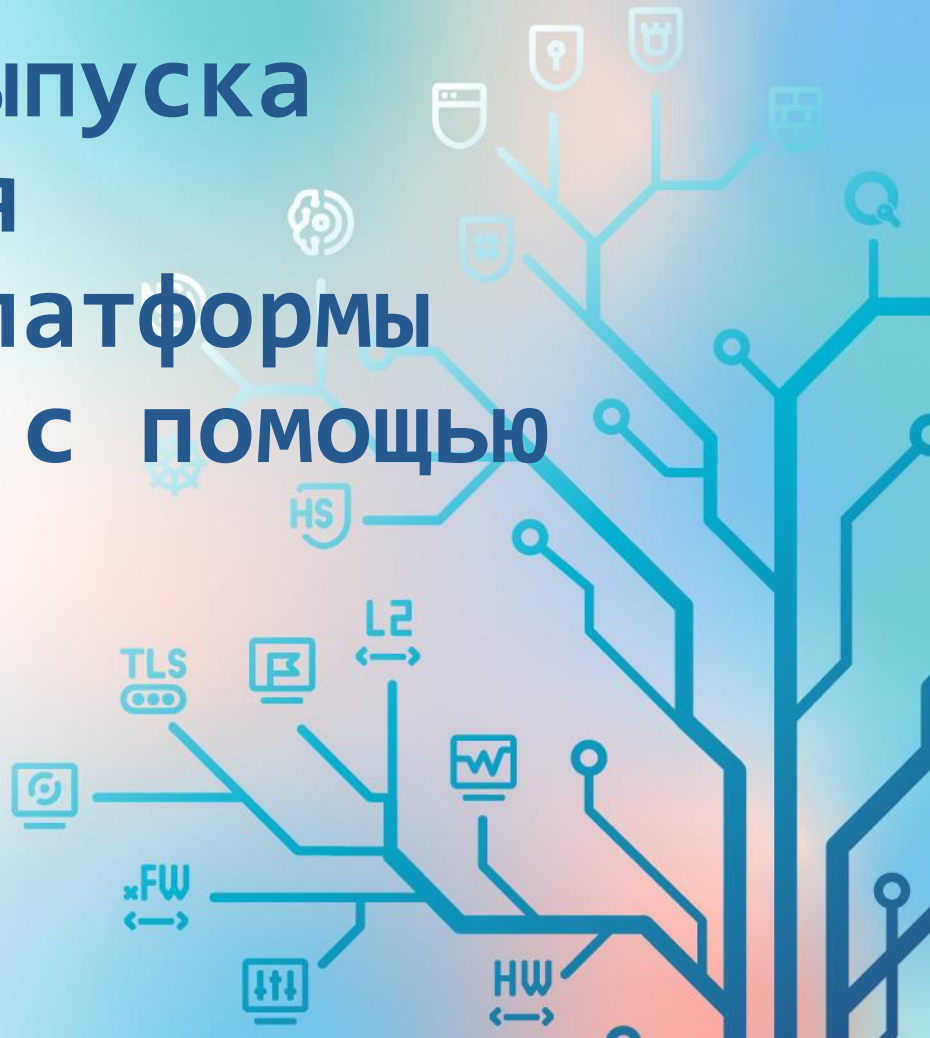
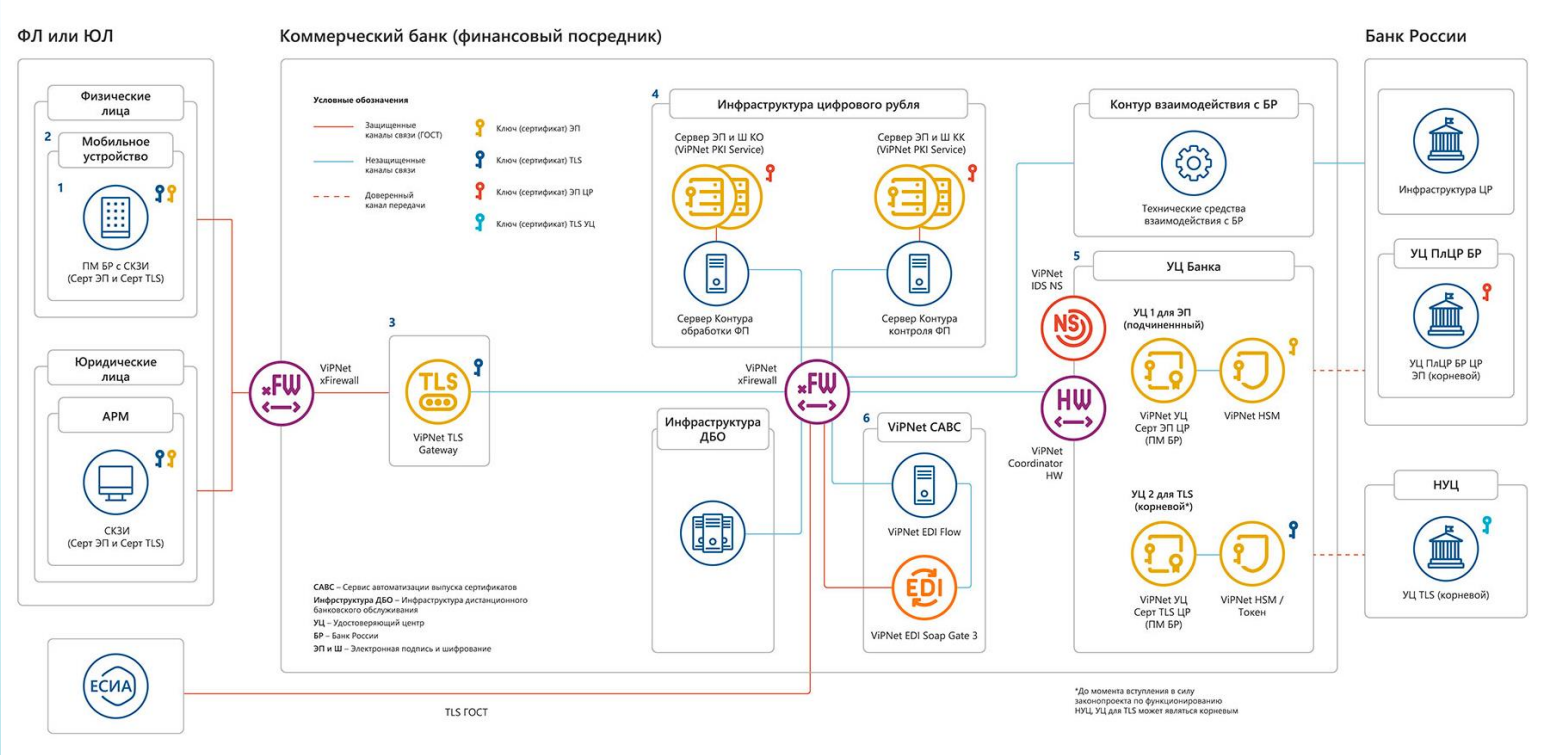
Автоматизация выпуска сертификатов для пользователей Платформы Цифрового рубля с помощью ViPNet CABC

Елена Новикова
Эмиль Капкаев

infotecs



Инфраструктура платформы ЦР



ViPNet САВС

Автоматизация процесса выпуска сертификатов

Безопасность данных:

- Обеспечение криптографической защиты информации
- Идентификация пользователя ПлЦР (ФЛ, ЮЛ и ИП)
  - проверки запросов пользователей ПлЦР на создание сертификатов (первичный/повторный)
  - проверки изданных сертификатов

Интеграция с существующими системами:

- Единой Системой Идентификации и Аутентификации (ЕСИА)
- Автоматизированными системами дистанционного банковского обслуживания (АС ДБО) банков
- Удостоверяющими центрами (ViPNet УЦ 4/5.x, УЦ КриптоПро 2.0)

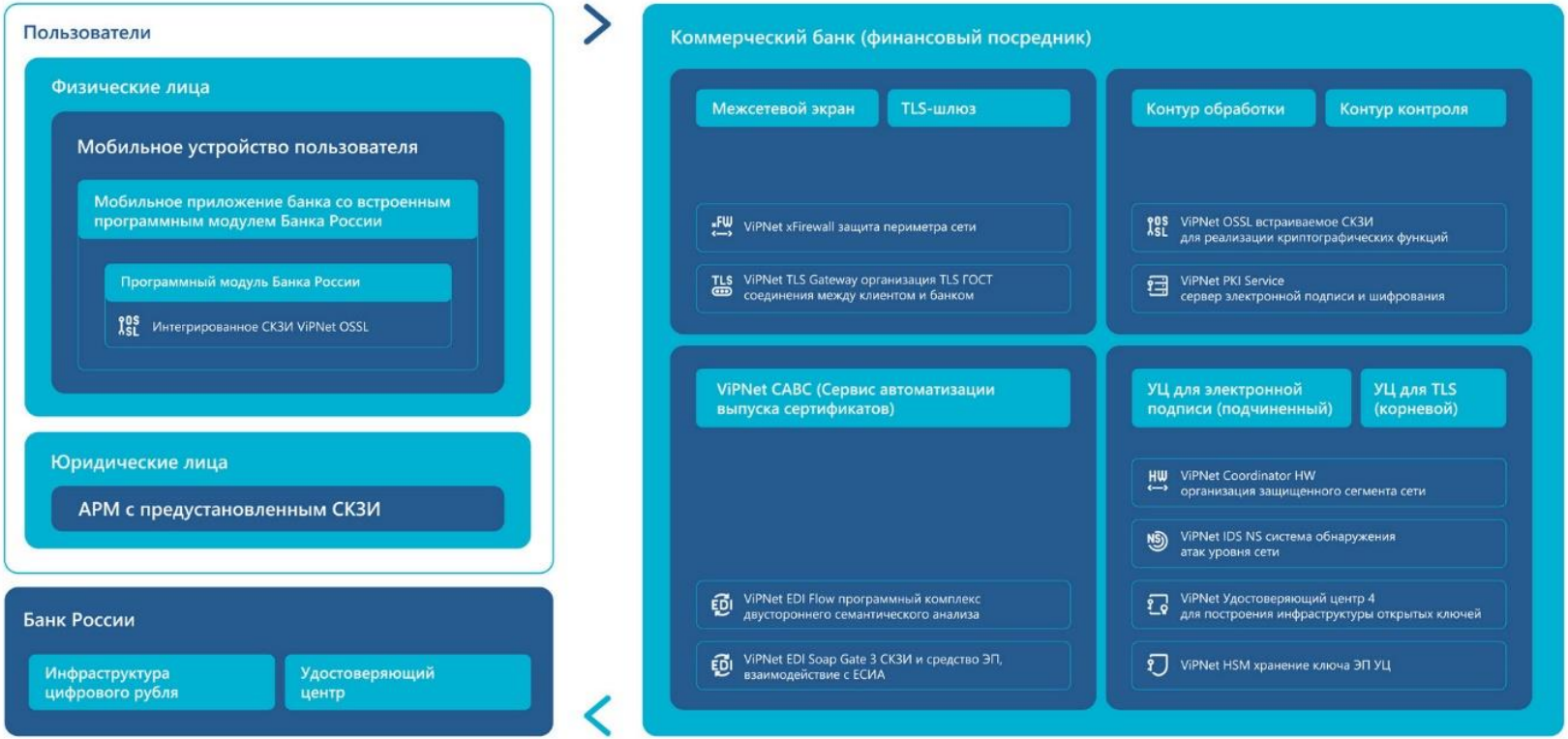
Актуальность сертификатов:

- Получение списков отозванных сертификатов и направление их в ПлЦР

Соблюдение нормативных требований:

- Соответствие требованиям нормативных документов регуляторов

Продукты ViPNet для платформы ЦР



Состав ViPNet CABC 1.0

infotecs

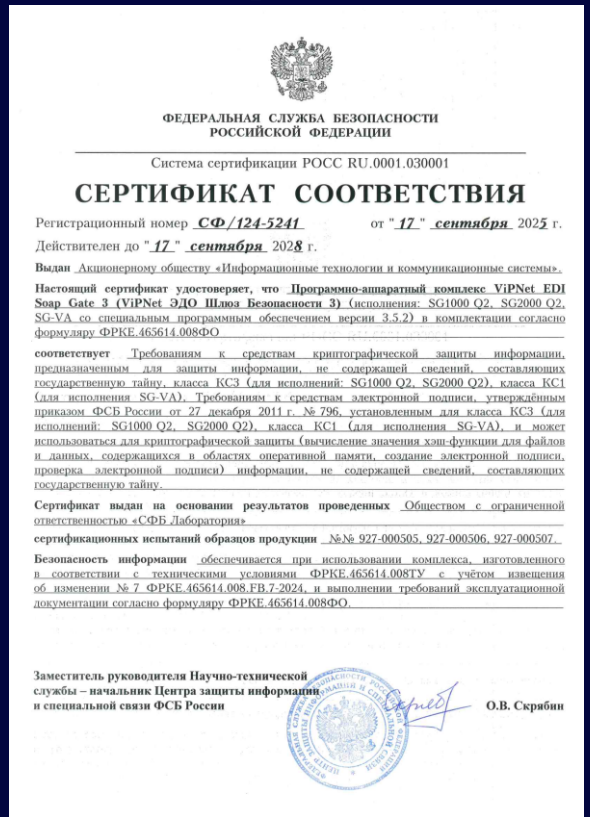
ViPNet EDI Soap Gate 3.6

ПАК СКЗИ и средство ЭП для взаимодействия с ЕСИА по OpenIDConnect в части идентификации пользователей ПлЦР, проставления и проверки ЭП по классу КС3

ViPNet EDI Flow 1.1

ПК управления ViPNet CABC и выполнения процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователей платформы ЦР

ViPNet EDI Soap Gate 3.5



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-5241** от "17" **сентября** 2025 г.

Действителен до "17" **сентября** 2028 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet EDI Soap Gate 3 (ViPNet ЭДО Шлюз Безопасности 3) (исполнения: SG1000 Q2, SG2000 Q2, SG-VA со специальным программным обеспечением версии 3.5.2) в комплектации согласно формуляру ФРКЕ.465614.008ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 (для исполнений: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VA), Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС3 (для исполнений: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VA), и может использоваться для криптографической защиты (вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, создание электронной подписи, проверка электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 927-000505, 927-000506, 927-000507.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.008ТУ с учётом извещения об изменении № 7 ФРКЕ.465614.008.ГВ.7-2024, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.008ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

- СКЗИ КС3 и средство ЭП КС3
- Регистрация в Едином реестре российских программ для ЭВМ и баз данных №3276
- Зарегистрирован в реестре Минпромторга и реестре Минцифры
- Исполнения: SG1000 и SG2000

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

ViPNet EDI Soap Gate 3.6

Криптошлюз для обмена электронными сведениями с применением электронной подписи

- Взаимодействие с ЕСИА для идентификации пользователя ПлЦР
- Проставление и проверка подписи ГОСТ
- Извлечение данных из файлов запросов формата PKCS#10 пользователей ПлЦР
- Извлекает данные полей изданных сертификатов
- Построение TLS ГОСТ 1.2, 1.3

ViPNet EDI Flow 1.1

Программный комплекс управления ViPNet CABC

- Взаимодействует с ИС банка, АС КР БР, ViPNet Certification Authority версии 4.6 и КриптоПро УЦ версии 2.0 (исп. 15, 16).

- авторизовывать пользователя через ЕСИА с целью получения доступа к персональным данным пользователя
- отправлять в УЦ запросы на издание сертификатов, а также получение сертификатов и списков аннулированных сертификатов (CRL)
- предоставляет API для авторизации в ЕСИА и отправки запросов в УЦ
- взаимодействует с АС ДБО по протоколу HTTP. Данные запросов и ответов передаются в формате JSON

Технические требования

ПК ViPNet EDI Flow

- Сервер
- ОС Astra Linux Special Edition версии 1.7.5 «Смоленск» и выше
- Средства антивирусной защиты
- средство межсетевого экранирования и систем обнаружения вторжений (ФСТЭК)
- СЗИ МДЗ (ФСТЭК)
- поддерживаемые браузеры:
  - ✓ Firefox – версии 118 и выше;
  - ✓ Chromium – версия 117

ViPNet EDI Soap Gate

- ПАК ViPNet ЭДО Шлюз безопасности в одном из исполнений:
  - ✓ViPNet ЭДО Шлюз безопасности SG1000 Q2;
  - ✓ViPNet ЭДО Шлюз безопасности SG2000 Q2.
- ViPNet ЭДО АРМ Контроль

Лицензии в ViPNet CABC*

ViPNet EDI Flow

- Лицензия выпускается отдельно на ViPNet EDI Flow 1.1

** Стоимость решения определяется суммой стоимости Лицензий. Различается в зависимости от исполнения ПАК ViPNet EDI Soap Gate 3.6 (SG1000/SG2000)*

ViPNet EDI Soap Gate

- Лицензия на ПАК ViPNet EDI Soap Gate 3.6 (SG1000/SG2000)
- Лицензии расширения:
  - ✓ Авторизация в ЕСИА
  - ✓ Получение данных в ЕСИА
  - ✓ Универсальный сервис подписи
  - ✓ ViPNet ЭДО АРМ Контроль

Проверки в ViPNet CABC

Первичный выпуск сертификата

- проверка ЭП файла запроса
- форматно-логический контроль файла запроса
- проверка соответствия данных пользователя ПлЦР из файла запроса и информации, полученной из ЕСИА

Повторный выпуск сертификата

- проверка ЭП файла запроса
- форматно-логический контроль файла запроса
- проверка идентификационных данных пользователя ПлЦР из файла запроса с использованием внутренних систем участника ПлЦР (АС ДБО)
- проверка соответствия данных из файла запроса с данными из действующего сертификата

Пользователи ViPNet САВС

Администраторы

- системный администратор
- администратор аудита
- администратор средств ЭП
- администратор резервного копирования и восстановления

Внешние системы

- АС ДБО
  - ✓ выпуск сертификата безопасности и сертификата ЭП
  - ✓ экспорт выпущенного сертификата безопасности и сертификата ЭП
  - ✓ CRL безопасности

Роли администраторов ViPNet CABC

Системный администратор

- управляет учётными записями администраторов Astra Linux и ViPNet EDI Flow, и учётными записями внешних систем;
- просматривает, копирует, настраивает параметры очистки и очищает журналы аудита в Astra Linux;
- настраивает параметры журнала учёта событий в ViPNet EDI Flow;
- управляет резервными копиями данных;
- настраивает параметры контроля целостности;
- просматривает данные о лицензии;
- настраивает средства антивирусной защиты и межсетевого экранирования;
- настраивает параметры СЗИ МДЗ.

Администратор аудита

- контролирует процессы выпуска сертификатов, получения маркера доступа в ЕСИА и запроса CRL из УЦ;
- просматривает, копирует и очищает журналы аудита в ViPNet EDI Flow.

Администратор средства ЭП

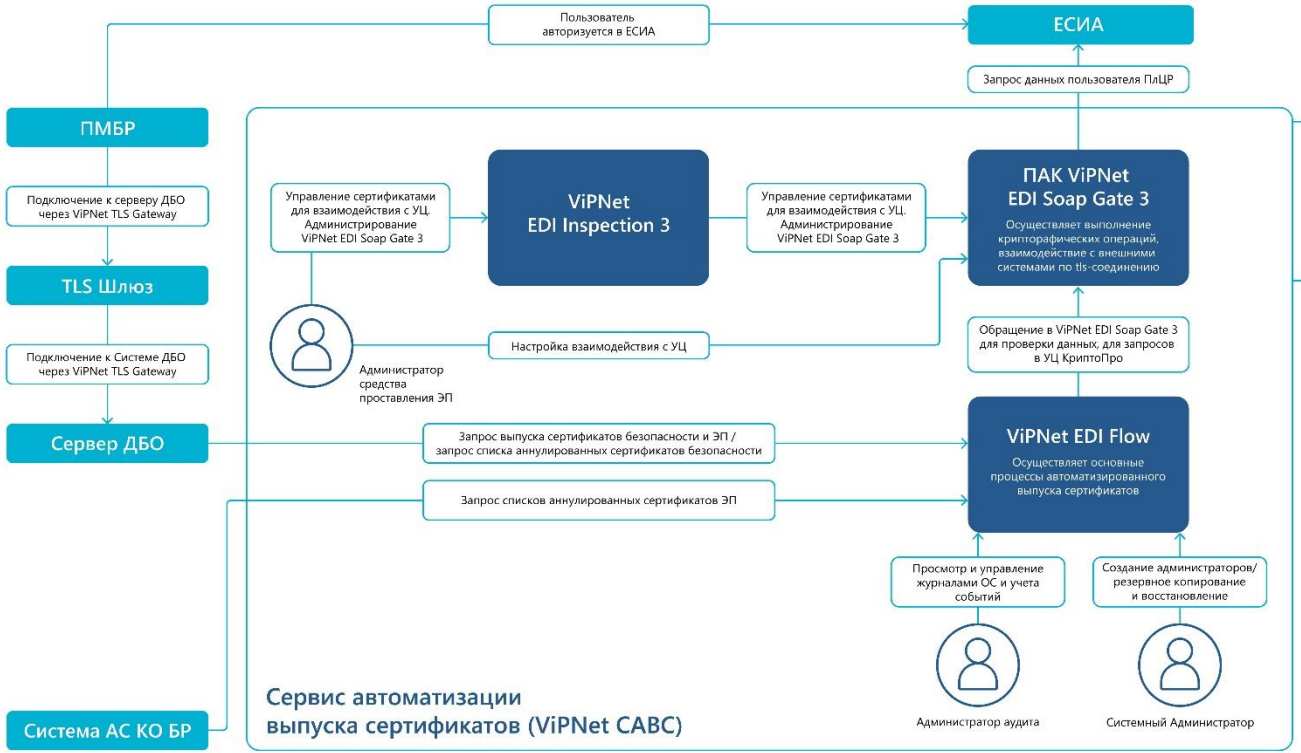
в ViPNet ЭДО Шлюз безопасности:

- настраивает параметры средств ЭП;
- настраивает параметры взаимодействия с ЕСИА и УЦ.

Администратор резервного копирования и восстановления

- создает резервные копии;
- Восстанавливает данные.

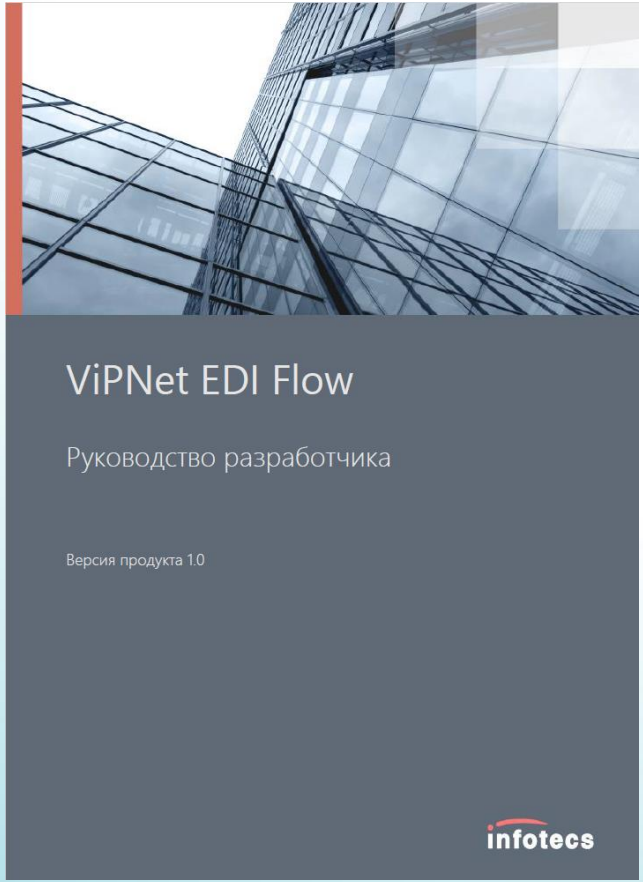
Схема работы ViPNet CABC



Проводимые в ViPNet CABC проверки:

- проверка ЭП файла запроса,
- ФЛК полей файла запроса,
- сверка данных файла запроса с данными ЕСИА/внешней информационной системы/выпущенного сертификата
- семантическая проверка полей сертификата

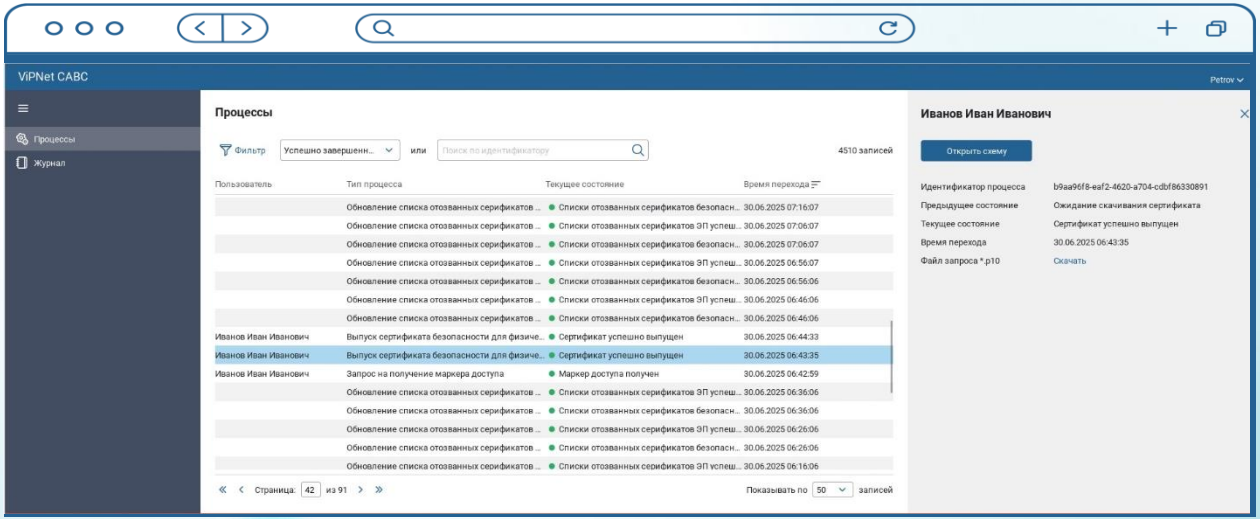
API ViPNet EDI Flow



Методы интеграции

- Аутентификация пользователя в ЕСИА
- Выпуск сертификата безопасности для ФЛ
- Выпуск сертификата безопасности для ФЛ – представителя ЮЛ
- Запрос списков аннулированных сертификатов

Интерфейс веб-приложения для администраторов ViPNet CABC



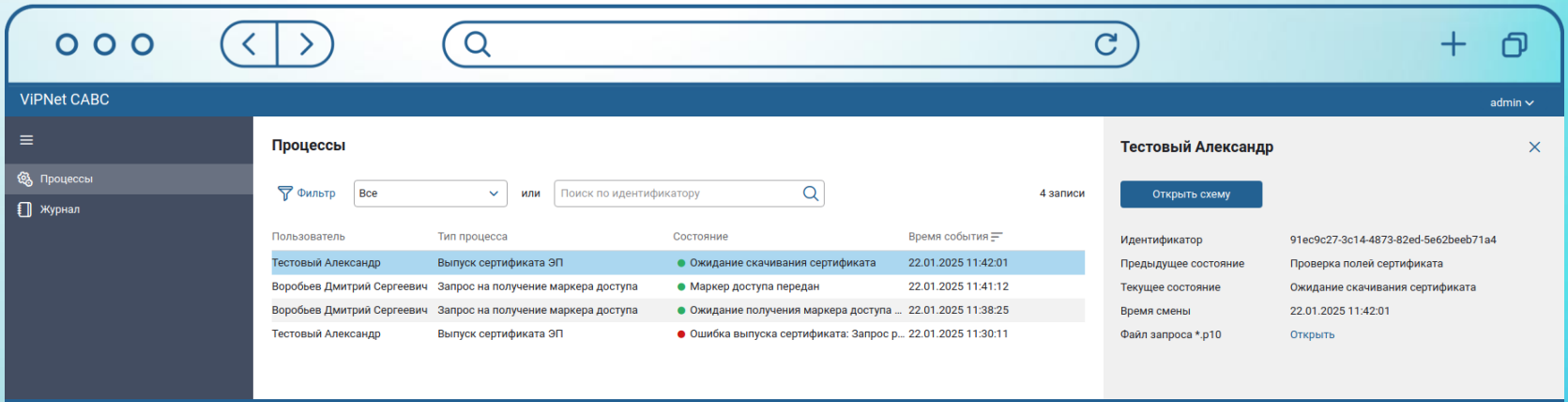
Фиксация процессов:

- сведения о результате проверок ЭП и ФЛК файла запроса PKCS#10;
- сведения о результатах сверки информации, полученной из ЕСИА с информацией в запросе на сертификат;
- сведения о направлении запроса на сертификат в сторону средств УЦ (средств УЦ Безопасности);
- сведения о результате выпуска сертификата;
- сведения о результате выполнения ФЛК выпущенного сертификата.

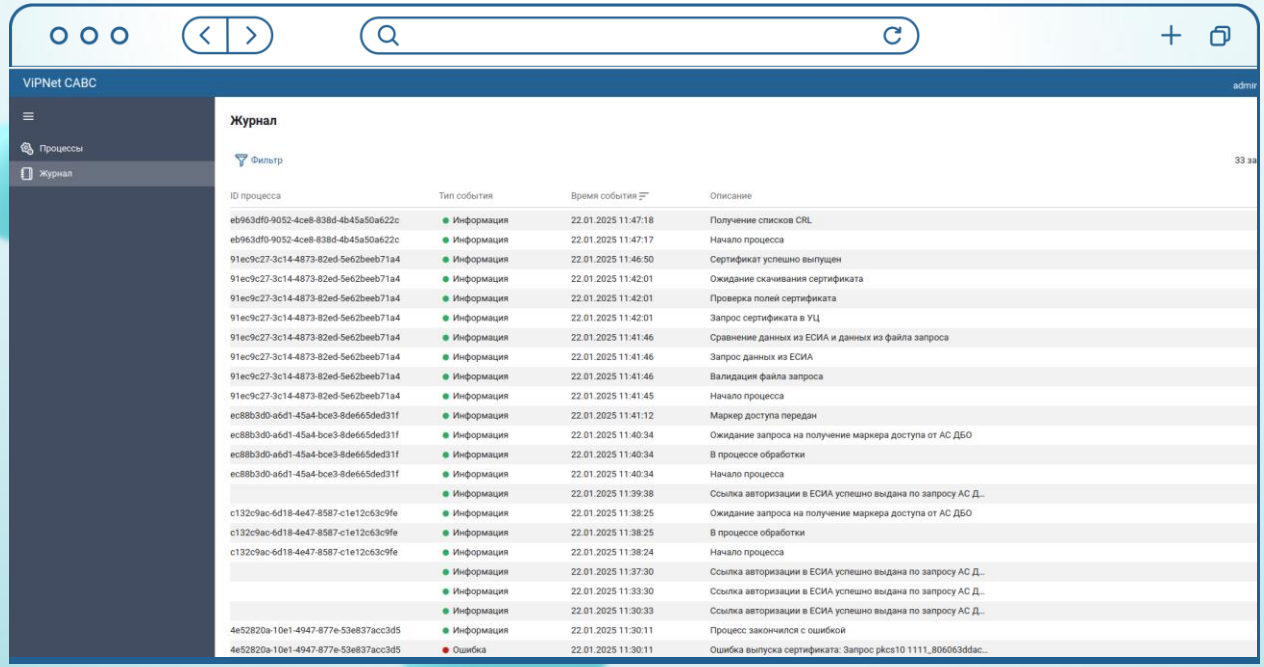
Отслеживание и управление процессом выпуска сертификатов

Виды процессов

- Выпуск сертификата безопасности для ФЛ;
- Выпуск сертификата безопасности для ФЛ – представителя ЮЛ;
- Выпуск сертификата ЭП для ФЛ;
- Выпуск сертификата ЭП для ФЛ – представителя ЮЛ;
- Запрос маркера доступа
- Обновление списка отозванных сертификатов безопасности
- Обновление списка отозванных сертификатов подписи



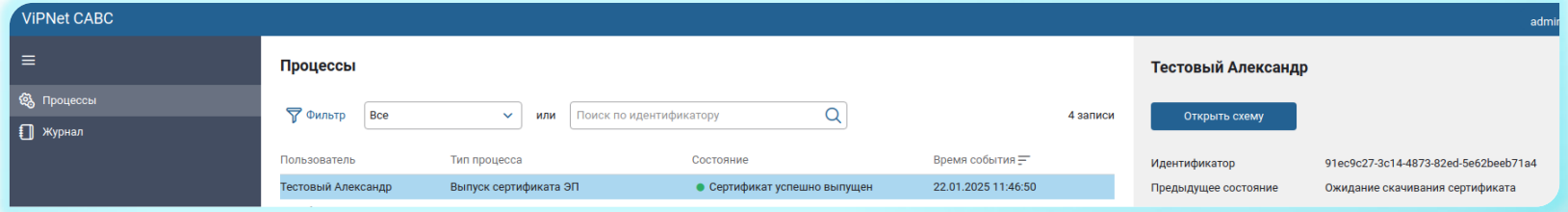
Регистрация событий в журнале учета событий

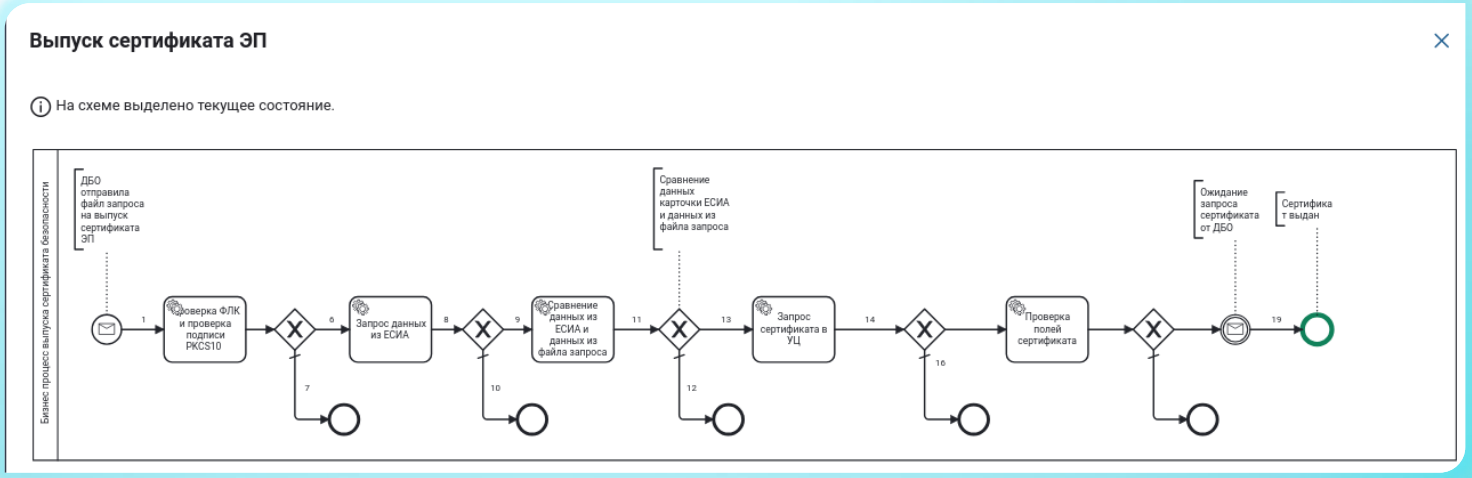


Фиксация событий:

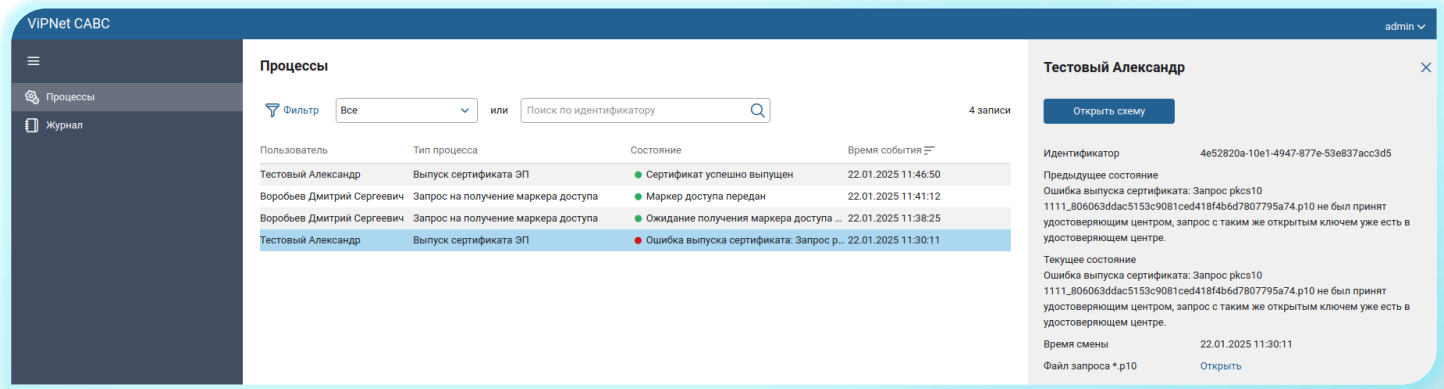
- сведения о результате проверок ЭП и ФЛК файла запроса PKCS#10;
- сведения о результатах сверки информации, полученной из ЕСИА с информацией в запросе на сертификат;
- сведения о направлении запроса на сертификат в сторону средств УЦ (средств УЦ Безопасности);
- сведения о результате выпуска сертификата;
- сведения о результате выполнения ФЛК выпущенного сертификата.

Пример для успешно выпущенного сертификата





Пример неудачного выпуска



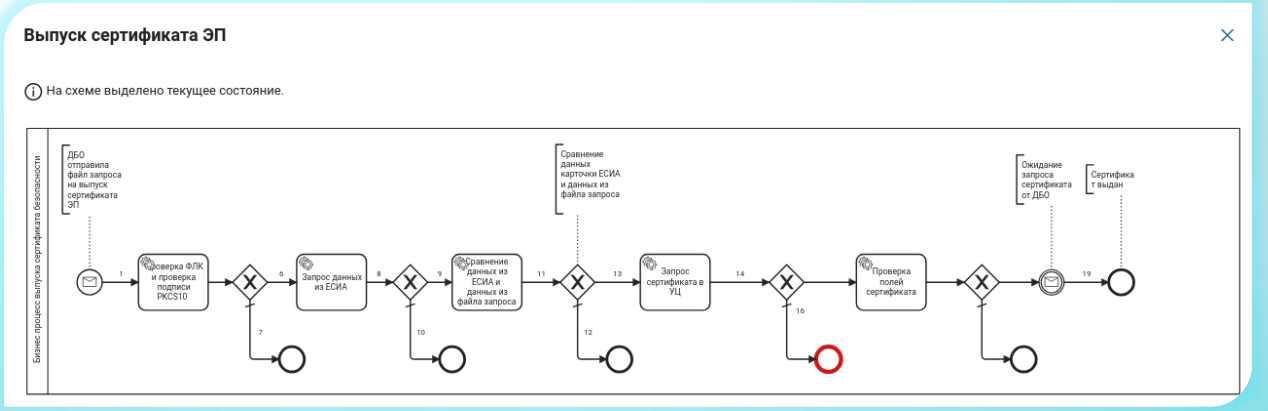
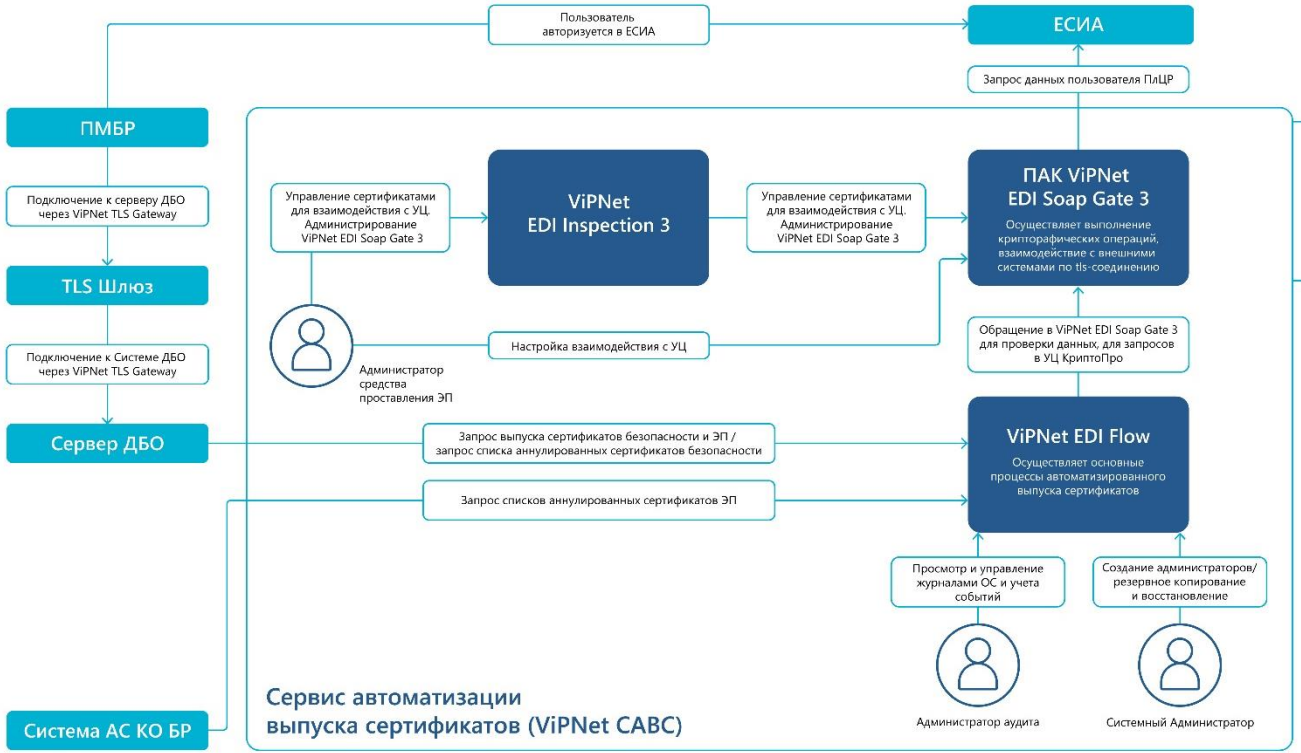


Схема работы ViPNet CABC



Проводимые в ViPNet CABC проверки:

- проверка ЭП файла запроса,
- ФЛК полей файла запроса,
- сверка данных файла запроса с данными ЕСИА/внешней информационной системы/выпущенного сертификата
- семантическая проверка полей сертификата

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

Спасибо за внимание!

Елена Новикова
Эмиль Капкаев