

Как защитить данные пользователей при открытии цифровых кошельков

Елена Новикова
Руководитель продуктового направления

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  infotecs
ФЕСТ



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



Состав ViPNet CABC



ViPNet EDI Soap Gate 3

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



ViPNet EDI Flow

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



VipNet EDI Soap Gate

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 Soap Gate


**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.463614.008ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КСЗ (для исполнений: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VA). Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КСЗ (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 Обществен 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.463614.008ТУ с учетом извещения об изменении № 7 ФРКЕ.463614.008.ВВ.7-2024, и выполнения требований эксплуатационной документации согласно формуляру ФРКЕ.463614.008ФО.

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


О.В. Скрибин



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



VipNet EDI Flow

Программный комплекс
управления VipNet CAB

- 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) через API VipNet EDI Flow.

Проверки в ViPNet САВС

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

Администраторы

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

Внешние системы

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

Роли администраторов ViPNet САВС

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

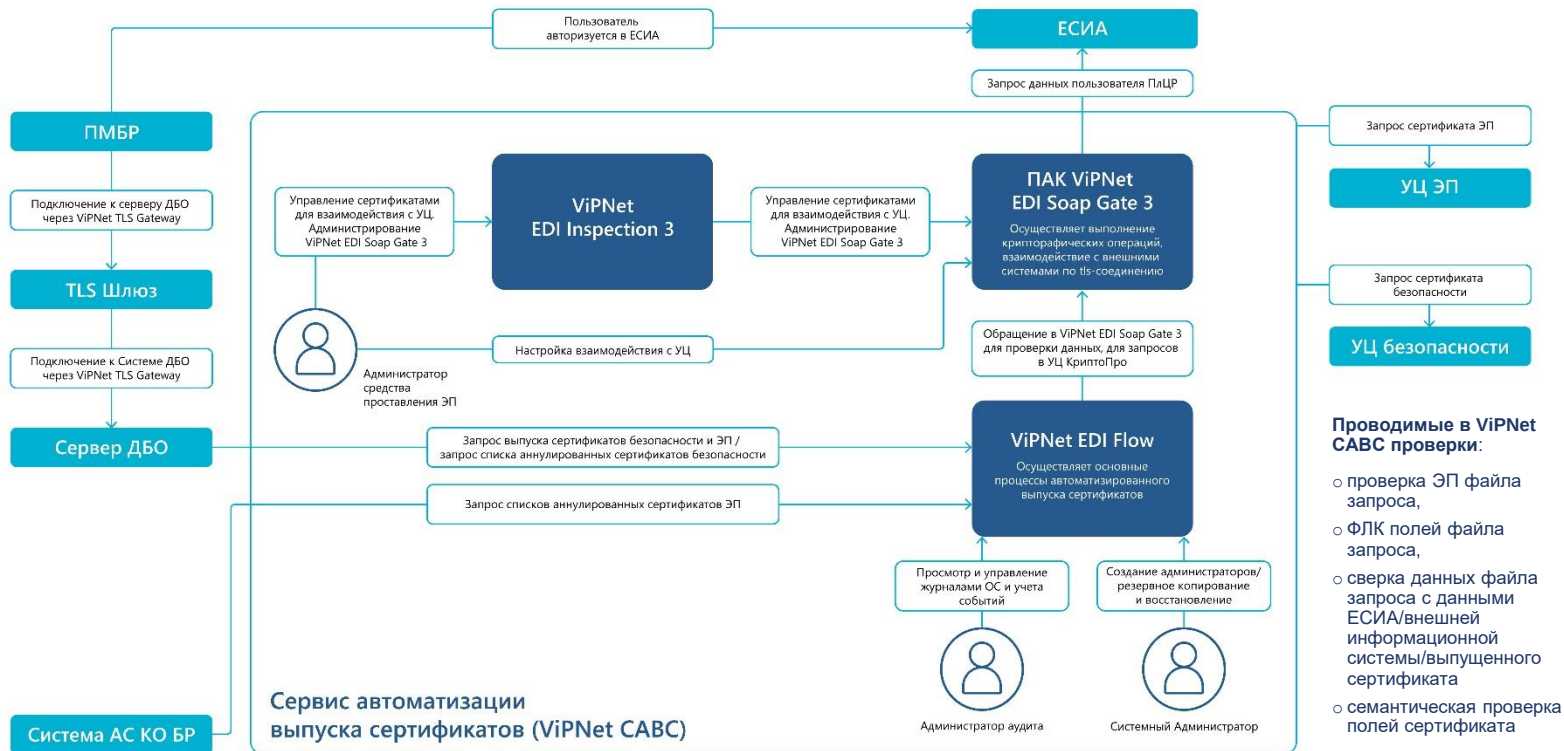
в ViPNet ЭДО Шлюз безопасности:

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

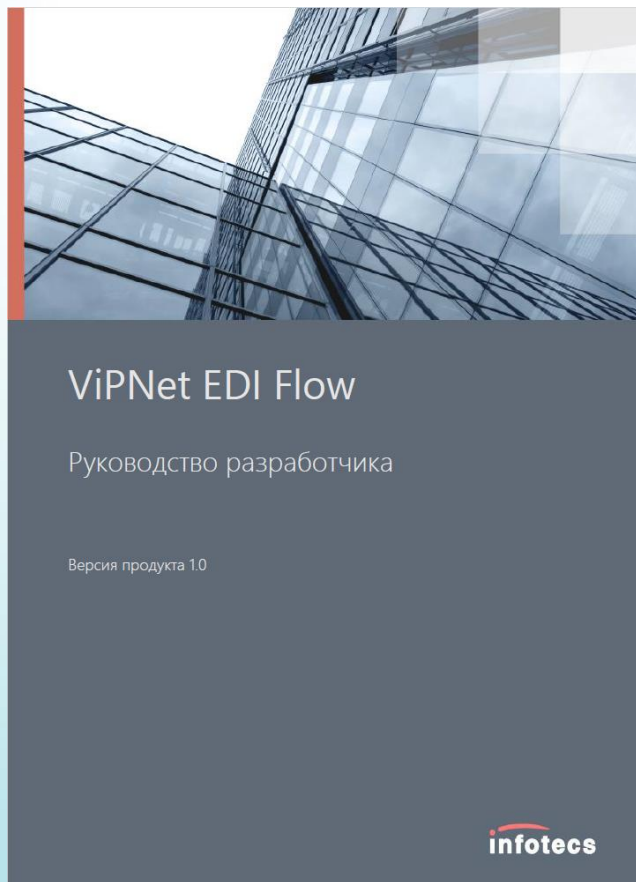
Администратор резервного копирования и восстановления

- создает резервные копии;
- Восстанавливает данные.

Схема работы ViPNet CABCS



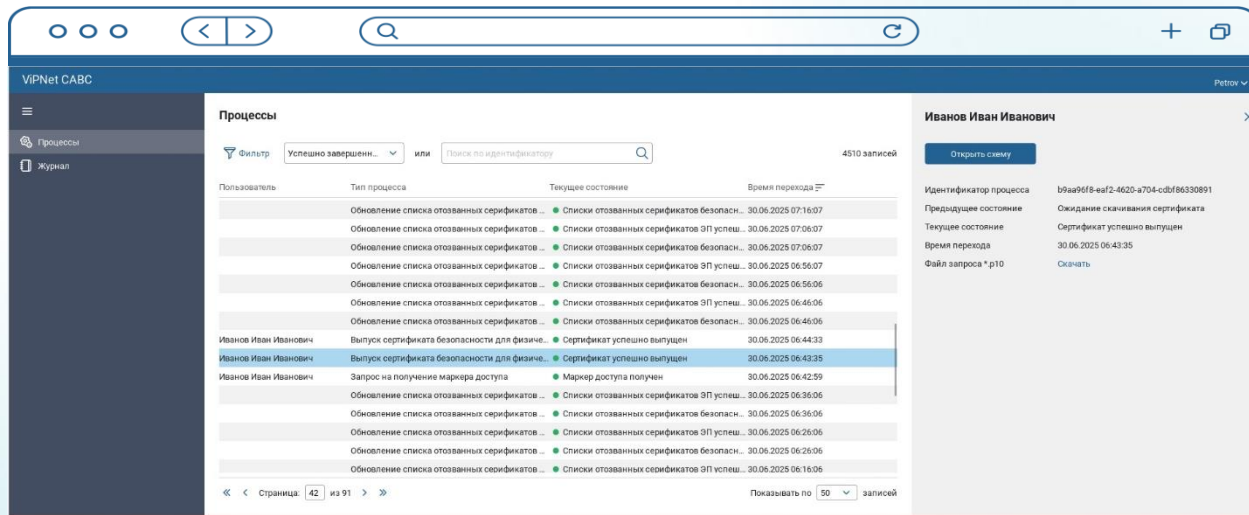
API ViPNet EDI Flow



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 пользователя ViPNet EDI Flow



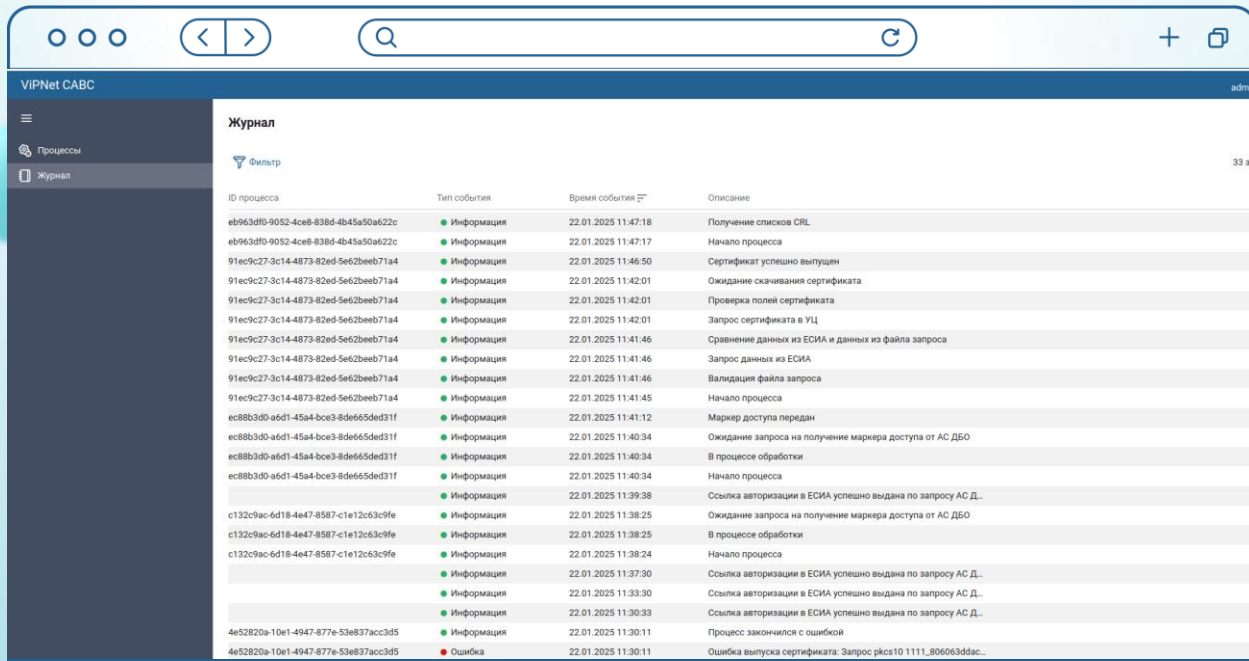
Фиксация процессов:

- 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.

- 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

13

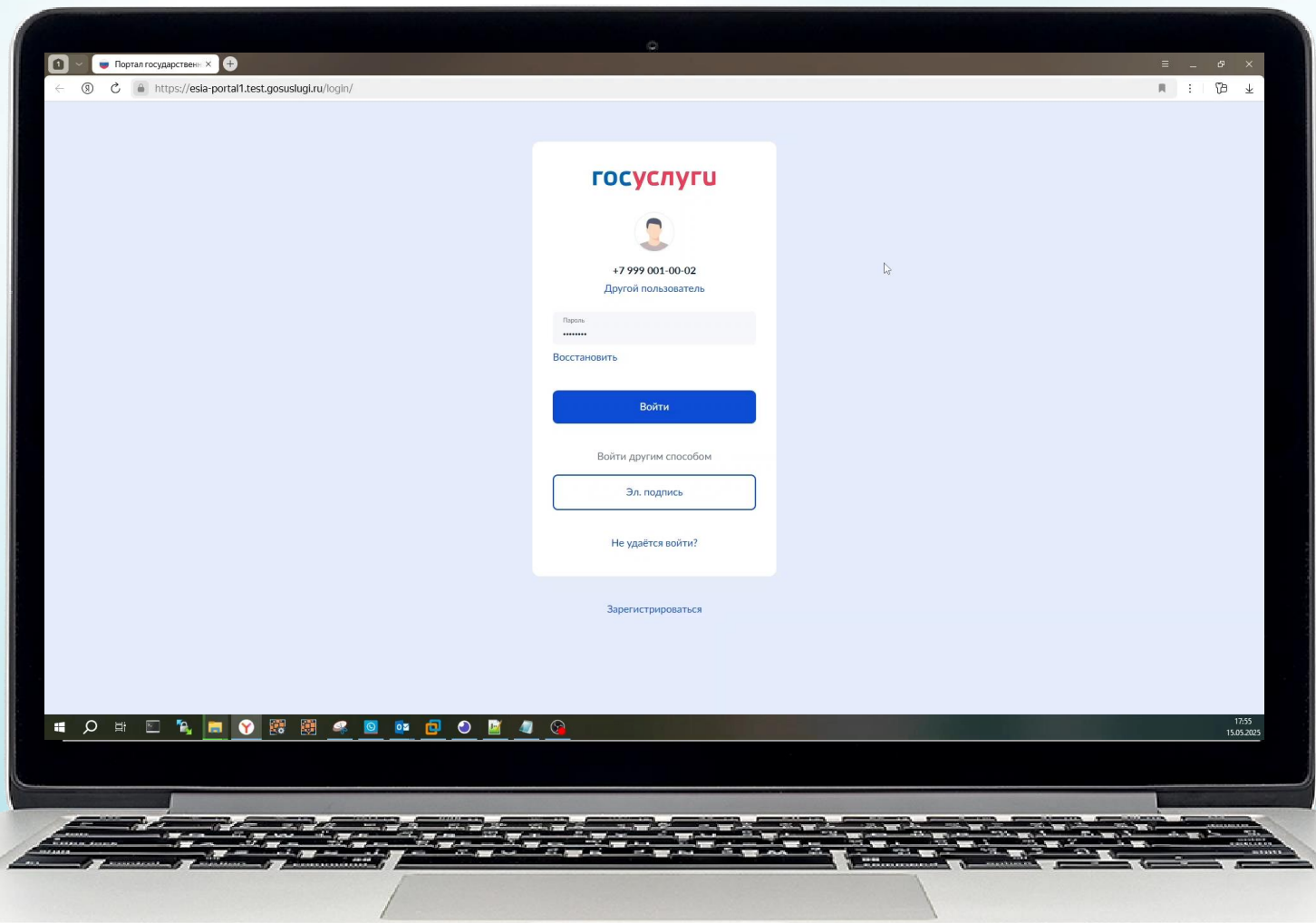
Регистрация событий в журнале учета событий



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
ec88b3d0-a6d1-45a4-bce3-8de665ded31f	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
c132c9ac-6d18-4e47-8587-c1e12c63c9fe	Информация	22.01.2025 11:37:30	Ссылка авторизации в ЕСИА успешно выдана по запросу АС Д...
c132c9ac-6d18-4e47-8587-c1e12c63c9fe	Информация	22.01.2025 11:33:30	Ссылка авторизации в ЕСИА успешно выдана по запросу АС Д...
c132c9ac-6d18-4e47-8587-c1e12c63c9fe	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...

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.

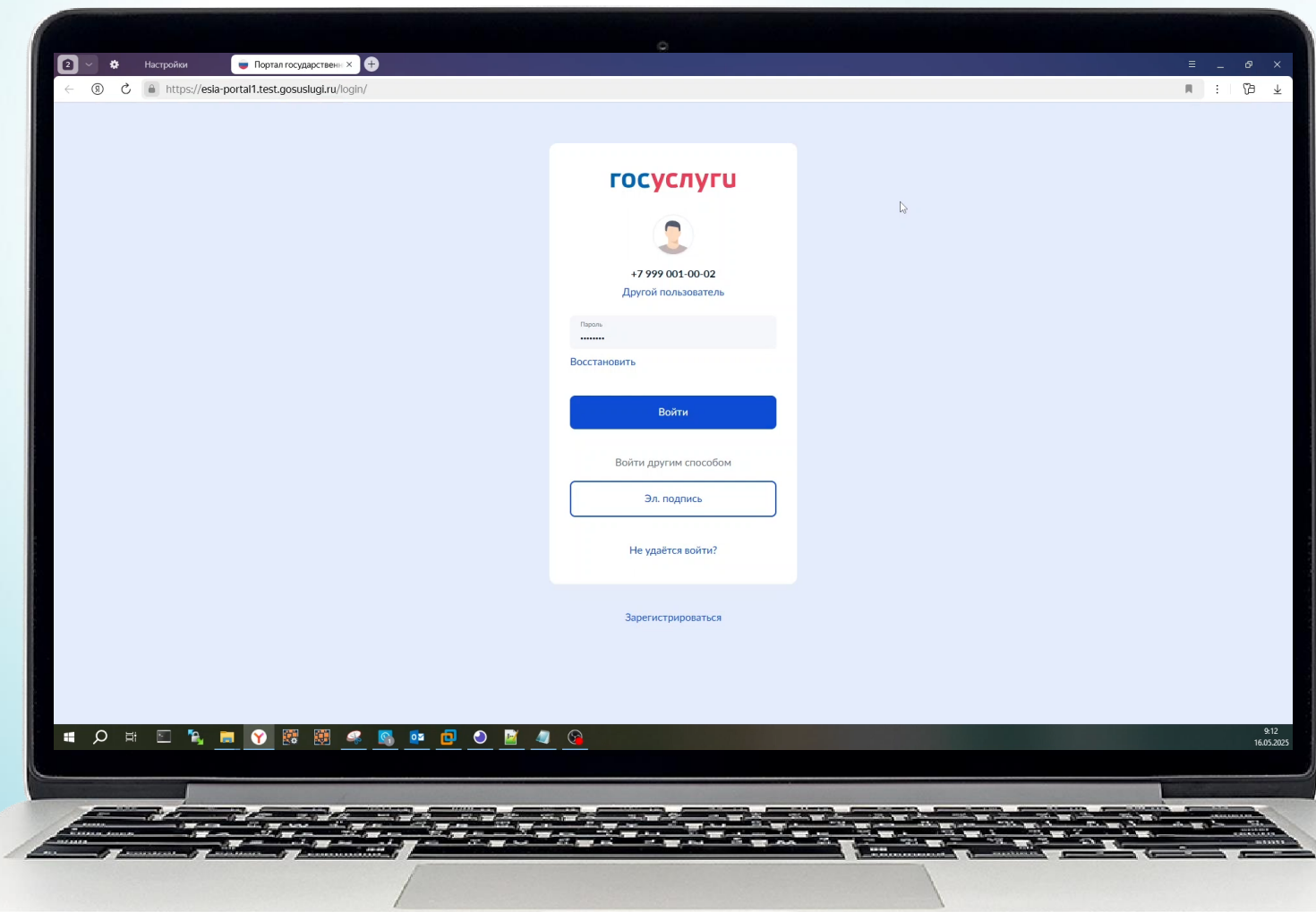


Техноinfotecs
Фест

Выпуск сертификата ЭП

Бизнес-процесс выпуска сертификата безопасности

```
graph LR; Start([ДБО отправила файл запроса на выпуск сертификата ЭП1]) -- 1 --> Task1[Проверка ФЛК и проверка подписи PKCS10]; Task1 -- 6 --> X1{X}; X1 -- 7 --> Loop1(( )); X1 -- 8 --> Task2[Запрос данных из ЕСИА]; Task2 -- 9 --> X2{X}; X2 -- 10 --> Loop2(( )); X2 -- 11 --> X3{X}; X3 -- 12 --> Loop3(( )); X3 -- 13 --> Task3[Запрос сертификата в УЦ]; Task3 -- 14 --> X4{X}; X4 -- 15 --> Loop4(( )); X4 -- 16 --> Task4[Проверка полей сертификата]; Task4 --> X5{X}; X5 --> Loop5(( )); X5 --> End([Сертификат выдан]);
```



Пример неудачного выпуска

VIPNet CAB

admin

Процессы

Журнал

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

Открыть схему

Идентификатор

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

Предыдущее состояние

Ошибка выпуска сертификата: Запрос pkcs10 1111_806063ddac5153c9081ced418f4b6d7807795a74.p10 не был принят удостоверяющим центром, запрос с таким же открытым ключом уже есть в удостоверяющем центре.

Текущее состояние

Ошибка выпуска сертификата: Запрос pkcs10 1111_806063ddac5153c9081ced418f4b6d7807795a74.p10 не был принят удостоверяющим центром, запрос с таким же открытым ключом уже есть в удостоверяющем центре.

Время смены

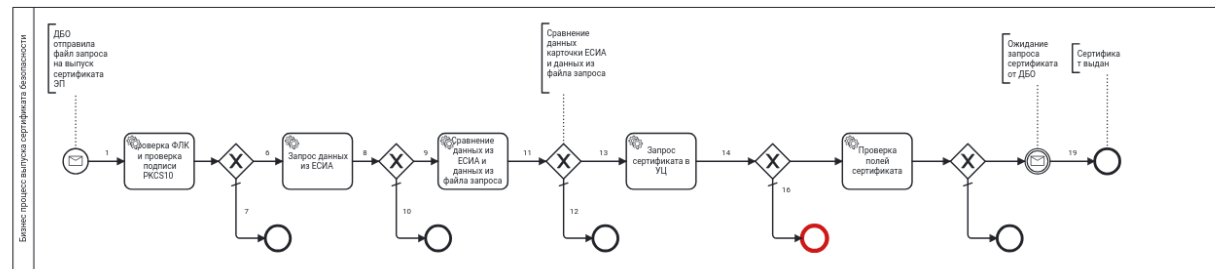
22.01.2025 11:30:11

Файл запроса * p10

Открыть

Выпуск сертификата ЭП

На схеме выделено текущее состояние.



ТЕХНО infotecs Фест

Елена Новикова
Руководитель продуктового направления



NBJ НАЦИОНАЛЬНЫЙ
БАНКОВСКИЙ ЖУРНАЛ



РУТОКЕН
Бизнес-ПРАКТИВ



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



PR integ

АТБ
ЭЛЕКТРОНИКА

infotecs
{-cademy}

m=rlion



Подписывайтесь
на наши соцсети,
там много интересного

