Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition

Руководство пользователя

Изделие	RU.АЛДЕ.03.01.020-01
Документ	34
Листов	46
Дата	12.12.2023

АННОТАЦИЯ

Настоящий документ представляет собой руководство оператора программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»[1].

Настоящий документ является эксплуатационным документом, содержащим описание действий оператора при работе с программным компонентом «Центр сертификации Aladdin Enterprise Certificate Authority»[2], обеспечивающим управление жизненным циклом сертификатов субъектов.

Настоящий документ содержит сведения о назначении программы, условиях его применения, порядке действий оператора по работе с Aladdin eCA CE, сообщениях, выдаваемых оператору в процессе работы.

Настоящий документ соответствует требованиям к разработке эксплуатационной документации, определённым в методическом документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённого приказам ФСТЭК России от 02 июня 2020 г. №76 по 4 уровню доверия.

Таблица 1 – Соответствие документации требованиям доверия – раздел 16 «Требования к разработке эксплуатационной документации»

Требования доверия (16.1 Руководство пользователя должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
режимов работы средства	раздел 2 «Условия выполнения программы»
принципов безопасной работы средств	раздел 2 «Условия выполнения программы»
функций и интерфейсов функций средства, доступных каждой роли пользователей	раздел 4 «Описание функций программы»
параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений	раздел 3 «Выполнение программы»
типов событий безопасности, связанных с доступными пользователю функциями средства	раздел 5 «Сообщения оператору»
действий после сбоев и ошибок эксплуатации средства	раздел 5 «Сообщения оператору»

Перед эксплуатацией программы рекомендуется внимательно ознакомиться с настоящим руководством.

[1] Далее по документу – программа, программное средство, Aladdin eCA

[2] Далее по документы – программный компонент, Центр сертификации Aladdin Enterprise Certificate Authority, Центр сертификации Aladdin eCA

Содержание

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Область применения

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» применяется как элемент систем защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации для предотвращения несанкционированного доступа к информации в автоматизированных (информационных) системах.

Программный компонент «Центр сертификации Aladdin eCA» является компонентом глобальной службы каталогов, отвечающим за управление криптографическими ключами субъектов.

1.2 Краткое описание возможностей

«Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» обеспечивает возможности:

- выпуска сертификатов Центра сертификации;
- выпуска сертификатов для субъектов доступа;
- экспорта открытого ключа сертификата, сертификата в контейнере #pkcs12 (с закрытым ключом), цепочки сертификатов центра сертификации на ключевой носитель;
- управления статусом сертификата доступа (отозвать или приостановить действие выпущенного сертификата субъекта, активировать);
- формирования списка всех выпущенных сертификатов в файл формата, удобного для просмотра;
- управления учетными записями пользователей (создание, назначение роли, удаление, редактирование, назначение доступа к субъектам ресурсных систем);
- управления ресурсными системами (подключение, обновление списка групп и субъектов);
- управления списком отозванных сертификатов (настройка периодов формирования и действия CRL, публикация CRL в ручном режиме);
- регистрации Центров валидации;
- управления журналом событий (архивация, очистка, экспорт журнала событий по выбранным критериям);
- разграничение доступа к интерфейсу и функционалу программы (на основании ролей).

1.3 Уровень подготовки пользователя

Операторы Aladdin eCA CE должны иметь навыки в работе с применением технических средств уровня семейства операционных систем Windows и семейства операционных систем Linux.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Поддерживаемые браузеры

Работа с программным компонентом «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» поддерживается через веб-браузеры операционных систем РЕД ОС 7.3, Astra Linux Special Edition 1.7 и Альт 10.

2.2 Поддерживаемые ключевые носители

Поддерживаемые модели электронных ключей (ключевых носителей):

- JaCarta PKI;
- JaCarta PRO;
- JaCarta-2 ГОСТ.

2.3 Режим функционирования программы

Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition функционирует в следующих режимах:

- штатный режим, при котором программа должна исправно функционировать, обеспечивая возможность круглосуточного выполнение задач и функций в полном объёме;
- сервисный режим, необходимый для проведения обслуживания (обновления программы).

Основным режимом функционирования программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» является штатный режим.

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

2.4 Доступ к программе

Для получения доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certificate Authority» необходимо обратиться к уполномоченному лицу, исполняющему обязанности администратора Центра сертификации для:

- создания новой учётной записи с ролью «Оператор» и выпуск сертификата в контейнере p12 для созданной учётной записи оператора.
- передачи сертификата лицу, исполняющему обязанности «Оператора», в контейнере p12 с атрибутом безопасности (паролем от контейнера) для дальнейшей аутентификации на веб-сервере Центра сертификации.

2.5 Принципы безопасной работы программного средства

К основным принципам безопасной работы программного средства относятся:

- выполнение ограничений по эксплуатации программного средства, приведённых в разделе 2 «Условия выполнения программы» настоящего документа;
- контроль физической сохранности средств вычислительной техники с установленным Средством двухфакторной аутентификации;
- сохранение в секрете пароля (PIN-кода) пользователя;
- исключение доступа посторонних лиц к персональному идентификатору.

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Запуск программы

- Запуск служб программного компонента осуществляет администратор Центра сертификации на сервере, где развёрнут Центр сертификации Aladdin Enterprise Certificate Authority.
  - Оператору предоставляется доступ к клиентской части посредством веб-интерфейса. Для запуска клиентской части Центра сертификации Aladdin Enterprise Certificate Authority запустите браузер;
  - выберите сертификат доступа аутентифицирующегося пользователя (см. Рисунок 3);
  - в адресную строку браузера введите ip-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority». Например:

```
https://172.22.5.21
```

3.2 Доступ пользователей к программе

3.2.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск

Полученный оператором контейнер сертификат доступа для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certificate Authority необходимо перенести любым удобным способом на жёсткий диск СВТ для его дальнейшей установки в хранилище сертификатов браузера для сохранения информации о доверенных сертификатах с целью успешного подключения к серверу на клиентской стороне.

Для установки сертификата в доверенное хранилище сертификатов вашего браузера выполните нижеописанные действия. Процесс установки сертификата доступа в доверенное хранилище рассмотрим на примере браузера Firefox:

- Откройте браузер Firefox – Настройки – Приватность и Защита – Сертификаты (см. Рисунок 1). Нажмите кнопку <Просмотр сертификатов>.

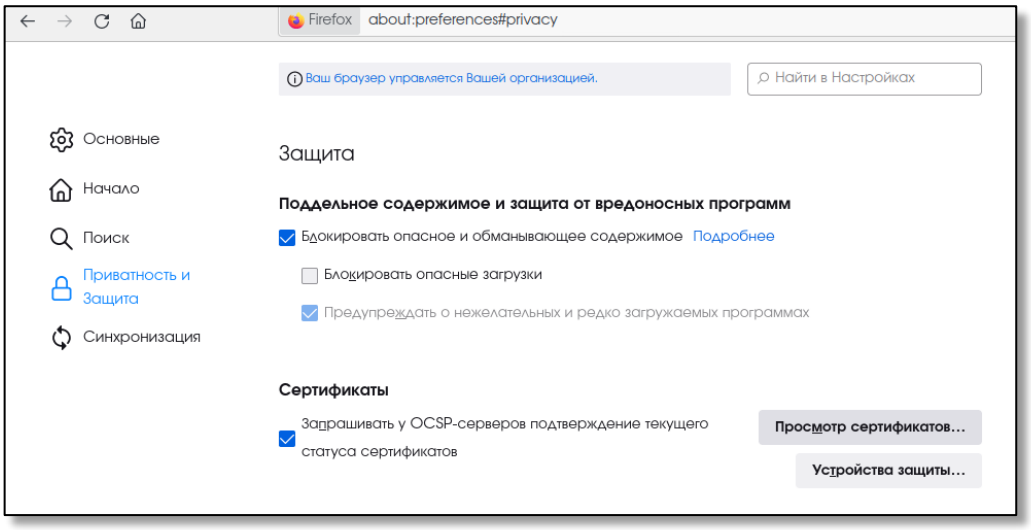


Рисунок 1 – Окно настроек браузера

- Выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку <Импортировать> (см. Рисунок 2).

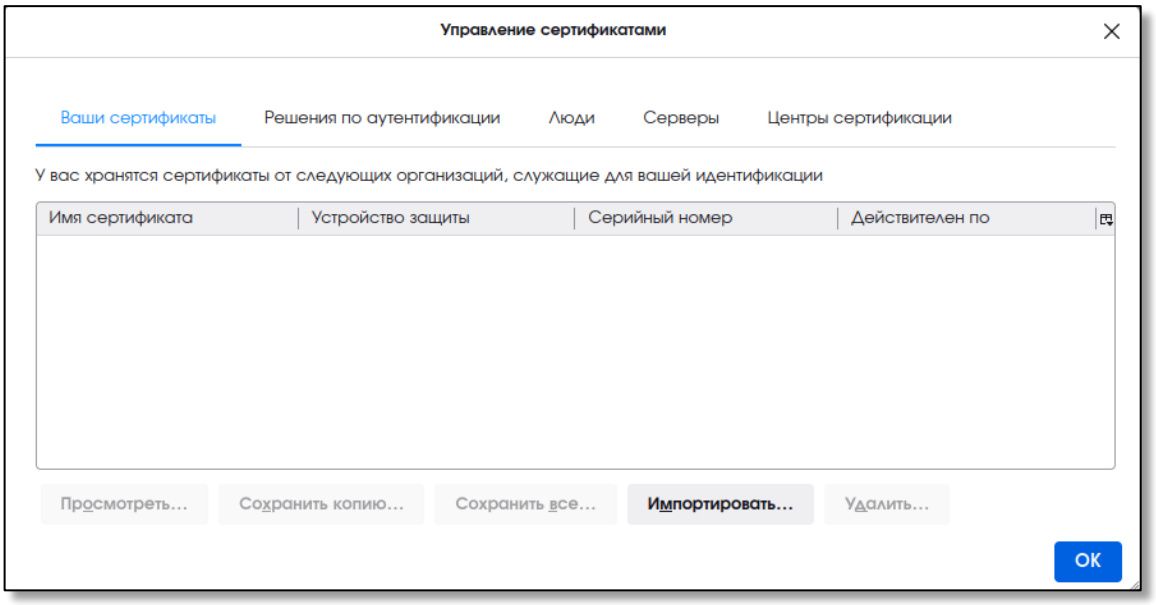


Рисунок 2 – Окно управления сертификатами

- Выберите контейнер .p12, содержащий закрытый ключ и сертификат доступа, перенесённый на жесткий диск, выпущенный для учётной записи пользователя (см. Рисунок 3).

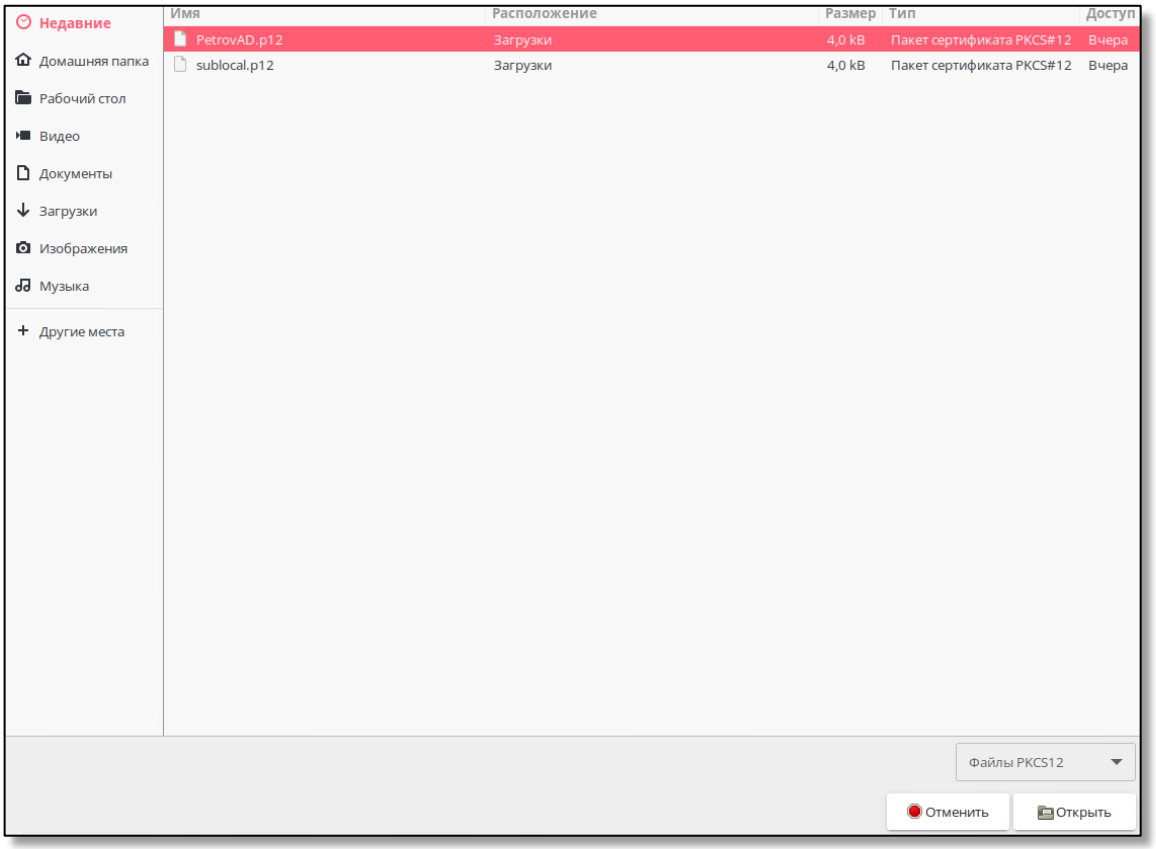


Рисунок 3 – Окно выбора импортируемого файла сертификата

- Введите пин-код загружаемого контейнера .p12 в открывшемся окне и нажмите кнопку <Ок> (см. Рисунок 4). Пин-код сертификата является атрибутом безопасности и должен быть передан администратором с контейнером закрытого ключа и сертификата.

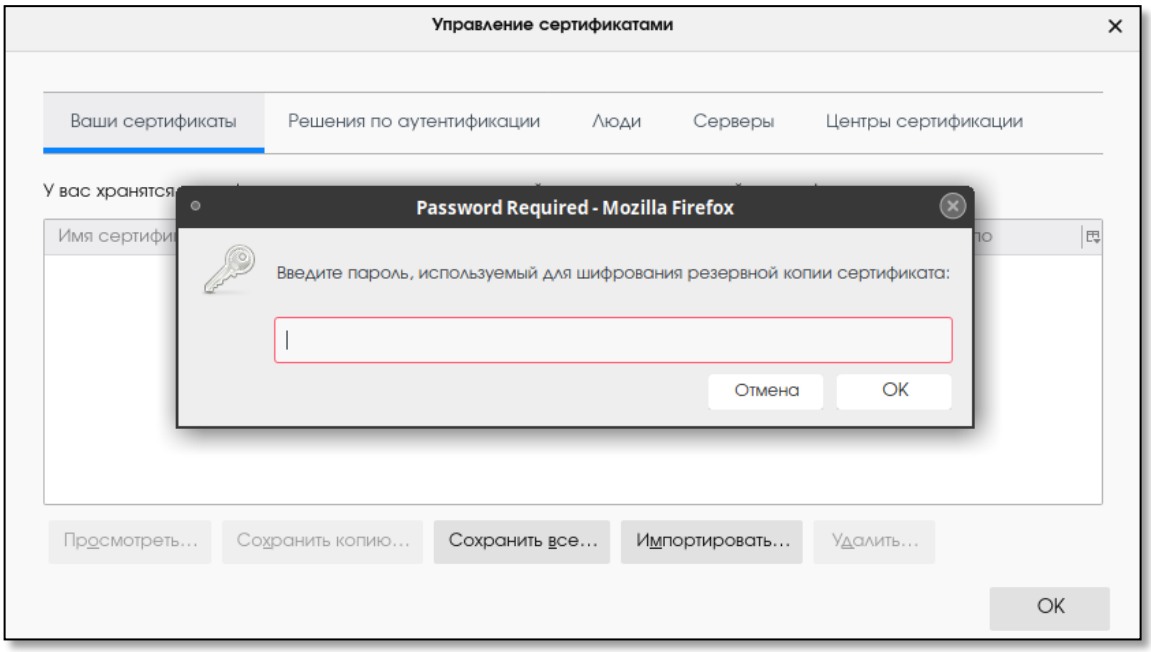


Рисунок 4 – Окно ввода пин-кода сертификата

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 5). Нажмите кнопку <ОК>.

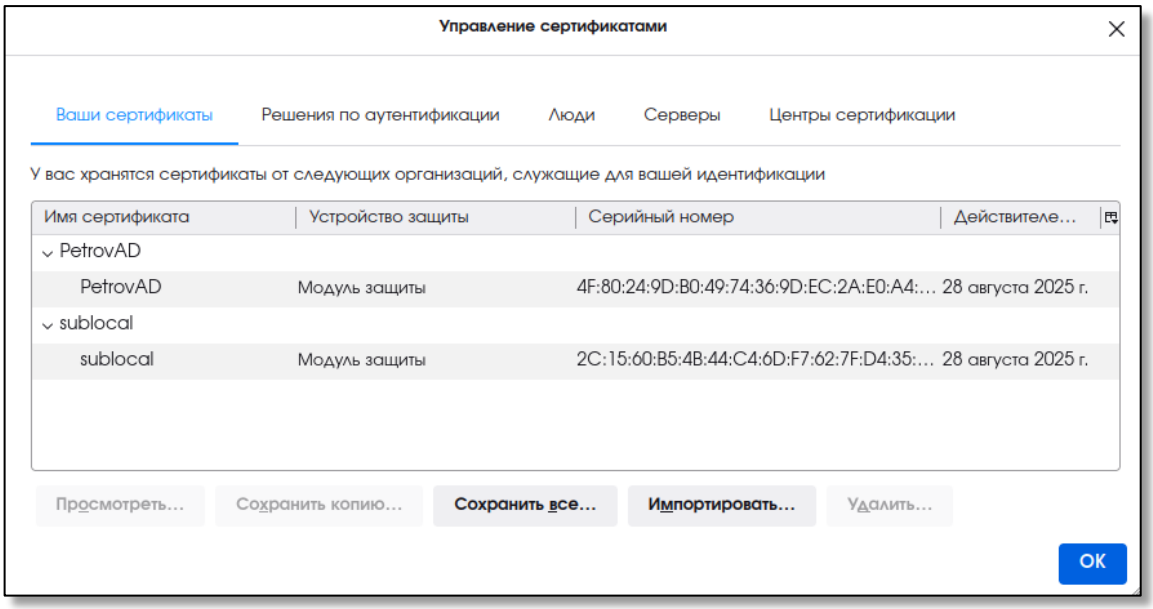


Рисунок 5 – Окно «Управление сертификатами»

- В адресную строку браузера введите ip-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».

Например:

```
https://172.22.5.21
```

- В открывшемся окне выберите сертификат для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certificate Authority (см. Рисунок 6). Нажмите кнопку <ОК>.

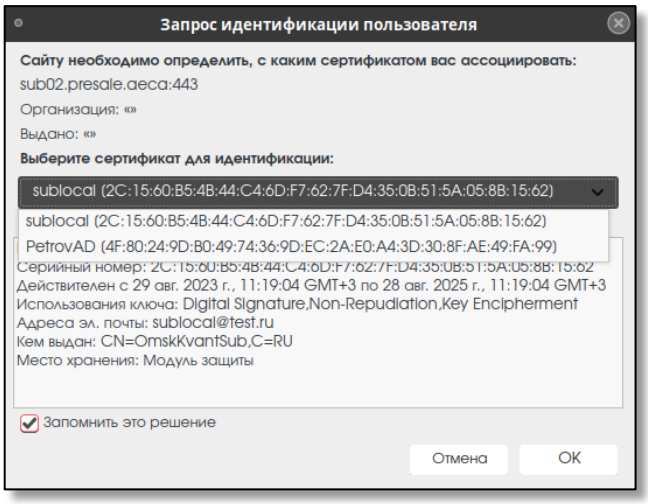


Рисунок 6 – Окно выбора сертификата для аутентификации

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 7). Нажмите кнопку <Дополнительно>.

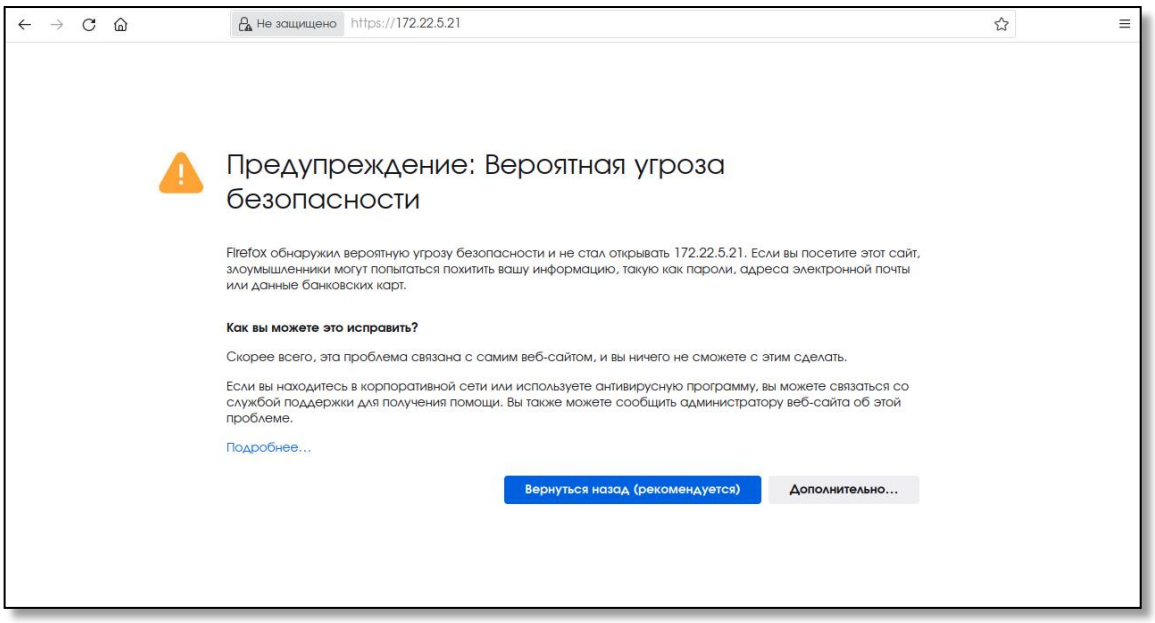


Рисунок 7 – Страница с предупреждением системы безопасности

- По нажатию кнопки <Дополнительно> на странице предупреждения системы безопасности осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 8). Нужно принять риски, нажав кнопку <Принять риск и продолжить> на текущей странице.

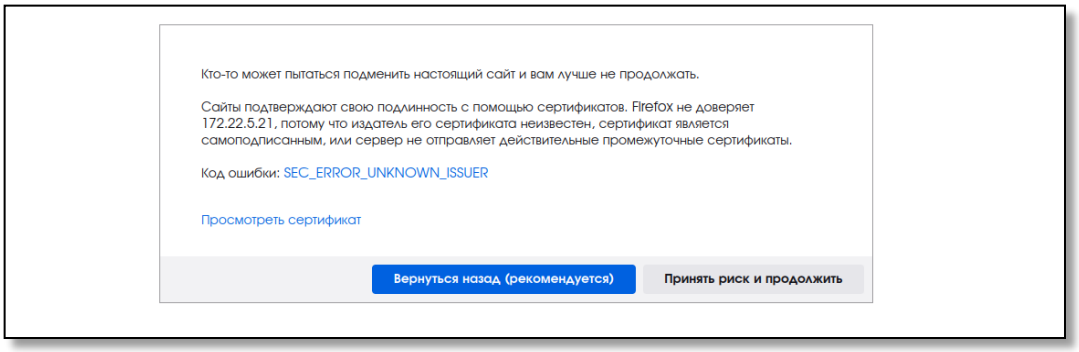


Рисунок 8 – Страница ошибки распознавания сертификата

- В случае отказа в доступе к веб-интерфейсу Центра сертификации Aladdin Enterprise Certificate Authority Оператор будет уведомлен сообщением об ошибке. Возможные причины отказа:
  - сертификат доступа пользователя не импортирован в доверенное хранилище браузера;
  - отсутствие издателя сертификата доступа, импортированного в доверенное хранилище браузера, в списке разрешённых издателей веб-сервера;
  - остановка работы служб Центра сертификации на веб-сервере;
  - срок действия сертификата доступа истёк;
  - действия сертификата было приостановлено или сертификат отозван.

В случае отказа доступа обратитесь к Администратору Центра сертификации Aladdin Enterprise Certificate Authority.

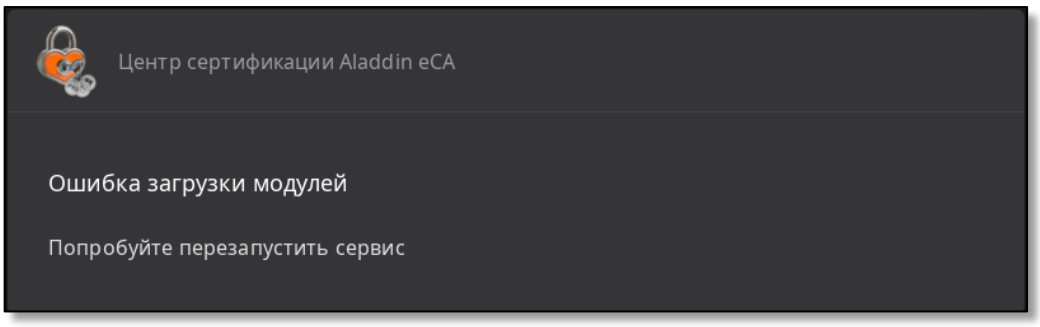


Рисунок 9 – Окно «Управление сертификатами»

- В случае успешной аутентификации пользователя будет сформировано защищённое соединение клиент – сервер и предоставлен доступ к веб-интерфейсу Центра сертификации Aladdin Enterprise Certificate Authority.

3.2.2 Аутентификация с использованием сертификата на ключевом носителе

3.2.2.1 Первичная настройка СВТ для двухфакторной аутентификации оператора по сертификату на ключевом носителе

- Для поддержки ключевых носителей произведите установку Единого Клиента JaCarta, для этого:
  - Скопируйте на компьютер в одну папку файлы из дистрибутива для дальнейшей инсталляции:
    - install.sh;
    - jacartauc_*_ro_x64.rpm;
    - jcpkcs11-2_*_x64.rpm;
    - jcsecurbio_*_x64.rpm;
    - RPM-GPG-KEY-ALADDIN_RD-AO.public (Открытый ключ АО "Аладдин Р.Д.").
  - Под пользователем с правами администратора запустите эмулятор терминала.
  - В эмуляторе терминала прейдите в папку с дистрибутивами, выполнив команду:

```
cd …/…/…
```

  - Установите Единый Клиент JaCarta, выполнив команду:

```
bash install.sh
```

Подробное описание процедуры установки Единого Клиента JaCarta приведено в разделе 4 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д.».

- Только для ОС Astra Linux Special Edition 1.7 произведите подготовку операционной системы, установив дополнительную библиотеку службы сетевой безопасности, выполнив команду от имени текущего пользователя:

```
apt install libnss3-tools
```

Текущий локальный пользователь должен иметь права на файлы в папке ~/.pki/nssdb/.

- Рекомендуется очистить кэш браузера и ранее применённые решения по аутентификации в браузере (для браузера Firefox: Настройки -> Приватность и защита -> Сертификаты -> Просмотр сертификатов).
- Выполните настройку браузера Firefox, если подключение к серверу Центра сертификации Aladdin Enterprise Certificate Authority будет выполнено в этом браузере:
  - откройте Настройки -> Приватность и защита -> Сертификаты -> Устройства защиты;
  - в диалоговом окне нажмите кнопка <Загрузить>;
  - в окне загрузки драйвера нажмите кнопку <Обзор> и выберите файл модуля `/lib64/libjcPKCS11-2.so` (см. Рисунок 10) и подтвердите загрузку модуля, нажав кнопку <ОК>;

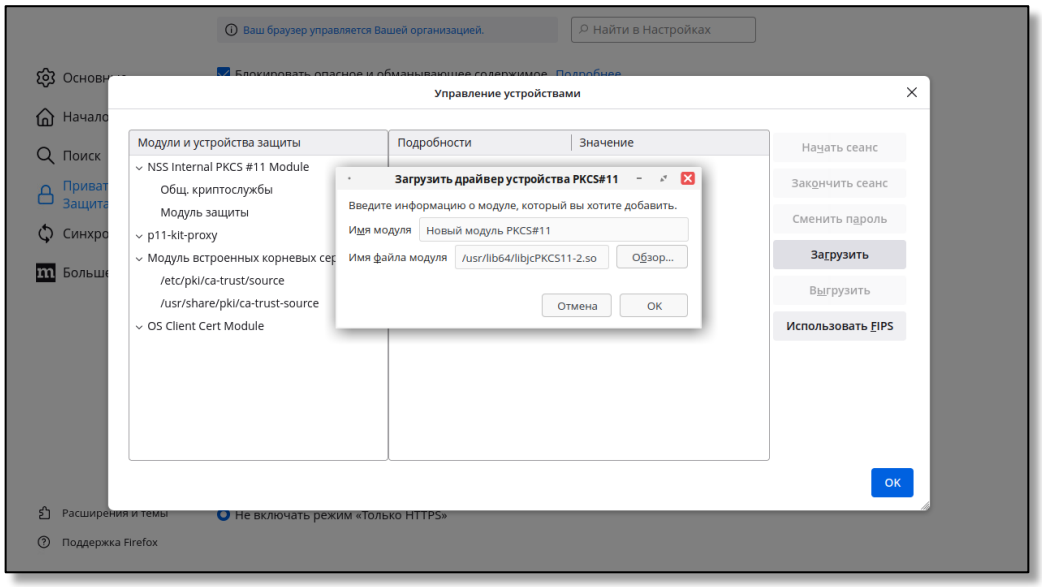


Рисунок 10 – Настройка браузера Firefox

  - перезапустите браузер.
- Выполните настройку браузера Chromium, если подключение к серверу Центра сертификации Aladdin Enterprise Certificate Authority будет выполнено в этом браузере посредством ОС РЕД ОС 7.3 или Альт 10:
  - удалите каталог локальной библиотеки сертификатов, выполнив команду:

```
rm -rf ~/.pki
```

  - создайте каталог локальной библиотеки сертификатов, выполнив команду под текущим пользователем:

```
mkdir ~/.pki/nssdb
```

  - инициализируйте локальную библиотеку сертификатов, выполнив команду под текущим пользователем:

```
certutil --empty-password -d ~/.pki/nssdb -N
```

  - подключите модуль к локальной библиотеке сертификатов `nssdb`, выполнив команду под текущим пользователем:

```
modutil -dbdir sql:.pki/nssdb/ -add “JaCarta” -libfile /usr/lib64/libjcPKCS11-2.so
```

  - перезапустите браузер.
- Выполните настройку браузера Chromium, если подключение к серверу Центра сертификации Aladdin Enterprise Certificate Authority будет выполнено в этом браузере посредством Astra Linux Special Edition 1.7:
  - подключите модуль `nssdb` для работы с сертификатами, выполнив команду:

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /lib/libjcPKCS11-2.so
```

- перезапустите браузер.

3.2.2.2 Двухфакторная аутентификации оператора по сертификату на ключевом носителе

- Полученный оператором ключевой носитель с записанным на нём сертификатом доступа для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certificate Authority необходимо подключить в USB-порт предварительного настроенного средства вычислительной техники – рабочего места оператора для его дальнейшей аутентификации с целью успешного подключения к серверу на клиентской стороне.

- Откройте браузер, для которого была выполнена первичная настройка двухфакторной аутентификации, и введите в адресную строку ip-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».

Например:

```
https://172.22.5.21
```

- В появившемся окне введите PIN-код ключевого носителя.

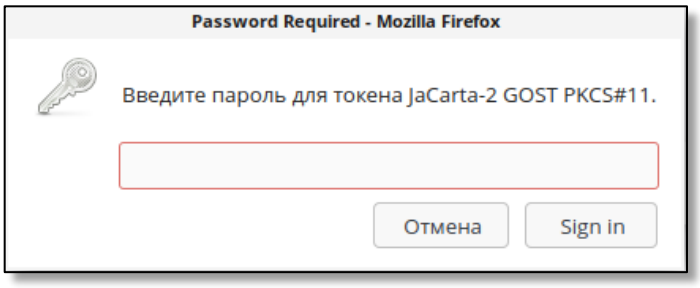


Рисунок 11 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

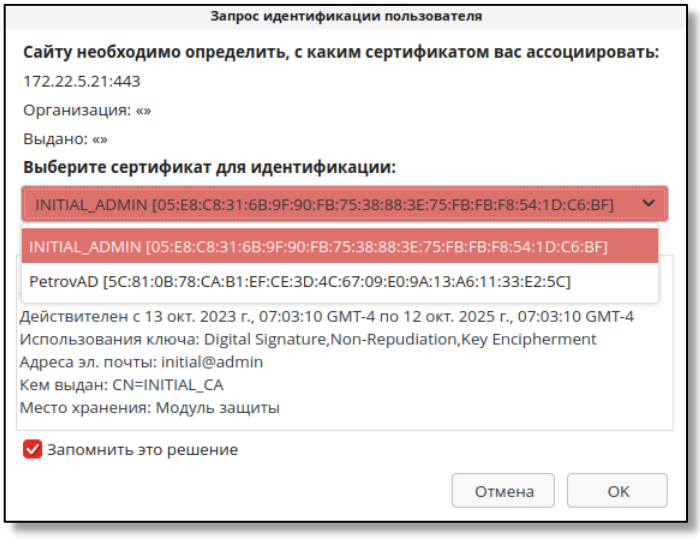


Рисунок 12 – Окно выбора сертификата пользователя для аутентификации на сервере

Время действия токена доступа – 3 минуты.

Время действия токена обновления – 24 часа, то есть по истечению времени действия токена обновления будет требоваться повторная аутентификация пользователя для доступа к серверу Центра сертификации.

4 ОПИСАНИЕ ФУНКЦИЙ ПРОГРАММЫ

4.1 Описание верхней панели «Центра сертификации»

Верхняя панель (см. Рисунок 13) Центра сертификации фиксирована и отображается на любом шаге или переходе между вкладками.

Рисунок 13 – Верхняя панель окна «Центра сертификации»

При наведении курсора на иконку панели всплывает соответствующее текстовое пояснение для каждого элемента.

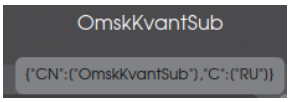
Верхняя панель содержит следующие элементы:

- 

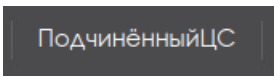
- тип активного ЦС (возможные варианты: Корневой или Подчиненный);

- 

- обозначение статуса ЦС, возможные варианты:
  - «активный» – соответствует зеленому цвету иконки,
  - «не инициализирован» – соответствует красному цвету иконки,
  - «истек срок действия сертификата» – соответствует оранжевому цвету иконки,
  - «истек срок действия лицензии» – соответствует красному цвету иконки);

- 

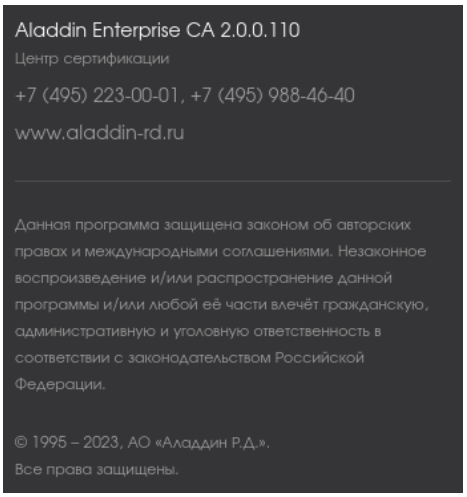
- имя текущего активного ЦС. При наведении курсора всплывают заданные имя и значения суффикса различающегося имени ЦС;

- 

- отображаемое имя текущего активного ЦС;

- 

- текущая авторизация учётной записи пользователя;

- 

- сведения о текущей версии программного компонента, контактная информация разработчика.

4.2 Описание боковой панели «Центра сертификации»

Боковая панель Центра сертификации закреплена и отображается на любом шаге или переходе между вкладками.

Полный вид боковой панели показан на Рисунок 14, компактный вид боковой панели приведен на Рисунок 15. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели.

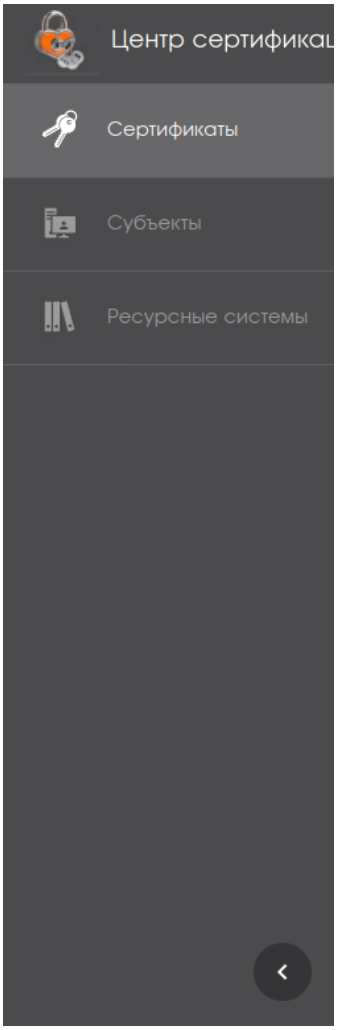


Рисунок 14 – Полный вид боковой панели

Рисунок 15 – Компактный вид боковой панели

Боковая панель состоит из разделов, определяющих соответствующие функции программы, доступные учётной записи с ролью «Оператор», и созданы для организации управления выпуском и жизненным циклом сертификатов доступа:

- Раздел «Сертификаты» – в данном разделе возможно:
  - посмотреть список всех выпущенных сертификатов субъектов, издателем которых является активный ЦС, с отображением статуса сертификата, срока действия, типа субъекта, имени субъекта и серийного номера сертификата;
  - произвести поиск выпущенных сертификатов по имени субъекта или серийному номеру;
  - отозвать или приостановить действие выпущенного сертификата субъекта;
  - посмотреть карточку выпущенного сертификата субъекта;
  - скачать сертификат субъекта в формате .pem;
  - скачать цепочку сертификатов;
  - скачать список выпущенных сертификатов в формате .csv;
  - применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);

- Раздел «Субъекты» – в данном разделе возможно:
  - произвести поиск субъекта по его имени (или части имени);
  - обновить список групп и субъектов;
  - посмотреть организационные группы субъектов локальной и подключенных ресурсных систем;
  - посмотреть существующие субъекты;
  - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
  - выпустить сертификат на основании запроса для субъекта;
  - выпустить сертификат на ключевом носителе для субъекта;
  - посмотреть все выпущенные сертификаты для каждого субъекта;
  - создать учётную запись для субъекта из группы «Users»;
  - посмотреть карточку субъекта;
  - опубликовать сертификат субъекта в ресурсную систему;
- Вкладка «Ресурсная система» – на данной вкладке возможно:
  - обновить список субъектов ресурсной системы и их данных в ручном режиме.

Далее в настоящем документе приводится полное описание доступных функций управления Центром сертификации для каждой вкладки.

4.3 Раздел «Сертификаты»

Раздел «Сертификаты» обеспечивает просмотр и управление сертификатами субъектов в соответствии с правами учётной записи пользователя. Пользователю с ролью «Оператор» доступен просмотр и управление сертификатами субъектов, права на которые предоставлены для учётной записи.

Переход на экран управления центра сертификации осуществляется по выбору раздела «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 14).

На данном экране отображаются все созданные сертификаты субъектов (см. Рисунок 16).

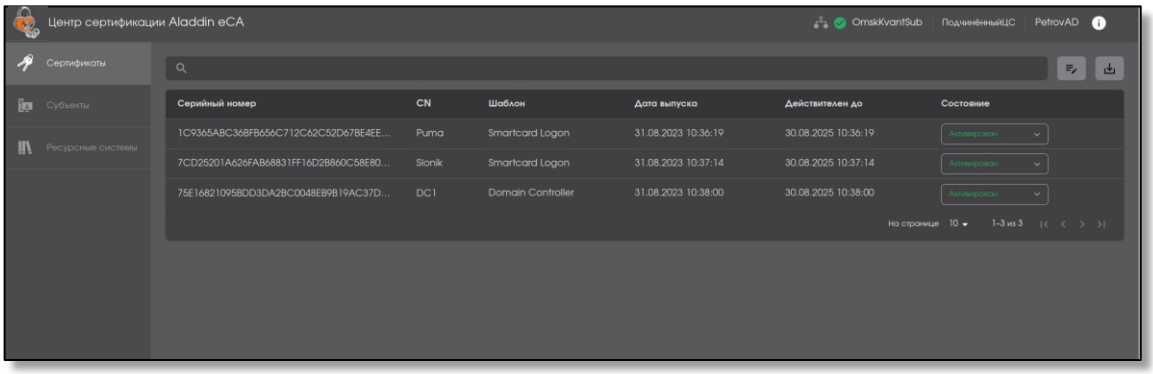


Рисунок 16 - Экран раздела меню «Сертификаты»

- На экране раздела «Сертификаты» отображены информационные элементы (табличные поля):
  - серийный номер сертификата;
  - имя субъекта (CN);
  - тип шаблона сертификата (шаблон);
  - дата выпуска сертификата;
  - дата срока окончания действия сертификата (действителен до);
  - текущий статус сертификата (состояние).
- Доступны следующие операции по работе с сертификатами:
  - поиск выпущенных сертификатов;
  - сортировка сертификатов;
  - скачивание сертификатов;
  - изменение статуса сертификатов;
  - просмотр карточки сертификата;

- экспорт списка выпущенных сертификатов с атрибутами;
- массовые операции с выпущенными сертификатами.

- Все созданные сертификаты субъектов на экране раздела отображаются в виде таблицы с пагинацией.

4.3.1 Поиск сертификатов

Строка поиска (см. Рисунок 17) предназначена для поиска сертификатов по имени (поле Common Name), альтернативному имени субъекта (поле SubjectAltName) и серийному номеру сертификата (поле Serial Number). Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

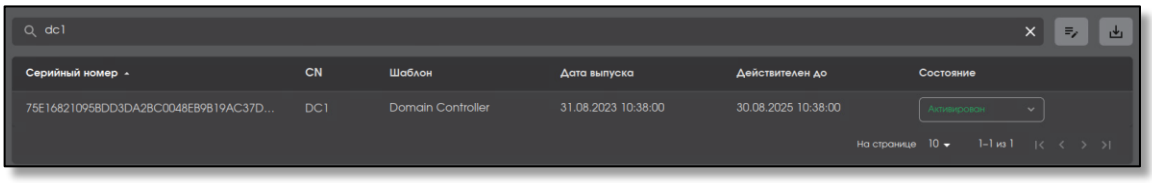


Рисунок 17 – Поисковая строка в разделе «Сертификаты»

- Для сброса результатов поиска и возврату к полному перечню сертификатов в экранной таблице удалите содержимое строки поиска.

4.3.2 Сортировка сертификатов

- Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 18):
  - «Серийный номер» – сортировка осуществляется в порядке возрастания или убывания значения;
  - «CN» – сортировка осуществляется в алфавитном порядке;
  - «Шаблон» – осуществляется группировка по типу шаблона;
  - «Дата выпуска», «Действителен до» – сортировка осуществляется в порядке возрастания или убывания значения даты.

- Сортировка происходит только по одному значению при нажатии на соответствующий заголовок таблицы. Активное значение, по которому выполнена фильтрация обозначен знаком  с правой стороны от заголовка таблицы.

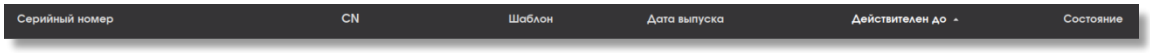


Рисунок 18 – Поля сортировки содержимого раздела «Сертификаты»

4.3.3 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку  (см. Рисунок 16) и в раскрывшемся подменю выберите пункт <Скачать сертификат> или «Скачать цепочку» в формате .pem (см. Рисунок 19).

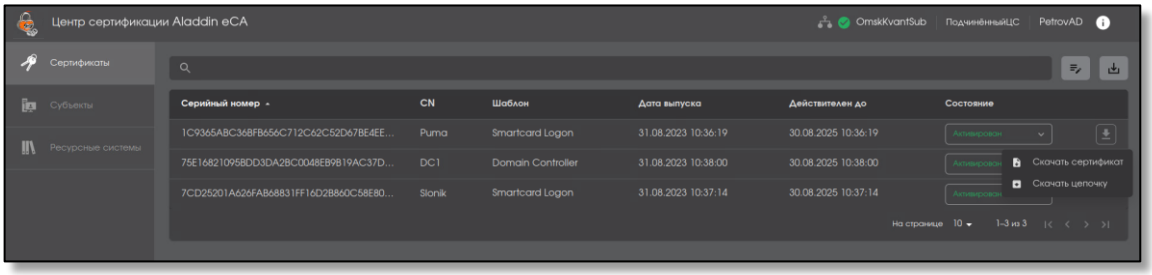


Рисунок 19 – Подменю «Скачать сертификат/цепочку»

4.3.4 Статус сертификатов

- Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в Таблица 2.

Таблица 2 – Доступные действия над сертификатами в зависимости от состояния

Состояние сертификата	Доступные действия		
	активация	приостановка	отзыв
активирован	□	+	+
приостановлен	+	□	+
отозван	□	□	□

- Смена состояния сертификата производится посредством выбора нужного значения из выпадающего меню при выделении строки сертификата (см. Рисунок 20).

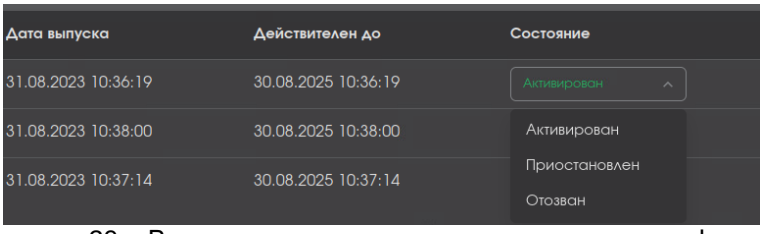


Рисунок 20 – Выпадающее меню смены состояния сертификата

- При смене состояния сертификата посредством радиокнопки появляется окно с запросом на подтверждение операции, в зависимости от типа операции предусмотрена различная активность для данного окна:
  - активация (см. Рисунок 21)

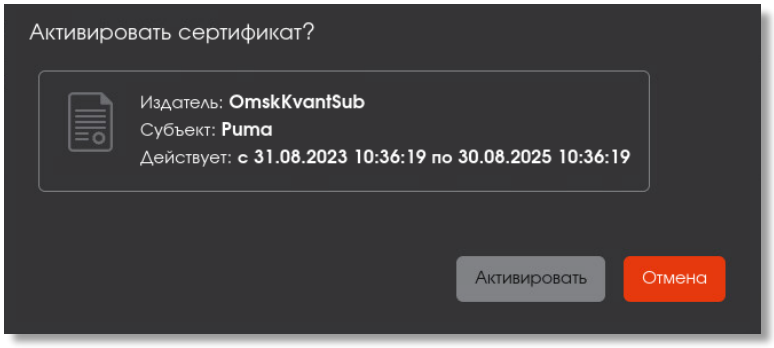


Рисунок 21 – Окно активации сертификата

  - приостановка действия сертификата (см. Рисунок 22):

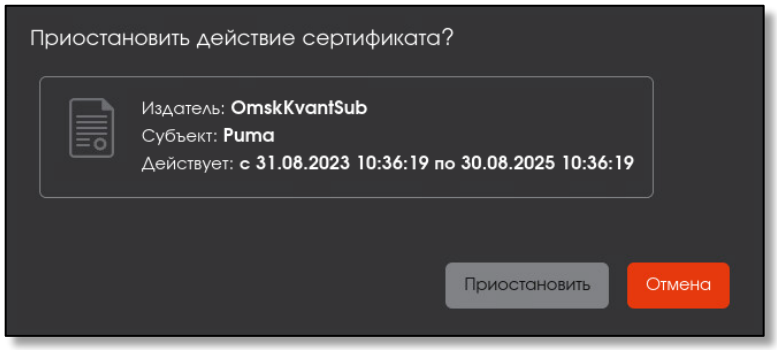


Рисунок 22 – Окно приостановки действия сертификата

- отзыв (см. Рисунок 23);

ВНИМАНИЕ! Данную операцию нельзя отменить.

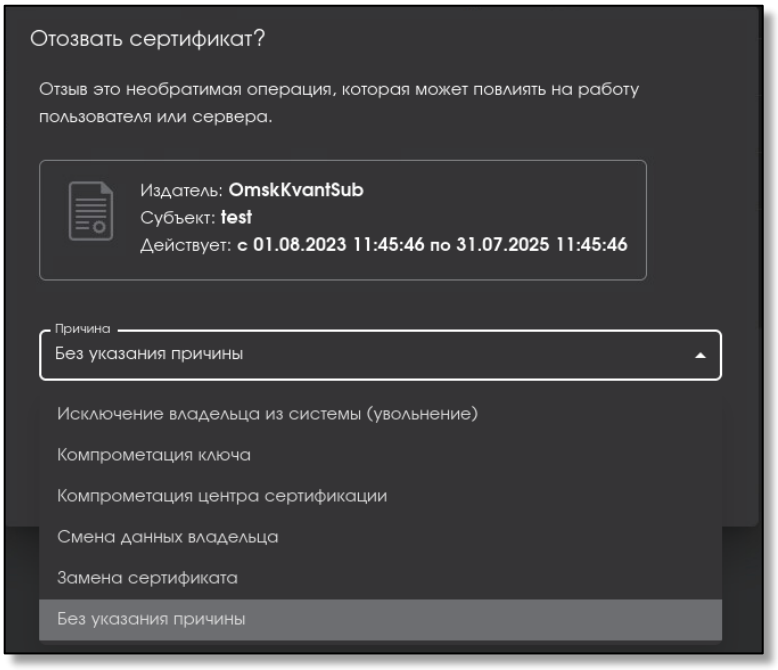


Рисунок 23 – Окно отзыва сертификата

Возможные причины отзыва (в соответствии с разделом 6.3.2 RFC5280):

- неиспользуемый (unused) – исключение владельца из системы/увольнение;
- принадлежность изменена (affiliation Changed) – смена данных владельца;
- приостановка полномочий владельца сертификата (certificateHold);
- компрометация ключа (keyCompromise);
- компрометация центра сертификации (cACompromise);
- заменен (сертификат) – заменен на иной сертификат;
- без указания причины (unspecified).

4.3.5 Карточка сертификата

- Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».
- Переход к экрану «Карточка сертификата» (см. Рисунок 24) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 16).

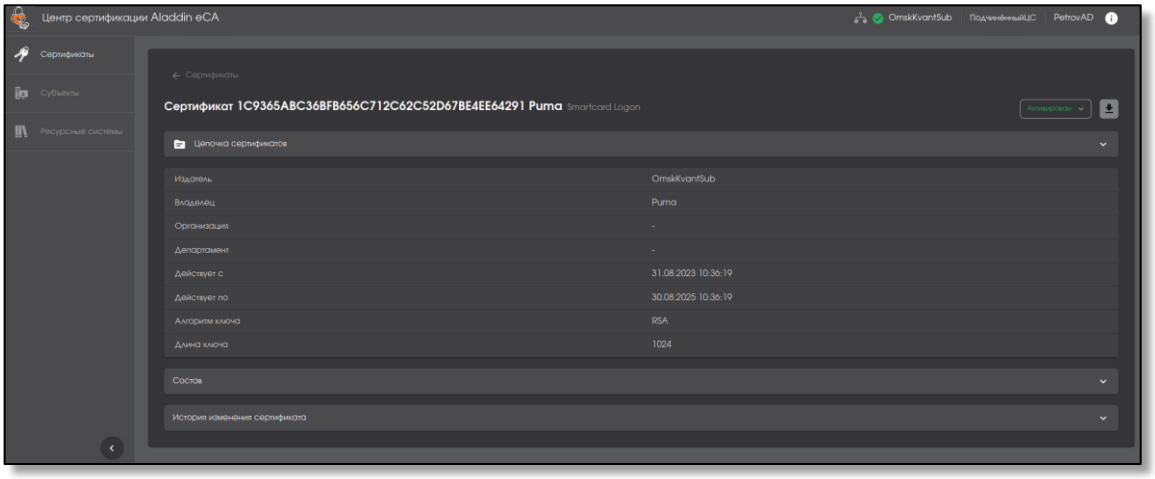


Рисунок 24 – Окно «Карточка сертификата»

- Оглавление карточки сертификата включает в себя:
  - тип (на Рисунке 21 – сертификат);
  - серийный номер сертификата (на Рисунке 21 – 1C9365AB…);
  - принадлежность (на Рисунке 21 – Puma);
  - шаблон сертификата (на Рисунке 21 – Smartcard Logon).
- Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке 

- Для изменения статуса сертификата выбрать из выпадающего списка действие 

в соответствие с Таблица 2 .
- Для скачивания сертификата наведите указатель мыши на выбранный сертификат и скачайте по нажатию появившейся кнопки  <Скачать сертификат> цепочку сертификатов или сертификат субъекта.
- Карточка сертификата содержит раскрывающиеся вкладки:
  - «Цепочка сертификатов». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены все Центры сертификации, участвующие в построении цепочки сертификатов, начиная с Корневого ЦС, на основе которого строится цепочка доверия сертификатам, до конечного Центра сертификации, выдавшего текущий сертификат субъекта (см. Рисунок 25).

Рисунок 25 – Окно карточки сертификата. Вкладка «Цепочка сертификатов»

  - «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ  . На раскрывшемся экране отображены следующие поля (см. Рисунок 26):
    - открытый ключ;
    - отпечаток;
    - версия;
    - параметр открытого ключа;
    - алгоритм цифровой подписи
    - основные ограничения;
    - использование ключа;
    - доступ информации о центре сертификации;
    - альтернативное имя субъекта;
    - идентификатор ключа центра;
    - идентификатор ключа субъекта;
    - расширенное использование ключа.

При переходе на выбранное поле, в правой части экрана будет отображена информация, соответствующая выделенному полю.

Рисунок 26 – Окно карточки сертификатов. Вкладка «Состав»

- «История изменения сертификата». Раскройте вкладку, нажав в строке с именем вкладки символ . На данной вкладке зафиксирована информация о всех совершённых над сертификатом действиях в хронологическом порядке. На раскрывшемся экране отображены поля (см. Рисунок 27):
  - дата – дата совершенного действия;
  - пользователь – учётная запись, под которой было совершенно данное действие;
  - событие – действие, совершённое над сертификатом.

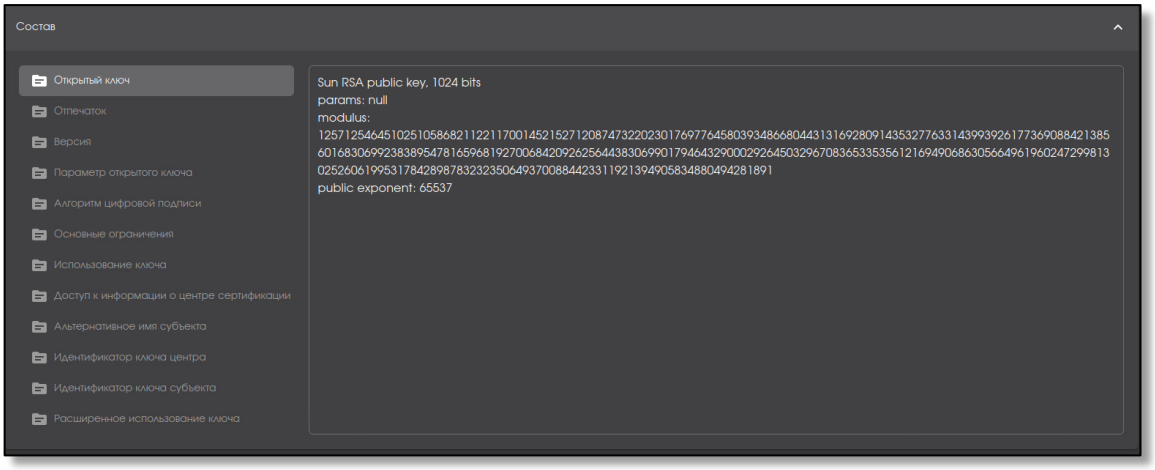


Рисунок 27 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

- Выход из карточки сертификата осуществляется по кнопке <Возврат> и по кнопкам разделов на боковой панели.

4.3.6 Экспорт списка выпущенных сертификатов

- При использовании учётной записи «Оператор» в список .csv файла будут собраны только выпущенные сертификаты тех субъектов, права доступа на которые назначены данному оператору.
- Для выгрузки списка сертификатов нажмите кнопку <Скачать все сертификаты в формате CSV>.
- В появившемся окне (см. Рисунок 28) введите имя файла и выберите папку для сохранения файла списка сертификатов. Нажмите кнопку <Сохранить>.

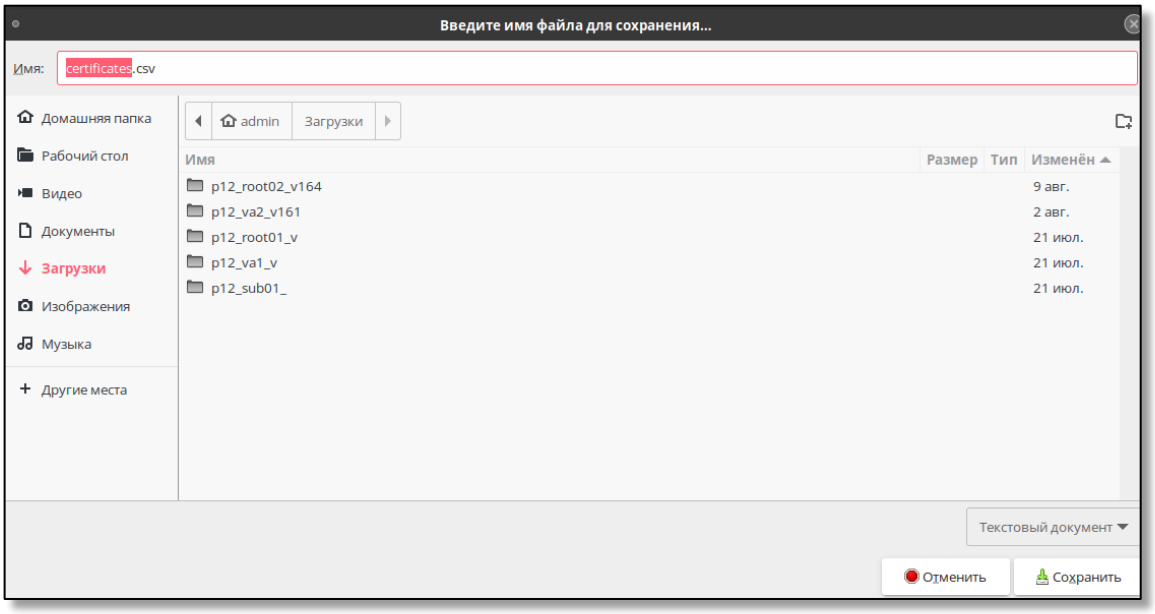


Рисунок 28 – Окно указания пути сохранения списка выпущенных сертификатов

- Выгруженный файл .csv представлен в текстовом формате для представления табличных данных, где строки текста содержат поля таблицы, разделённые запятыми. Сформированная таблица содержит следующие столбцы (см. Рисунок 29):
  - fingerprint – содержит уникальный числовой отпечаток сертификата;
  - cafingerprint – содержит уникальный числовой отпечаток сертификата центра, подписавшего сертификат;
  - expire date – содержит значение даты «годен до»;
  - issuerdn – содержит отличительное имя издателя;
  - revocation date – содержит дату отзыва;
  - revocation reason – содержит причину отзыва;
  - serialnumber – содержит серийный номер сертификата;
  - status – содержит текущий статус сертификата;
  - subjectdn – содержит отличительное имя держателя сертификата;
  - create date – содержит дату выпуска сертификата;
  - username – содержит имя держателя сертификата;
  - subject alt name – содержит дополнительные имена держателя;
  - template – содержит наименование шаблона;
  - algorithm – содержит обозначение алгоритма;
  - key length – содержит длину ключа;
  - history – содержит историю изменений сертификата в формате JSON.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	fingerprint	cafingerprint	expire date	issuerdn	revocation date	revocation reason	serialnumber	status	subjectdn	create date	username	subject alt name	template	algorithm	key length
2	532af36b5656	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 13:18	Revoked: Cessation c	7f7b2814f9a1ea	HOLD	CN=SubCA242	###########	SubCA242	null	OCSP Signer	RSA	2048
3	c32484f9822d6	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	29644f7f1ac7c6	HOLD	CN=DC	###########	DC	dNSName=DC, gu	Domain Cont	RSA	2048
4	5258bc09c2061	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	699edc111ec1e	REVOKED	CN=cheburge	###########	cheburgen	rfc822name=cheb	Smartcard Lo	RSA	1024
5	47b18421ec42	0f83238c98d88	###########	CN=SubCA242,		Active	5110646ee2431	ACTIVE	CN=SubCA242	###########	SubCA242-web	dNSName=SubCA	WEB-Server	RSA	2048
6	7c13052621aff	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	67f2c7275957b8	REVOKED	CN=OP1_242	###########	OP1_242	rfc822name=op1@	WEB-Client	RSA	2048
7	52f46cc8e30f6	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	79878f39c5d53(	REVOKED	CN=OP2_242	###########	OP2_242	rfc822name=op2@	WEB-Client	RSA	2048
8	c411492ef40dc	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	171a95d06d320	REVOKED	CN=koltakova	###########	koltakovav	rfc822name=eaca	Smartcard Lo	RSA	2048
9	f830f0ccb22a0	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 14:46	Revoked: Cessation c	659787bd69df9	HOLD	CN=tushkan	###########	tushkan	rfc822name=tushk	Smartcard Lo	RSA	2048
10	dec1c1520014	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	6360503883063	HOLD	CN=SUBCA	###########	SUBCA	dNSName=SUBCA	Domain Cont	RSA	3072
11	110ffbd7a6f1a	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	560f36c6f48609	REVOKED	CN=ttttttt	###########	ttttttt	rfc822name=tt@t	Smartcard Lo	RSA	2048
12	bd8e4c114e36	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	09feb09eaf14e(	REVOKED	CN=OP1_242	###########	OP1_242	rfc822name=test@	WEB-Client	RSA	2048
13	f9c96f3951e7c	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 10:03	Suspended: Certifica	54a9be9b4d1da	REVOKED	CN=ushkan	###########	ushkan	rfc822name=ushk	Smartcard Lo	RSA	2048
14	8c32419d620b	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	360c202d0731a(	REVOKED	CN=tushkan	###########	tushkan	dNSName=tushka	Domain Cont	RSA	2048
15	bed018556db8	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 12:38	Suspended: Certifica	6a60fb1d27e71	REVOKED	CN=SUBCA	###########	SUBCA	dNSName=SUBCA	Domain Cont	RSA	3072
16	d93b3f0eb9dc	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 12:37	Suspended: Certifica	3bfa0b012fbd3(	REVOKED	CN=OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP,	Domain Cont	RSA	2048
17	3e352d5bf4f9c	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	1dc1aac2042d3(	REVOKED	CN=paukan	###########	paukan	rfc822name=pauk	Smartcard Lo	RSA	2048
18	4810c3f5cbbb5	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 13:28	Suspended: Certifica	35e5fc0c041cc8	REVOKED	CN=testop	###########	testop	rfc822name=swsd	WEB-Client	RSA	1024
19	3614fc6ce3245	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 15:01	Suspended: Certifica	201fe017d371d(	REVOKED	CN=DC	###########	DC	dNSName=DC, gu	Domain Cont	RSA	2048
20	4f2b63a93d73	0f83238c98d88	###########	CN=SubCA242,		Active	762a8430c0356(	ACTIVE	CN=operator	###########	operator	rfc822name=swsd	WEB-Client	RSA	2048
21	8b5c6e050346	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 17:30	Suspended: Certifica	7061a34d5576b(	REVOKED	CN=operator	###########	operator	rfc822name=test@	WEB-Client	RSA	2048
22	06335097415b	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 15:57	Suspended: Certifica	2df664eb41687	REVOKED	CN=paukan	###########	paukan	rfc822name=pauk	Smartcard Lo	RSA	2048
23	01f4dade2341	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 16:37	Suspended: Certifica	124f06965c59bc	REVOKED	CN=Guest	###########	Guest	dNSName=Guest,	Domain Cont	RSA	2048
24	07e080b9ca0b	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 17:49	Suspended: Certifica	5fa7bd4816ce9(	REVOKED	CN=test	###########	test	rfc822name=test@	Smartcard Lo	RSA	2048
25	fcb8cd2875a1e	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	6ed38ad110d43	HOLD	CN=kruchinin	06.09.2022 0:37	kruchinina	rfc822name=alex	Smartcard Lo	RSA	2048
26	ad3e9bed85d1(	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 8:50	Suspended: Certifica	365612cc14a7f9	REVOKED	CN=C‹PIP° PIP	###########	C‹PIP° PIP°	rfc822name=dfsd	Smartcard Lo	RSA	2048
27	23421a1f5bdc	0f83238c98d88	###########	CN=SubCA242,		Active	513c1b4479c38(	ACTIVE	CN=OP2_242	###########	OP2_242	rfc822name=swsd	WEB-Client	RSA	2048
28	8defcb24f54d(	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 12:02	Revoked: Cessation c	4d70ce1e01f42(	HOLD	CN=CLIENT2	###########	CLIENT2	dNSName=CLIENT	Domain Cont	RSA	2048
29	9ba4eecd5179	0f83238c98d88	###########	CN=SubCA242,	05.09.2022 15:58	Active	666cbb74489ed	ACTIVE	CN=OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP,	Domain Cont	RSA	2048
30	c73f85322b4a8	0f83238c98d88	###########	CN=SubCA242,		Active	17b0c9697f993(	ACTIVE	CN=OP1_242	###########	OP1_242	rfc822name=op1@	WEB-Client	RSA	2048
31	df1f61efba662	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	3c131d8839d6d	HOLD	CN=koltakova	###########	koltakovav	rfc822name=eaca	Smartcard Lo	RSA	2048
32	88bb73a7ae71	0f83238c98d88	###########	CN=SubCA242,	05.09.2022 16:11	Revoked: Cessation c	7aae5b17cf1c57	HOLD	CN=testuser2	###########	testuser2	rfc822name=testu	Smartcard Lo	RSA	2048

Рисунок 29 – Пример экспортированного файла списка выпущеных сертификатов.csv

4.3.7 Массовые операции с сертификатами

- Для массовой операции, применяемой к выбранному множеству сертификатов доступа, нажмите кнопку  <Массовые операции>, которая запускает окно выполнения массовой операции (см. Рисунок 30).

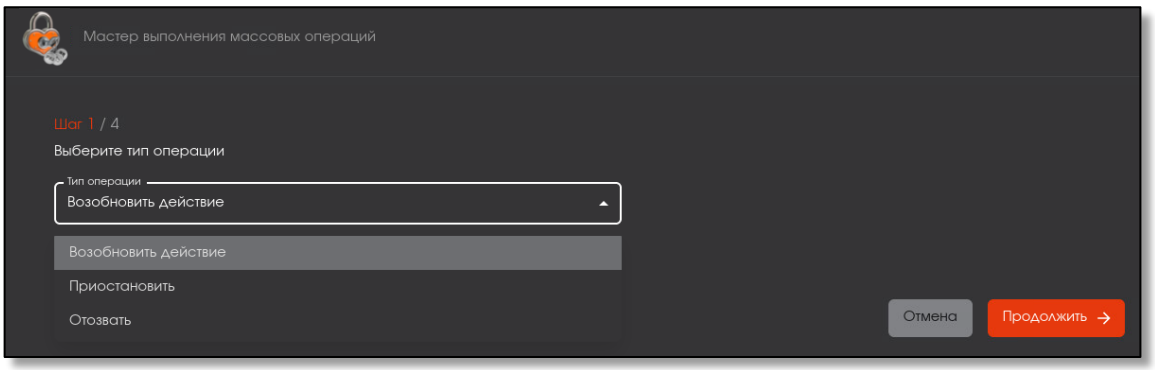


Рисунок 30 – Окно выполнения массовых операций. Шаг 1

- Выберите необходимую операцию из раскрывающегося списка. Доступны следующие типы операций:
  - возобновление действия;
  - приостановить;
  - отозвать.

При выборе операции «Отозвать» дополнительно необходимо будет указать причину отзыва из выпадающего списка.

- Нажмите ставшую активной кнопку <Продолжить>.
- Далее необходимо осуществить поиск сертификатов по отличительному имени субъекта Subject Distinguished Names, для которых требуется применить выбранную операцию, в левом поле окна Шага 2 (см. Рисунок 31). Поиск сертификатов производится с учётом текущего статуса сертификата и выбранного типа операции на шаге 1. Например, при выборе типа операции «Возобновить» поиск осуществляется только среди сертификатов со статусом «Приостановлен», для которых допустимо выполнить данный тип операции.
- Выберите, найденные сертификаты, отметив их флажками .
- Перенесите отмеченные флажками сертификаты в правую часть окна, нажав кнопку , которая находится между правой и левой частью окна выполнения операции.

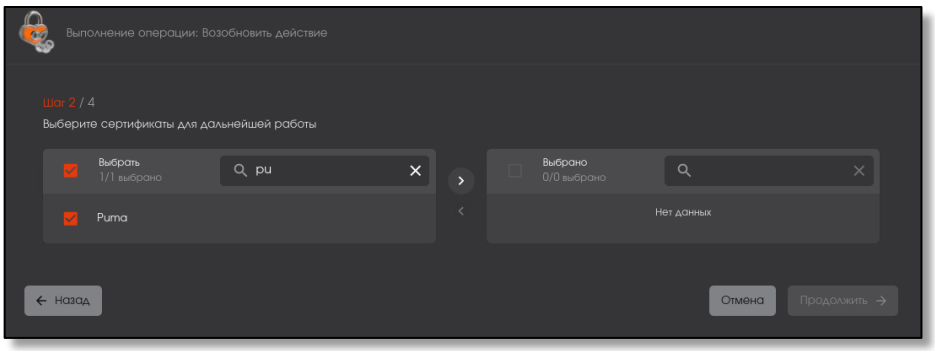


Рисунок 31 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

- В случае необходимости исключения из выбранных сертификатов, к которым будет применена массовая операция, отметьте флажками сертификата из списка в правой части окна, и нажмите кнопку .

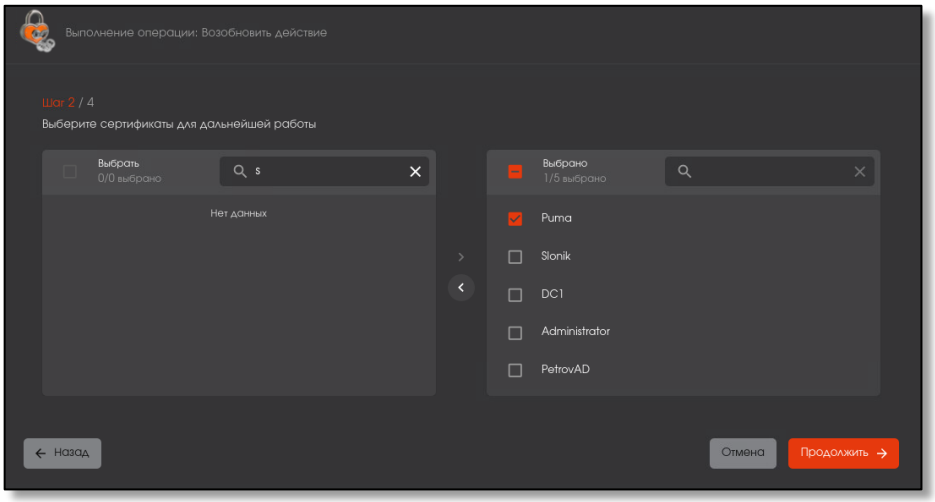


Рисунок 32 – Окно выполнения массовых операций. Шаг 2. Редактирование списка выбранных сертификатов

- Для перехода на следующий шаг нажмите кнопку <Продолжить>.
- В открывшемся окне подтвердите действие, нажав кнопку «Применить» (см. Рисунок 33).

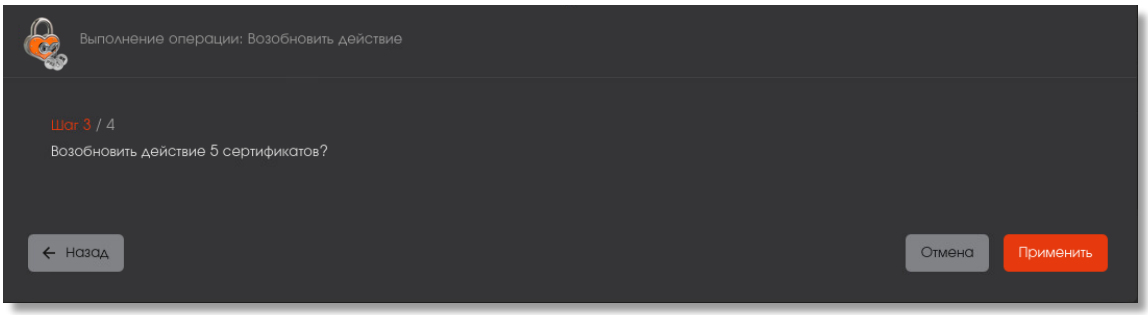


Рисунок 33 – Окно выполнения массовых операций. Шаг 3

- В случае успешного выполнения операции администратор будет уведомлён на шаге 4.

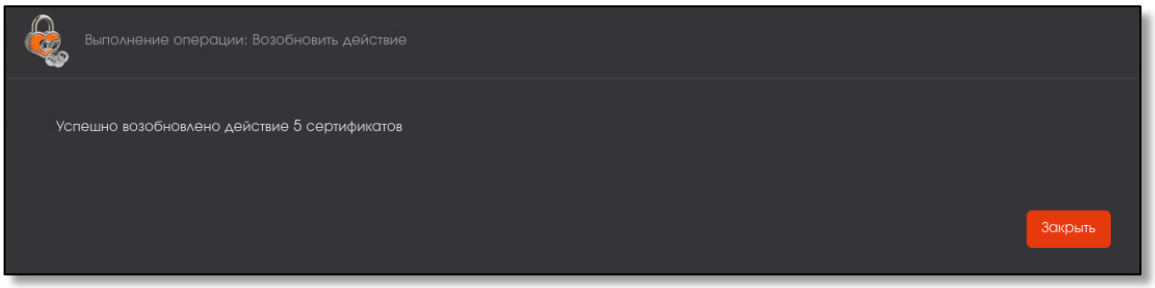


Рисунок 34 – Окно выполнения массовых операций. Шаг 4

4.4 Раздел «Субъекты»

Раздел «Субъекты» обеспечивает возможность просмотра субъектов подключенных служб каталога, выпуска сертификатов для субъектов, на которые предоставлены права авторизованному пользователю с ролью «Оператор».

- Переход в раздел «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 14).

- После выбора источника в поле «Внешние ресурсные системы», субъекты будут отображены в виде списка в окне раздела «Субъекты (см. Рисунок 35).

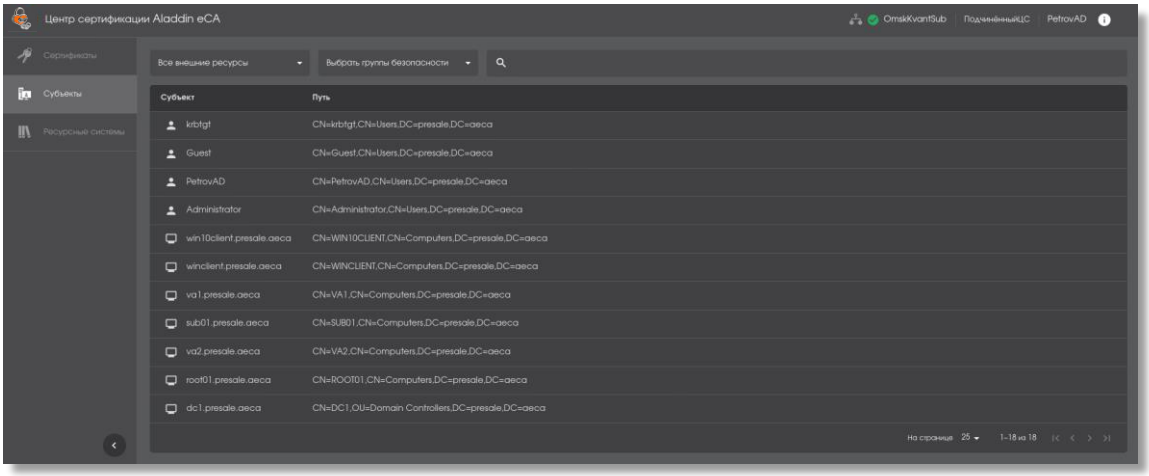


Рисунок 35 – Экран раздела меню «Субъекты». Подключенный ресурс

- На экране раздела «Субъекты» отображены информационные элементы (табличные поля):
  - субъект – полное имя субъекта;
  - путь, состоящий из компонентов: отличительного имени субъекта (например, CN=Puma), контейнера отличительного имени (например, CN=Users, DC=presale, DC=aeca), состоящего из организационной группы (например, CN=Users) и доменных компонентов (полного DNS-имени) (например, DC=presale, DC=aeca).

- Доступны следующие операции по работе с сертификатами:
  - выпуск сертификатов доступа для субъектов;
  - сортировка субъектов;
  - поиск субъектов;
  - выбор внешней ресурсной системы;
  - выбор группы безопасности ресурсной системы;
  - просмотр карточки субъекта.

4.4.1 Выбор внешней ресурсной системы

В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 36):

Рисунок 36 – Верхняя панель экранной формы вкладки «Субъекты»

- поле «Все внешние ресурсы». Внешний ресурс формируется в результате подключения к службе каталогов доменных служб Samba DC, ALD PRO, FreeIPA или MS Active Directory. По нажатию на поле в раскрывающемся меню выберите ресурсную систему, из списка тех, на которые предоставлены права для авторизованного пользователя с ролью «Оператор», для отображения субъектов внешних ресурсных систем;

4.4.2 Фильтрация субъектов

- В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 36):
  - поле «Выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в развернувшемся меню выберите необходимую группу. В случае, если группа безопасности не выбрана, то будут отображены все субъекты выбранной ресурсной системы. В списке «Выбрать группу безопасности» отображаются только те группы безопасности, которые содержат один или более субъектов. Группы безопасности, не имеющие членов, не будут показаны в списке и не доступны для выбора;

4.4.3 Поиск субъектов

- В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 36):
  - поле поиска, в котором осуществляется поиск субъектов по компонентам SubjectDN и SubjectAltName в выбранной ресурсной системе. Для поиска начните ввод имени субъекта в строке, поиск начинается автоматически через 1 секунду после прекращения ввода с клавиатуры. Для сброса поиска и отображения всех субъектов выбранной ресурсной системы очистите строку поиска.

4.4.4 Сортировка субъектов

Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 37):

- «Субъект» – сортировка осуществляется в алфавитном порядке;
- «Путь» – сортировка осуществляется в алфавитном порядке содержимого атрибута «Common Name».

Сортировка происходит только по одному значению при нажатии на соответствующий заголовок таблицы. Активное значение, по которому выполнена сортировка обозначено знаком ▲ с правой стороны от заголовка таблицы.

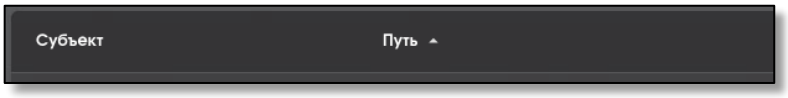


Рисунок 37 – Поля сортировки содержимого экрана раздела «Сертификаты»

4.4.5 Карточка субъекта

- Просмотра данных субъекта возможен посредством страницы «Карточка субъекта».
- Переход к экрану «Карточка субъекта» (см. Рисунок 39) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 35).

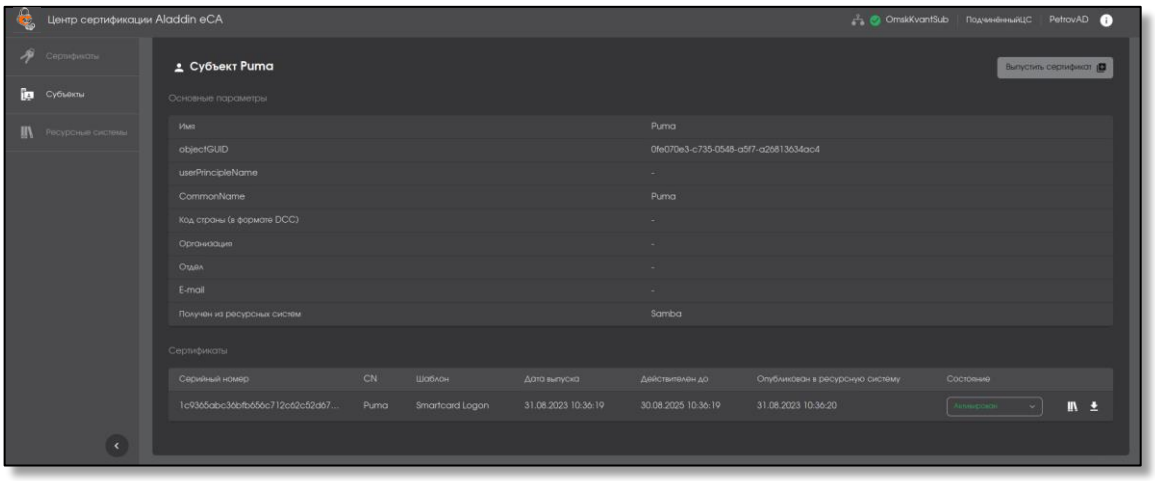
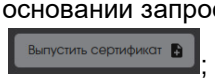


Рисунок 38 – Окно просмотра карточки субъекта

- Карточка субъекта включает в себя следующие информационные поля:
  - имя;
  - objectGUID;
  - UserPrincipleName;
  - CommonName;
  - код страны;
  - организацию;
  - отдел;
  - e-mail;
  - получен из ресурсных систем
  - сведения обо всех сертификатах, ранее выпущенных для субъекта:
    - серийный номер;
    - Common Name владельца сертификата;
    - шаблон;
    - дата выпуска
    - дата окончания действия;
    - дата публикации в ресурсную систему.
- Доступные действия в карточке субъекта:
  - выпуск сертификата для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку <Выпустить сертификат> 

;
  - опубликовать сертификат в ресурсную систему. По нажатию на кнопку  происходит запись сертификата в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат. Если атрибут `userCertification` заполнен, то происходит перезапись содержимого;
  - скачать сертификат выбранного субъекта по указанному для сохранения файла пути по кнопке  <Скачать>;
  - изменить статус сертификатов, выпущенных для данного субъекта в соответствии с Таблица 2 в поле сертификата «Состояние».

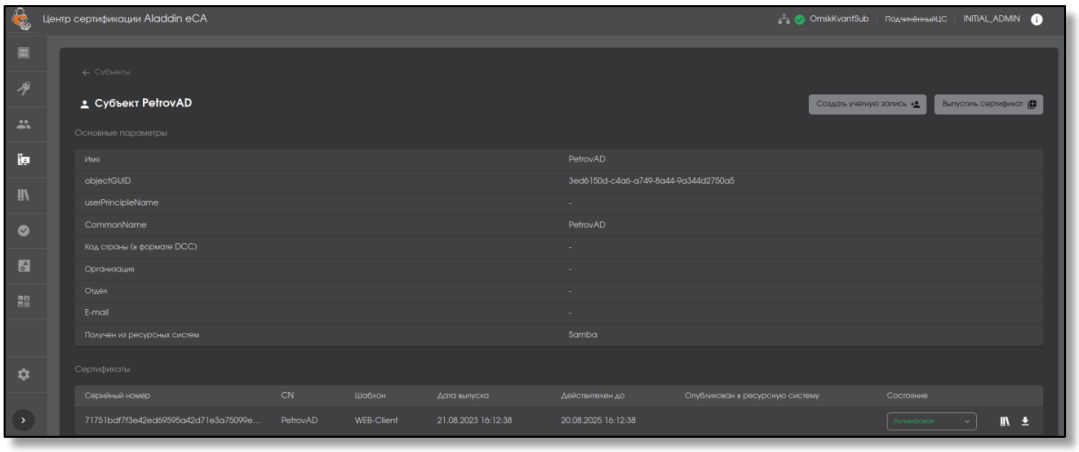


Рисунок 39 – Окно просмотра карточки субъекта

- Выход из карточки субъекта осуществляется по кнопке <Возврат> ← Субъекты в раздел «Субъекты» и по кнопкам разделов боковой панели.

4.4.6 Выпуск сертификата для субъекта ресурсной системы

В результате выпуска сертификата для субъекта ресурсной системы будет сгенерирована ключевая пара в соответствии с заданными параметрами криптографии.

- Выберите субъект, для которого необходимо создать сертификат, нажмите появившуюся кнопку  <Выпустить сертификат> и выберите способ создания из выпадающего списка (см. Рисунок 40).

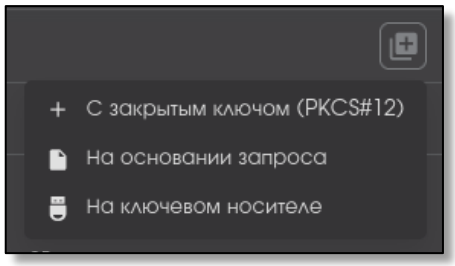


Рисунок 40 - Окно выпуска сертификата для субъекта ресурсной системы

- При выпуске сертификатов для субъектов внешних ресурсных систем возможно публиковать сертификат в формате LDIF в атрибут `userCertification` субъекта ресурсной системы, проставив флаг в чек-боксе «Публиковать сертификат в ресурсную систему» окна выпуска сертификата. По умолчанию флаг выполнения публикации сертификата включен.

- После выбора шаблона субъекта ресурсной системы на следующем шаге поля автоматически заполняются данными субъекта в соответствии:
  - в поле «Имя» передаются данные атрибута Common name содержимого записи LDAP. Поле не изменяемое;
  - в поле «RFC 822 Name» передается содержимое атрибута userPrincipalName записи LDAP. Данные в этом поле можно отредактировать. Если атрибут userPrincipalName не задан, то необходимо ввести в пустое поле окна создания сертификата нужное значение;
  - в поле «MS UPN» передается содержимое атрибута userPrincipalName записи LDAP. Данные в этом поле можно отредактировать. Если атрибут userPrincipalName не задан, то необходимо ввести в пустое поле окна создания сертификата нужное значение.

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля вручную.

4.4.6.1 Выпуск сертификата с закрытым ключом pkcs#12

- В открывшемся окне создания сертификата (см. Рисунок 41) выберите шаблон создаваемого сертификата из выпадающего списка (описание полей для каждого шаблона приведено в Приложении А).

Чек-бокс «Публиковать сертификат в ресурсную систему» активирован по умолчанию для публикации сертификата во внешнюю ресурсную систему. Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат.

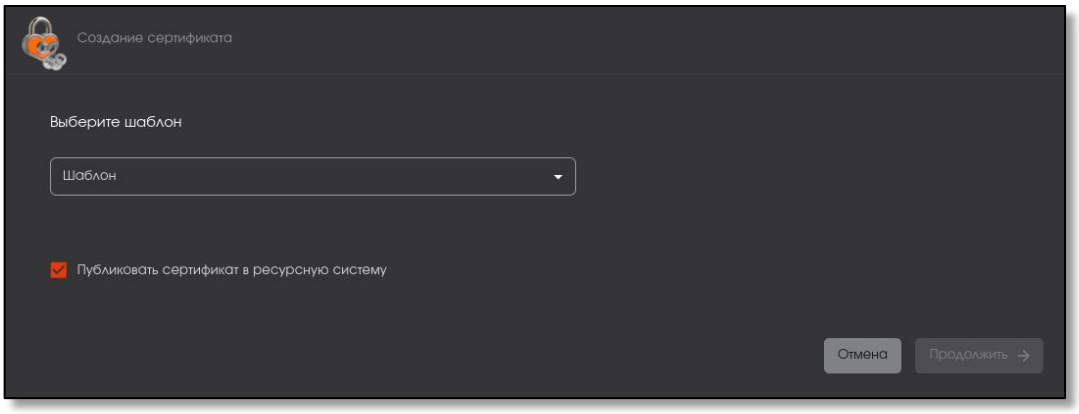


Рисунок 41 – Окно создания сертификата PKCS#12. Выбор шаблона

- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.
- После выбора шаблона для субъекта открывается окно ввода данных в соответствующие поля, определённые типом выбранного шаблона (см. Рисунок 42). После ввода всех данных кнопка «Продолжить» становится активной.
- Вводимые данные не должны содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами.

Рисунок 42 – Окно создания сертификата PKCS#12. Шаг 1

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 43). Правила ввода пароля:
  - для просмотра вводимых символов необходимо нажать кнопку на текущей строке;
  - пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;
  - если в пароле используются запрещенные символы, то рамка поля ввода приобретает красный цвет;
  - если пароли не совпадают, то рамка поля подтверждения окрашивается в красный цвет.

Кнопка <Продолжить> доступна только после ввода и верного повторения пароля в соответствии с правилами ввода.

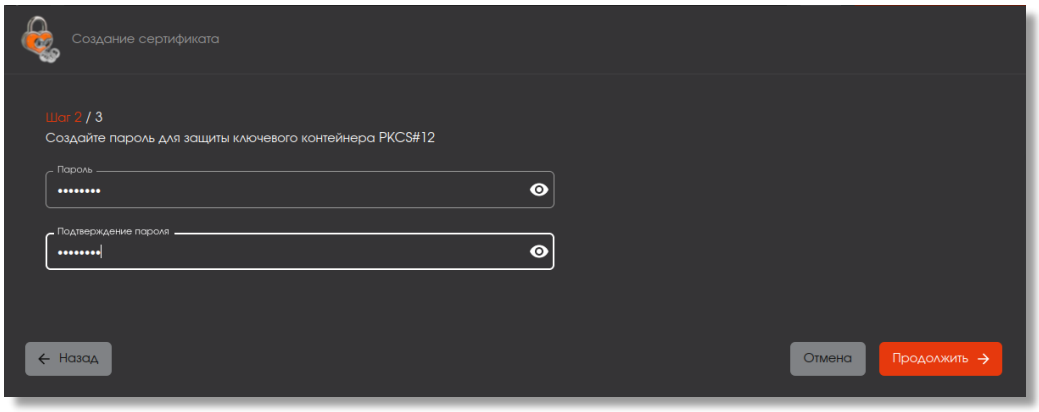


Рисунок 43 – Окно создания сертификата PKCS#12. Шаг 2

- В следующем окне требуется определить параметры шифрования (см. Рисунок 44):
  - алгоритм ключа;
  - длину ключа.

Параметры определяются шаблоном сертификата и выбираются в соответствии с техническими требованиями шаблона.

После определения всех параметров шифрования становится доступной для нажатия кнопка <Создать сертификат>.

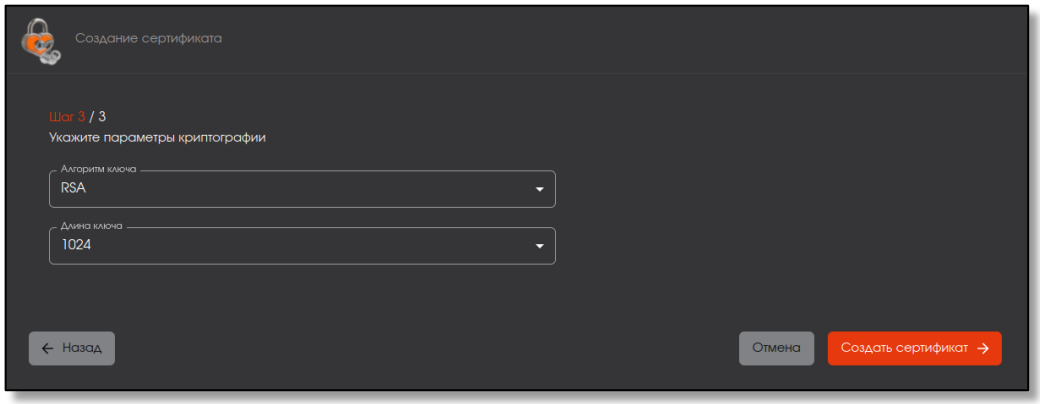


Рисунок 44 - Окно создания сертификата PKCS#12. Шаг 3

- По завершению работы мастера создания сертификата субъекта администратор видит окно, изображенное на Рисунок 45. В окне отображена общая информация о созданном сертификате (издатель, субъект, срок действия) и возможность скачать созданный сертификат.

> **Внимание! Сертификат и закрытый ключ в контейнере pkcs#12 возможно скачать только в последнем окне выпуска сертификата «об успешном создании сертификата» по нажатию на кнопку <Скачать>. Далее, после закрытия окна, скачивание выпущенного сертификата для субъекта в разделе «Сертификаты» доступно только в формате .pem!**

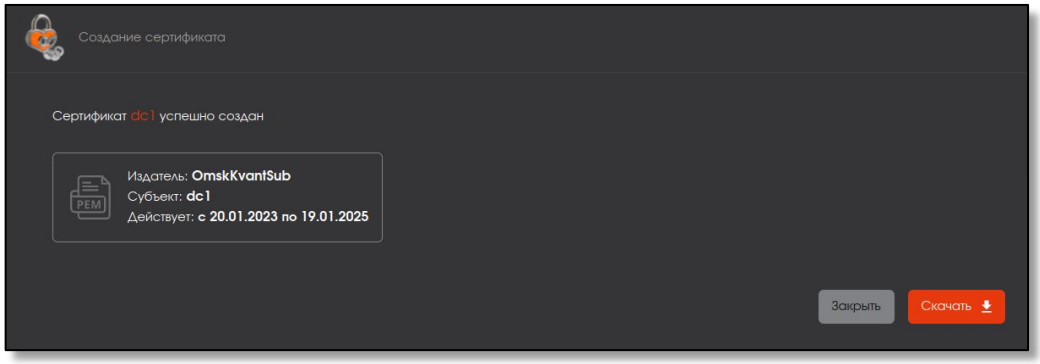


Рисунок 45 – Окно по результату успешного завершения создания сертификата PKCS#12

4.4.6.2 Выпуск сертификата с закрытым ключом pkcs#12 для контроллера ALD PRO

Для выпуска сертификата контроллеру ALD PRO:

- В открывшемся окне выбираем шаблон сертификата «ALD PRO Domain Controller» и нажимаем ставшую активной кнопку «Продолжить» (см. Рисунок 46).

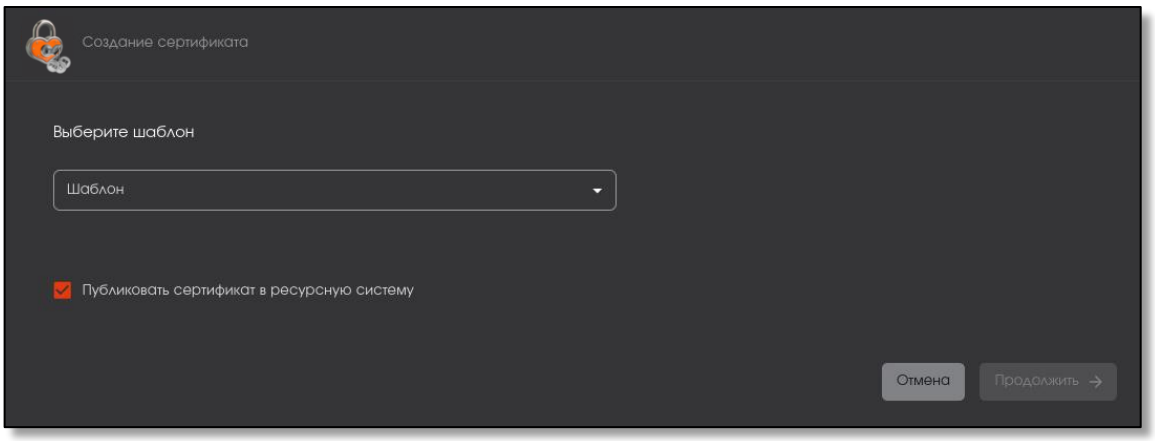


Рисунок 46 – Окно создания сертификата. Выбор шаблона контроллера домена ALD PRO

- В открывшемся окне необходимо ввести данные контроллера домена ALD PRO в соответствующие поля в случае, если данные субъекта ресурсной системы их не содержат (см. Рисунок 47):
  - в поле «Имя» укажите имя контроллера домена ALD PRO, для которого выпускается сертификат;
  - в поле «Организация» укажите полное имя домена;
  - в поле «MS UPN» укажите данные в формате «krbtgt/полное имя домена@полное имя домена»;
  - в поле «Kerberos 5 Principal Name» укажите в формате «krbtgt/полное имя домена@полное имя домена»;

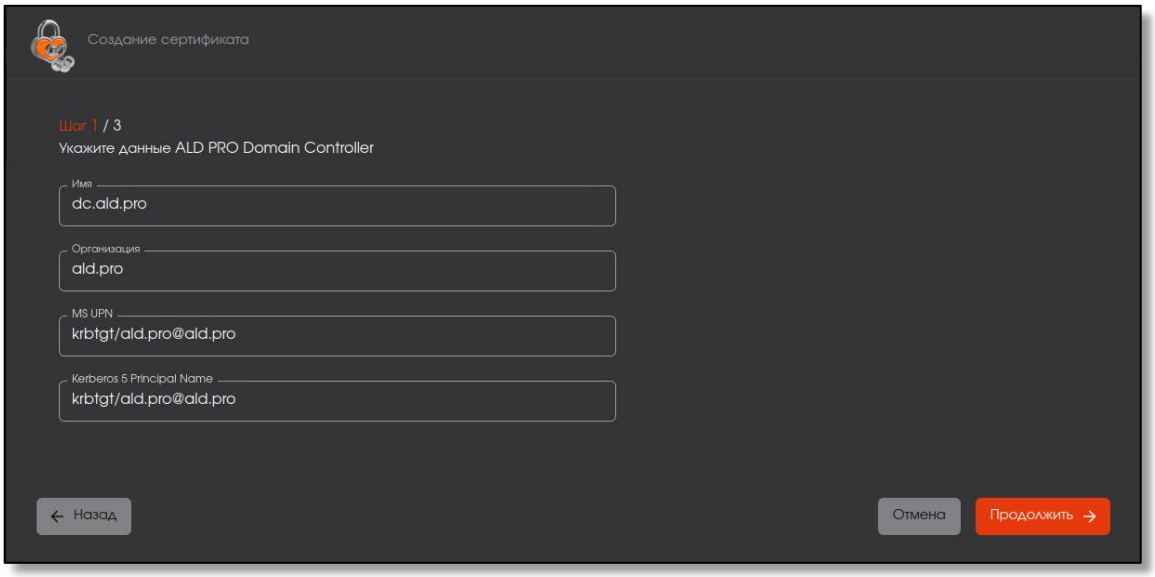


Рисунок 47 – Окно создания сертификата. Ввод данных контроллера домена ALD PRO

- На следующем шаге создайте пароль для защиты ключевого контейнера PKCS#12 и нажмите ставшую активной кнопку «Продолжить» (см. Рисунок 48).

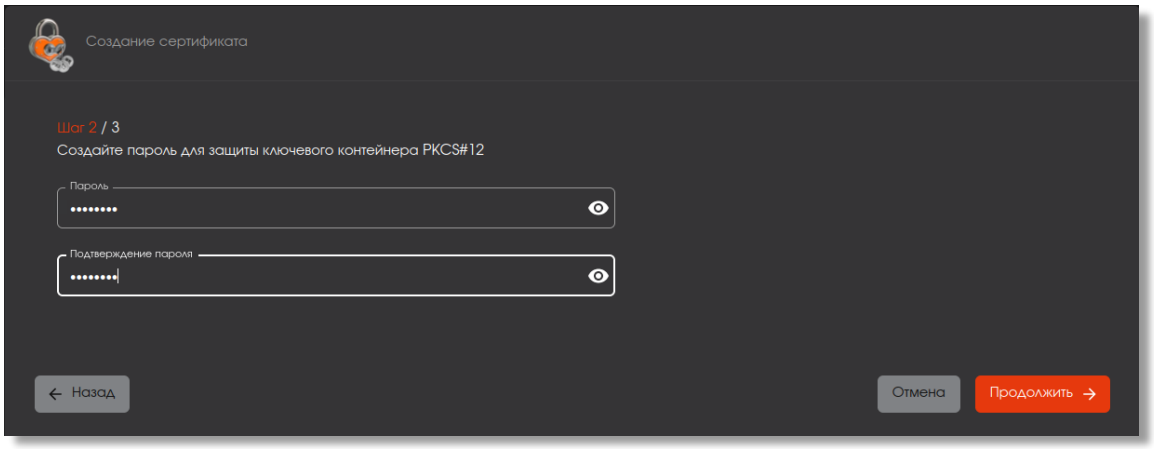


Рисунок 48 – Окно создания сертификата. Установка пароля контейнера PKCS#12

- Далее в открывшемся окне выберите параметры криптографии и нажмите ставшую активной кнопку «Создать сертификат» (см. Рисунок 49).

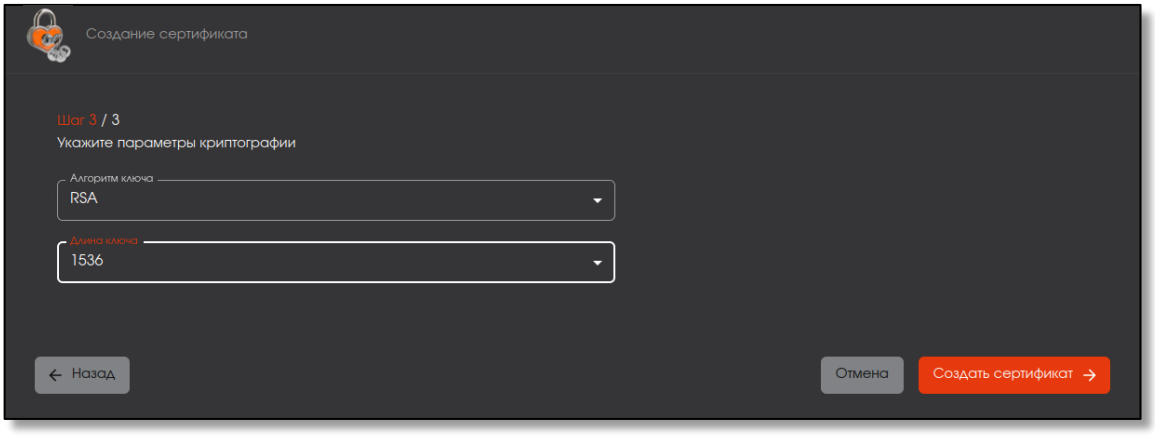


Рисунок 49 – Окно создания сертификата. Выбор параметров криптографии сертификата

- После создания сертификата в открывшемся окне необходимо скачать сертификат контроллера домена ALD PRO по кнопке «Скачать» (см. Рисунок 50).

> **Внимание! Сертификат и закрытый ключ в контейнере pkcs#12 возможно скачать только в последнем окне выпуска сертификата «об успешном создании сертификата» по нажатию на кнопку <Скачать>. Далее, после закрытия окна, скачивание выпущенного сертификата для субъекта в разделе «Сертификаты» доступно только в формате .pem!**

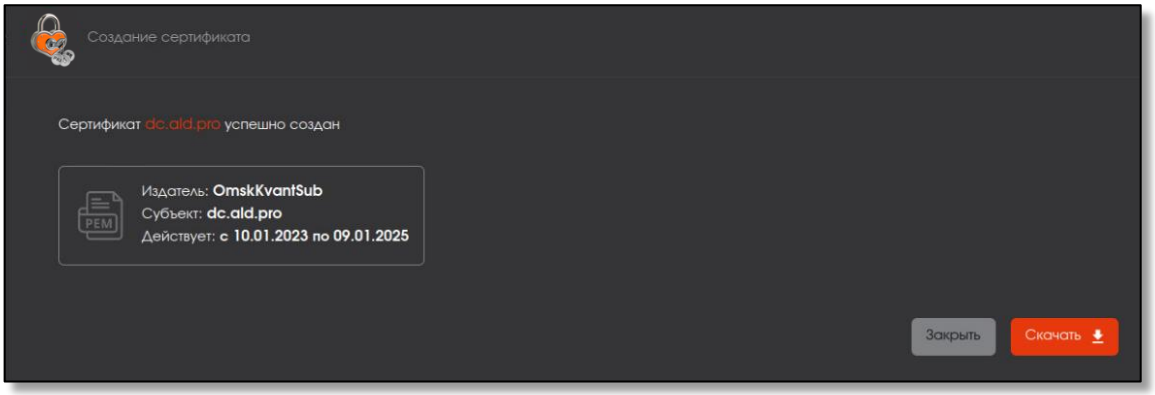


Рисунок 50 – Окно создания сертификата. Успешное создание сертификата контроллера домена ALD PRO

4.4.6.3 Выпуск сертификата субъекта по запросу

- Предварительные условия выполнения сценария:

- файл-запрос для субъекта должен быть подготовлен заранее на стороннем ЦС (например, при помощи ПО «Единый клиент JaCarta»);
- расширение файл-запроса не имеет существенного значения, но предполагается, что оно будет `***.csr` или `***.pem`;
- файл-запрос должен быть сформирован с учетом известных данных выбранного шаблона компонента «Центр сертификации Aladdin Enterprise Certification Authority». Например, для использования шаблона «Domain Controller» в запросе должны быть указаны параметры DNS Name и MS GUID;
- по файлу-запроса ранее не был выпущен сертификат.

- В открывшемся окне (см. Рисунок 51) необходимо выбрать и загрузить файл-запрос, а также выбрать шаблон сертификата в соответствии с запросом (предполагается, что администратор заранее знает для какого субъекта загружается файл-запрос и какой шаблон необходимо выбрать).

- Чек-бокс «Публиковать сертификат в ресурсную систему» активирован по умолчанию для публикации сертификата во внешнюю ресурсную систему. Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат.

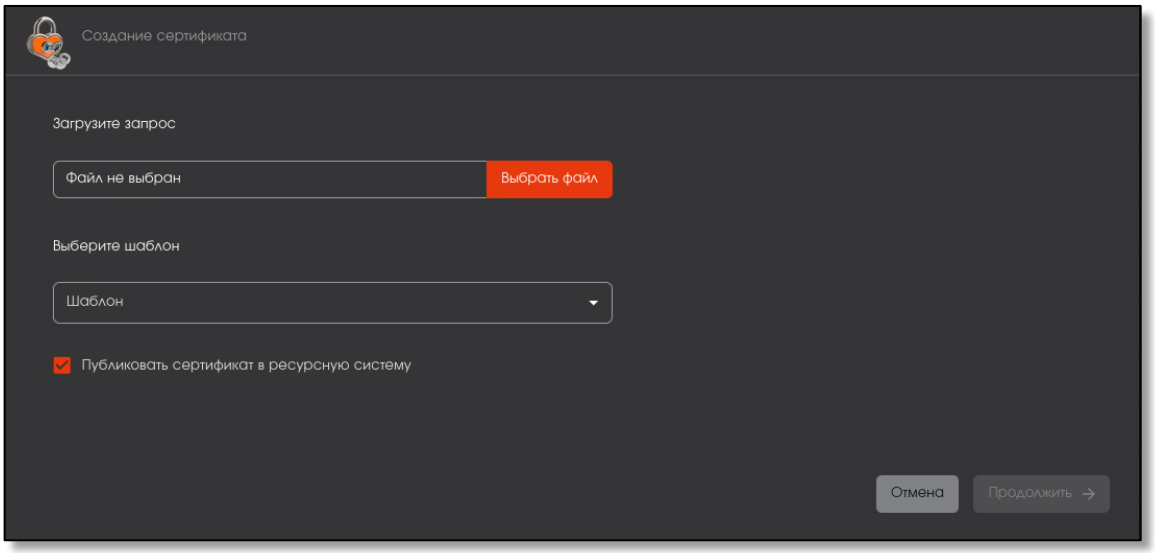


Рисунок 51 – Окно создания сертификата. Загрузка запроса и выбор шаблона

- При необходимости, возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке <Изменить>.

- После загрузки файла запроса и выбора шаблона нажать активировавшуюся кнопку <Продолжить>.

- Программа проверяет запрос на наличие субъекта:
  - при соответствии данных запроса и выбранного шаблона открывается окно с данными шаблона и принятыми данными из файла запроса (см. Рисунок 52).
  - если субъект не обнаружен – создается новый субъект, для которого выдается сертификат.

- Программа проверяет запрос на соответствие полей запроса на сертификат и выбранного шаблона в соответствии с Таблица 3.

Таблица 3 – Проверка соответствия полей запроса шаблону выпускаемого сертификата

Поле в шаблоне	Поле в запросе	Поле в сертификате	Поле профиля субъекта программы
проверка поля Subject DN			
Есть, обязательное	Есть	Из запроса	-
Есть, обязательное	Нет	Ошибка №1	-

Поле в шаблоне	Поле в запросе	Поле в сертификате	Поле профиля субъекта программы
Есть, необязательное	Есть	Из запроса	-
Есть, необязательное	Нет	Прочерк	-
Нет	Есть	Ошибка №3	-
Нет	Нет	Строка отсутствует	-
проверка пол Subject Alt Name			
Есть, обязательное	Есть	Из запроса	Нет
Есть, обязательное	Нет	Ошибка №1	Нет
Есть, обязательное	Есть	Из запроса	Есть
Есть, обязательное	Нет	Ошибка №1	Есть
Есть, необязательное	Есть	Из запроса	Нет
Есть, необязательное	Нет	Отсутствует	Нет
Есть, необязательное	Есть	Из запроса	Есть
Есть, необязательное	Нет	Из субъекта	Есть
Нет	Есть	Ошибка №3	Нет
Нет	Нет	Строка отсутствует	Нет
Нет	Есть	Ошибка №2	Есть
Нет	Нет	?	Есть

Примечание:
Ошибка №1: «Не задано обязательное поле»
Ошибка №2: «Поле не соответствует формату, указанному в шаблоне»

- На следующем шаге в окне создания сертификата по запросу для существующего или нового субъекта обозначены (см. Рисунок 52):
  - обязательные к заполнению поля шаблона, отмеченные знаком ✓✓ и необязательные поля шаблон, отмеченные знаком ✓;
  - значения запроса, соответствующие полям выбранного шаблона сертификата;
  - финальное представление данных, попадающих в сертификат.

ВНИМАНИЕ! Окно с данными шаблона на Рисунок 52 приведено в ознакомительных целях, количество и наименование полей зависят от выбранного шаблона.

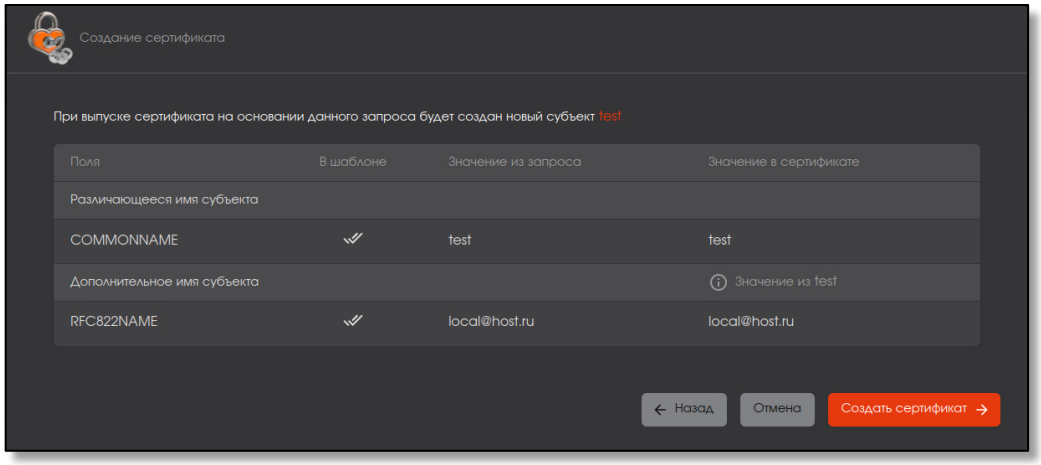


Рисунок 52 – Окно создания сертификата на основании запроса для нового субъекта

ВНИМАНИЕ! ! Поле «общее имя» (CN) всегда идет на первом месте.

- Отображение данных в окне создания сертификата для существующего и нового субъектов разделены на две основные части:
  - различающееся имя субъекта (Subject DN)
  - дополнительное имя субъекта (Subject AltName).

В случае, если в файле-запросе существуют дополнительные поля субъектных идентификаторов, отсутствующие в текущей реализации (для справки - http://oidref.com/2.5.4, таблица children), то они идентифицируются по параметру OID.

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 53).

Внимание! Сертификат и закрытый ключ в контейнере pkcs#12 возможно скачать только в последнем окне выпуска сертификата «об успешном создании сертификата» по нажатию на кнопку <Скачать>. Далее, после закрытия окна, скачивание выпущенного сертификата для субъекта в разделе «Сертификаты» доступно только в формате .pem!

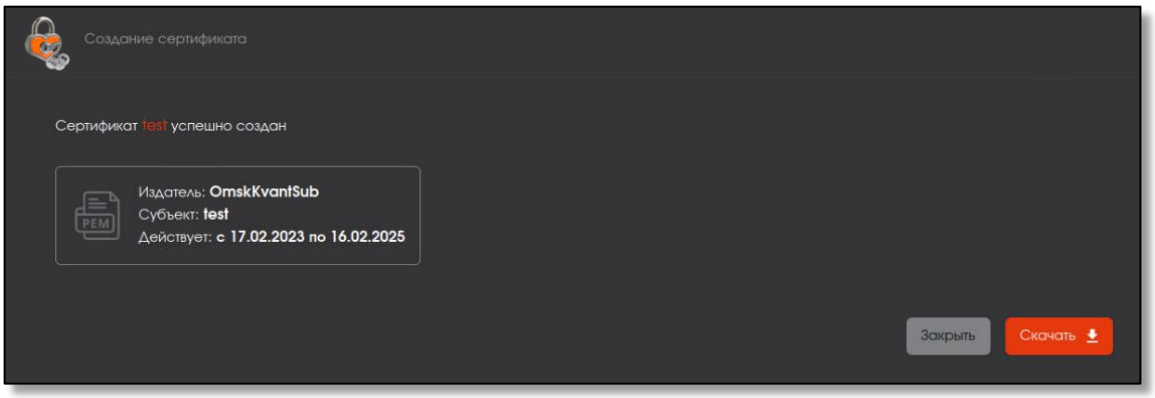


Рисунок 53 – Окно успешного создания сертификата субъекта на основании запроса

4.4.6.4 Выпуск сертификата субъекта на ключевом носителе

Предварительные условия выполнения сценария:

- Убедитесь, что поддерживаемый электронный ключ присоединен к АРМ выпускающего Центра сертификации;

- Убедитесь, что на сервере выпускающего Центра сертификации установлено ПО JC-WebClient версии 4.3.2 или 4.3.3 для дальнейшей работы с ключевыми носителями из браузера.

- Нажатие кнопки <Создать (Выпустить) сертификат> - «на ключевом носителе» стартует сценарий по созданию сертификата на ключевом носителе.

- В случае если электронный ключ успешно подключен, в открывшемся окне (см. Рисунок 54) необходимо выбрать ключевой носитель из выпадающего списка в поле «Устройство», ввести его пин-код и указать шаблон для выпуска сертификата. Переход на следующий шаг осуществляется в случае ввода корректного PIN-кода электронного ключа.

- Чек-бокс «Публиковать сертификат в ресурсную систему» доступен только при выпуске сертификата в разделе «Субъекты» для субъектов внешних ресурсных систем, и активирован по умолчанию для публикации сертификата во внешнюю ресурсную систему. Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной систе-

мы, для которого выпущен сертификат.

- После ввода всех данных кнопка «Продолжить» становится активной.

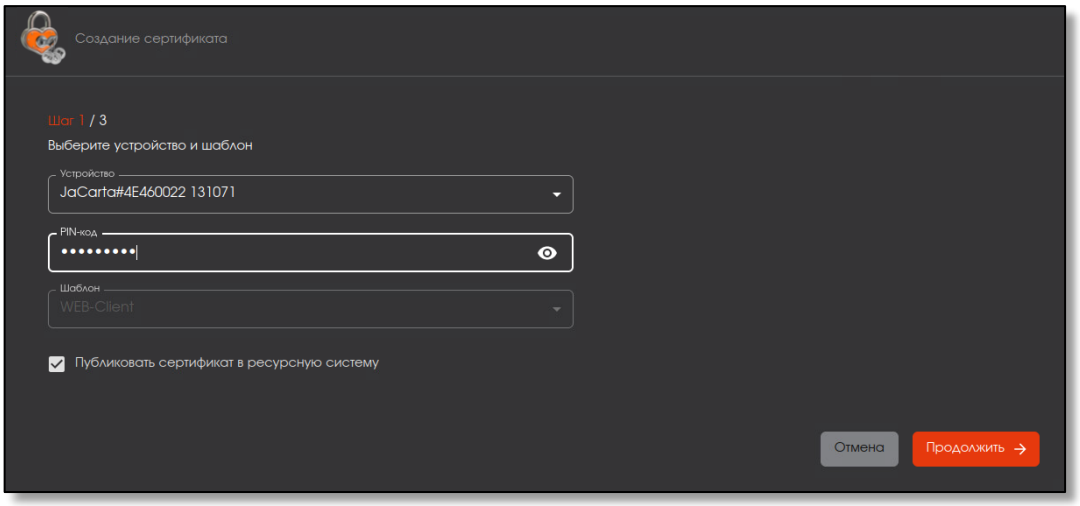


Рисунок 54 – Окно создания сертификата на электронном ключе. Шаг 1

- В зависимости от выбранного шаблона выпускаемого сертификата на предыдущем шаге заполняем поля на следующем шаге (см. Рисунок 55). Более подробное описание полей шаблона приведено в Приложение А. Описание полей шаблонов сертификатов.

- При выпуске сертификата для учётной записи субъекта внешней ресурсной системы шаблон «Web-client» будет определён по умолчанию. В открывшемся окне поле «Имя» заполнено данными Common Name пользователя учётной записи и не подлежит редактированию, поля «RFC 822» и «Name MS UPN» подлежат редактированию и автоматически заполнены, если сертификат выпускается для учетной записи доменного пользователя и в атрибутах доменного пользователя указан userPrincipalName, в случае, если данный атрибут не задан или сертификат выпускается для учетной записи пользователя локального ресурса, то данные поля будут пустыми.

- При выпуске сертификата для учётной записи или субъекта внешней ресурсной системы поля будут заполнены автоматически имеющимися данными для субъекта в ресурсной системе. Данные доступны для редактирования, кроме поля «Имя», заполненного в соответствии с данными Common Name субъекта ресурсной системы.

- Нажмите кнопку <Продолжить>, ставшую активной, после заполнения всех полей экранной формы создания сертификата на втором шаге.

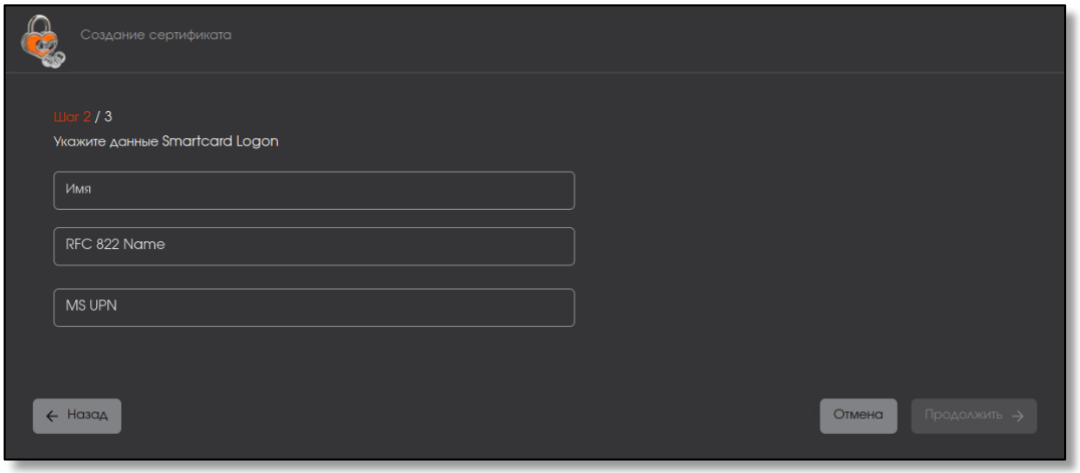


Рисунок 55 – Окно создания сертификата на электронном ключе. Шаг 2

- Далее необходимо выбрать параметры криптографии (см. Рисунок 56).
- После выбора алгоритма нажмите кнопку <Создать сертификат>.

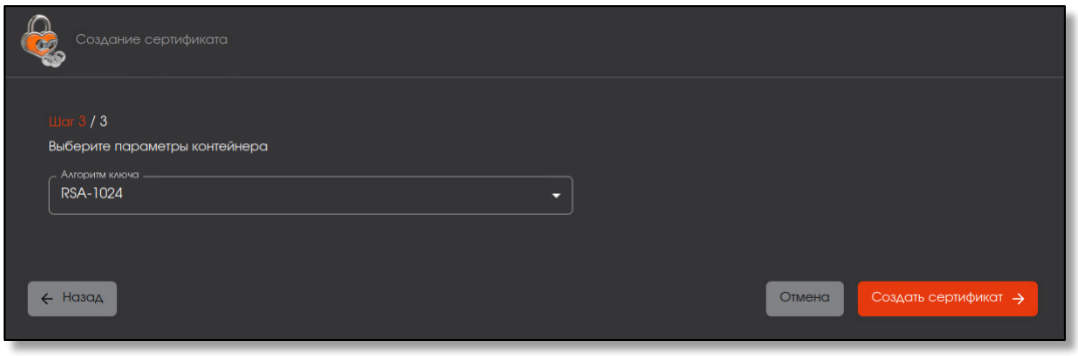


Рисунок 56 – Окно создания сертификата на электронном ключе. Шаг 3

- Далее осуществляются все необходимые операции для выпуска и записи сертификата на ключевой носитель:
  - генерация ключевой пары на основе данных заполненного шаблона сертификата на предыдущем шаге;
  - генерация запроса на основе данных заполненного шаблона сертификата на предыдущем шаге;
  - выпуск сертификата;
  - запись сертификата на ключевой носитель.
- Процессы выполняются автоматически и после завершения процессов станут доступны кнопки <Скачать сертификат> и <Скачать цепочку сертификатов> (см. Рисунок 57).

Внимание! Сертификат и закрытый ключ в контейнере pkcs#12 возможно скачать только в последнем окне выпуска сертификата «об успешном создании сертификата» по нажатию на кнопку <Скачать>. Далее, после закрытия окна, скачивание выпущенного сертификата для субъекта в разделе «Сертификаты» доступно только в формате .pem!

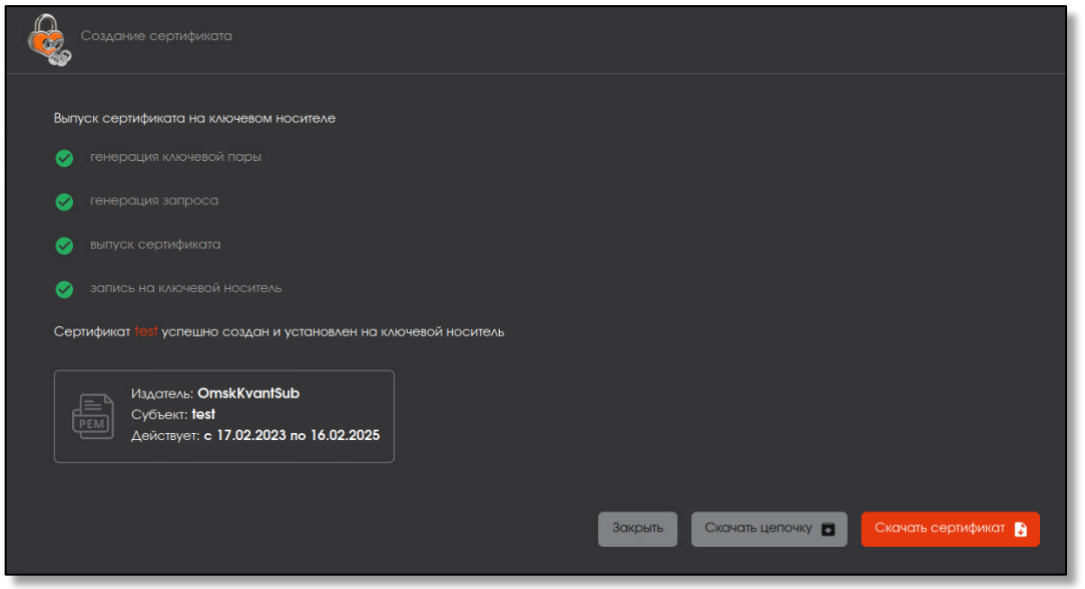


Рисунок 57 – Окно успешного создания сертификата субъекта на электронном ключе

4.5 Раздел «Ресурсная система»

Раздел «Ресурсная система» обеспечивает получение данных субъектов с целью упрощенного выпуска сертификатов субъектам служб каталогов Linux и Microsoft, а также централизованную публикацию выпущенных сертификатов в карточку субъекта службы каталогов.

Переход в раздел «Ресурсная система» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 14).

- На основном экране «Ресурсной системы» отображены информационные поля (см. Рисунок 58):
  - подключаемая ресурсная система – Samba DC, РЕД АДМ, MS AD, FreeIPA или ALD PRO;
  - отображаемое имя – показывает отображаемое имя ресурса;
  - логин – отображается полный параметр учетной записи Администратора домена, имеющего права доступа к домену;
  - последнее обновление – отображается дата и время последней синхронизации базы субъектов источника с базой данных программного компонента;
  - статус – отображается статус подключения к источнику;
  - субъекты – показывает количество загруженных субъектов из источника.

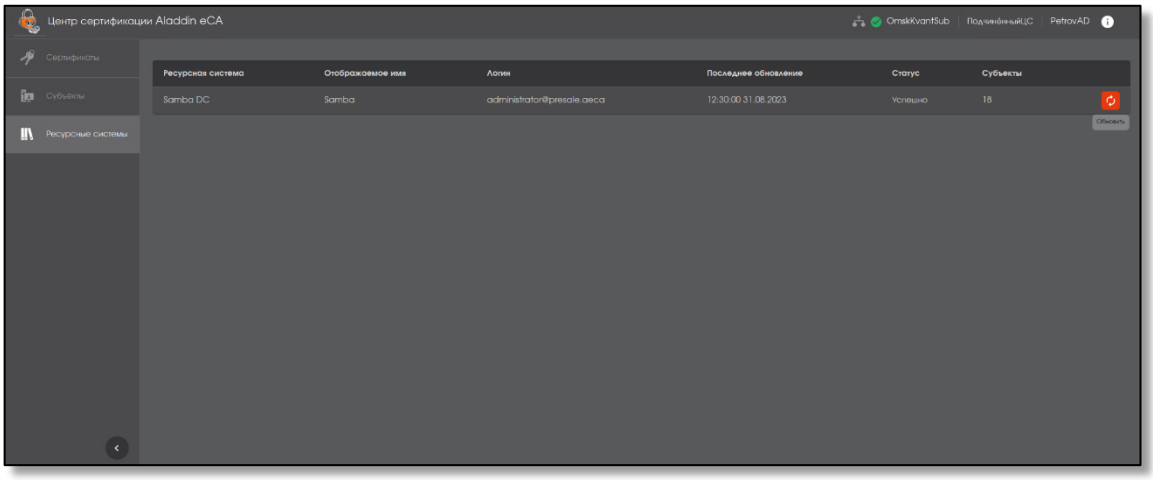


Рисунок 58 – Экран раздела «Ресурсная система»

- Центр сертификации Aladdin Enterprise Certificate Authority позволяет загрузить из нескольких ресурсных систем Samba DC, РЕД АДМ, MS AD, FreeIPA или ALD PRO:
  - список пользователей;
  - список компьютеров;
  - список организационных групп;
  - список групп безопасности.

- Работа с разделом «Ресурсные системы» предусматривает выполнение следующих сценариев использования:
  - обновление списка субъектов и их данных в ручном режиме.

4.5.1 Обновление ресурсной системы

- Автоматическая синхронизация списка субъектов из ресурсной системы осуществляется каждые 30 минут.

- Помимо автоматической синхронизации возможно ручное обновление списка субъектов ресурсной системы. Для ручного обновления подключенной ресурсной системы наведите курсор на созданный ресурс и нажмите появившуюся в строке кнопку  <Обновить>, расположенную в правой части строки с названием подключаемого ресурса (см. Рисунок 58) - осуществляется загрузка данных для каждого существующего субъекта из ресурсной системы:
  - список пользователей;
  - список ПК в домене;
  - список организационных групп;
  - список групп безопасности.

- В результате обновления ресурсной системы состав объектов будет синхронизирован:
  - переименованы существующие объекты;
  - изменены существующие связи (включения в группы и т.д.);
  - обновлён список субъектов (добавлены новые группы и объекты, удалены субъекты).

- Для каждого загруженного пользователя и компьютера будет создан субъект и подгружены все поля, относящиеся к SubjectDN и SubjectAltName. Преобразование содержимого записи LDAP в поля базы субъектов ресурсной системы происходит в соответствии с Таблица 4. Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.

Таблица 4 – Преобразование данных субъектов ресурсной системы

Поле в базе субъектов ресурсной системы	**Поле в базах Samba DC MS AD**	**Поле в базах ALD PRO FreeIPA**
name	name	serverHostName/CN
MS_GUID	objectGUID	ipaUniquelD
MS UPN	userPrincipalName	krbPrincipalName
CommonName	CN	CN
RFC822Name	name или dNSHostName	CN или ServerHostName
CountryCode	C или CountryCode (в формате DCC)	-
objectGuid	objectGUID	ipaUniqueID
Organization	Organization	Organization
Department	Department	Department

5 СООБЩЕНИЯ ОПЕРАТОРУ

Сообщения оператору представляют собой текст сообщения в модальном окне под полем ввода пароля или пин-кода, которое появляется по центру текущего окна входа в систему и сообщает об ошибке или обязательном действии, которое не выполнено. Список всех возможных сообщения для оператора приведён в Таблица 5.

Таблица 5 – Оповещения программы

№ п/п	Сообщение об ошибке/ уведомление	Описание	Действие оператора
1	Не задано обязательное поле	Сообщение об ошибке при выпуске сертификата по запросу. В загружаемом запросе отсутствует поле, которое является обязательным в выбранном шаблоне	Вернуться на предыдущий шаг и сменить шаблон на подходящий или Пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>
2	Поле не соответствует формату, указанному в шаблоне	Сообщение об ошибке при выпуске сертификата по запросу. Загружаемый запрос содержит поле, которое отсутствует в выбранном шаблоне	
3	Для работы с ключевым носителем должно быть установлено ПО JC-WebClient. Установите необходимое ПО и перезапустите мастер выпуска сертификатов	Сообщение об ошибке при выпуске сертификата на ключевом носителе ПО JC-WebClient предварительно не установлено	Для выпуска сертификата на электронном ключе установить ПО JC-WebClient версии 4.3.2 или 4.3.3
4	Нет доступных устройств. Подключите устройство и перезапустите мастер создания сертификата	Сообщение об ошибке при выпуске сертификата на ключевом носителе Электронный носитель не подключен	Для выпуска сертификата на электронном ключе подсоедините ключевой носитель к USB-порту и запустите мастер создания сертификатов
5	Алгоритм не поддерживается выбранной моделью ключевого носителя	Сообщение об ошибке при выпуске сертификата на ключевом носителе Выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя	Для выпуска сертификата на электронном ключе выберите поддерживаемый ключевой носитель, присоедините ключевой носитель к USB-порту и запустите мастер создания сертификатов
6	Синхронизация запущена	Уведомление о успешном запуске обновления ресурсной системы	___
7	Ресурс с указанным идентификатором не найден	Ошибка при запуске обновления ресурсной системы	Выбрать актуальную ресурсную систему

№ п/п	Сообщение об ошибке/ уведомление	Описание	Действие оператора
8	Не удалось найти объект сущности по идентификатору: ${id}	Сообщение об ошибке при выпуске сертификата	Выбрать актуальный и активный субъект
9	[Ошибка публикации] Невозможно опубликовать сертификат в ресурсную систему. Связь между сертификатом и субъектом не обнаружена.	Сообщение об ошибке при выпуске сертификата. Сертификат невозможно опубликовать в ресурсную систему	Обратиться к администратору домена
10	Не должны присутствовать одновременно параметры SubjectId и UserId.	Сообщение об ошибке при выпуске сертификата. Ошибка присутствия одновременно параметров субъекта и юзера	Выбрать только одни параметры
11	Ошибка получения шаблона	Сообщение об ошибке при выпуске сертификата. Ошибка при выборе шаблона	Выбрать актуальный и активный шаблон
12	Время действия активной лицензии истекло	Сообщение об ошибке при приостановке, отзыве и активации сертификата.	Использовать актуальную лицензию
Примечание: в случае возникновения ошибок, связанных с работой JC-WebClient, администратор будет уведомлён сообщением, согласно описанию ошибки в документации JC-WebClient SDK: https://developer.aladdin-rd.ru/archive/jc-webclient/4.0.0/api/addendum/errors.html https://developer.aladdin-rd.ru/archive/jc-webclient/3.1.1/api/addendum.html			

ПРИЛОЖЕНИЕ А. ОПИСАНИЕ ПОЛЕЙ ШАБЛОНОВ СЕРТИФИКАТОВ

Наименование поля Aladdin eCA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
Domain controller – шаблон сертификата контроллера домена				
имя	CommonName	имя контроллера домена	DC01	A-Я, a-я, A-Z, a-z, 0-9, ., _, -, пробел
доменное имя	DC	домен	example.com	A-Я, a-я, A-Z, a-z, 0-9, ., -

MS GUID	objectGUID / ipaUniqueID	глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена
		
		Для получения значения идентификатора в среде РЕД ОС 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.
			92625ee510e248479554779d1f43f751 (32 знака)	ввод символов в рамках шестнадцатеричной системы счисления;
				длина строго 32 знака; A-Z, a-z, 0-9

пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	A-Z, a-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	2048, 3072, 4096, 256, 384, 521	-

Наименование поля Aladdin eCA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
ALD PRO Domain controller – шаблон сертификата контроллера домена ALD PRO				
имя	CommonName	имя контроллера домена ALD PRO	dc.ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
организация	-	полное имя домена	ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
MS UPN	objectGUID / ipaUniqueID	данные в формате «krbtgt/полное имя домена@полное имя домена»	krbtgt/ald.pro@ald.pro	Строка вида “text@text” А-Я, а-я, A-Z, a-z, 0-9, ., @, /, _, -
Kerberos KPN	-	в формате «krbtgt/полное имя домена@полное имя домена»	krbtgt/ald.pro@ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., @, /, _, -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	A-Z, a-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	1024, 1536, 2048, 3072, 4096, 6144, 8192	-
Smartcard Logon ALD PRO – шаблон сертификата пользователя ALD PRO				
имя	CommonName	имя пользователя ALD PRO		А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
организация	-	полное имя домена	ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@example.com	А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
MS UPN	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
Smartcard Logon – шаблон сертификата пользователя				
имя	CommonName	имя пользователя	IvanovaAN	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
организация	-	полное имя домена	ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел

Наименование поля Aladdin eCA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@ald.pro	Строка вида “text@text” А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
MS UPN	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@ald.pro	Строка вида “text@text” А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	2048, 3072, 4096	-
Web-client – шаблон сертификата учетной записи				
имя	CommonName	имя веб-клиента	Operator01	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@example.com	Строка вида “text@text” и только указанные символы: А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
MS UPN	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	Строка вида “text@text” А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	1024,1536,2048,3072,4096,6144, 8192	-
Web-server – шаблон сертификата веб-сервера				

Наименование поля Aladdin eCA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
общее имя	CommonName	имя веб-сервера	Center01	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
доменное имя	DC	полное доменное имя сервера, где развёрнут Центр сертификации	example.com	А-Я, а-я, A-Z, a-z, 0-9, ., -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	1024,1536,2048,3072,4096,6144, 8192	-
S/MIME – шаблон сертификата электронной почты				
имя	CommonName	имя пользователя	ivanova	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@example.com	Строка вида “text@text А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	192,224,256,384,521,1024, 1536,2048,3072,4096,6144,8192	-

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности (администратор) – сотрудник (специалист), ответственный за приёмку и ввод в эксплуатацию изделия, а также роль в центре сертификации, которой доступны функции локального администрирования. Физическое лицо (уполномоченный пользователь), имеющее роль «Администратора», должно быть указано в организационно-распорядительных документах организации, эксплуатирующей ПО.

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.

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

Оператор – сотрудник (специалист) или система (приложение, сервис) и соответствующая роль в центре сертификации, отвечающая за управление жизненным циклом сертификатов субъектов.

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.

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

Токен доступа – это уникальная последовательность символов (букв, цифр и символов), основанная на формате JSON. Токен доступа используется для передачи данных для аутентификации в клиент-серверных приложениях. Токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в дальнейшем использует данный токен для подтверждения своей личности.

Токен обновления – это уникальная последовательность символов (букв, цифр и символов), основанная на формате JSON. Токен обновления выдается сервером в результате успешной аутентификации и используется для получения нового токена доступа и обновления токена обновления.

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 компонент «Центр сертификации» является частью Центра сертификатов Aladdin Enterprise Certificate Authority Certified Edition.

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
СВТ	–	Средство вычислительной техники
СУБД	–	Система управления базами данных
УЦ	–	Удостоверяющий центр
ЦС	–	Центр сертификатов
Aladdin eCA CE	–	Центр сертификатов Aladdin Enterprise Certificate Authority Certified Edition
CRL	–	Certificate Revocation List
AIA	–	Authority Information Access
URL	–	Uniform Resource Locator

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					