

СКЗИ для легитимной работы с ЕСИА, СМЭВ и ЦП



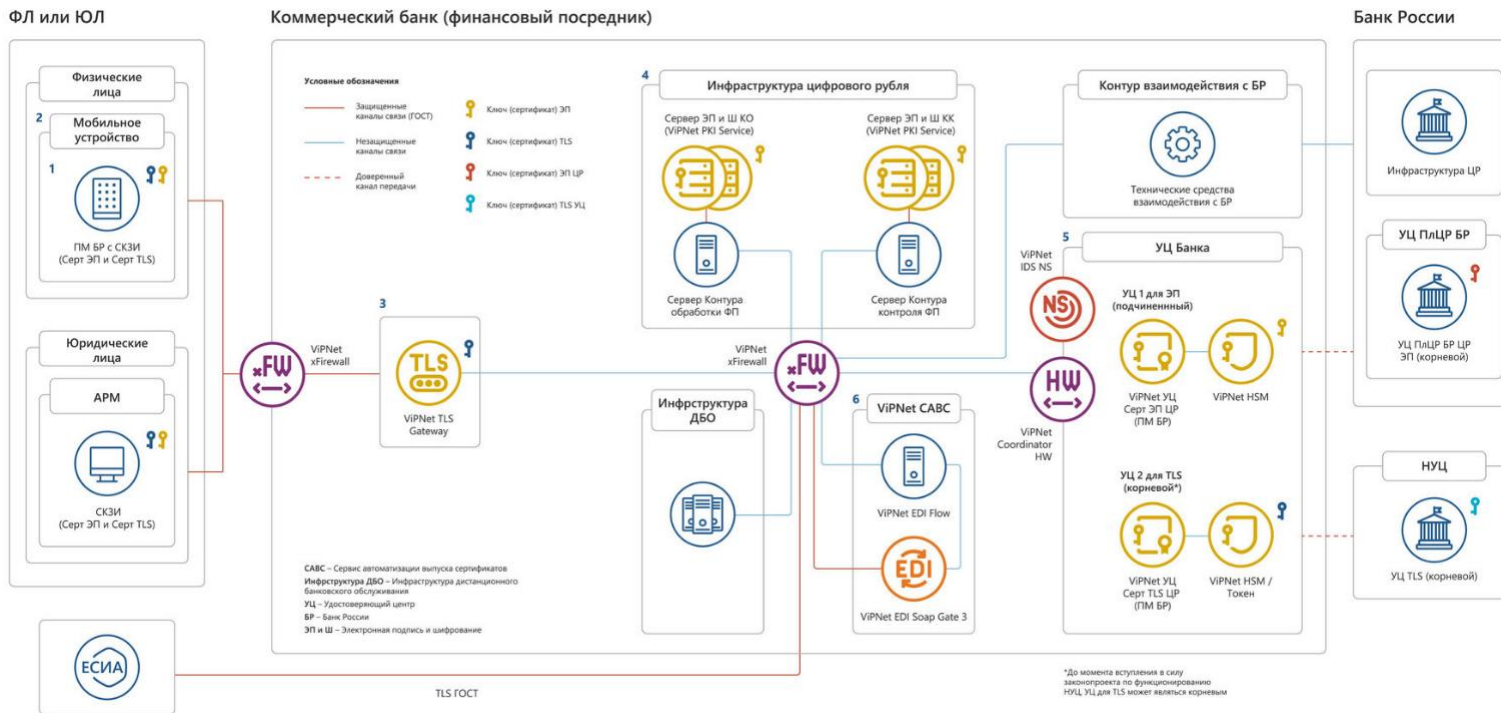
Елена Новикова

Руководитель продуктового направления

инфотекс
ТЕХНОДЕСТ

Белый поток

Общая схема инфраструктуры ЦР





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 – ЦБ России и ФСБ России



Состав ViPNet CABCS 1.0



ViPNet EDI Soap Gate 3

ПАК СКЗИ и средство ЭП для взаимодействия с ЕСИА по OpenID Connect в части идентификации пользователей ПлЦР, проставления и проверки ЭП



ViPNet EDI Flow

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



VIPNet EDI Soap Gate



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-5418 от "06" марта 2026 г.
Действителен до "06" марта 2029 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».
Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс VIPNet EDI Soap Gate 3 (VIPNet ЭДЮ Шлюз Безопасности 3) (использование: SG1000 Q2, SG2000 Q2, SG-VА со специальным программным обеспечением версии 3.0) в комплектации согласно формуляру ФРКЕ 465614.008ФО с учётом внесения № 8 ФРКЕ 465614.008.1.В.8.2025

соответствует Требованиям в средствах криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 (для исполнения: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VА). Требованиям в средствах электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС3 (для исполнения: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VА), и может использоваться для криптографической защиты (вычисление значения хэш-функции для данных, содержащихся в областях инициальной области, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи, защита (соединение) 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 обеспечена при использовании комплекта, изготовленного в соответствии с техническими условиями ФРКЕ 465614.008ТУ с учётом внесения № 8 ФРКЕ 465614.008.1.В.8.2025 и выполнения требований эксплуатационной документации согласно формуляру ФРКЕ 465614.008ФО с учётом внесения № 8 ФРКЕ 465614.008.1.В.8.2025.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России



Скрибин

О.В. Скрибин

- Соответствует требованиям ФСБ России к СКЗИ и ЭП по классу КС3 и КС1 (нет требования о проведении ОВ при подключении ИС организации)
- Действующий сертификат до 6 марта 2029 года (СМЭВЗ)
- Заключение от 26 декабря 2025 года о соответствии требованиям ФСБ России к СКЗИ КС3 и средство ЭП КС3, в том числе для взаимодействия с ЕСИА, СМЭВЗ
- Регистрация в Едином реестре российского ПО №3276 и в реестре Минпромторга

VipNet EDI Soap Gate

Криптошлюз для обмена
электронными сведениями
с применением электронной
подписи



- Соответствует Регламенту ЕСИА 2.47+ и Методическим рекомендациям ЕСИА 3.48+
- Авторизация и аутентификация пользователей в ЕСИА с помощью протокола авторизации OAuth 2.0 и расширения OpenID Connect
- Построение защищенного канала связи по протоколу TLS ГОСТ 1.2, 1.3
- Заверение данных ЭП определенного формата и ее проверка, включая проверку действительности сертификата ключа проверки ЭП, 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 EDI Flow

Программный комплекс
управления VipNet CABС

- Контроль и выполнение процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователям ПлЦР
- Обеспечивает взаимодействие между АС ДБО, VipNet EDI Soap Gate и УЦ. Для интеграции АС ДБО с VipNet EDI Flow предоставляется REST API (Справочник разработчика)
- Идентифицирует пользователя ПлЦР в ЕСИА
- Отправляет запросы в УЦ на выпуск сертификатов безопасности и сертификатов ЭП для пользователей ПлЦР
- Получает и распространяет списки отозванных сертификатов



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/128-4946 от "17" июля 2024 г.

Действителен до "28" февраля 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс «VIPNet Удостоверяющий центр 4 (версия 4.6)» (исполнения: 1, 2) в комплектации согласно формуляру ФРКЕ.00114-07.30.01.ФО

соответствует требованиям ФСБ России к информационной безопасности удостоверяющих центров класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), предназначенных для обработки информации, не содержащей сведений, составляющих государственную тайну, Требованиям к средствам удостоверяющего центра, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), и Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория» сертификационных испытаний образцов продукции №№ 769С-000507, 769С-000508.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00114-07.30.01.ФО.

Временно исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России



В.А. Шуринов

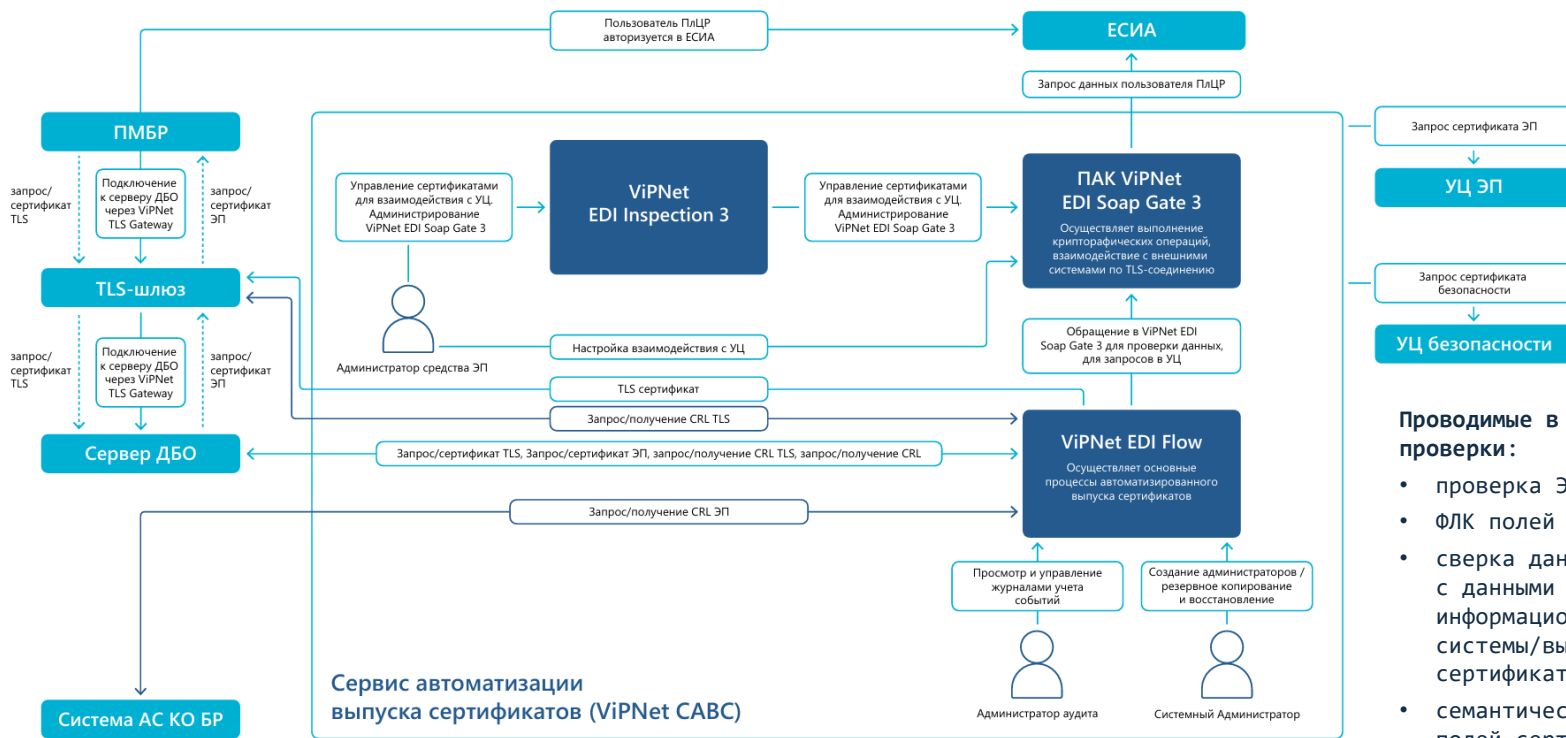
Сертификация: VIPNet УЦ 4.6

- Два исполнения: средство УЦ КС2 и КС3 для ОС Windows
- Текущий сертификат действует до 28.02.2026
- Новый сертификат СФ/128-5392 получен 27 января 2026 года действует до 31 декабря 2026

VIPNet УЦ 5

- Сертификат до конца 2026 года

Схема работы ViPNet CABС



Проводимые в ViPNet CABС 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

Роли администраторов ViPNet САВС

Системный администратор (совмещает роль администратора резервного копирования и восстановления)

- создание, удаление, настройка прав и редактирование учетных записей администраторов
- настройка параметров журнала аудита
- запрет на изменение журнала аудита

Администратор аудита

- просмотр журнала аудита
- копирование журналов аудита
- полная очистка журналов

Администратор средства ЭП

Проверки в ViPNet СABC

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

Отслеживание и управление процессом выпуска сертификатов

Виды процессов

- Обработка запроса на сертификат безопасности
- Обработка запроса на сертификат подписи
- Обмен авторизационного кода на маркер доступа в ЕСИА
- Обновление списка отозванных сертификатов безопасности
- Обновление списка отозванных сертификатов подписи

The screenshot displays the VIPNet CAB web interface. The top navigation bar includes the title 'VIPNet CAB', a search bar, and a user profile 'admin'. The main content area is divided into two sections: 'Процессы' (Processes) and a detailed view for 'Тестовый Александр'.

Процессы

Фильтр: Все | Поиск по идентификатору

Пользователь	Тип процесса	Состояние	Время события
Тестовый Александр	Выпуск сертификата ЭП	Ожидание скачивания сертификата	22.01.2025 11:42:01
Воробьев Дмитрий Сергеевич	Запрос на получение маркера доступа	Маркер доступа передан	22.01.2025 11:41:12
Воробьев Дмитрий Сергеевич	Запрос на получение маркера доступа	Ожидание получения маркера доступа ...	22.01.2025 11:38:25
Тестовый Александр	Выпуск сертификата ЭП	Ошибка выпуска сертификата: Запрос р...	22.01.2025 11:30:11

Тестовый Александр

Открыть схему

Идентификатор	91ec9c27-3c14-4873-82ed-5e62beeb71a4
Предыдущее состояние	Проверка полей сертификата
Текущее состояние	Ожидание скачивания сертификата
Время смены	22.01.2025 11:42:01
Файл запроса *.p10	Открыть

Регистрация событий в журнале событий

Фиксация событий:

- каждого этапа обработки запросов на выпуск сертификата
- этапов работы с CRL
- этапов взаимодействия с ЕСИА

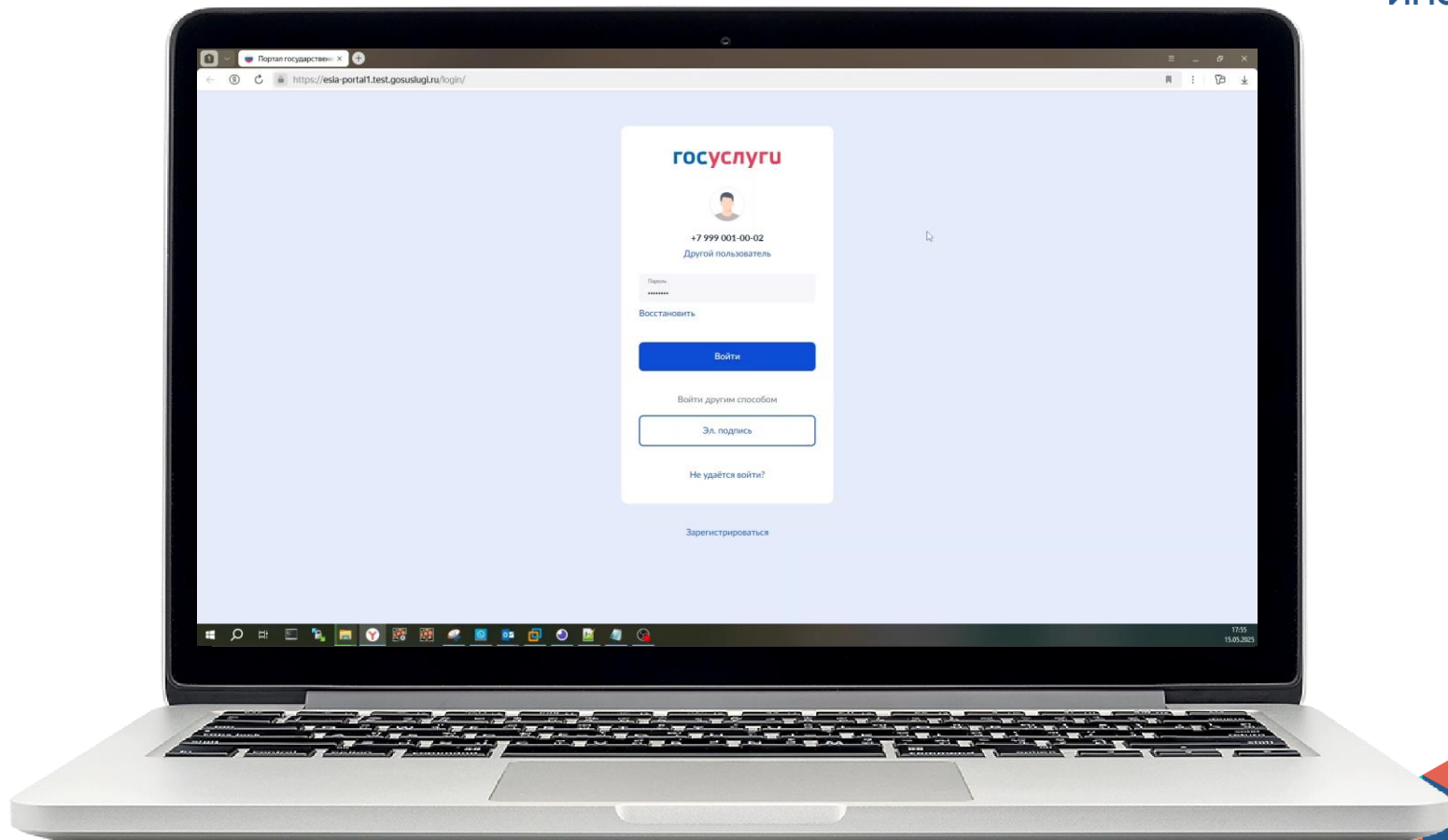
Системный администратор:

- механизмы по обнаружению несанкционированных изменений журналов аудита

Администратор аудита:

- просмотр журналов аудита
- копирование журналов аудита
- полная очистка журналов аудита

ID процесса	Тип события	Время события	Описание
eb963df0-9052-4ce8-838d-4b45a50a622c	Информация	22.01.2025 11:47:18	Получение списков CRL
eb963df0-9052-4ce8-838d-4b45a50a622c	Информация	22.01.2025 11:47:17	Начало процесса
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:46:50	Сертификат успешно выпущен
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:42:01	Ожидание скачивания сертификата
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:42:01	Проверка полей сертификата
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:42:01	Запрос сертификата в УЦ
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:41:46	Сравнение данных из ЕСИА и данных из файла запроса
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:41:46	Запрос данных из ЕСИА
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:41:46	Валидация файла запроса
91ec9c27-3c14-4873-82ed-5e62beeb71a4	Информация	22.01.2025 11:41:45	Начало процесса
ec88b3d0-a6d1-45a4-bce3-8de665ded31f	Информация	22.01.2025 11:41:12	Маркер доступа передан
ec88b3d0-a6d1-45a4-bce3-8de665ded31f	Информация	22.01.2025 11:40:34	Ожидание запроса на получение маркера доступа от АС ДБО
ec88b3d0-a6d1-45a4-bce3-8de665ded31f	Информация	22.01.2025 11:40:34	В процессе обработки
ec88b3d0-a6d1-45a4-bce3-8de665ded31f	Информация	22.01.2025 11:40:34	Начало процесса
	Информация	22.01.2025 11:39:38	Ссылка авторизации в ЕСИА успешно выдана по запросу АС Д...
c132c9ac-6d18-4e47-8587-c1e12c63c9fe	Информация	22.01.2025 11:38:25	Ожидание запроса на получение маркера доступа от АС ДБО
c132c9ac-6d18-4e47-8587-c1e12c63c9fe	Информация	22.01.2025 11:38:25	В процессе обработки
c132c9ac-6d18-4e47-8587-c1e12c63c9fe	Информация	22.01.2025 11:38:24	Начало процесса
	Информация	22.01.2025 11:37:30	Ссылка авторизации в ЕСИА успешно выдана по запросу АС Д...
	Информация	22.01.2025 11:33:30	Ссылка авторизации в ЕСИА успешно выдана по запросу АС Д...
	Информация	22.01.2025 11:30:33	Ссылка авторизации в ЕСИА успешно выдана по запросу АС Д...
4e52820a-10e1-4947-877e-53e837acc3d5	Информация	22.01.2025 11:30:11	Процесс закончился с ошибкой
4e52820a-10e1-4947-877e-53e837acc3d5	Ошибка	22.01.2025 11:30:11	Ошибка выпуска сертификата: Запрос pkcs10 1111_806063ddac...



Пример для успешно выпущенного сертификата

VIPNet CABV admin

Процессы

Фильтр: Все или Поиск по идентификатору

4 записи

Пользователь	Тип процесса	Состояние	Время события
Тестовый Александр	Выпуск сертификата ЭП	Сертификат успешно выпущен	22.01.2025 11:46:50

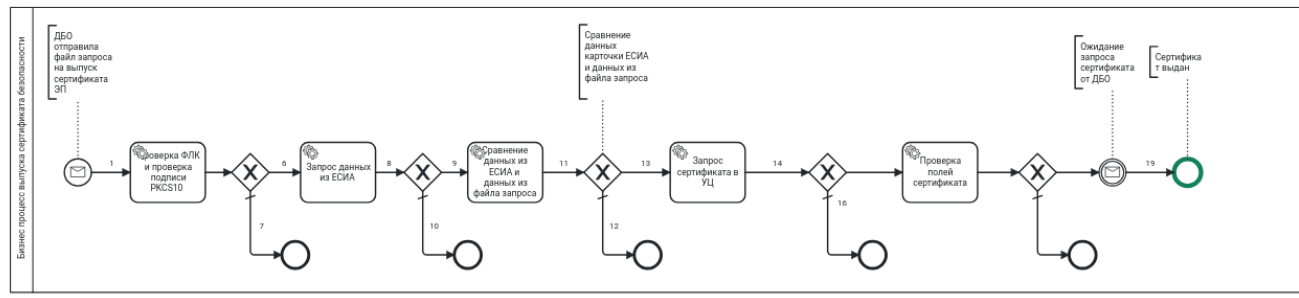
Тестовый Александр

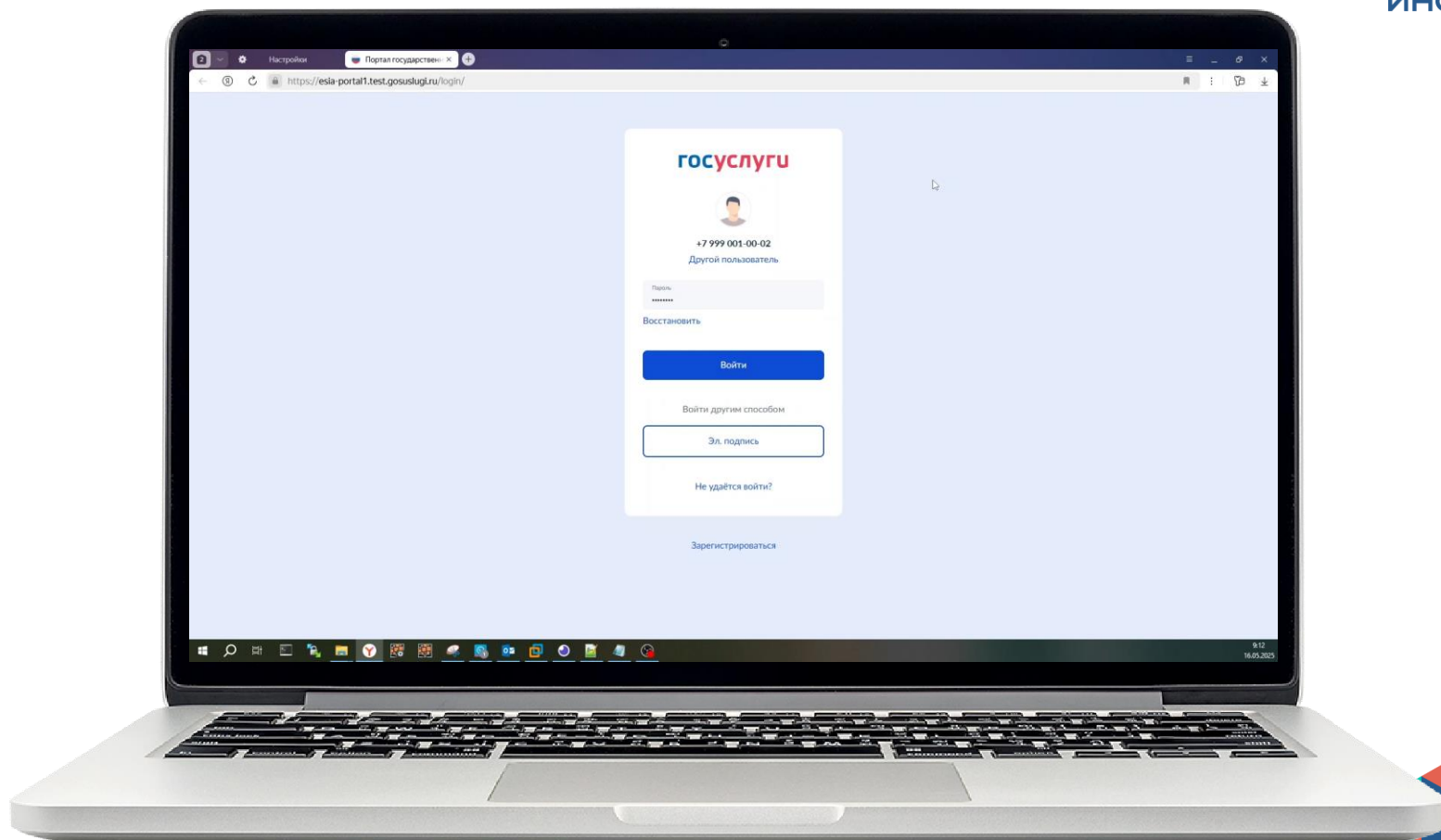
Открыть схему

Идентификатор: 91ec9c27-3c14-4873-82ed-5e62beeb71a4
 Предыдущее состояние: Ожидание скачивания сертификата

Выпуск сертификата ЭП

На схеме выделено текущее состояние.





Пример неудачного выпуска

VIPNet CABС admin

Процессы

Фильтр: Все или Поиск по идентификатору 4 записи

Пользователь	Тип процесса	Состояние	Время события
Тестовый Александр	Выпуск сертификата ЭП	Сертификат успешно выпущен	22.01.2025 11:46:50
Воробьев Дмитрий Сергеевич	Запрос на получение маркера доступа	Маркер доступа передан	22.01.2025 11:41:12
Воробьев Дмитрий Сергеевич	Запрос на получение маркера доступа	Ожидание получения маркера доступа	22.01.2025 11:38:25
Тестовый Александр	Выпуск сертификата ЭП	Ошибка выпуска сертификата: Запрос р...	22.01.2025 11:30:11

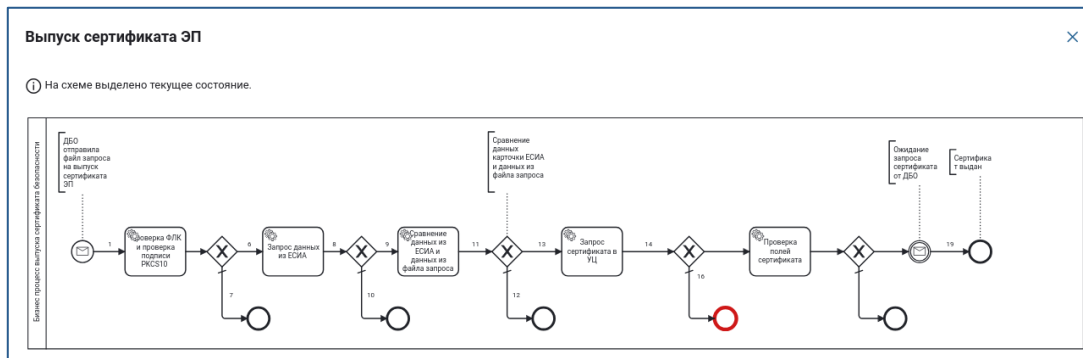
Тестовый Александр

Идентификатор: 4e52820a-10e1-4947-877e-53e837acc3d5

Предидущее состояние
Ошибка выпуска сертификата: Запрос rkcs10 1111_806063ddac5153c9081ced418f4bd7807795a74.p10 не был принят удостоверяющим центром, запрос с таким же открытым ключем уже есть в удостоверяющем центре.

Текущее состояние
Ошибка выпуска сертификата: Запрос rkcs10 1111_806063ddac5153c9081ced418f4bd7807795a74.p10 не был принят удостоверяющим центром, запрос с таким же открытым ключем уже есть в удостоверяющем центре.

Время смены: 22.01.2025 11:30:11
Файл запроса *p10: Открыть



САНКТ
ПЕТЕРБУРГ

инфотекс
ТЕХНОДЕСТ

Подписывайтесь
на наши соцсети



инфотекс
Академия



AMPIRE

TELEOFIS

КОМФОРТЕЛ
оператор связи бизнес-класса

RVTOKEH
ФАКТИВ

TS Solution

AXOFT