



Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition KG KG

Руководство получателя сертификатов

Издание	33714370.03.01.001
Документ	33714370.03.01.001 34 02
Версия	2.3.0
Листов	60
Дата	30.09.2025

АННОТАЦИЯ

Настоящий документ представляет собой руководство пользователя с ролью «Получатель сертификатов» (далее – получатель сертификатов) программного комплекса «Центр регистрации Aladdin Enterprise Registration Authority¹» (входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG»²), предназначенного для заведения и обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов), выпускаемых в программном комплексе «Центр сертификации Aladdin Enterprise Certification Authority»³ (входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG»).

Получатели сертификатов являются субъектами ресурсной системы⁴ (доменной службы каталогов), подключенной как к Центру регистрации eRA, так и к Центру сертификации eCA.

Настоящий документ является эксплуатационным документом, содержащим описание действий получателя сертификатов по управлению заявками на выпуск сертификатов, а также выпущенными по данным заявкам сертификатам. Настоящий документ содержит сведения о назначении программы, условиях ее выполнения и порядке получения доступа к интерфейсу управления.

Перед эксплуатацией программы рекомендуется внимательно ознакомиться с настоящим руководством.

¹ Далее по документу – программа или Центр регистрации Aladdin eRA.

² Далее по документу – Центр сертификатов доступа Aladdin eCA CE.

³ Далее по документу – Центр сертификации Aladdin eCA.

⁴ Далее по документу – РС.

СОДЕРЖАНИЕ

Аннотация.....	2
1 Назначение программы.....	5
1.1 Область применения.....	5
1.2 Состав программы.....	5
1.3 Функции программы.....	5
1.4 Уровень подготовки пользователя.....	6
2 Условия выполнения программы.....	7
2.1 Поддерживаемые веб-браузеры.....	7
2.2 Поддерживаемые ключевые носители.....	7
2.3 Режим функционирования программы.....	7
3 Доступ к программе.....	8
3.1 Подключение к веб-интерфейсу.....	8
3.2 Настройка Kerberos в веб-браузере.....	10
3.2.1 Настройка веб-браузера Mozilla Firefox.....	10
3.2.2 Настройка веб-браузера Chromium.....	11
3.3 Описание элементов веб-интерфейса.....	12
4 Управление заявками на выпуск сертификатов.....	15
4.1 Общие сведения о заявках.....	15
4.2 Просмотр записей о заявках.....	16
4.3 Просмотр карточки заявки на выпуск сертификата.....	20
4.4 Создание заявок на выпуск сертификатов.....	23
4.4.1 Создание заявки на основании запроса PKCS#10.....	23
4.4.2 Создание заявки с закрытым ключом PKCS#12.....	25
4.4.3 Создание заявки на ключевом носителе.....	28
4.5 Отмена заявки.....	32
5 Управление выпущенными по заявкам сертификатами.....	34
5.1 Общие сведения о работе с сертификатами.....	34
5.2 Выгрузка сертификата.....	34
5.3 Выгрузка цепочки сертификатов.....	35
5.4 Выгрузка контейнера PKCS#12.....	36
5.5 Выгрузка списка отозванных сертификатов (CRL).....	36
5.6 Выгрузка цепочки сертификатов издателя.....	36
5.7 Отзыв сертификата.....	37
5.8 Импорт сертификата на ключевой носитель.....	38
6 Поддержка протоколов MS-XCEP и MS-WSTEP.....	40

6.1 Создания политики регистрации сертификатов41

6.2 Запрос нового сертификата43

6.3 Перевыпуск сертификатов.....44

Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов45

Термины и определения57

Обозначения и сокращения59

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Область применения

Центр регистрации Aladdin eRA входит в состав Центра сертификатов доступа Aladdin eCA CE KG, который применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификацию при управлении доступом субъектов ⁵ доступа к объектам ⁶ доступа в автоматизированной (информационной) системе.

Центр регистрации Aladdin eRA предназначен для формирования и обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов) ⁷, выпускаемых Центром сертификации Aladdin eCA из состава Центра сертификатов доступа Aladdin eCA CE.

1.2 Состав программы

Центр регистрации Aladdin eRA является клиент-серверным веб-приложением и состоит из следующих программных компонентов:

- Программный компонент «Серверная часть Центра регистрации.

Программный компонент реализует функции программы, для выполнения которых оно предназначено в заданных условиях применения, в части формирования идентификационной информации, необходимой для выпуска сертификатов безопасности, выпуска и обслуживания сертификатов.

- Программный компонент «Клиентская часть Центра регистрации».

Программный компонент реализует интерфейс, с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации».

1.3 Функции программы

Основные функции Центра регистрации Aladdin eRA, доступные получателю сертификатов:

- Создание (заведения) заявок на выпуск собственных сертификатов.
- Просмотр собственных заявок на выпуск сертификатов и заявок, созданных для получателя сертификатов уполномоченными пользователями Центра регистрации Aladdin eRA с ролями «Администратор» и «Оператор».
- Создание заявок через программный интерфейс по протоколу WS-Trust X.509v3 Token Enrollment Extensions (WSTEP) ⁸.
- Загрузка файлов запросов для собственных заявок на выпуск сертификатов по запросу.
- Выгрузка сертификатов, цепочки сертификатов, списка отозванных сертификатов (CRL) и цепочки сертификатов Центра сертификации Aladdin eCA, издавшего сертификат для получателя сертификатов (субъекта PC).
- Импорт сертификатов на ключевые носители.

⁵ Субъект доступа представляет собой одну из сторон информационного взаимодействия, которая инициирует получение и получает доступ. Субъектами доступа могут являться как физические лица (пользователи), так и средства вычислительной техники (устройства), а также вычислительные процессы, инициирующие получение и получающие доступ от имени пользователей, программ, средств вычислительной техники и других программно-аппаратных устройств информационно-телекоммуникационной инфраструктуры.

⁶ Объект доступа представляет собой одну из сторон информационного взаимодействия, предоставляющую доступ. Объектами доступа могут являться как средства вычислительной техники (устройства), так и их вычислительные процессы.

⁷ Далее по документу – сертификаты.

⁸ В соответствии с документом «OASIS WS-Trust 1.3. WS-Trust X.509 Token Profile (WSTEP)».

- Выгрузка контейнера закрытого ключа для заявок на выпуск сертификата с закрытым ключом.
- Отзыв собственных сертификатов.

1.4 Уровень подготовки пользователя

Получатели сертификатов (субъекты PC) Цента регистрации Aladdin eRA должны иметь навыки в работе с применением технических средств уровня семейств операционных систем Windows и Linux.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Поддерживаемые веб-браузеры

Работа с веб-интерфейсом Центра регистрации Aladdin eRA поддерживается через веб-браузеры операционных систем РЕД ОС, Astra Linux Special Edition, Альт и SberLinux OS Server, а также операционных систем семейства Windows.

2.2 Поддерживаемые ключевые носители

Поддерживаемые модели электронных ключей (ключевых носителей):

- Jakarta:
 - JaCarta PKI.
 - JaCarta PRO.
 - JaCarta-2 PKI/ГОСТ.
 - JaCarta-2 ГОСТ.
 - JaCarta-3
- Рутокен:
 - Рутокен ЭЦП 3.0.
 - Рутокен ЭЦП 2.0.
 - Рутокен ЭЦП 2.0 Flash.
 - Рутокен ЭЦП PKI.

Для работы с ключевыми носителями JaCarta используется приложение JC-WebClient. Рекомендуется использовать приложение последней версии для 64-битных систем.

Для работы с ключевыми носителями Рутокен используется ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин».

Порядок установки JC-WebClient и ПО «Рутокен Плагин» приведен в Приложении 2.

2.3 Режим функционирования программы

Центр регистрации Aladdin eRA функционирует в следующих режимах:

- Штатный режим, при котором программа исправно функционирует, обеспечивая возможность круглосуточного выполнения задач и функций в полном объеме.
- Сервисный режим, необходимый для проведения обслуживания (обновления программы).

Основным режимом функционирования Центра регистрации Aladdin eRA является штатный режим.

Аварийный режим работы, при отказах/сбоях серверного общесистемного и специального программного обеспечения и оборудования, не предусматривается.

3 ДОСТУП К ПРОГРАММЕ

3.1 Подключение к веб-интерфейсу

Веб-интерфейс представляется собой графический интерфейс в виде совокупности динамических веб-страниц, отображаемых в веб-браузере. Веб-интерфейс реализован клиентским компонентом Центра регистрации Aladdin eRA и предназначен для управления серверным компонентом Центра регистрации Aladdin eRA (выполнения доступных пользователю в рамках его полномочий действий).

Подключение к веб-интерфейсу Центра регистрации Aladdin eRA выполняется из веб-браузера удаленно по сети передачи данных с компьютера получателя сертификатов (субъекта PC). Учетная запись получателя сертификатов автоматически активируется (регистрируется) после первой успешной авторизации в Центре регистрации Aladdin eRA.

Канал управления является защищенным – организован по протоколу HTTPS/TLS с односторонней или двусторонней аутентификацией⁹ и шифрованием передаваемых данных. Для проверки подлинности сертификата веб-сервера Центра регистрации Aladdin eRA получите у администратора и установите в хранилище «Доверенные корневые центры сертификации» корневой сертификат издающего Центра сертификации Aladdin eCA, к которому подключен Центр регистрации Aladdin eRA.

Получатели сертификатов (субъекты PC) (пользователи с доменными учётными записями¹⁰) могут проходить идентификацию и аутентификацию в Центре регистрации Aladdin eRA по комбинации доменного имени и пароля или по Kerberos-билету. Для успешной аутентификации в веб-браузере должна быть настроена Kerberos-аутентификация (инструкция по настройке приведена в разделе 3.2). Информация о домене отображена в окне авторизации в поле «Домен».

Порядок подключения к веб-интерфейсу Центра регистрации Aladdin eRA:

- Запустите веб-браузер и в адресной строке введите IP-адрес или доменное имя компьютера, на котором установлен Центр регистрации Aladdin eRA (например, <https://172.22.5.21>).
- На открывшейся странице с предупреждением системы безопасности (см. Рисунок 1) нажмите кнопку <Дополнительно>, примите риск и продолжите подключение.

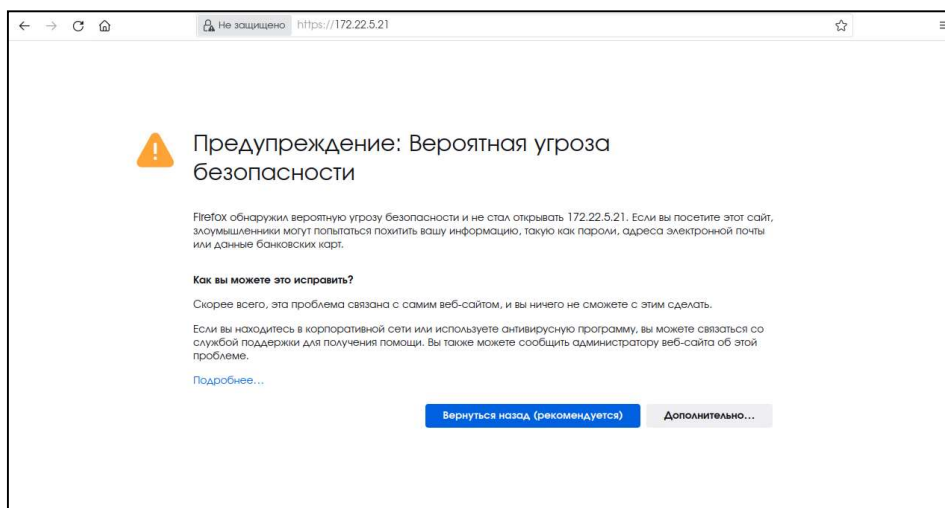


Рисунок 1 – Страница с предупреждением системы безопасности

⁹ Двусторонняя аутентификация обеспечивается, если на компьютере получателя сертификатов в хранилище ОС или используемого веб-браузера установлен сертификат, выпущенный в Центре сертификации Aladdin eCA, к которому подключен Центр регистрации Aladdin eRA, а при подключении к веб-интерфейсу получатель сертификатов выбрал его. При этом аутентификация в Центре регистрации Aladdin eRA по данному сертификату получателю сертификатов недоступна.

¹⁰ Учётные записи, находящиеся в домене, к которому подключён Центр регистрации Aladdin eRA.

- После установки TLS-соединения для неаутентифицированного пользователя отображается интерфейс для прохождения процедуры идентификации и аутентификации (см. Рисунок 2).

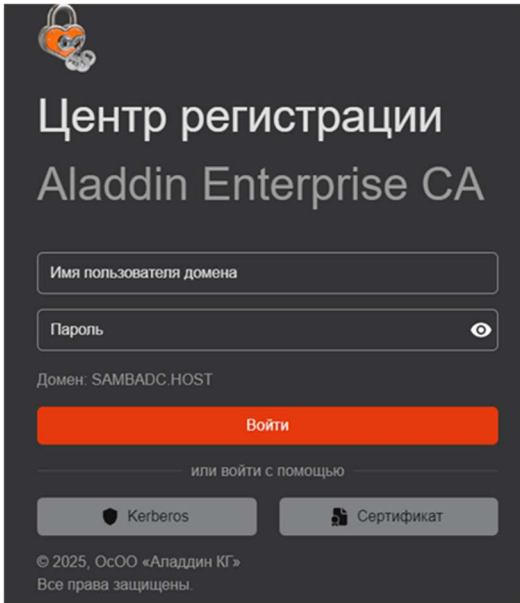



Рисунок 2 – Окно авторизации

- Для идентификации и аутентификации по комбинации доменного имени и пароля введите в соответствующих полях доменное имя и пароль учетной записи получателя сертификатов (субъекта PC), нажмите на кнопку **<Войти>**.
- Для идентификации и аутентификации с помощью Kerberos-билета нажмите кнопку  Kerberos.

Если у пользователя отсутствовала ¹¹ учётная запись в Центре регистрации Aladdin eRA, то она будет автоматически создана с ролью «Получатель сертификатов» после первой авторизации.

В результате получателю сертификатов (субъекту PC) будет предоставлен доступ к веб-интерфейсу Центра регистрации Aladdin eRA (описание см. в разделе 3.3).

При идентификации и аутентификации по доменному имени и паролю могут возникать ошибки, приведенные в таблице ниже (Таблица 1).

Таблица 1 – Типовые ошибки при аутентификации по доменному имени и паролю

Ошибка	Описание
«Аккаунт заблокирован»	Доменная учётная запись или учётная запись заблокирована в программе
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи в Центре регистрации Aladdin eRA.

¹¹ Проверка связи осуществляется путём сравнения идентификатора учётной записи в домене с идентификаторами учётных записей в базе данных Центра регистрации Aladdin eRA.

При аутентификации по Kerberos-билету могут возникать ошибки, приведенные в таблице ниже (Таблица 2).

Таблица 2 – Типовые ошибки при аутентификации по Kerberos-билету

Ошибка	Описание
«Full authentication is required to access this resource»	Браузер не был настроен для аутентификации по Kerberos-билету – необходимо выполнить инструкцию по настройке браузера.
«Срок действия Kerberos-билета истек»	Срок действия Kerberos-билета истек – необходимо получить новый билет или продлить срок его действия.
«Аккаунт заблокирован»	Доменная учётная запись или учётная запись в программе заблокирована.
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи в программе.

3.2 Настройка Kerberos в веб-браузере

Для того, чтобы в веб-браузере получателя сертификатов при работе с Центром регистрации Aladdin eRA была доступна аутентификация по Kerberos-билету необходимо внести доменное имя Центра регистрации Aladdin eRA в список доверенных URI, для которых используется аутентификация по Kerberos-билету.

3.2.1 Настройка веб-браузера Firefox

Далее в примере:

- `aeca.al.kg.com`, `aeca1.al.kg.com` – доменные имена Центров регистрации Aladdin eRA
- `al.kg.com` – домен, (`AL.KG.com` – realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Запустите веб-браузер Mozilla Firefox.
- В адресной строке введите `about:config`.
- Нажмите на кнопку **<Принять риск и продолжить>**.
- В поле поиска введите `negotiate`, чтобы ограничить список отображаемых параметров.
- Установите параметру `network.negotiate-auth.trusted-uris` одно из следующих значений (см. Рисунок 3):
 - Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, введите полное доменное Центра регистрации Aladdin eRA (например, `aeca.al.kg.com`).
 - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена с точкой в начале (например, `.al.kg.com`).
 - Чтобы разрешить SPNEGO аутентификацию для нескольких Центров регистрации Aladdin eRA, введите их полные доменные имена через запятую (например, `aeca.al.kg.com, aeca1.al.kg.com`).
- Продублируйте введенное значение параметра `network.negotiate-auth.trusted-uris` в параметре `network.negotiate-auth.delegation-uris`.

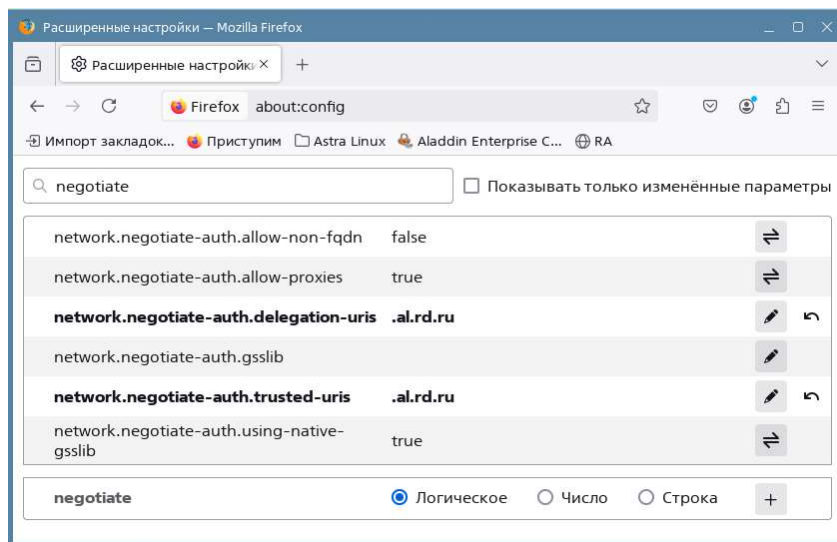


Рисунок 3 – Настройка Kerberos-аутентификации в веб-браузере Mozilla Firefox

3.2.2 Настройка веб-браузера Chromium

Далее в примере:

- `aeca.al.kg.com`, `aeca1.al.kg.com` – доменные имена Центров регистрации Aladdin eRA
- `al.kg.com` – домен, (`AL.KG.com` – realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Создайте в каталоге `/etc/chromium/policies/managed` файл `policies.json`, выполнив следующую команду с правами суперпользователя:

```
sudo touch /etc/chromium/policies/managed/policies.json
```

- Откройте файл для редактирования, выполнив следующую команду с правами суперпользователя:

```
sudo nano /etc/chromium/policies/managed/policies.json
```

- В файле `policies.json` укажите следующие политики в формате JSON:

```
{
  "AuthServerAllowlist": "*.al.kg.com",
  "AuthSchemes": "ntlm,negotiate"
}
```

Примечания:

- Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, укажите для политики «AuthServerAllowlist» полное доменное Центра регистрации Aladdin eRA (например, `aeca.al.kg.com`).
- Чтобы разрешить SPNEGO аутентификацию для целого домена, укажите для политики «AuthServerAllowlist» имя домена (например, `*.al.kg.com`).
- Чтобы разрешить SPNEGO аутентификацию для нескольких Центров регистрации Aladdin eRA, укажите для политики «AuthServerAllowlist» их полные доменные имена через запятую (например, `aeca.al.kg.com, aeca1.al.kg.com`).
- Запустите веб-браузер Chromium и введите в адресной строке `chrome://policy`.
- Убедитесь, что политики были применены (см. Рисунок 4).

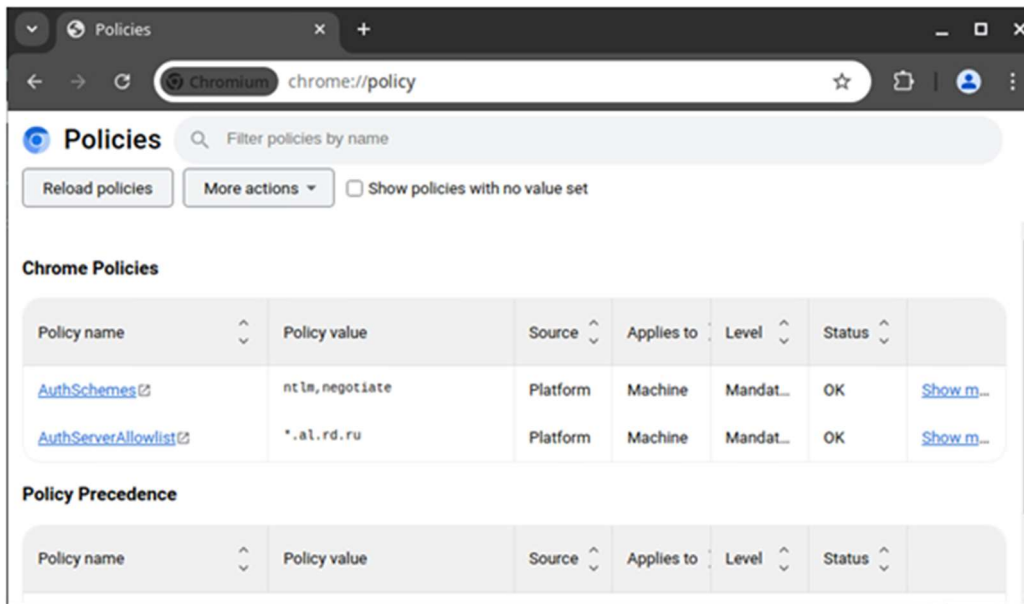


Рисунок 4 – Настройка Kerberos-аутентификации в веб-браузере Chromium

3.3 Описание элементов веб-интерфейса

Главный экран веб-интерфейса Центра регистрации Aladdin eRA для получателя сертификатов (субъекта PC) представлен на рисунке ниже (Рисунок 5).

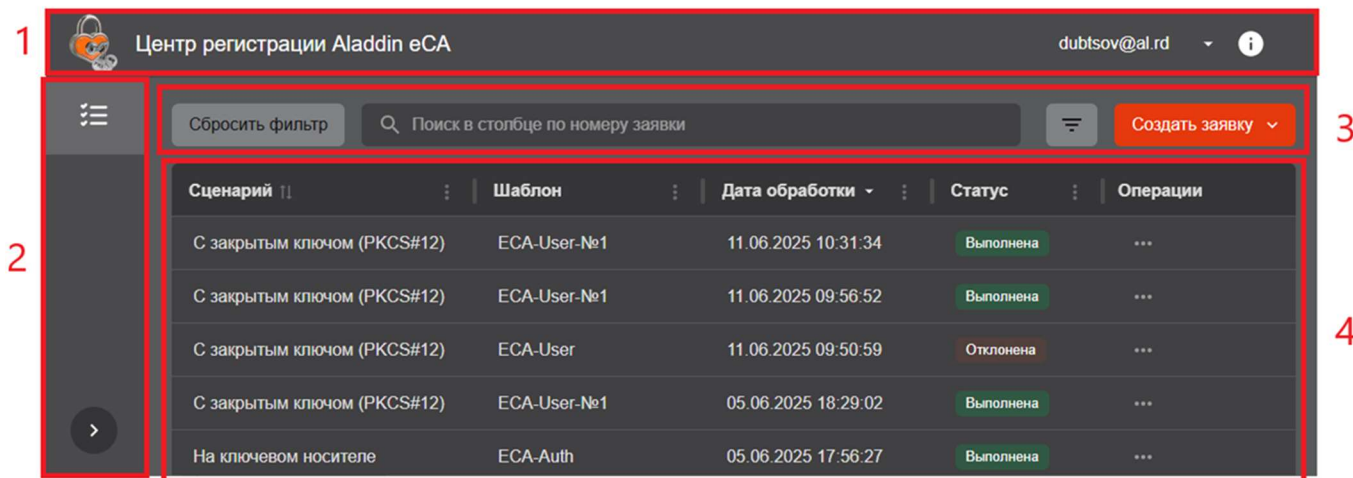


Рисунок 5 – Основные элементы веб-интерфейса

Цифрами на рисунке обозначены:

1 Верхняя панель (заголовок)

Заголовок отображается на всех страницах веб-интерфейса Центра регистрации Aladdin eRA и содержит следующие инструменты:

- Меню авторизованного получателя сертификатов (Рисунок 6).

Название меню соответствует имени учетной записи пользователя. Меню предназначено завершения рабочей сессии текущего пользователя. Для этого выберите в меню пункт <Выход>.

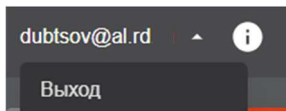



Рисунок 6 – Завершение рабочей сессии

-  - значок предназначен для предоставления сведений о текущей версии программы, контактной информации разработчика, правах на программное обеспечение (Рисунок 7).

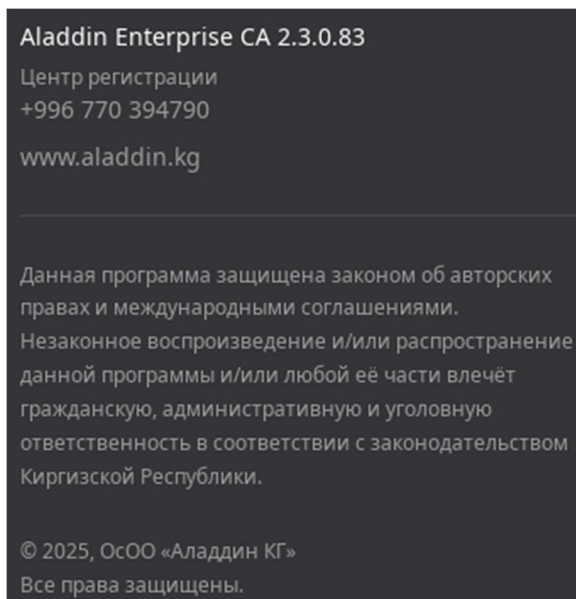




Рисунок 7 – Информация о программе

2 Боковая панель (панель навигации)

Боковая панель закреплена и отображается на любом шаге или переходе между разделами при ширине окна браузера больше или равной 1200 px. При ширине окна браузера менее 1200 px боковая панель скрыта и отображается только при нажатии на кнопку , которая отображается только в данном режиме.

Полный вид боковой панели показан на рисунке ниже (Рисунок 8). Скрытый вид боковой панели показан на рисунке выше (Рисунок 5). Выбор вида боковой панели происходит по нажатию кнопки , расположенной внизу данной панели.

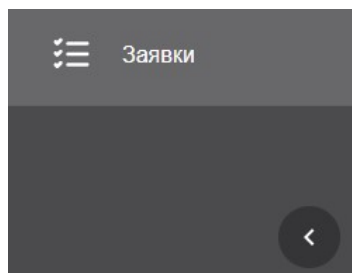


Рисунок 8 – Полный и скрытый виды боковой панели

Для получателя сертификатов боковая панель состоит из одного раздела «Заявки», предоставляющего следующие возможности:

- Просмотр списка заявок в табличном виде.
- Просмотр карточки заявки.
- Создание заявки на выпуск сертификата на основании запроса.
- Создание заявки на выпуск сертификата с закрытым ключом PKCS#12.
- Создание заявки на выпуск сертификата на ключевом носителе.
- Отмена заявки.
- Выгрузка сертификата.

- Импорт сертификата на ключевой носитель.
- Выгрузка цепочки сертификатов.
- Выгрузка контейнера закрытого ключа PKCS#12.
- Выгрузка CRL издателя.
- Выгрузка цепочки сертификатов издателя.
- Отзыв сертификата.

3 Панель инструментов

Панель предназначена для размещения элементов управления информацией, представленной на панели просмотра (кнопки, поле поиска, меню).

4 Панель просмотра

Панель предназначена для отображения информации раздела (списка заявок и карточки выбранной заявки).

4 УПРАВЛЕНИЕ ЗАЯВКАМИ НА ВЫПУСК СЕРТИФИКАТОВ

4.1 Общие сведения о заявках

Процесс подачи заявки на выпуск сертификата включает:

- Выбор шаблона, по которому будет выпущен сертификат.



Получателю сертификатов (субъекту PC) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту PC), так и группе безопасности, в которую входит получатель сертификатов (субъект PC). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

- Редактирование (при необходимости) атрибутов сертификата согласно выбранному шаблону (не выполняется при подаче заявки на основание запроса на сертификат PKCS#10¹²).
- Указание пароля для защиты контейнера PKCS#12 (только при подаче заявки с закрытым ключом PKCS#12¹³).
- Выбор алгоритма и длины ключа для генерации ключевой пары (не выполняется при подаче заявки на основание запроса на сертификат PKCS#10).

Получателю сертификатов (субъекту PC) доступны следующие действия по управлению заявками на выпуск сертификатов:

- Подача (создание) новой заявки:
 - На основании запроса PKCS#10 (см. раздел 4.4.1).
 - С закрытым ключом PKCS#12 (см. раздел 4.4.2).
 - На ключевом носителе (см. раздел 4.4.3).
- Просмотр информации о созданных заявках (в том числе и о заявках, созданных уполномоченными пользователями Центра регистрации Aladdin eRA с ролями «Администратор» и «Оператор» (см. раздел 4.2)).
- Просмотр карточки заявки с подробной информацией (в том числе информации о сертификате после его выпуска в Центре сертификации Aladdin eCA по данной заявке) (см. раздел 4.3).
- Отмена созданной заявки, которая еще не рассмотрена уполномоченными пользователями Центра регистрации Aladdin eRA с ролями «Администратор» и «Оператор» или обработана после создания Центром регистрации Aladdin eRA с ошибкой (см. раздел 4.5).

Заявка на выпуск сертификата имеет следующие атрибуты:

- Номер заявки – уникальный идентификатор, назначаемый заявке при создании.
- Статус – текущий статус заявки:
 - Ошибка выпуска – выпуск сертификата по данной заявке завершился ошибкой.
 - Отклонена – заявка отклонена уполномоченным пользователем Центра регистрации Aladdin eRA.


¹² В соответствии с документом «RFC 2986. PKCS #10: Certification Request Syntax Specification Version 1.7».

¹³ В соответствии с документом «RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1»

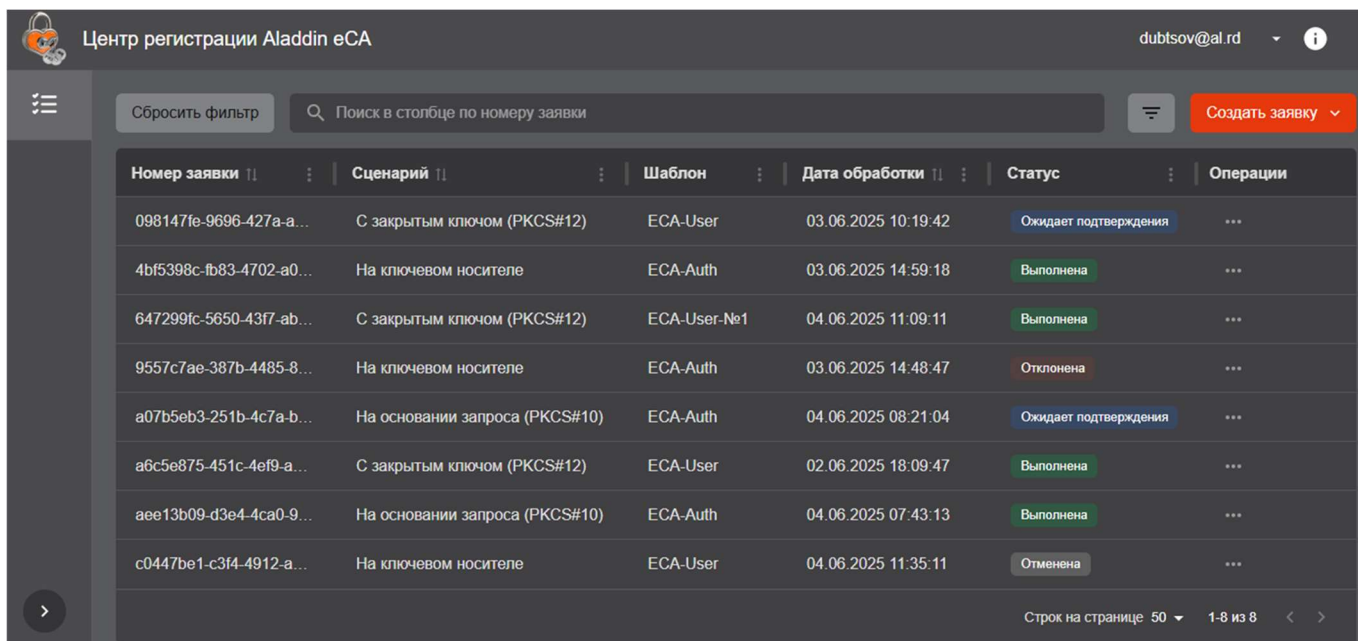
- Ожидает подтверждения – заявка создана, получателю сертификатов (субъекту) назначены правила выпуска с автоматизированной (ручной) обработкой заявок уполномоченным пользователем Центра регистрации Aladdin eRA.
- Выполнена – заявка обработана, в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта) успешно выпущен сертификат.
- Отменена – заявка отменена получателем сертификатов (субъектом) или иным уполномоченным пользователем Центра регистрации Aladdin eRA.
- Ожидает импорта на КН – заявка обработана, в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта) успешно выпущен сертификат, который ожидает импорта на ключевой носитель.
- Новая – статус присваивается заявке при ее регистрации, сразу после этого происходит обработка заявки и её статус изменяется. Данный статус может быть отображен в веб-интерфейсе в случае ошибки при первичной обработке заявки.
- Общая информация о заявке:
 - Сценарий – наименование сценария, по которому была создана заявка на выпуск сертификата:
 - На основании запроса (PKCS#10).
 - С закрытым ключом (PKCS#12).
 - На ключевом носителе.
 - WSTEP ¹⁴.
 - Шаблон – шаблон, по которому будет или уже выпущен сертификат.
 - Центр сертификации – центр сертификации, в котором будет и уже выпущен сертификат по данной заявке, на основании используемого в сценарии создания заявки шаблона.
 - Внешний идентификатор – идентификатор из запроса на выпуск сертификата PKCS#10.
 - Дата создания – дата и время создания заявки.
 - Дата обработки – дата и время последней смены статуса (обработки) заявки (например, создание или отмена заявки).
 - Комментарий – комментарий, указанный уполномоченным пользователем Центра регистрации Aladdin eRA при обработке заявки.
- Информация об истории изменения заявки:
 - Дата – дата и время события, связанного с изменением заявки.
 - Имя учётной записи – отображаемое имя пользователя (получателя сертификатов), сделавшего изменение в заявке.
 - Событие – описание события, связанного с изменениями заявки (например, создание заявки).

4.2 Просмотр записей о заявках

Получателю сертификатов (субъекту PC) доступен просмотр созданных им заявок, а также заявок, созданных для него уполномоченными пользователями Центра регистрации Aladdin eRA с ролями «Администратор» и «Оператор».

Для просмотра информации о заявках на сертификаты подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки** (см. Рисунок 9).

¹⁴ Заявки по сценарию «WSTEP» создаются в Центре регистрации Aladdin eRA автоматически в результате обработки запросов получателей сертификатов (субъектов PC) по протоколу MS-WSTEP (см. раздел 6).



Центр регистрации Aladdin eCA

Сбросить фильтр

Поиск в столбце по номеру заявки

Создать заявку

Номер заявки	Сценарий	Шаблон	Дата обработки	Статус	Операции
098147fe-9696-427a-a...	С закрытым ключом (PKCS#12)	ECA-User	03.06.2025 10:19:42	Ожидает подтверждения	...
4bf5398c-fb83-4702-a0...	На ключевом носителе	ECA-Auth	03.06.2025 14:59:18	Выполнена	...
647299fc-5650-43f7-ab...	С закрытым ключом (PKCS#12)	ECA-User-№1	04.06.2025 11:09:11	Выполнена	...
9557c7ae-387b-4485-8...	На ключевом носителе	ECA-Auth	03.06.2025 14:48:47	Отклонена	...
a07b5eb3-251b-4c7a-b...	На основании запроса (PKCS#10)	ECA-Auth	04.06.2025 08:21:04	Ожидает подтверждения	...
a6c5e875-451c-4ef9-a...	С закрытым ключом (PKCS#12)	ECA-User	02.06.2025 18:09:47	Выполнена	...
aee13b09-d3e4-4ca0-9...	На основании запроса (PKCS#10)	ECA-Auth	04.06.2025 07:43:13	Выполнена	...
c0447be1-c3f4-4912-a...	На ключевом носителе	ECA-User	04.06.2025 11:35:11	Отменена	...

Строк на странице 50 1-8 из 8

Рисунок 9 – Просмотр списка заведенных заявок получателя сертификатов (субъекта PC)

Информация о заявках отображается списком в табличном виде.

По умолчанию в колонках таблицы отображаются следующие атрибуты заявок на выпуск сертификатов:

- Номера заявок.
- Сценарии, по которым заведены заявки.
- Наименования шаблонов, по которым будут и уже выпущены сертификаты по заявкам.
- Дата и время последней смены статуса (обработки) заявок.
- Текущие статусы заявок.

Записи о заявках выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 10).

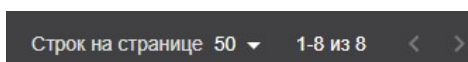






Рисунок 10 – Инструменты навигации списка заявок

Описание инструментов навигации:

- > – переход на следующую страницу списка.
- < – переход на предыдущую страницу списка.
- [] – выбор количества записей, отображаемых на одной странице списка.

Для удобства анализа информации о заявках в списке вы можете управлять видимостью колонок таблицы с заявками. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок  **<Действие колонки>** и в открывшемся списке ¹⁵ выберите  **<Скрыть [название колонки] колонку>** (см. Рисунок 11). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок  **<Действие колонки>** и в открывшемся списке выберите  **<Показать все колонки>** (см. Рисунок 11).

¹⁵ Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

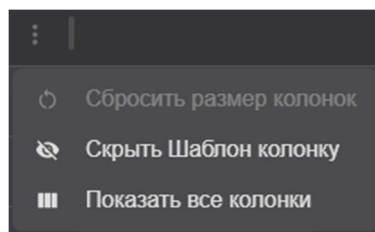


Рисунок 11 – Список действий с колонкой **[Шаблон]**


Для поиска заявок в списке вы можете выполнить сортировку (упорядочивание) записей о заявках по выбранному атрибуту, представленному в соответствующей колонке. В зависимости от информации, представленной в колонке списка, упорядочивание записей может выполняться по следующим принципам:



- В алфавитном порядке.
- В порядке убывания или возрастания временных меток.

Сортировка (упорядочивание) записей о заявках возможна по следующим атрибутам (колонкам):

- По номеру заявки в алфавитном порядке.
- По сценариям заведения заявок в алфавитном порядке.
- По дате и времени последней смены статуса (обработки) заявок в порядке убывания или возрастания временных меток.

По умолчанию сортировка записей о заявках в списке выполнена по номеру заявки в алфавитном порядке (в порядке возрастания).

Чтобы выполнить сортировку записей о заявках по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок  **<Действие колонки>** и в открывшемся списке ¹⁶ (см. Рисунок 12) выберите:

- Для упорядочивания по возрастанию –  **<Сортировать [название колонки] по возрастанию>**.
- Для упорядочивания по убыванию –  **<Сортировать [название колонки] по убыванию>**.

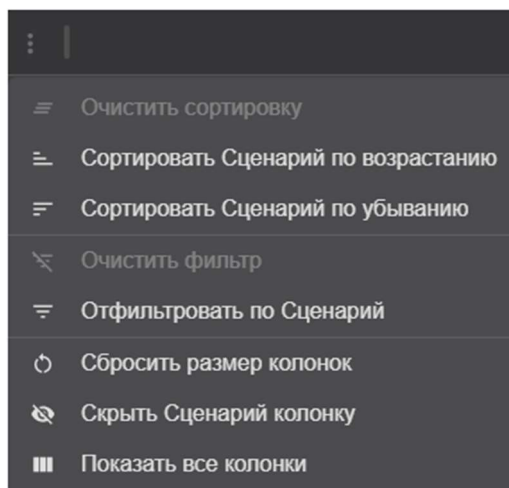







Рисунок 12 – Список действий с колонкой **[Сценарий]**

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками ¹⁷ (см. Рисунок 12):

-  – сортировка выполнена в порядке возрастания.
-  – сортировка выполнена в порядке убывания.
-  – сортировка не выполнена.

¹⁶ Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.




¹⁷ Менять порядок сортировки, а также отменять сортировку можно, последовательно щелкая на значок статуса сортировки по колонке.


Чтобы отменить сортировку записей о заявках по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок  **<Действие колонки>** и в открывшемся списке ¹⁸ (см. Рисунок 12) выберите  **<Очистить сортировку>**.

Для поиска заявок в списке вы можете выполнить выборку записей о заявках с помощью фильтров, расположенных в заголовках колонок. Каждый фильтр предназначен для выборки информации по атрибуту заявки, представленному в данной колонке. Возможно выполнить выборку информации, применив одновременно несколько фильтров.

Выборку записей о заявках возможно выполнить с помощью фильтров по следующим атрибутам:

- По сценариям заведения заявок.
- По дате и времени последней смены статуса (обработки) заявок.
- По статусам заявок.

По умолчанию фильтры скрыты. Чтобы использовать фильтры, нажмите на панели инструментов кнопку  **<Фильтр>** или щелкните в заголовке колонок **[Сценарий]**, **[Дата обработки]** или **[Статус]** значок  **<Действие колонки>** и в открывшемся списке (см. Рисунок 12) выберите  **<Отфильтровать по [название колонки]>** (см. Рисунок 13).

Чтобы скрыть фильтры, нажмите на панели инструментов кнопку  **<Фильтр>**. При этом выборка записей о заявках, выполненная с помощью фильтров, сохраняется.

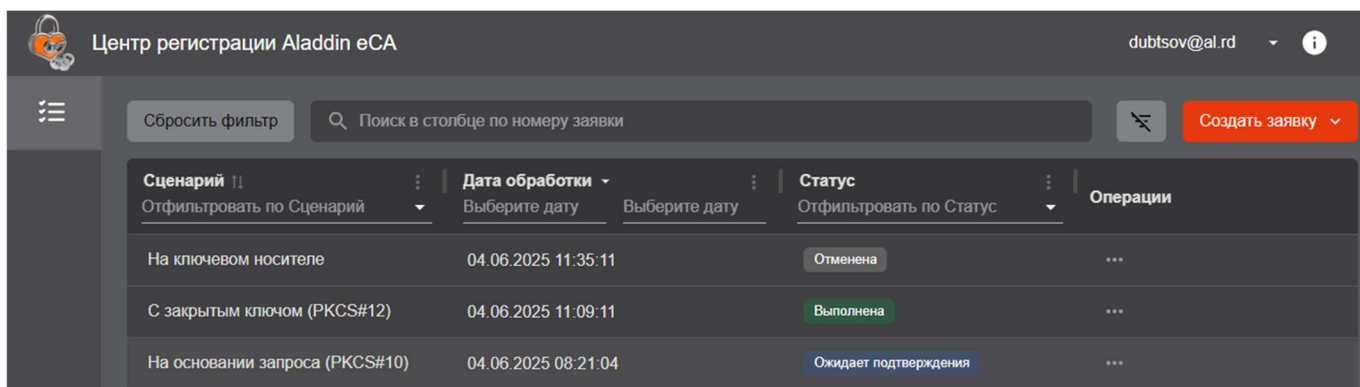


Рисунок 13 – Отображение фильтров в заголовках колонок включено

Чтобы выполнить выборку информации с помощью фильтра (открыть окно фильтра), щелкните название фильтра в заголовке колонки.

Фильтры по атрибутам заявок, представленным в колонках **[Сценарий]** (см. Рисунок 14а) и **[Статус]** (см. Рисунок 14б), обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов.

Фильтр по атрибуту заявок, представленном в колонке **[Дата обработки]** (см. Рисунок 14в), обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок (см. Рисунок 14).

Признаком применения фильтра является значок  в заголовке соответствующей колонки (см. Рисунок 14).

¹⁸ Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

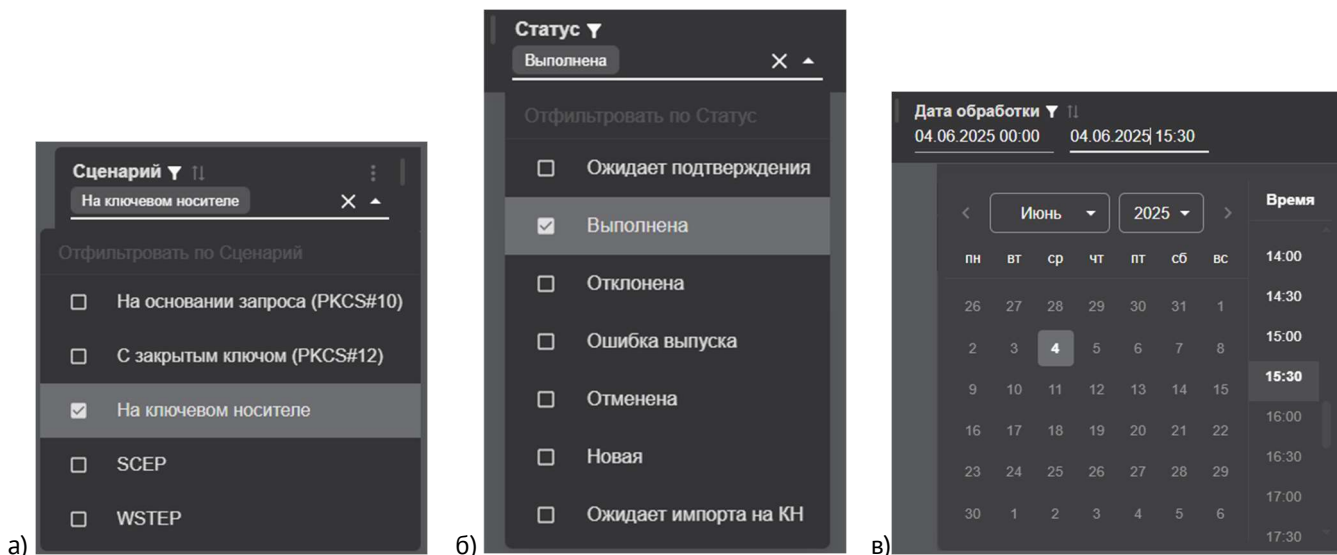


Рисунок 14 – Указание критериев выборки в фильтрах

Чтобы отменить действие определенного фильтра, щелкните в заголовке колоноки значок **<Действие колоноки>** и в открывшемся списке (см. Рисунок 12) выберите **<Очистить фильтр>** или щелкните в заголовке колоноки значок (только для колонок **[Сценарий]** (см. Рисунок 14а) и **[Статус]** (см. Рисунок 14б)).

Чтобы отменить действие всех фильтров, нажмите на панели инструментов кнопку **Сбросить фильтр**.

Чтобы выполнить выборку записей о заявках по их номерам, введите в поисковой строке, расположенной на панели инструментов, ключевое слово, содержащееся в номере заявки (см. Рисунок 15). Для отмены выборки заявок по их номерам щелкните в поисковой строке значок .

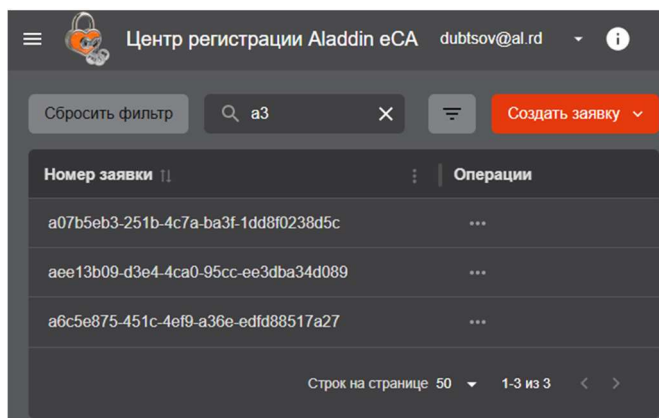


Рисунок 15 – Выборка заявок по их номерам с помощью поисковой строки

4.3 Просмотр карточки заявки на выпуск сертификата

Карточка заявки содержит представленную в удобном для анализа виде подробную информацию о заявке, а также информацию о сертификате в случае, если по заявке уже выпущен сертификат.

Чтобы открыть карточку заявки:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Найдите нужную заявку (см. раздел 4.2) и щелкните запись о ней в списке.

В результате откроется карточка заявки.

Карточка заявки, по которой еще не выпущен сертификат, представлена на рисунке ниже (см. Рисунок 16). Описание атрибутов заявки приведено в разделе 4.1.

Заявка №a07b5eb3-251b-4c7a-ba3f-1dd8f0238d5c

Ожидает подтверждения

Заявка

Сценарий

На основании запроса (PKCS#10)

Шаблон

ECA-Auth

Центр сертификации

CA-1

Внешний идентификатор

-

Дата создания

04.06.2025 08:21:04

Дата обработки

04.06.2025 08:21:04

Комментарий

-

История изменения заявки

Дата	Имя учетной записи	Событие
04.06.2025 08:21:04	dubtsov@al.rd	Создание заявки
04.06.2025 08:21:04	dubtsov@al.rd	Обработка заявки

Рисунок 16 – Карточка заявки, по которой еще не выпущен сертификат

Карточка заявки, по которой уже выпущен сертификат, представлена на рисунке ниже (см. Рисунок 17). Описание атрибутов заявки (блоки «Заявка» и «История изменений заявки») приведено в разделе 4.1.

← Заявки

Заявка №647299fc-5650-43f7-ab0e-283aed67a633

Выполнена

Сертификат активирован

Заявка

Цепочка сертификатов

Издатель

Root-CA2

Владелец

Дубцов

SDN владельца

CN=Дубцов,C=RU,C=BY

Действует с

04.06.2025 11:09:27

Действует по

04.06.2027 11:09:27

Алгоритм ключа

RSA

Длина ключа

1024

Состав сертификата

История изменения заявки

Рисунок 17 – Карточка заявки, по которой выпущен сертификат

Карточка заявки, по которой уже выпущен сертификат (см. Рисунок 17), содержит также информацию о выпущенном по ней сертификате (статус сертификата, блоки «Цепочка сертификатов», «Информация о сертификате» и «Состав сертификата»).

Статус сертификата отображен на панели инструментов карточки заявки. После выпуска сертификату назначается статус «Активирован». Получатель сертификатов (субъект PC) уполномочен при необходимости отозвать сертификат (см. раздел 5.7).

В блоке «Цепочка сертификатов» (см. Рисунок 18) представлена иерархическая коллекция сертификатов, которая ведёт от сертификата, выпущенного по данной заявке, к корню доверия (корневому центру сертификации).

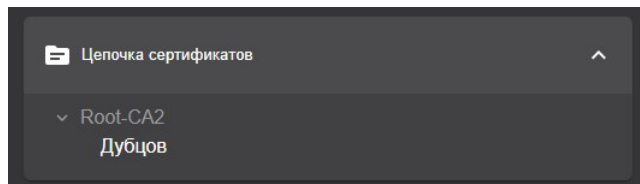


Рисунок 18 – Блок «Цепочка сертификатов»

В блоке «Информация о сертификате» (см. Рисунок 19) представлена следующая информацию о сертификате:

- Издатель – поле «Issuer» сертификата.
- Владелец – атрибут «CN» из поля «Subject» сертификата.
- SDN владельца – поле «Subject» сертификата.
- Действует с – атрибут «Not Before» из поля «Validity» сертификата.
- Действует по – атрибут «Not After» из поля «Validity» сертификата.
- Алгоритм ключа – атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата.
- Длина ключа – атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата.

В блоке «Состав сертификата» (см. Рисунок 19) представлена следующая информация о сертификате:

- Серийный номер – поле «Serial Number» сертификата.
- Открытый ключ – поле «Subject Public Key Info».
- Отпечаток – вычисляемое значение, отсутствует в сертификате.
- Версия – поле «Version» сертификата.
- Параметр открытого ключа – всегда «X509».
- Алгоритм цифровой подписи – поле «Signature Algorithm».
- Основные ограничения – поле «X509v3 Basic Constraints».
- Использование ключа – поле «X509v3 Key Usage» сертификата.
- Доступ к информации о центре сертификации – поле «Authority Information Access».
- Идентификатор ключа центра – поле «X509v3 Authority Key Identifier» сертификата.
- Альтернативное имя субъекта – поле «X509v3 Subject Alternative Name» сертификата.
- Идентификатор ключа субъекта – поле «X509v3 Subject Key Identifier» сертификата.
- Расширенное использование ключа – поле «X509v3 Extended Key Usage» сертификата.

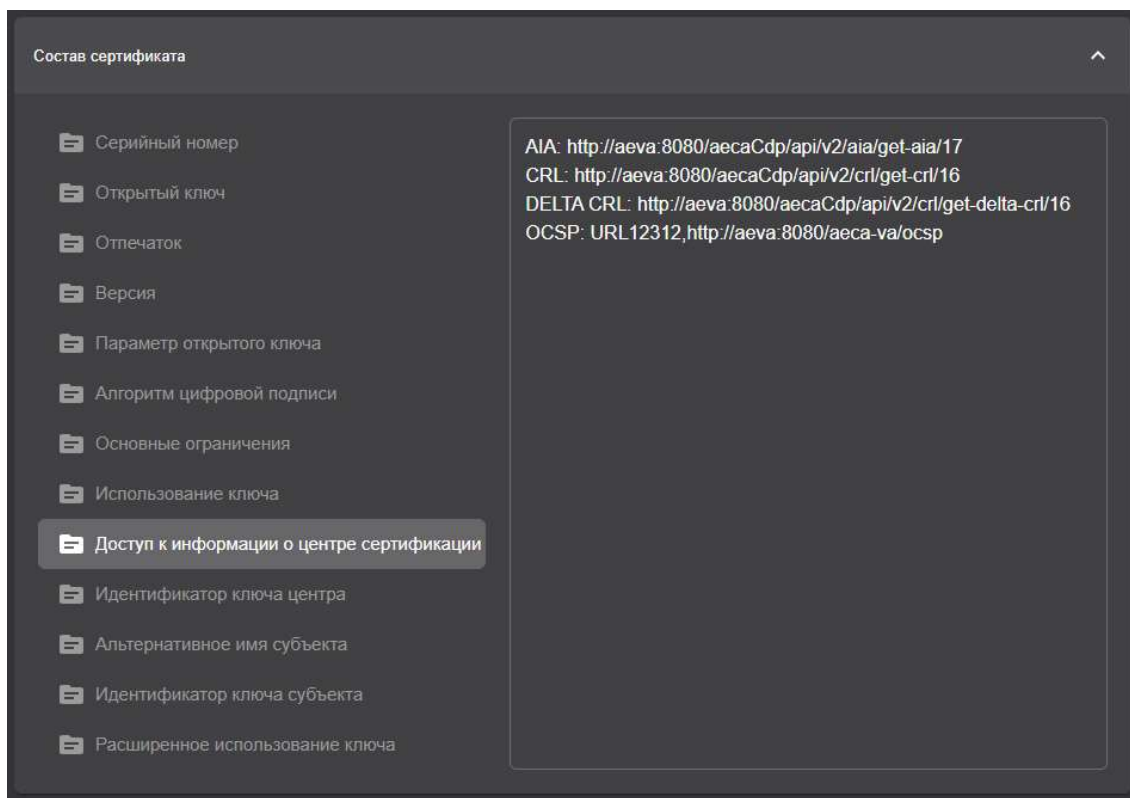


Рисунок 19 – Блок «Состав сертификата»

4.4 Создание заявок на выпуск сертификатов


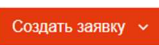
Внимание! Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

4.4.1 Создание заявки на основании запроса PKCS#10

Предварительные условия для создания заявки на основании запроса на выпуск сертификата PKCS#10:

- Файл с запросом на выпуск сертификата PKCS#10 в формате CSR или REQ для получателя сертификата (субъекта ресурсной системы) должен быть предварительно подготовлен средствами стороннего ПО (например, с помощью приложения Единый клиент JaCarta).
- Файл с запросом на выпуск сертификата PKCS#10 должен быть сформирован с учетом известных данных шаблонов Центра сертификации Aladdin eCA, доступных получателю сертификатов (субъекту ресурсной системы) на основании назначенных ему уполномоченным пользователем Центр регистрации Aladdin eRA правил выпуска сертификатов (например, для использования шаблона «Domain Controller» для создания заявки на выпуск сертификата в запросе должны быть указаны атрибуты «DNS Name» и «MS GUID»).
- На основании предоставленного при создании заявки файла с запросом ранее в Центре сертификации Aladdin eCA, к которому подключен Центр регистрации Aladdin eRA, не было выпущено сертификатов.

Порядок создания заявки на выпуск сертификата на основании запроса PKCS#10:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- На панели инструментов нажмите кнопку  и выберите в открывшемся списке сценарий создания заявки **<На основании запроса>** (см. Рисунок 20).

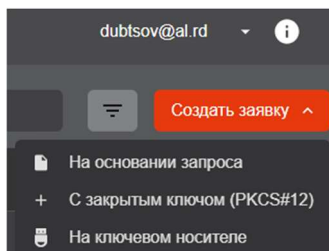


Рисунок 20 – Выбор сценария создания заявки

- В открывшемся окне «Создание заявки» (см. Рисунок 21):
 - Нажмите кнопку **Выбрать файл** и укажите путь к файлу с запросом на сертификат.
 - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат ¹⁹.
 - Нажмите кнопку **Создать заявку**.

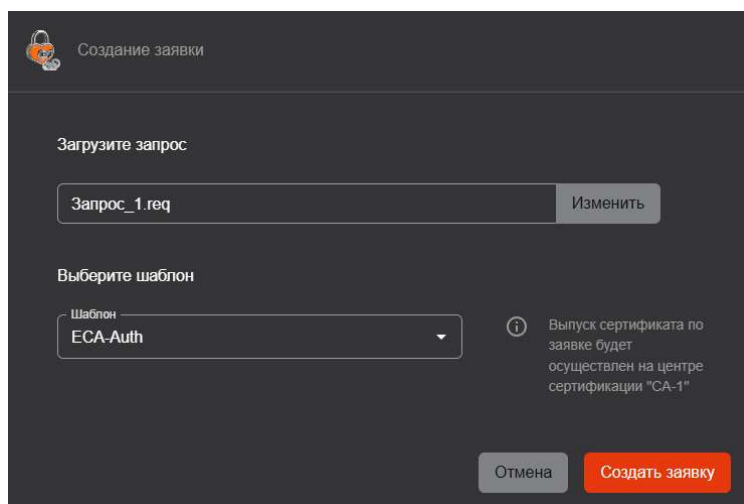


Рисунок 21 – Выбор файла с запросом и шаблона для выпуска сертификата

После заведения заявки файл с запросом на выпуск сертификата PKCS#10 можно выгрузить из Центра регистрации Aladdin eRA. Выгрузка доступна при любом статусе заявки. Выгрузку файла с запросом возможно выполнить как при просмотре списка заявок, так и из карточки заявки:

- Найдите заявку, из которой нужно выгрузить запрос, в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **...** **<Операции строки>** и выберите в открывшемся списке **<Скачать запрос PKCS#10>** (см. Рисунок 22).

¹⁹ Получателю сертификатов (субъекту PC) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту PC), так и группе безопасности, в которую входит получатель сертификатов (субъект PC). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

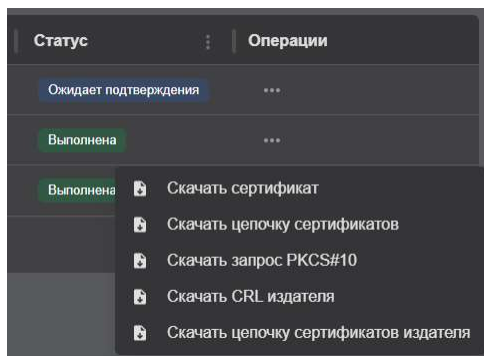


Рисунок 22 – Выгрузка запроса на выпуск сертификата

- Откройте карточку заявки, из которой нужно выгрузить запрос, (см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать запрос PKCS#10>** (см. Рисунок 23).

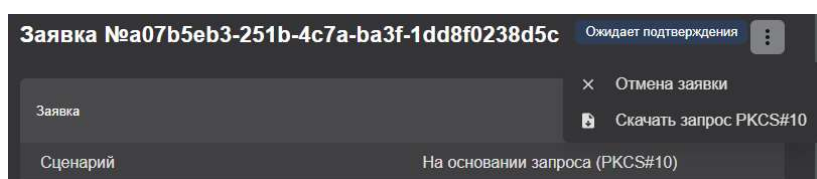


Рисунок 23 – Выгрузка запроса на выпуск сертификата

4.4.2 Создание заявки с закрытым ключом PKCS#12

Порядок создания заявки с закрытым ключом PKCS#12:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку **Создать заявку** и выберите в открывшемся списке сценарий создания заявки **<На основании запроса>** (см. Рисунок 20).
- В открывшемся окне «Создание заявки» (шаг 1 сценария) (см. Рисунок 24) в списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат ²⁰, и нажмите кнопку **Продолжить**.

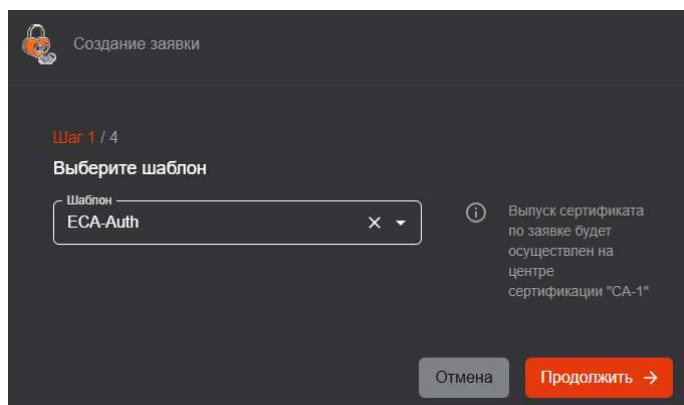


Рисунок 24 – Выбор шаблона для выпуска сертификата

²⁰ Получателю сертификатов (субъекту PC) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту PC), так и группе безопасности, в которую входит получатель сертификатов (субъект PC). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

- В открывшемся окне «Создание заявки» (шаг 2 сценария) (см. Рисунок 25) укажите атрибуты получателя сертификатов (субъекта PC):



Значения атрибутов заполняются автоматически в соответствии с данными получателя сертификатов (субъекта PC), полученными из Центра сертификации Aladdin eCA, выберите в списке атрибута нужное значение или добавьте новый такой же атрибут с другим значением.

- При необходимости выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта PC) содержится несколько значений (см. Рисунок 25).

Рисунок 25 – Редактирование атрибутов получателя сертификатов (субъекта PC)



- При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку  и выберите в списках новых атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта PC) содержится несколько значений) (см. Рисунок 26).

Рисунок 26 – Добавлен новый атрибут

- При необходимости добавленные атрибуты можно удалять. Для этого нажмите рядом со списком атрибута кнопку .



В случае отсутствия у получателя сертификатов (субъекта PC) обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке (см. Рисунок 27). При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

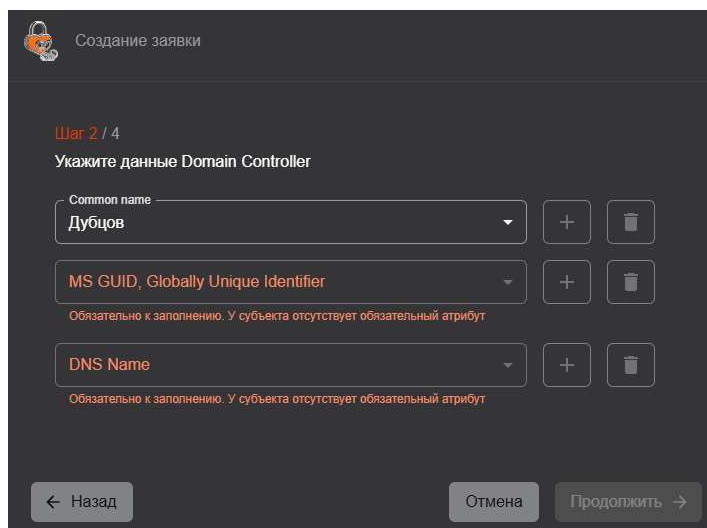


Рисунок 27 – У получателя сертификатов (субъекта PC) отсутствуют обязательные по шаблону атрибуты



Если у получателя сертификатов (субъекта PC) отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить (см. Рисунок 28).

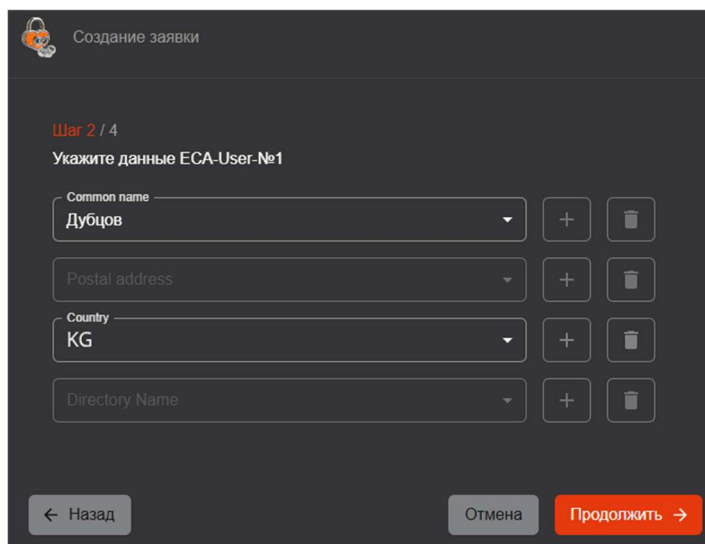


Рисунок 28 – У получателя сертификатов (субъекта PC) отсутствуют необязательные по шаблону атрибуты

- После редактирования атрибутов получателя сертификатов (субъекта PC) нажмите кнопку


Продолжить →

- В открывшемся окне «Создание заявки» (шаг 3 сценария) (см. Рисунок 29) в соответствующих полях задайте и подтвердите пароль для контейнера PKCS#12 и нажмите кнопку **Продолжить →**.

Пароль должен удовлетворять следующим требованиям:

- Длина – не менее **8** символов.
- Пароль должен содержать не менее одного символа из следующих категорий:
 - Строчные буквы английского алфавита от **a** до **z**.
 - Прописные буквы английского алфавита от **A** до **Z**.
 - Десятичные цифры от **0** до **9**.



Для просмотра вводимых символов пароля щелкните в поле значок .

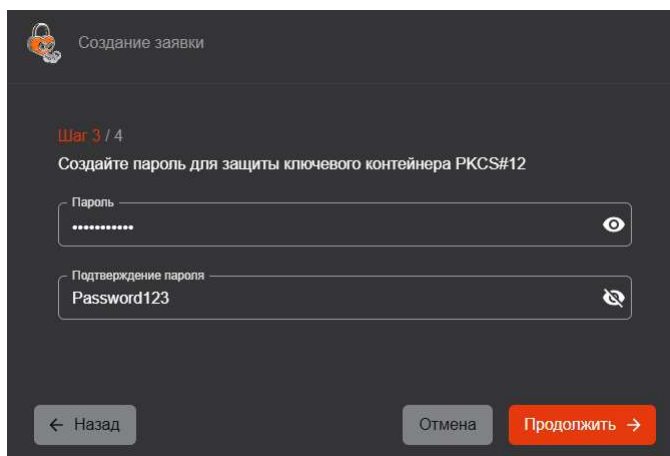


Рисунок 29 – Установка пароля для контейнера PKCS#12

- В открывшемся окне «Создание заявки» (шаг 4 сценария) (см. Рисунок 30):
 - В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
 - В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
 - Нажмите кнопку **Создать заявку**.

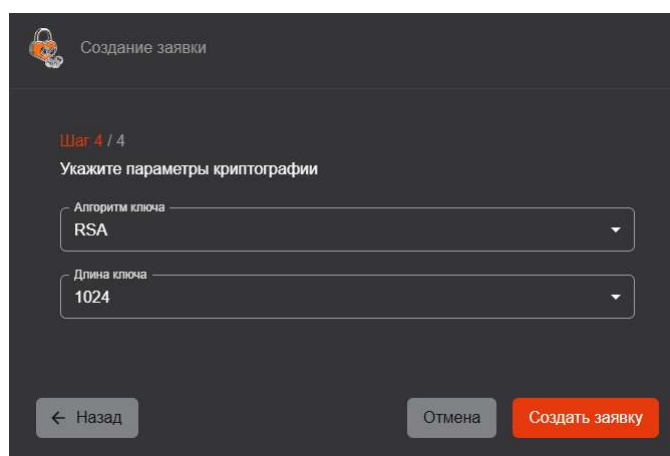


Рисунок 30 – Выбор алгоритма выработки ключевой пары и длины ключа

4.4.3 Создание заявки на ключевом носителе


Внимание! Выпуск сертификатов с алгоритмом ключа ГОСТ Р 34.10-2012 и длиной ключа 512 возможен только на ключевых носителях JaCarta-3.

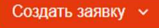
Внимание! Ограничения по возможностям генерации для ключевых носителей Рутокен приведены на [официальном сайте производителя](#).

Предварительные условия для создания заявки на выпуск сертификата на ключевом носителе:

- На компьютере, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- К компьютеру, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должен быть подключен поддерживаемый ключевой носитель (электронный ключ).

Порядок создания заявки для импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.

- На панели инструментов нажмите кнопку  и выберите в открывшемся списке сценарий создания заявки **<На ключевом носителе>** (см. Рисунок 20).



Если приложение JC-WebClient или ПО «Рутокен Плагин» не установлено (см. Рисунок 31) или к компьютеру не подключен ключевой носитель (см. Рисунок 32), создать заявку на ключевом носителе невозможно.

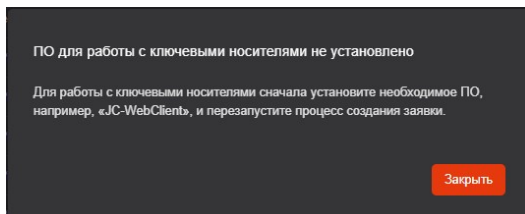


Рисунок 31 – Приложение JC-WebClient не установлено

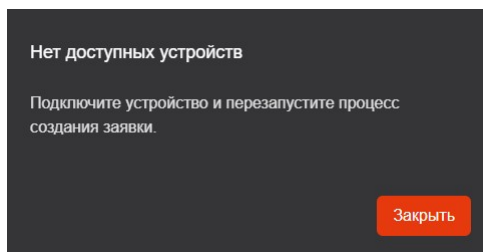

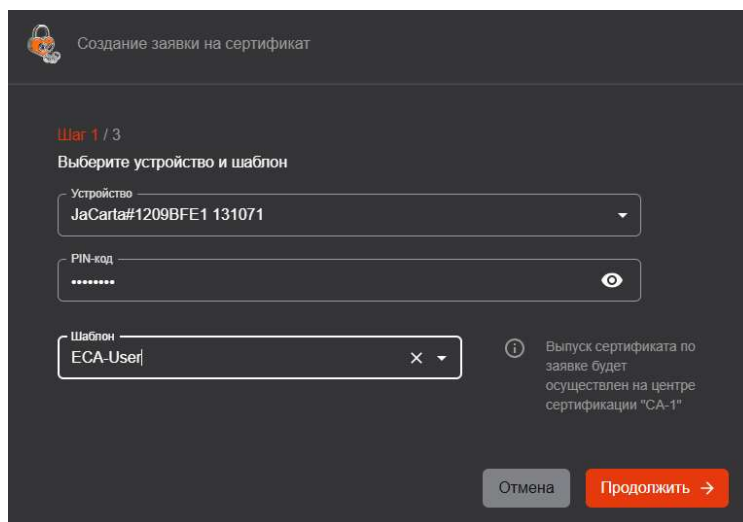


Рисунок 32 – Ключевой носитель не подключен к компьютеру

- В открывшемся окне «Создание заявки на сертификат» (шаг 1 сценария) (см. Рисунок 33):
 - В списке «Устройство» выберите подключенный ключевой носитель.
 - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
 - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат ²¹.
 - Нажмите кнопку .



²¹ Получателю сертификатов (субъекту РС) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту РС), так и группе безопасности, в которую входит получатель сертификатов (субъект РС). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

Рисунок 33 – Выбор ключевого носителя и шаблона для выпуска сертификата

- В открывшемся окне «Создание заявки на сертификат» (шаг 2 сценария) (см. Рисунок 34) укажите атрибуты получателя сертификатов (субъекта PC):

Значения атрибутов заполняются автоматически в соответствии с данными получателя сертификатов (субъекта PC), полученными из Центра сертификации Aladdin eCA. Выберите в списке атрибута нужное значение или добавьте новый такой же атрибут с другим значением.

- При необходимости выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта PC) содержится несколько значений) (см. Рисунок 34).

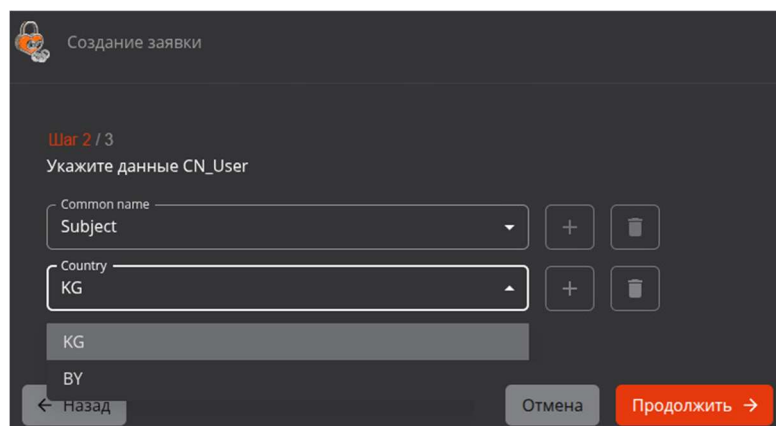



Рисунок 34 – Редактирование атрибутов получателя сертификатов (субъекта PC)

- При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку  и выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта PC) содержится несколько значений) (см. Рисунок 35).

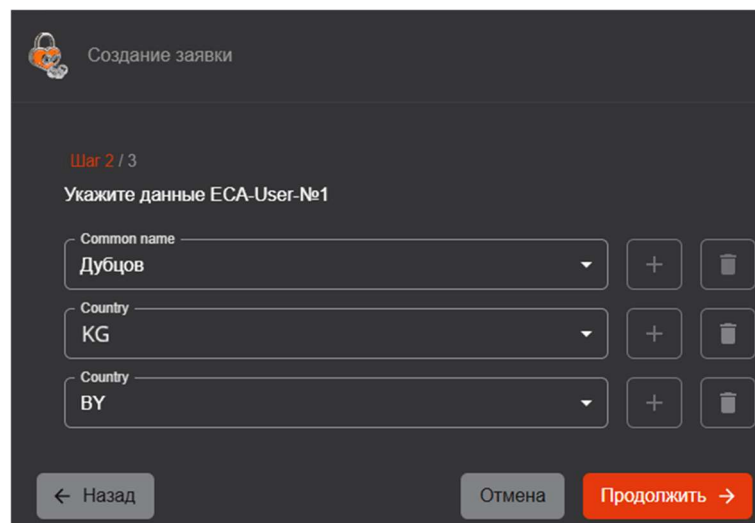





Рисунок 35 – Добавлен новый атрибут

- Добавленные новые атрибуты можно удалять. Для этого нажмите рядом с атрибутом кнопку .

В случае отсутствия у получателя сертификатов (субъекта PC) обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке (см. Рисунок 27). При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

Если у получателя сертификатов (субъекта PC) отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить (см. Рисунок 28).

- После редактирования атрибутов пользователя (субъекта) нажмите кнопку .

- В открывшемся окне «Создание заявки на сертификат» (шаг 3 сценария) (см. Рисунок 36):
 - В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
 - В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
 - Нажмите кнопку .

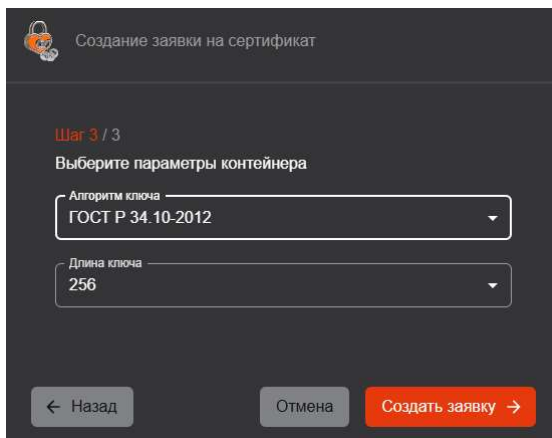



Рисунок 36 – Выбор алгоритма выработки ключевой пары и длины ключа

- В открывшемся окне «Создание заявки на сертификат» (процесс формирования заявки и его результат) (см. Рисунок 37) отображаются процессы:
 - Генерации ключевой пары.
 - Генерации запроса.
 - Создания заявки.

Успешное завершения каждого процесса помечается значком .

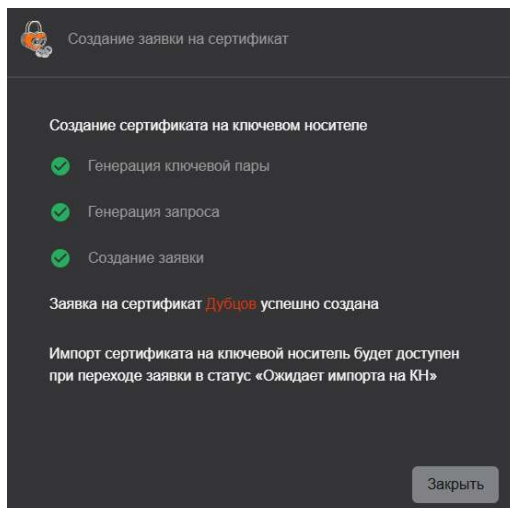



Рисунок 37 – Заявка на выпуск сертификата на ключевом носителе заведена успешно

В случае возникновения ошибок при формировании заявки процесс помечается значком .



Некоторые типы ключевых носителей поддерживают определенный набор алгоритмов выработки ключевых пар (например, в приведенном ниже примере при создании заявки на выпуск сертификата на электронном ключе JaCarta-2 ГОСТ был выбран неподдерживаемый алгоритм RSA) (см. Рисунок 38).

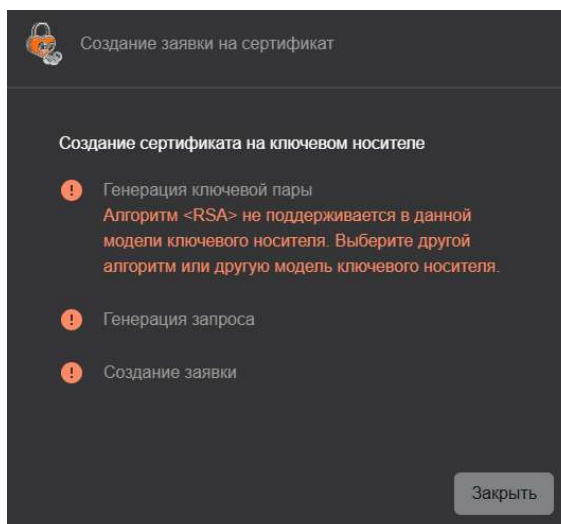


Рисунок 38 – Выбранный алгоритм не поддерживается в используемом ключевом носителе

Для завершения процесса создания заявки в независимости от его результата нажмите кнопку .

Импорт сертификата на ключевой носитель (см. раздел 5.8) будет доступен (статус заявки «Ожидает импорта на КН») после одного из следующих событий:




- Подтверждение заявки уполномоченным пользователем и выпуск сертификата в Центре сертификации Aladdin eCA.
- Автоматическое подтверждение заявки и выпуск сертификата в Центре сертификации Aladdin eCA.

4.5 Отмена заявки

Получатель сертификатов (субъект PC) может отменить только созданные им заявки (например, по причине указания в заявке некорректных данных). Отменить заявку возможно, если ее статус «Ожидает подтверждения» или «Ошибка выпуска».

Выполнить отмену заявки возможно как при просмотре списка заявок, так и из карточки заявки.

Порядок отмены заявки, созданной получателем сертификатов (субъектом PC), способом №1:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Иницируйте процесс отмены заявки одним из следующих способов:
 - Найдите заявку, которую необходимо отменить, в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Отмена заявки>** (см. Рисунок 39).

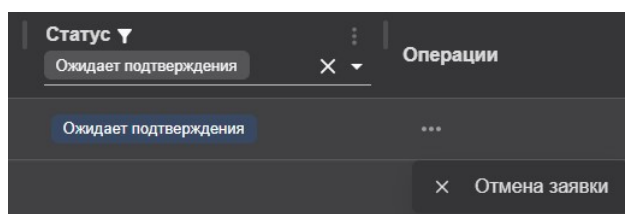




Рисунок 39 – Инициализация процесса отмены заявки на выпуск сертификата в списке

- Откройте карточку заявки, которую необходимо отменить (см. раздел 4.3), на панели инструментов карточки заявки щелкните значок  и выберите в открывшемся списке  **<Отмена заявки>** (см. Рисунок 40).

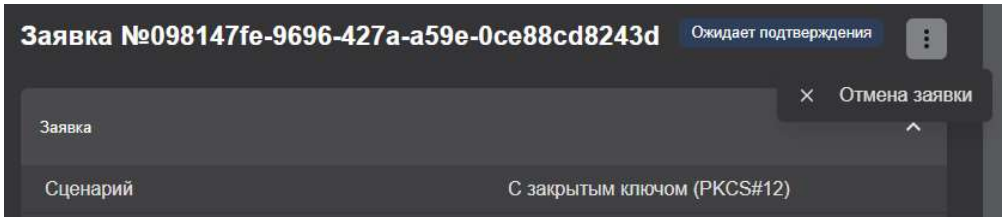



Рисунок 40 – Инициализация процесса отмены заявки на выпуск сертификата из ее карточки

- В открывшемся окне в поле «Комментарий» укажите причину отмены заявки и нажмите кнопку  (см. Рисунок 41).

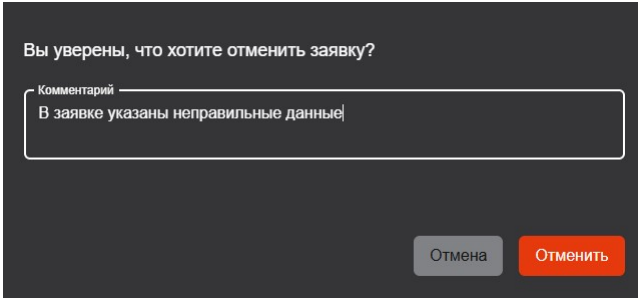


Рисунок 41 – Указание причин перед отменой заявки на выпуск сертификата



После отмены заявки указанный комментарий будет доступен для просмотра в карточке заявки (см. раздел 4.3) в атрибуте «Комментарий» блока «Заявка» (см. Рисунок 42).

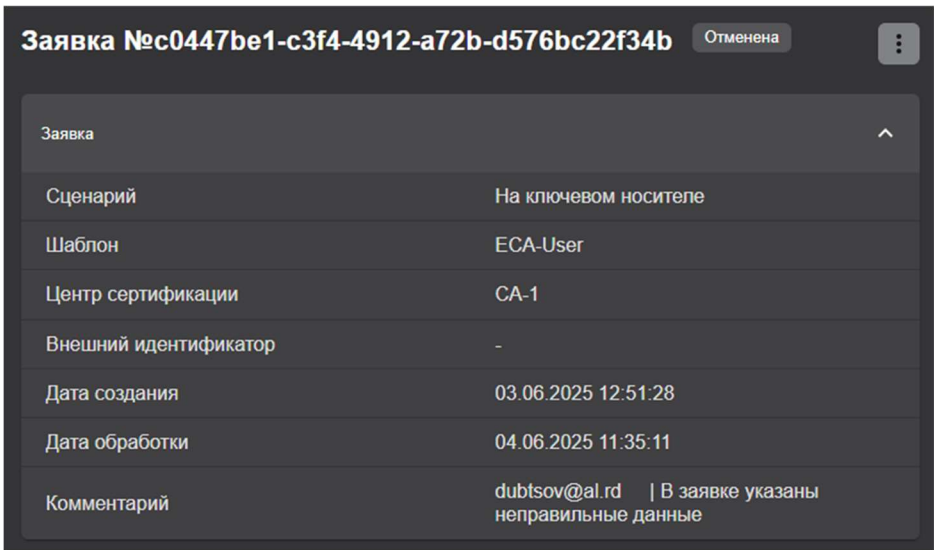


Рисунок 42 – Комментарий занесен в карточку отменной заявки

5 УПРАВЛЕНИЕ ВЫПУЩЕННЫМИ ПО ЗАЯВКАМ СЕРТИФИКАТАМИ

5.1 Общие сведения о работе с сертификатами

Инициализация процесса выпуска сертификата в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта PC) начинается:

- После подтверждения заявки уполномоченными пользователями Центра регистрации Aladdin eRA с ролями «Администратор» или «Оператор» в ручном режиме (режим определяется правилами выпуска, установленными для получателя сертификатов (субъекта PC)).
- В автоматическом режиме (режим определяется правилами выпуска, установленными для получателя сертификатов (субъекта PC)).

После успешного выпуска сертификата заявке, по которой он был выпущен, назначается статус «Выполнена».



Заявкам, заведенным по сценарию на ключевом носителе, после успешного выпуска сертификатов назначается статус «Ожидает импорта на КН». Статус «Выполнен» назначается таким заявкам после импорта сертификата на ключевой носитель (см. раздел 5.8).

После выпуска сертификата получателю сертификатов (субъекту PC) доступны следующие операции:

- Выгрузка файла с сертификатом в формате PEM (см. раздел 5.2).
- Выгрузка файла цепочки сертификатов в формате PEM (см. раздел 5.3).
- Выгрузка файла со списком отозванных сертификатов (CRL) в формате CRL (см. раздел 5.5).
- Выгрузка файла с цепочкой сертификатов издателя в формате PEM (см. раздел 5.6).
- Выгрузка файла с контейнером закрытого ключа PKCS#12 в формате P12 (см. раздел 5.4).



Выгрузка доступна только для заявок, заведенных по сценарию с закрытым ключом PKCS#12 (см. раздел 4.4.2).

- Отзыв сертификатов, выпущенных по заявкам (см. раздел 5.7).



Получателю сертификатов (субъекту PC) доступен отзыв как сертификатов, выпущенных по собственным заявкам, так и сертификатов, выпущенных по заявкам, заведенным уполномоченными пользователями с ролями «Администратор» и «Оператор» Центра регистрации Aladdin eRA.

- Импорт сертификата на ключевой носитель (см. раздел 5.8).




Импорт доступен только для заявок, заведенных по сценарию на ключевом носителе (см. раздел 4.4.3).



Если по подтвержденной заявке или обрабатываемой в автоматическом режиме сертификат не выпущен по какой-ли причине, такой заявке назначается статус «Ошибка выпуска».

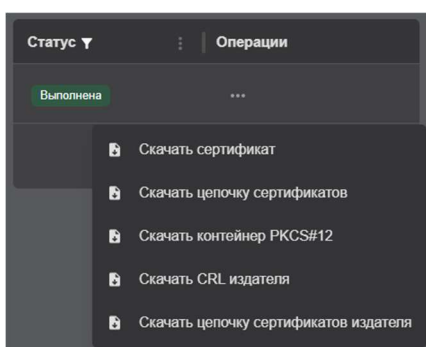
5.2 Выгрузка сертификата

Выгрузку файла с сертификатом возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

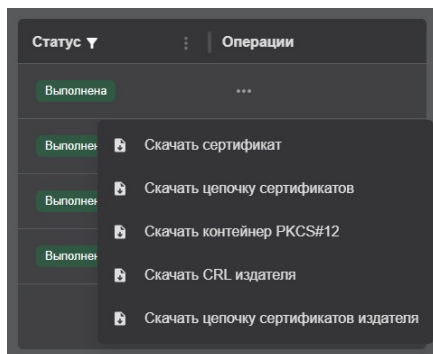
Порядок выгрузки сертификата получателя сертификатов (субъекта PC):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Выгрузите файл одним из следующих способов:

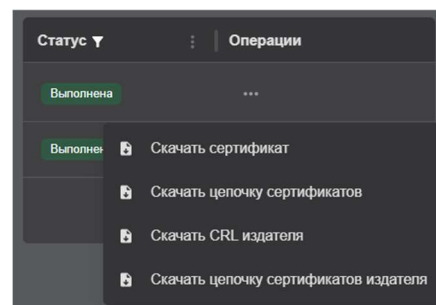
- Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Скачать сертификат>** (см. Рисунок 43).



а) Заявка на основании запроса PKCS#10





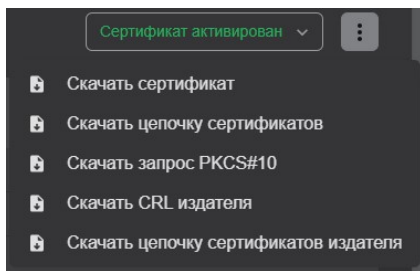
б) Заявка с закрытым ключом PKCS#12



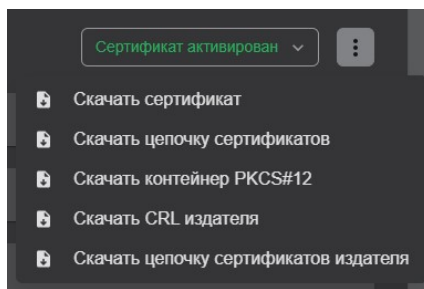
в) Заявка на ключевом носителе²²

Рисунок 43 – Выгрузка сертификата, выпущенного по заявкам с разными сценариями создания

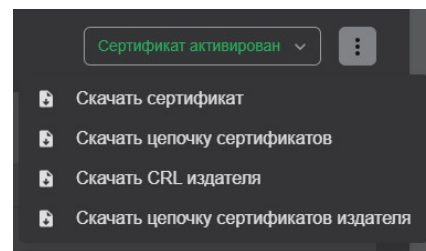
- Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок  и выберите в открывшемся списке  **<Скачать сертификат>** (см. Рисунок 44).



а) Заявка на основании запроса PKCS#10



б) Заявка с закрытым ключом PKCS#12








в) Заявка на ключевом носителе²³

Рисунок 44 – Выгрузка сертификата, выпущенного по заявкам с разными сценариями создания

5.3 Выгрузка цепочки сертификатов

Выгрузку файла с цепочкой сертификатов возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки цепочки сертификата получателя сертификатов (субъекта PC):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Выгрузите файл одним из следующих способов:
 - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Скачать цепочку сертификатов>** (см. Рисунок 43).
 - Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок  и выберите в открывшемся списке  **<Скачать цепочку сертификатов>** (см. Рисунок 44).






²² Заявка на ключевом носителе после импорта сертификата на ключевой носитель.

²³ Заявка на ключевом носителе после импорта сертификата на ключевой носитель.

5.4 Выгрузка контейнера PKCS#12

Выгрузку файла с контейнером PKCS#12 возможно выполнить как при просмотре списка заявок, так и из карточки заявки.






Порядок выгрузки контейнера PKCS#12:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Выгрузите файл одним из следующих способов:
 - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Скачать контейнер PKCS#12>** (см. Рисунок 43).
 - Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок  и выберите в открывшемся списке  **<Скачать контейнер PKCS#12>** (см. Рисунок 44).

5.5 Выгрузка списка отозванных сертификатов (CRL)

Выгрузку файла со списком отозванных сертификатов (CRL) возможно выполнить как при просмотре списка заявок, так и из карточки заявки.






Порядок выгрузки списка отозванных сертификатов (CRL):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Выгрузите файл одним из следующих способов:
 - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Скачать CRL издателя>** (см. Рисунок 43).
 - Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок  и выберите в открывшемся списке  **<Скачать CRL издателя>** (см. Рисунок 44).

5.6 Выгрузка цепочки сертификатов издателя

Выгрузку файла с цепочкой сертификатов издателя возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки цепочки сертификатов издателя:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Выгрузите файл одним из следующих способов:
 - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Скачать цепочку сертификатов издателя>** (см. Рисунок 43).
 - Откройте карточку заявки см. раздел 4.3), на панели инструментов щелкните значок  и выберите в открывшемся списке  **< Скачать цепочку сертификатов издателя>** (см. Рисунок 44).

5.7 Отзыв сертификата

Чтобы отозвать сертификат, заявка по которой он был выпущен должна быть в статусе «Выполнена», а статус сертификата «Активирован».



Отзыв сертификата является необратимой операцией, которая может повлиять на работу получателя сертификатов (субъекта PC). Получателю сертификатов доступен отзыв сертификатов, выпущенных только по собственным заявкам.

Порядок отзыва сертификата:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Откройте карточку заявки, по которой был выпущен сертификат, требующий отзыва (см. раздел 4.3).
- На панели инструментов карточки заявки нажмите кнопку и выберите в открывшемся списке **<Сертификат отозван>** (см. Рисунок 45).

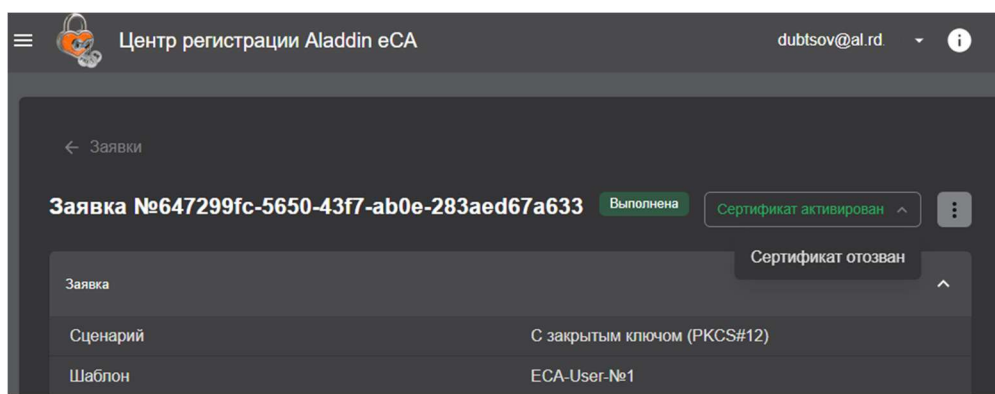


Рисунок 45 – Отзыв сертификата

- В открывшемся окне выберите в списке «Причина» причину отзыва сертификата, оставьте обязательный комментарий в поле «Комментарий» и нажмите кнопку (см. Рисунок 46);

Отозвать сертификат?

Отзыв – это необратимая операция, которая может повлиять на работу пользователя или сервера.

Издатель: **Root-CA2**
 Субъект: **петров**
 Действует: с 18.03.2025 15:23:55 по 18.03.2027 15:23:55

Причина

Без указания причины

Комментарий *

Компрометация

Рисунок 46 – Указание причины отзыва сертификата

В результате сертификат будет отозван (см. Рисунок 47).

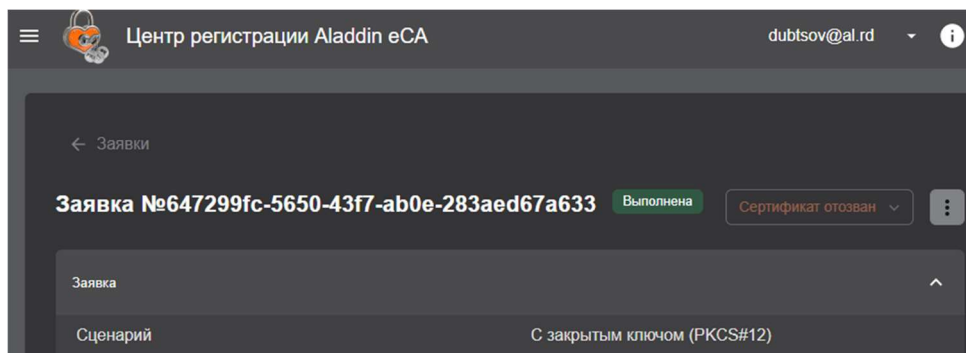


Рисунок 47 – Сертификат отозван

5.8 Импорт сертификата на ключевой носитель

Предварительные условия для импорта сертификата на ключевой носитель:

- На компьютере, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- К компьютеру, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должен быть подключен поддерживаемый ключевой носитель (электронный ключ).
- Заявка, по которой был выпущен сертификат для последующего импорта на ключевой носитель, должна иметь статус «Ожидает импорта на КН».

Порядок импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Иницилируйте процесс импорта сертификата на ключевой носитель одним из следующих способов:
 - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Импортировать на КН>** (см. Рисунок 48).

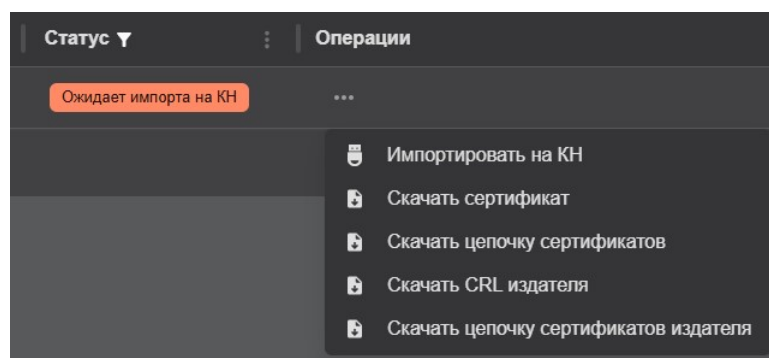


Рисунок 48 – Инициализация процесса импорта сертификата на ключевой носитель из списка



Если приложение JC-WebClient или ПО «Рутокен Плагин» не установлено (см. Рисунок 31) или к компьютеру не подключен ключевой носитель (см. Рисунок 32), создать заявку на ключевом носителе невозможно.

- Откройте карточку заявки, на панели инструментов карточки заявки щелкните значок **<Операции строки>** и выберите в открывшемся списке **<Импортировать на КН>** (см. Рисунок 49).
- В открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 50):
 - В списке «Устройство» выберите подключенный ключевой носитель.
 - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
 - Нажмите кнопку **Импортировать**.



Рисунок 49 – Инициализация процесса импорта сертификата на ключевой носитель из карточки заявки

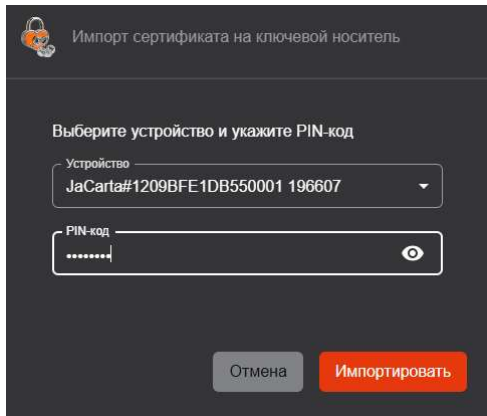


Рисунок 50 – Импорт сертификата на ключевой носитель



При импорте сертификата, открытый ключ которого не соответствует закрытому ключу на ключевом носителе, возникает ошибка «Ключевой носитель не содержит закрытый ключ, соответствующий открытому ключу из сертификата».



Центр регистрации Aladdin eRA последовательно проходит по списку ключевых пар на выбранном при импорте ключевом носителе. Все неуспешные попытки создания контейнера завершаются ошибкой, возвращаемой приложением JC-WebClient или ПО «Рутокен Плагин». При этом Центр регистрации Aladdin eRA не отображает ошибку для каждой ключевой пары, генерируемую приложением JC-WebClient или ПО «Рутокен Плагин», а выводит общую ошибку «Ключевой носитель не содержит закрытый ключ, соответствующий открытому ключу из сертификата».

- В случае успешного импорта сертификата на ключевой носитель в открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 51) проверьте данные сертификата и нажмите кнопку

Заккрыть

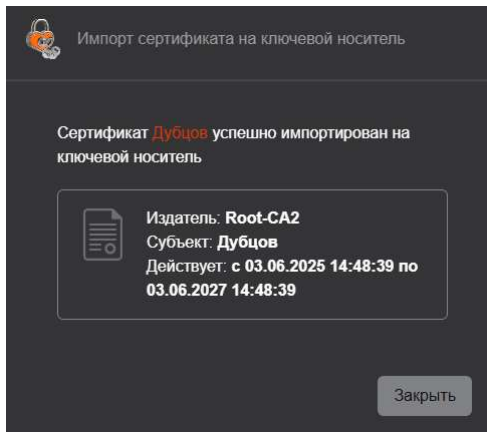


Рисунок 51 – Импорт сертификата на ключевой носитель успешно выполнен

6 ПОДДЕРЖКА ПРОТОКОЛОВ MS-XCEP И MS-WSTEP

Центр регистрации Aladdin eRA реализует серверные компоненты по протоколам MS-XCEP ²⁴ и MS-WSTEP ²⁵. Реализация данных серверных компонентов обеспечивает выполнение автоматического сценария распространения сертификатов получателям сертификатов (субъектам PC) по протоколу MS-WSTEP.

Сервер политик выпуска сертификатов (CEP-сервер) и сервер выпуска сертификатов (CES-сервер), реализуемые Центром регистрации Aladdin eRA в соответствии с протоколами MS-XCEP и MS-WSTEP, доступны по URL **https://[HOSTNAME]/wstep-service/engine**, где [HOSTNAME] – IP-адрес или доменное имя Центра регистрации Aladdin eRA.

Центр регистрации Aladdin eRA в рамках реализации функций CEP-сервера (при получении запроса на получение политики) и функций CES-сервера (при получении запроса на выпуск сертификата) обеспечивает следующие способы аутентификации пользователей домена, к которому он подключен:

- По имени и паролю доменной учетной записи получателя сертификатов.
- По Kerberos-билету.

Центр регистрации Aladdin eRA при получении запроса на получение политики в случае успешной аутентификации получателя сертификат (субъекта PC), от имени которого был выполнен запрос, возвращает в ответе политику выпуска сертификатов.

Шаблоны в ответе на запрос получения политики представляют собой шаблоны Центра сертификации Aladdin eCA, подключенного к Центру регистрации Aladdin eRA, преобразованные в шаблоны по протоколу MS-XCEP (далее – шаблоны CEP).

При этом в шаблоны CEP преобразовываются только шаблоны Центра сертификации Aladdin eCA одновременно удовлетворяющие следующим условиям:

- Шаблоны определены в правилах выпуска Центра регистрации Aladdin eRA, назначенных для получателя сертификатов (субъекта PC).
- В правилах выпуска Центра регистрации Aladdin eRA, назначенных для получателя сертификатов (субъекта PC), выбран автоматический режим обработки заявок на сертификаты.
- В шаблонах, назначенных получателю сертификатов (субъекту PC) правилами выпуска, доступен алгоритм генерации ключевой пары RSA.

Центр регистрации Aladdin eRA при получении запроса на выпуск сертификата в случае успешной аутентификации выполняет следующие действия:

- Создает от имени получателя сертификатов (субъекта PC) новую заявку на сертификат на основании запроса по шаблону, указанному в данном запросе на сертификат.

Для заявок, создаваемых в ходе обработки запроса, указан сценарий «WSTEP». При создании заявки и последующем выпуске сертификата в Центре сертификации Aladdin eCA атрибуты запроса на сертификат автоматически переопределяются атрибутами субъекта из Центра сертификации Aladdin eCA, требуемыми по шаблону. Для поля, требуемого по шаблону, используются все имеющиеся у получателя сертификата (субъекта PC) в соответствующем атрибуте значения. В случае ошибки создания заявки Центра регистрации Aladdin eRA возвращает сообщение об ошибке.

²⁴ Описание протокола MS-XCEP доступно по ссылке: <https://winprotocoldoc.z19.web.core.windows.net/MS-XCEP/%5bMS-XCEP%5d.pdf>

²⁵ Описание протокола MS-WSTEP доступно по ссылке: <https://winprotocoldoc.z19.web.core.windows.net/MS-WSTEP/%5bMS-WSTEP%5d.pdf>

- В случае успешного выпуска сертификата по созданной заявке Центр регистрации Aladdin eRA генерирует и отправляет пользователю ответное сообщение с выпущенным по заявке сертификатом, а также цепочкой данного сертификата.

Если после создания заявки сертификат по ней не был успешно выпущен, Центр регистрации Aladdin eCA возвращает сообщение об ошибке.

6.1 Создания политики регистрации сертификатов

Порядок создания политики регистрации сертификатов в ОС Windows:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог **Сертификаты – текущий пользователь > Личное > Сертификаты**.
- Вызовите контекстное меню и выберите **Все задачи > Дополнительные операции > Управление политиками регистрации сертификатов** (см. Рисунок 52).

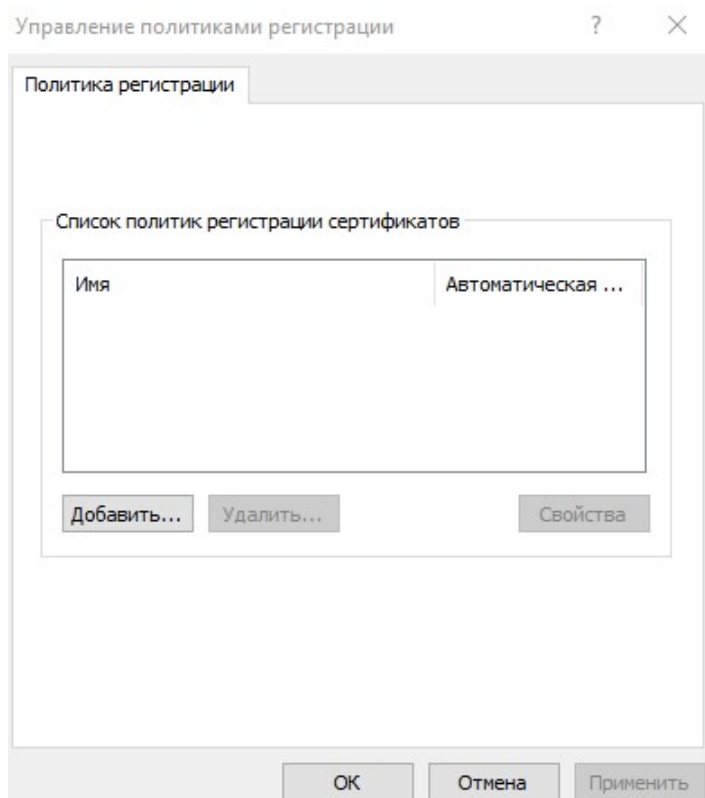


Рисунок 52 – Управление политиками регистрации сертификатов

- В открывшемся окне «Управление политикам и регистрации» нажмите кнопку **<Добавить...>**.

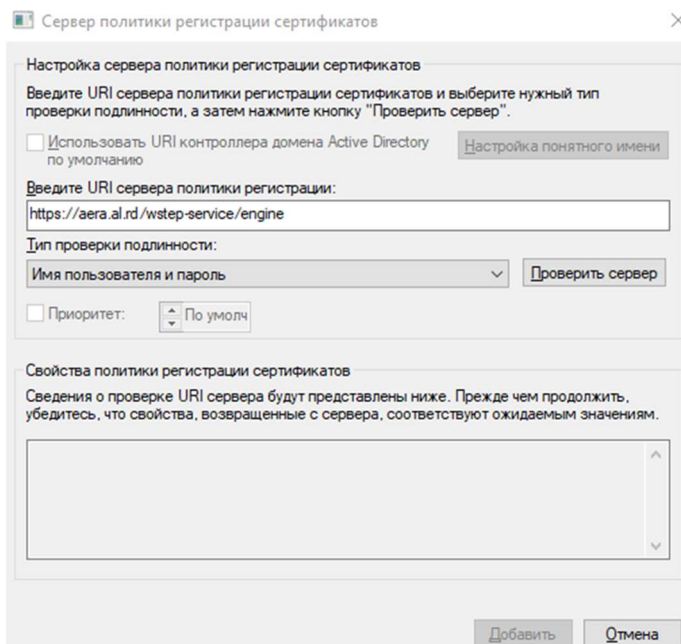


Рисунок 53 – Управление политиками регистрации сертификатов

- В открывшемся окне «Сервер политики регистрации сертификатов» выполните следующие действия:
 - В соответствующем поле введите URL сервера политик выпуска сертификатов Центра регистрации Aladdin eRA.
 - В списке «Тип проверки подлинности» выберите:
 - «Имя пользователя и пароль» для аутентификации по имени и паролю вашей доменной учетной записи.
 - «Встроенная проверка подлинности Windows» для аутентификации по Kerberos-билету.
 - Нажмите кнопку **<Проверить сервер>**.

При выбранном способе аутентификации по имени и паролю укажите их в соответствующих поля открывшегося окна и нажмите кнопку **<ОК>**.

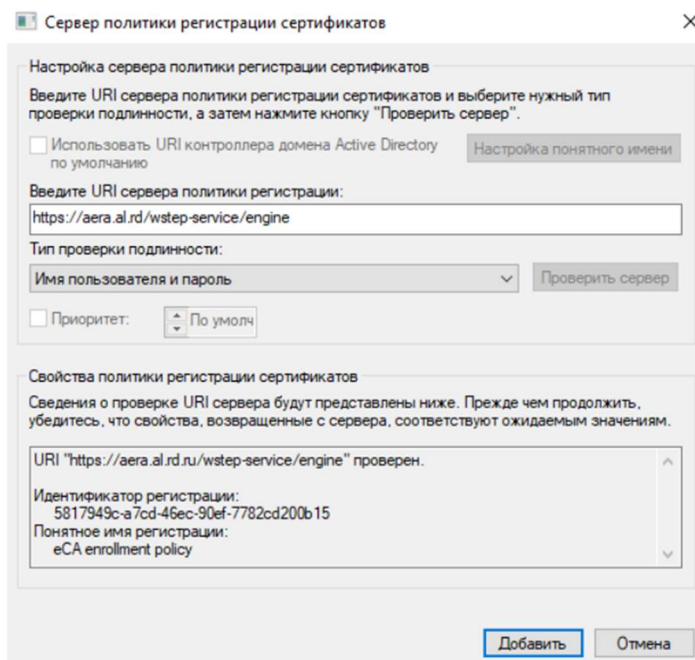


Рисунок 54 – Проверка сервера выполнена успешно

- В случае успешной проверки сервера нажмите кнопку **<Добавить>**.

- В окне «Управление политикам и регистрации» нажмите кнопку **<Применить>**, а затем **<ОК>**.

6.2 Запрос нового сертификата

Порядок запроса сертификата:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог **Сертификаты – текущий пользователь > Личное > Сертификаты**.
- Для запроса нового сертификата вызовите контекстное меню каталога «Сертификаты» и выберите **Все задачи > Запросить новый сертификат**.
- В открывшемся окне мастера регистрации сертификатов на 1 шаге нажмите кнопку **<Далее>**.

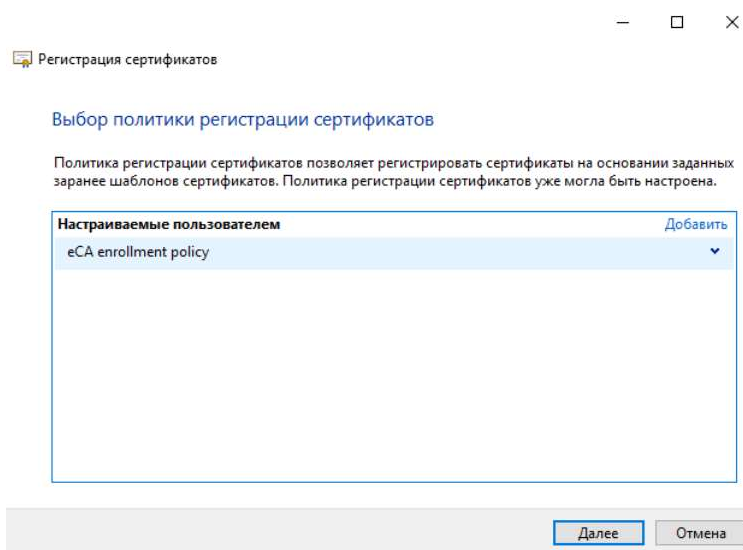


Рисунок 55 – Выбор политики регистрации сертификатов

- На 2 шаге мастера регистрации сертификатов выберите политику **eCA enrollment policy** и нажмите кнопку **<Далее>**.

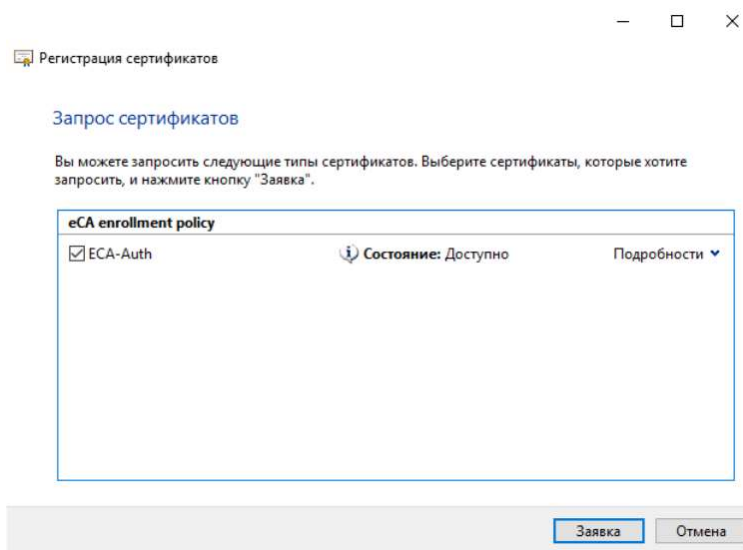


Рисунок 56 – Выбор шаблона для выпуска сертификата

- На 3 шаге мастера регистрации сертификатов выберите шаблоны, по которым необходимо выпустить сертификаты, и нажмите кнопку **<Заявка>**.

- На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 57).

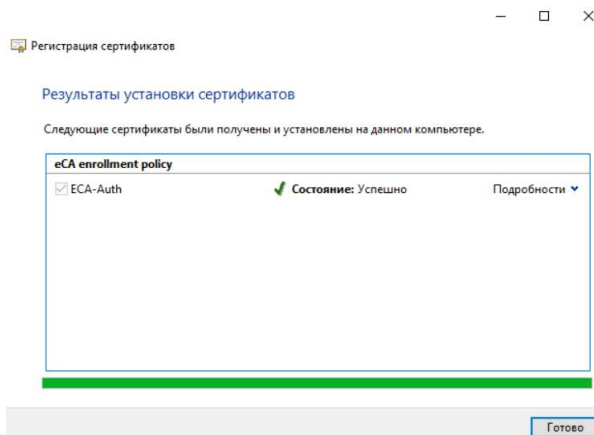


Рисунок 57 – Сертификат получен и успешно установлен в хранилище

6.3 Перевыпуск сертификатов

Центр регистрации Aladdin eRA поддерживает перевыпуск сертификатов с новым ключом и с тем же ключом, на котором был выпущен текущий сертификат.

Порядок перевыпуска сертификата:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог **Сертификаты – текущий пользователь > Личное > Сертификаты**.
- Для запроса нового сертификата вызовите контекстное меню выбранного сертификата и выберите необходимый сценарий перевыпуска или выпуска нового сертификата:
 - **Все задачи > Обновить сертификат с новым ключом.**
 - **Все задачи > Запросить сертификат с новым ключом.**
 - **Все задачи > Дополнительные операции > Обновить сертификат с тем же ключом.**
 - **Все задачи > Дополнительные операции > Запросить новый сертификат с тем же ключом.**
- В открывшемся окне мастера регистрации сертификатов на 1 шаге нажмите кнопку **<Далее>**.

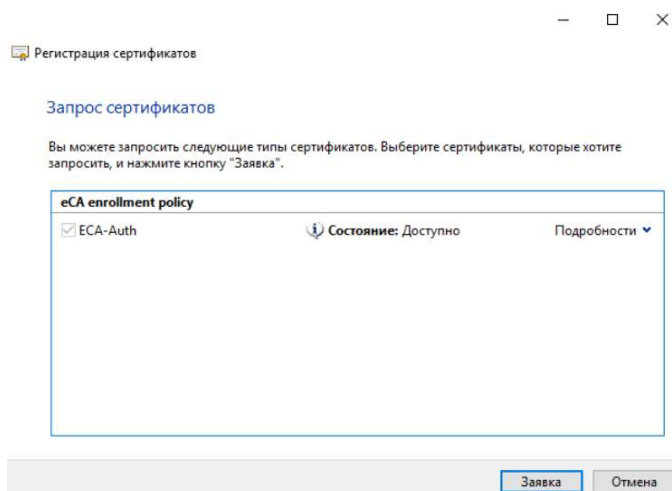


Рисунок 58 – Отправка заявки для выпуска сертификата

- На 2 шаге мастера регистрации сертификатов нажмите кнопку **<Заявка>**.
- На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 57).

ПРИЛОЖЕНИЕ 1. ОПИСАНИЕ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] ECA-Auth	8ecba810-7f48-4c4e-b803-99a97146e2ba	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name	+	+	-		
ECDSA	256															
ГОСТ Р34.10-2012	Выключен															
[Deprecated] ECA-User	2d58b30c-3965-4555-9af4-fec4552af21e	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиент - Защита электронной почты	-	Common name	+	+	-		
ECDSA	256															
ГОСТ Р 34.10-2012	256															
[Deprecated] ECA-WEB-Server	25bbd733-4d8c-43ce-ba5a-e9826eb7b16c	2y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей	+	- Аутентификация сервера	-	Common name	+	+	DNS name	+	+
ECDSA	256															
ГОСТ Р 34.10-2012	256															
[Deprecated] Domain Controller	bf2dac0a-f05f-49dd-95b4-e50691489b6a	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Центр распространения ключей Kerberos - SSH сервер	-	Common name ²⁶	+	+	DNS name ²⁷	+	+
ECDSA	256															
ГОСТ Р 34.10-2012	Выключен	MS GUID ²⁸														

²⁶ Имя контроллера домена.

²⁷ FQDN – полное доменное имя вашего сервера.

²⁸ Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена. Для получения значения идентификатора в среде РЕД ОС и SberLinux OS Server выполните команду: `samba-tool computer show <hostname> | grep objectGUID`. Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] Smartcag Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name ²⁹	+	+	MS UPN ³⁰	+	+
					ECDSA	256								RFC 822 Name ³¹		
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name ³²	+	+	MS UPN ³³	+	+
					ECDSA	256								RFC 822 Name ³⁴		
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей	+	Аутентификация сервера	-	Common name ³⁵	+	+	DNS name ³⁶	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										

²⁹ Имя пользователя.

³⁰ Имя входа пользователя в формате e-mail адреса.

³¹ Почтовый адрес пользователя, может совпадать с MS UPN.

³² Имя веб-клиента.

³³ Имя входа пользователя в формате e-mail адреса.

³⁴ Почтовый адрес пользователя, может совпадать с MS UPN.

³⁵ Имя веб-сервера.

³⁶ FQDN – полное доменное имя вашего сервера.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name ³⁷	+	+	RFC 822 Name ³⁸	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffeaf	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name ³⁹	+	+	MS UPN ⁴⁰	+	+
					ECDSA	256					Organization ⁴¹	-	+	Kerberos KPN ⁴²	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] ALD PRO Smartcagk Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name ⁴³	+	+	MS UPN ⁴⁴	+	+
					ECDSA	256					Organization ⁴⁵	-	+	RFC 822 Name ⁴⁶	+	+
					ГОСТ Р 34.10-2012	Выключен										

³⁷ Имя пользователя.

³⁸ почтовый адрес пользователя, может совпадать с MS UPN.

³⁹ Имя контроллера домена ALD PRO.

⁴⁰ Данные в формате «krbtgt/полное имя домена@полное имя домена».

⁴¹ Организация.

⁴² Данные в формате «krbtgt/полное имя домена@полное имя домена».

⁴³ Имя пользователя ALD PRO.

⁴⁴ Имя входа пользователя в формате e-mail адреса.

⁴⁵ Организация.

⁴⁶ Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата									
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта						
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.				
[Deprecated] OCSP Signer	aac2e49b-9c8e-4869-80c1-ee f526ba75ab	2y	-	-	RSA	1024	Цифровая подпись	+	OCSP подписант	-	Common name	+	+	-						
					ECDSA	256														
					ГОСТ Р 34.10-2012	Выключе н														
[Deprecated] Root CA	9129245a-eaad-4ebc-a2a4-88 45ac0336fb	7d24y	-	-	RSA	1024	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+				
					ECDSA	256					Unique Identifier (UID)	-	+	DNS name	-	+				
					ГОСТ Р 34.10-2012	256					Given name	-	+	MS UPN	-	+				
											Initials	-	+	MS GUID	-	+				
											Surname	-	+	IP address	-	+				
											Organizational unit	-	+	Directory Name	-	+				
											Locality	-	+	Uniform resource identifier	-	+				
											State or province	-	+	Registered Identifier (OID)	-	+				
											Domain component	-	+	Permanent identifier	-	+				
											Country	-	+	Xmpp address	-	+				
											Postal code	-	+	Service Name	-	+				
											Business category	-	+	Subject Identification Method	-	+				
											Telephone number	-	+	Kerberos KPN	-	+				
											Pseudonym	-	+							
											Postal address	-	+							
											Street	-	+							
											Name	-	+							
											Title	-	+							
											Domain qualifier	-	+							

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата														
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта											
											Поле	Област.	Валидац.	Поле	Област.	Валидац.									
											Description	-	+												
											Unstructured address	-	+												
											Unstructured name	-	+												
											Email Address (E)	-	+												
											Serial number	-	+												
											Organization	-	+												
											ИНН	-	+												
											ОГРН	-	+												
											ОГРНИП	-	+												
											СНИЛС	-	+												
											ИНН ЮЛ	-	+												
[Deprecated] Sub CA	af3b0355-1798-4c64-98f7-a9c70407db1c	7d24y	--	-	RSA	1024	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+									
											Unique Identifier (UID)	-	+	DNS name	-	+									
											Given name	-	+	MS UPN	-	+									
											Initials	-	+	MS GUID	-	+									
											Surname	-	+	IP address	-	+									
											Organizational unit	-	+	Directory Name	-	+									
											Locality	-	+	Uniform resource identifier	-	+									
											State or province	-	+	Registered Identifier (OID)	-	+									
											Domain component	-	+	Permanent identifier	-	+									
											Country	-	+	Xmpp address	-	+									
											Postal code	-	+	Service Name	-	+									
											Business category	-	+	Subject Identification Method	-	+									
														ECDSA	256										
														ГОСТ Р 34.10-2012	256										

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
											Telephone number	-	+	Kerberos KPN	-	+
											Pseudonym	-	+			
											Postal address	-	+			
											Street	-	+			
											Name	-	+			
											Title	-	+			
											Domain qualifier	-	+			
											Description	-	+			
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			
											ИНН	-	+			
											ОГРН	-	+			
											ОГРНИП	-	+			
											СНИЛС	-	+			
											ИНН ЮЛ	-	+			
[Deprecated] SCEP Management	3e5df3d4-683c-4252-b862-467589c2225b	25y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей - Шифрование данных	+	-	-	Common name	+	-	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
User	f215f72f-9a9a-45c8-83e8-25879d52dcf6	1y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиент - Защита электронной почты	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
Domain Controller	eca2ad3d-944e-48ce-ba7b-114f16ad8fd4	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Центр распространения ключей Kerberos - SSH сервер	-	Common name ⁴⁷	+	+	DNS name ⁴⁸	+	+
					ECDSA	256								MS GUID ⁴⁹	+	+
					ГОСТ Р 34.10-2012	256										
Smartcag Logon	682225f6-f189-412f-a456-c480d42efaa8	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name ⁵⁰	+	+	MS UPN ⁵¹	+	+
					ECDSA	256								RFC 822 Name ⁵²	+	+
					ГОСТ Р 34.10-2012	256										
WEB-Client	18ecaacc-43d6-4aaa-afcc-1bc8e547e6f5	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name ⁵³	+	+	MS UPN ⁵⁴	+	+
					ECDSA	256								RFC 822 Name ⁵⁵	+	+
					ГОСТ Р 34.10-2012	256										

⁴⁷ Имя контроллера домена.

⁴⁸ FQDN – полное доменное имя вашего сервера.

⁴⁹ Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена. Для получения значения идентификатора в среде РЕД ОС и SberLinux OS Server выполните команду: `samba-tool computer show <hostname> | grep objectGUID`. Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

⁵⁰ Имя пользователя.

⁵¹ Имя входа пользователя в формате e-mail адреса.

⁵² Почтовый адрес пользователя, может совпадать с MS UPN.

⁵³ Имя веб-клиента.

⁵⁴ Имя входа пользователя в формате e-mail адреса.

⁵⁵ Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
WEB-Server	61c901fa-c823-4899-87a0-df4035291fa0	1y	-	-	RSA	2048	- Цифровая подпись - Шифрование ключей	+	Аутентификация сервера	-	Common name ⁵⁶	+	+	DNS name ⁵⁷	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
S/MIME	0a7c4a9f-b260-46c5-94c5-58de5e977678	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name ⁵⁸	+	+	RFC 822 Name ⁵⁹	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
ALD PRO Domain Controller	83afddde-5729-4562-a7ed-260f1c0f73d7	1y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name ⁶⁰	+	+	MS UPN ⁶¹	+	+
					ECDSA	256					Organization ⁶²	-	+	Kerberos KPN ⁶³	+	+
					ГОСТ Р 34.10-2012	Выключен										

⁵⁶ Имя веб-сервера.

⁵⁷ FQDN – полное доменное имя вашего сервера.

⁵⁸ Имя пользователя.

⁵⁹ почтовый адрес пользователя, может совпадать с MS UPN.

⁶⁰ Имя контроллера домена ALD PRO.

⁶¹ Данные в формате «krbtgt/полное имя домена@полное имя домена».

⁶² Организация.

⁶³ Данные в формате «krbtgt/полное имя домена@полное имя домена».

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата									
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта						
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.				
ALD PRO Smartcakg Logon	85e99e47-479f-407e-98f8-ad13d51435a7	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name ⁶⁴	+	+	MS UPN ⁶⁵	+	+				
					ECDSA	256					Organization ⁶⁶	-	+	RFC 822 Name ⁶⁷	+	+				
					ГОСТ P 34.10-2012	256														
OCSP Signer	eeb625cb-861e-458c-94ae-79b2e05090e5	1y	-	-	RSA	2048	Цифровая подпись	+	OCSP подписант	-	Common name	+	+	-						
					ECDSA	256														
					ГОСТ P 34.10-2012	256														
Root CA	a1eb9d3a-b9b5-4e6d-8f2d-587ca9cc6554	15y	-	-	RSA	4096	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+				
					ECDSA	384					Unique Identifier (UID)	-	+	DNS name	-	+				
					ГОСТ P 34.10-2012	512					Given name	-	+	MS UPN	-	+				
											Initials	-	+	MS GUID	-	+				
											Surname	-	+	IP address	-	+				
											Organizational unit	-	+	Directory Name	-	+				
											Locality	-	+	Uniform resource identifier	-	+				
											State or province	-	+	Registered Identifier (OID)	-	+				
											Domain component	-	+	Permanent identifier	-	+				
											Country	-	+	Xmpp address	-	+				
											Postal code	-	+	Service Name	-	+				

⁶⁴ Имя пользователя ALD PRO.

⁶⁵ Имя входа пользователя в формате e-mail адреса.

⁶⁶ Организация.

⁶⁷ Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Business category	-	+	Subject Identification Method	-	+
											Telephone number	-	+	Kerberos KPN	-	+
											Pseudonym	-	+			
											Postal address	-	+			
											Street	-	+			
											Name	-	+			
											Title	-	+			
											Domain qualifier	-	+			
											Description	-	+			
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			
											Место рождения	-	+			
											Дата рождения	-	+			
											ИНН	-	+			
											ОГРН	-	+			
											ОГРНИП	-	+			
											СНИЛС	-	+			
											ИНН ЮЛ	-	+			
Sub CA	4f56589e-7e80-4fbe-b49f-662c9ba9a335	7y	--	-	RSA	3072	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
					ECDSA	256					Unique Identifier (UID)	-	+	DNS name	-	+
											Given name	-	+	MS UPN	-	+
											Initials	-	+	MS GUID	-	+
											Surname	-	+	IP address	-	+
					Organizational unit	-					+	Directory Name	-	+		

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
											Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Locality	-	+	Uniform resource identifier	-	+
											State or province	-	+	Registered Identifier (OID)	-	+
											Domain component	-	+	Permanent identifier	-	+
											Country	-	+	Xmpp address	-	+
											Postal code	-	+	Service Name	-	+
											Business category	-	+	Subject Identification Method	-	+
											Telephone number	-	+	Kerberos KPN	-	+
											Pseudonym	-	+			
											Postal address	-	+			
											Street	-	+			
											Name	-	+			
											Title	-	+			
											Domain qualifier	-	+			
											Description	-	+			
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			
											Место рождения	-	+			
											Дата рождения	-	+			
											ИНН	-	+			
											ОГРН	-	+			
											ОГРНИП	-	+			
											СНИЛС	-	+			
											ИНН ЮЛ	-	+			

SCEP Management	77004b9d-e195-40a3-ae0-dca5ad403f49	25y	-	-	RSA	2048	- Цифровая подпись - Шифрование ключей - Шифрование данных	+	-	-	Common name	+	-	-
					ECDSA	256								
					ГОСТ Р 34.10-2012	256								

ПРИЛОЖЕНИЕ 2. УСТАНОВКА ПО ДЛЯ РАБОТЫ С КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

Установка JC-WebClient

JC-WebClient обеспечивает выпуск сертификатов на электронных ключевых носителях JaCarta. JC-WebClient необходимо установить на компьютер, с которого будет выполняется подключение к Клиентской части Центра регистрации Aladdin eRA.

Внимание! При установке и использовании JC-WebClient сертифицированная среда функционирования не обеспечивается.

Скачайте дистрибутив JC-WebClient [с веб-сайта производителя](#) и установите зависимости.

Установите JC-WebClient, выполнив следующую команду с правами суперпользователя:

РЕД ОС

```
sudo dnf install JC-WebClient-x64-x.x.x.xxxx.rpm
```

SberLinux OS Server»

```
sudo dnf install JC-WebClient-x64-x.x.x.xxxx.rpm
```

Astra Linux SE

```
sudo apt install -f JC-WebClient-x64-x.x.x.xxxx.deb
```

Альт Сервер

```
sudo apt-get install JC-WebClient-x64-x.x.x.xxxx.rpm
```

Перейдите в каталог `/etc/rc.d/init.d/`, выполнив команду:

```
cd /etc/rc.d/init.d/
```

Выполните запуск JC-WebClient, выполнив следующую команду с правами суперпользователя:

```
sudo sh jcmon start
```

Установка Рутокен плагина и его расширения

ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин» обеспечивает выпуск сертификатов на электронных ключевых носителях Рутокен. ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин» необходимо установить на компьютер, с которого будет выполняется подключение к Клиентской части Центра регистрации Aladdin eRA.

Внимание! При установке и использовании ПО «Рутокен Плагин» и его браузерного расширения «Адаптер Рутокен Плагин» сертифицированная среда функционирования не обеспечивается.

Скачайте дистрибутив ПО «Рутокен Плагин» с [официального сайта производителя](#).

Установите ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен» по инструкции с [официального сайта производителя](#).

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация – действия по проверке подлинности идентификатора пользователя. Под аутентификацией понимается ввод пароля или PIN-кода на средстве вычислительной техники в открытом контуре, а также процессы, реализующие проверку этих данных.

Заявка – это заявление от пользователя на получение сертификата, полученное через API или веб-интерфейс, содержащее совокупность данных о пользователе (запрос на сертификат (CSR)).

Ключевой носитель – это сущность в центре сертификации, соответствующая физическому токenu, программному или аппаратному модулю безопасности Hkagware Security Module (HSM). С помощью крипто-токена ЦС осуществляет хранение ключей и выполнение криптографических операций.

Сертификат – выпущенный центром сертификации цифровой документ в форматах x509v3 или другом поддерживаемом формате, подтверждающий принадлежность владельцу закрытого ключа или каких-либо атрибутов и предназначенный для аутентификации в информационной системе.

Список отозванных сертификатов (Certificate Revocation List – CRL) – список аннулированных (отозванных) сертификатов, издаётся центром сертификации по запросу или с заданной периодичностью на основании запросов об отзыве сертификатов.

Субъект – пользователь информационной системы или устройство (сервер, шлюз, маршрутизатор). Субъекту для строгой аутентификации в информационной системе в центре сертификации выдаётся сертификат. Синоним – конечная сущность (end entity).

Тикет (ticket) – временные данные, выдаваемые клиенту для аутентификации на сервере, на котором располагается необходимый сервис.

Центр регистрации – это функциональный компонент программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG», предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты и сертификатов пользователей; обработки заявок пользователей на выпуск сертификата.

Центр сертификации – комплекс средств, задача которых заключается в обеспечении жизненного цикла сертификатов пользователей и устройств информационной системы, а также в создании инфраструктуры для обеспечения процессов идентификации и строгой аутентификации в информационной системе. Программный комплекс «Центр сертификации Aladdin Enterprise Certificate Authority» является частью программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG».

Kerberos – сетевой протокол аутентификации, который обеспечивает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

Keytab-файл – это файл, содержащий пары Kerberos-принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля.

Веб-интерфейс (user interface - UI) – интерфейс, обеспечивающий передачу информации между пользователем-человеком и программно-аппаратными компонентами компьютерной системы.

Шаблон субъекта – шаблон, на основании которого необходимо создавать субъекты. Шаблон определяет свойства субъекта (subject name, alternative name), свойства сертификата (криптографию, срок действия, назначение, политики и проч.), а также инфраструктурные характеристики (реквизиты для доставки сертификатов, возможности отзыва, хранения и проч.).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	–	Операционная система
ПО	–	Программное обеспечение
РС		Ресурсная система
СУБД	–	Система управления базами данных
CRL	–	Certificate Revocation List
URL	–	Uniform Resource Locator

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]