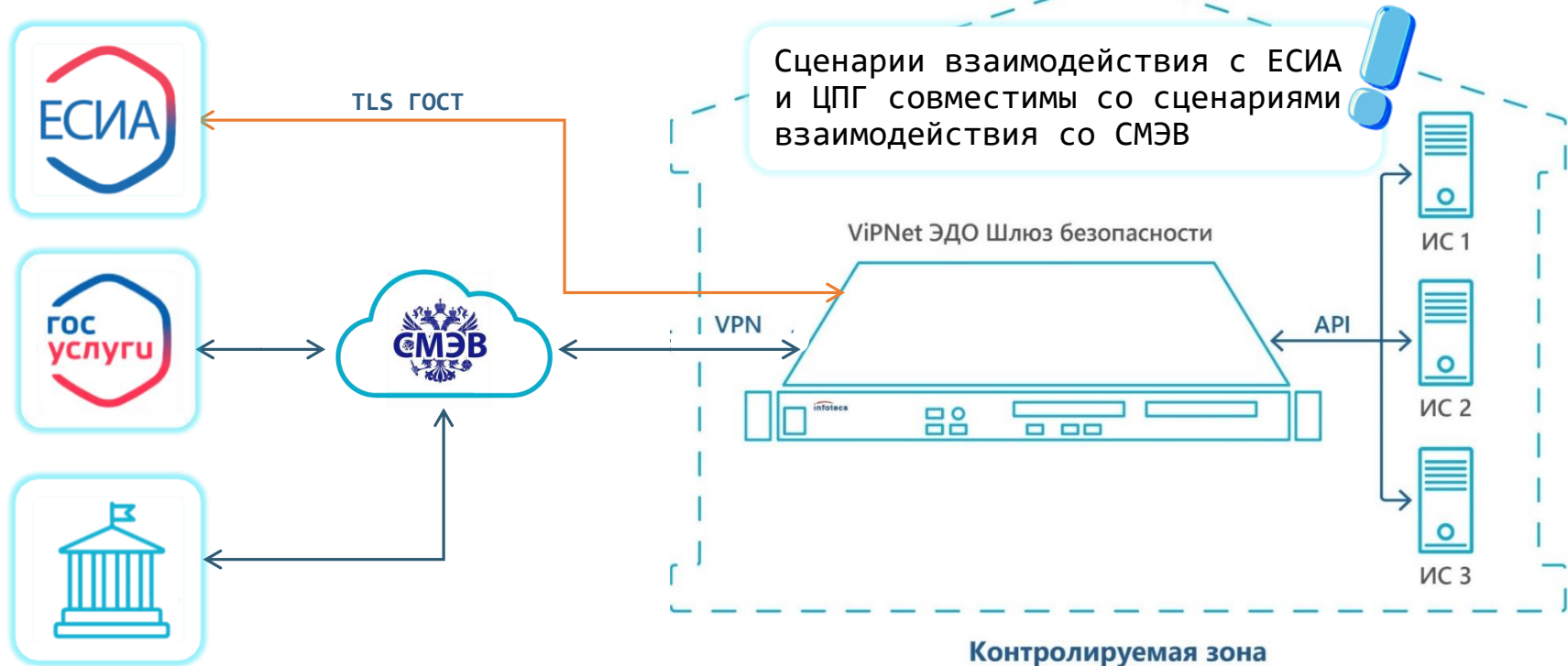
- Работа со СМЭВ3: XSDUnit (REST API)
- Работа со СМЭВ3: SMEVProxy (SOAP API)
- Сервис подписи: SignUnit
- Авторизация в ЕСИА
- Получение данных из ЕСИА
- Получение данных из ЦПГ

**лицензии расширения к ViPNet EDI Soap Gate опциональны*

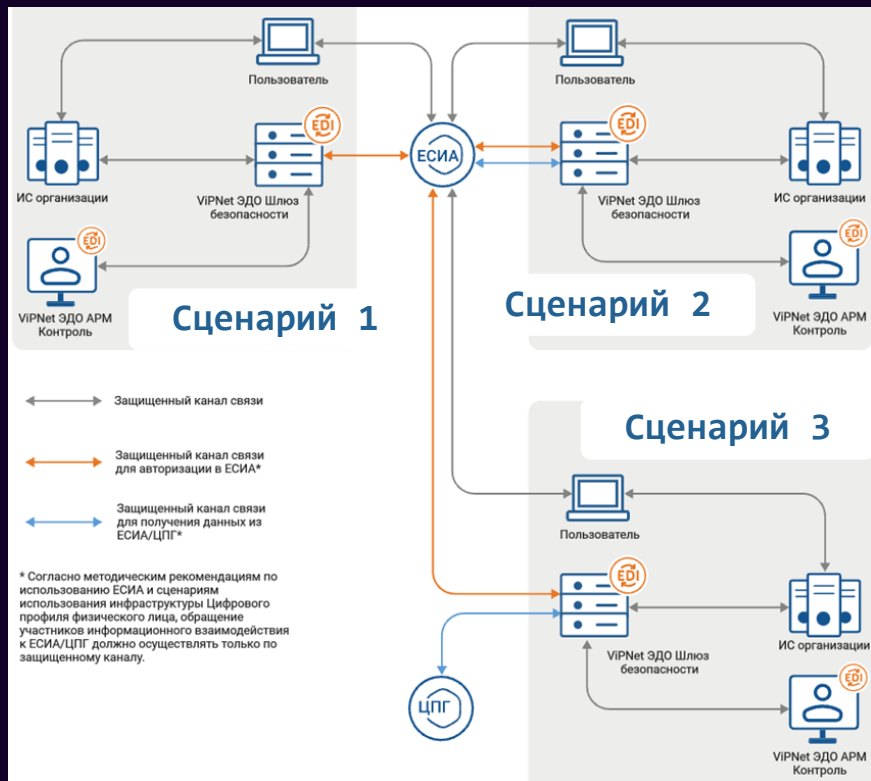


ViPNet EDI 3.6 (АИ проводится)

Работа со СМЭВ, ЕПГУ, ЕСИА, ЦПГ



Сценарии взаимодействия с ЕСИА и ЦПГ*



Сценарий 1

Авторизация пользователей ИС в ЕСИА

Сценарий 2

Авторизация пользователей ИС в ЕСИА и получение данных пользователей из ЕСИА

Сценарий 3

Авторизация пользователей в ЕСИА и получение данных пользователей из ЦПГ

**Формирование запросов и ответов осуществляется с помощью собственной информационной системы заказчика. Отправка запросов в ЕСИА, а также получение ответов на запросы производится с использованием ViPNet EDI Soap Gate 3.*

Преимущества ViPNet EDI



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



Подходит для внедрения в рамках программы импортозамещения



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



Обеспечивает уровень защищенности обрабатываемой информации по классу КСЗ



Автоматизирует процесс запроса и предоставления сведений из БД государственных органов



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

Технологическое партнерство*

1. Компании – разработчики собственных решений, где предполагается встраивание продуктов ИнфоТеКС (компонентов ViPNet, крипто-библиотек и других продуктов ViPNet)
2. Компании – разработчики аппаратных платформ и программных компонент, которые могут быть использованы в собственных продуктах ИнфоТеКС
3. Компании, участвующие в технологических испытаниях по проверке на совместимость своего продукта с продуктом ИнфоТеКС
4. Компании, предлагающие иные формы сотрудничества

*Отправить заявку:

<https://infotecs.ru/partners/become-technology-partner//>



Коммерческое партнерство*

1. Наличие на момент подписания партнерского соглашения действующих лицензий ФСБ России на распространение и обслуживание СКЗИ
2. Наличие в штате не менее двух обученных специалистов с действующими сертификатами администраторов ViPNet. Проведение обучения специалистов по курсу администратора ViPNet должно осуществляться в учебном центре компании ИнфоТеКС

*Отправить заявку:

<https://infotecs.ru/partners/become-commercial-partner/>



ТЕХНО infotecs Фест

Новикова Елена
Руководитель продуктового направления



NBJ НАЦИОНАЛЬНЫЙ
БАНКОВСКИЙ ЖУРНАЛ



РУТОКЕН
Бизнес-ПРАКТИК



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



PR integ

АТБ
ЭЛЕКТРОНИКА

infotecs
{-cademy}

m=rlion



Подписывайтесь
на наши соцсети,
там много интересного

