



Центр сертификатов доступа
Aladdin Enterprise Certificate Authority
Certified Edition

Руководство пользователя

Изделие RU.АЛДЕ.03.01.020-01

Документ 34

Версия 2.0.1.406

Автор Липатова Ю.А.

Листов 55

Дата 14.05.2024

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 приказом 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 документам – программный компонент, Центр сертификации Aladdin Enterprise Certificate Authority, Центр сертификации Aladdin eCA

Содержание

Аннотация.....	2
1 Назначение программы	5
1.1 Область применения.....	5
1.2 Краткое описание возможностей.....	5
1.3 Уровень подготовки пользователя.....	5
2 Условия выполнения программы.....	6
2.1 Поддерживаемые браузеры.....	6
2.2 Поддерживаемые ключевые носители.....	6
2.3 Режим функционирования программы.....	6
2.4 Доступ к программе	6
2.5 Принципы безопасной работы программного средства.....	6
3 Выполнение программы.....	7
3.1 Запуск программы.....	7
3.2 Доступ пользователей к программе	7
3.2.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск.....	7
3.2.2 Аутентификация с использованием сертификата на ключевом носителе.....	11
4 Описание функций программы.....	14
4.1 Описание верхней панели «Центра сертификации»	14
4.2 Описание боковой панели «Центра сертификации».....	15
4.3 Раздел «Сертификаты».....	16
4.3.1 Поиск сертификатов.....	17
4.3.2 Сортировка сертификатов	17
4.3.3 Фильтрация сертификатов.....	18
4.3.4 Скачивание сертификатов	18
4.3.5 Статус сертификатов	19
4.3.6 Карточка сертификата	20
4.3.7 Экспорт списка выпущенных сертификатов	22
4.3.8 Массовые операции с сертификатами.....	24
4.4 Раздел «Субъекты».....	25
4.4.1 Просмотр субъектов ресурсных систем	26
4.4.2 Поиск субъектов.....	27
4.4.3 Фильтрация субъектов.....	27
4.4.4 Сортировка субъектов	27
4.4.5 Карточка субъекта.....	28
4.4.6 Субъекты локальной ресурсной системы	33

4.4.7	Субъекты внешнего ресурса	33
4.4.8	Создание сертификата для субъекта ресурсной системы.....	34
4.5	Раздел «Ресурсная система».....	43
4.5.1	Обновление ресурсной системы	44
5	Сообщения оператору	46
	Приложение 1. Описание полей шаблонов сертификатов	48
	Термины и определения	53
	Обозначения и сокращения	54
	Лист регистрации изменений.....	55

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 выполнения 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 выпуска 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 сертификата 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>.

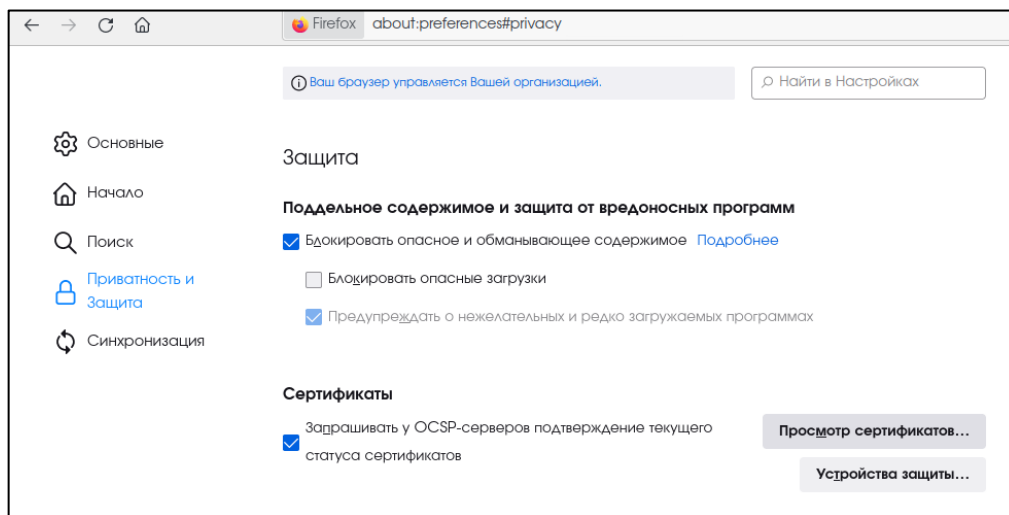


Рисунок 1 – Окно настроек браузера

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

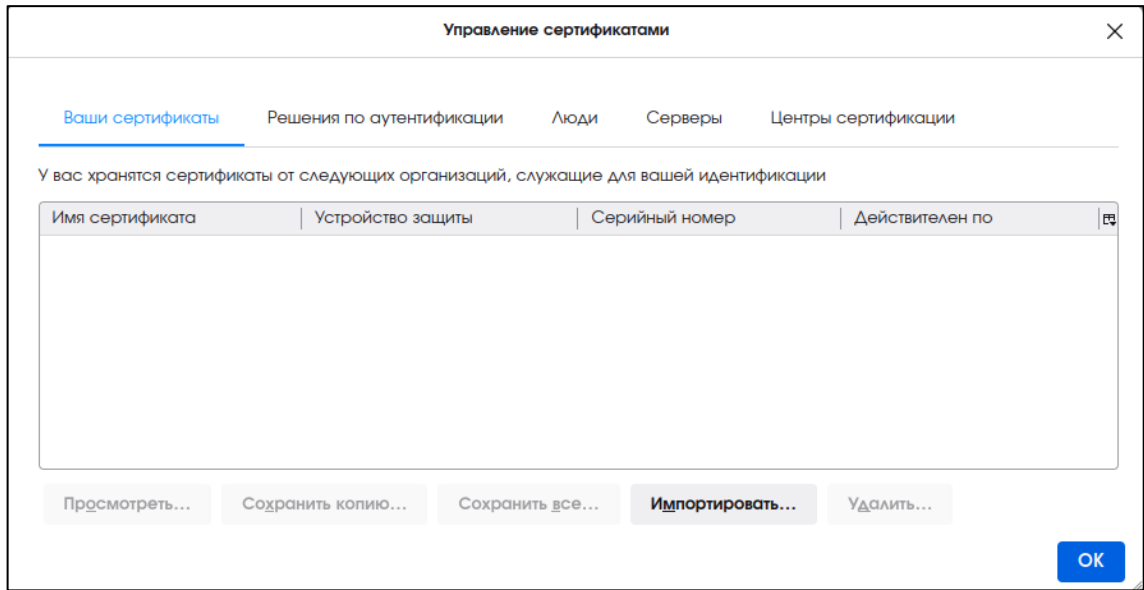


Рисунок 2 – Окно управления сертификатами

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

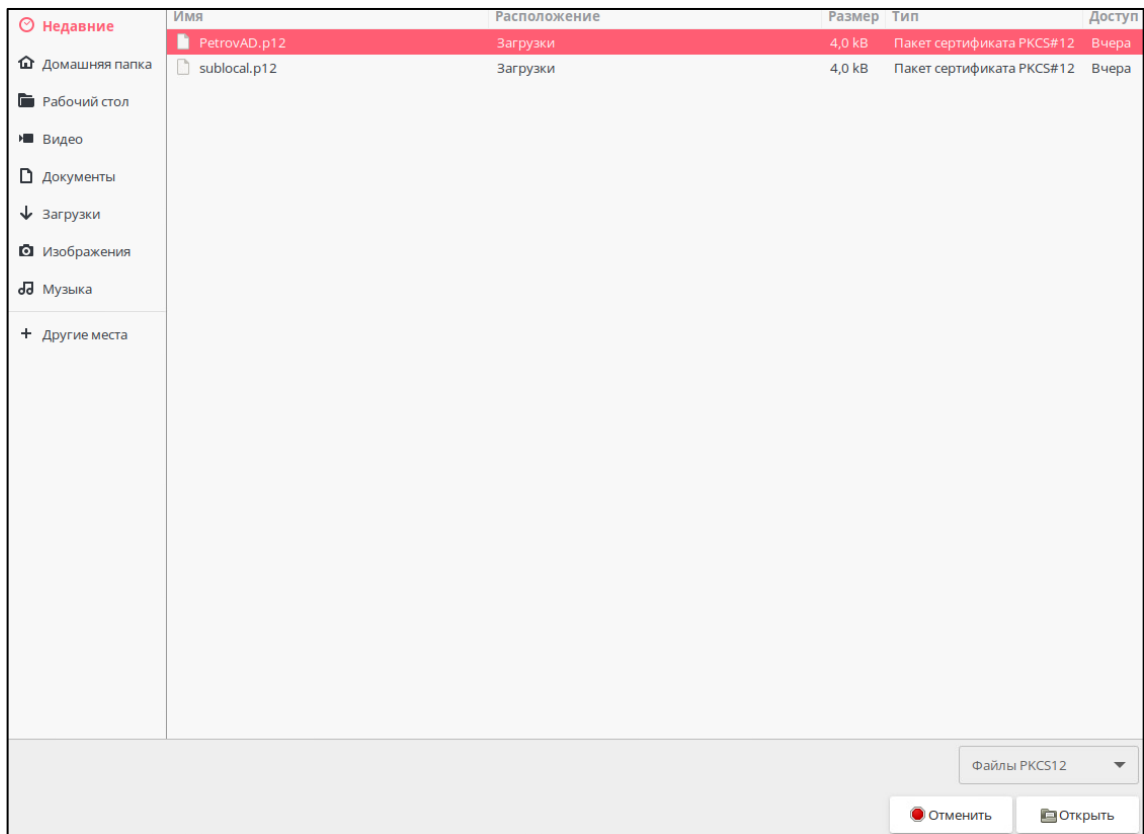


Рисунок 3 – Окно выбора импортируемого файла сертификата

- 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.

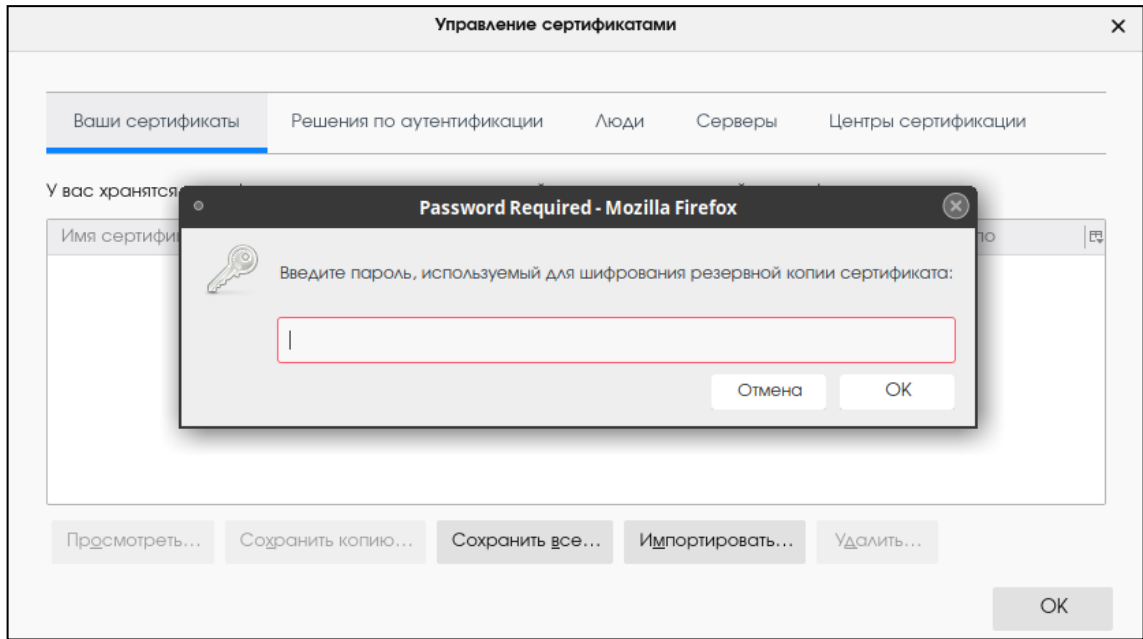


Рисунок 4 – Окно ввода пин-кода сертификата

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

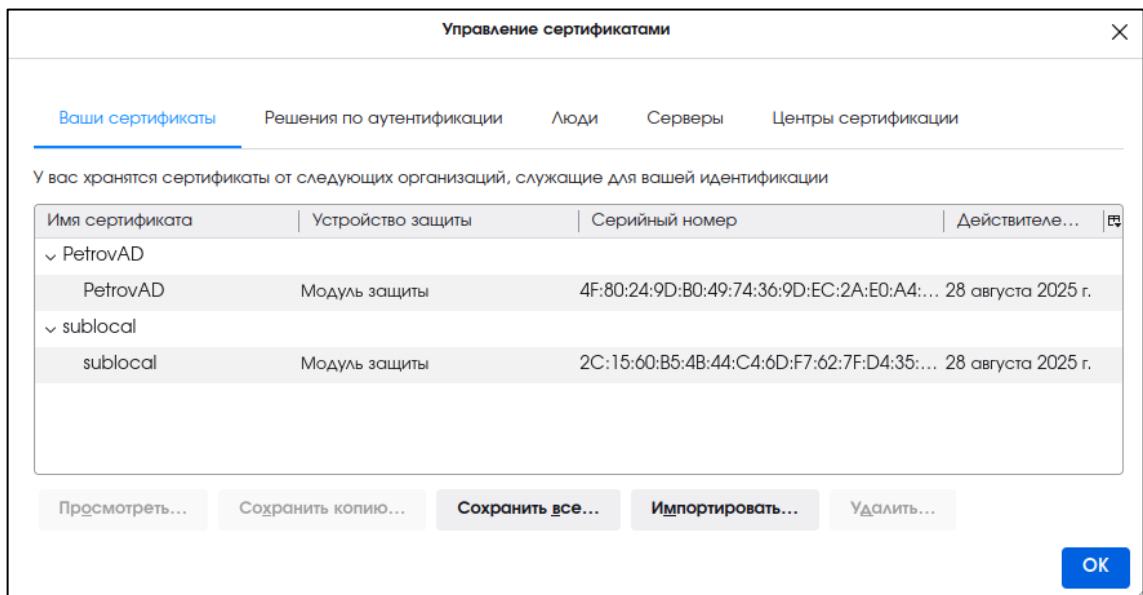


Рисунок 5 – Окно «Управление сертификатами»

- 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://sub02.presale.aeca
```

Для безопасного доверенного соединения при обращении к серверу Центра сертификации используйте доменное имя, указанное в атрибуте сертификата web-сервера Subject alternative name (SAN) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера.

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

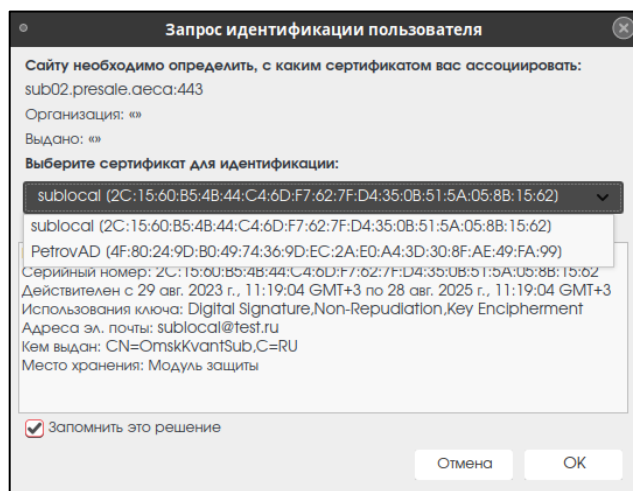


Рисунок 6 – Окно выбора сертификата для аутентификации

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

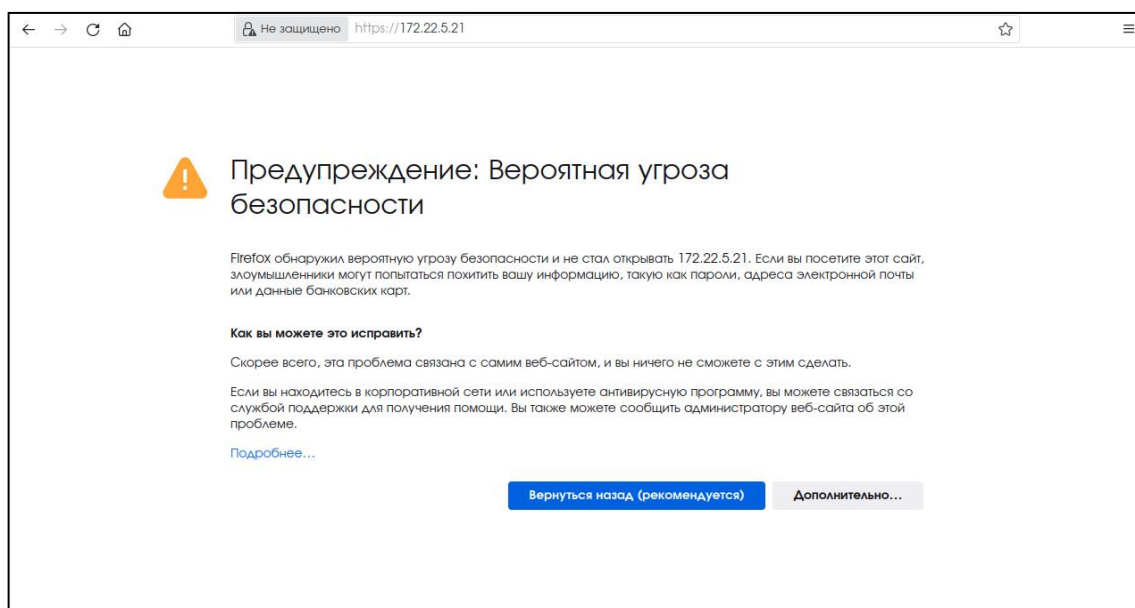


Рисунок 7 – Страница с предупреждением системы безопасности

- 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.

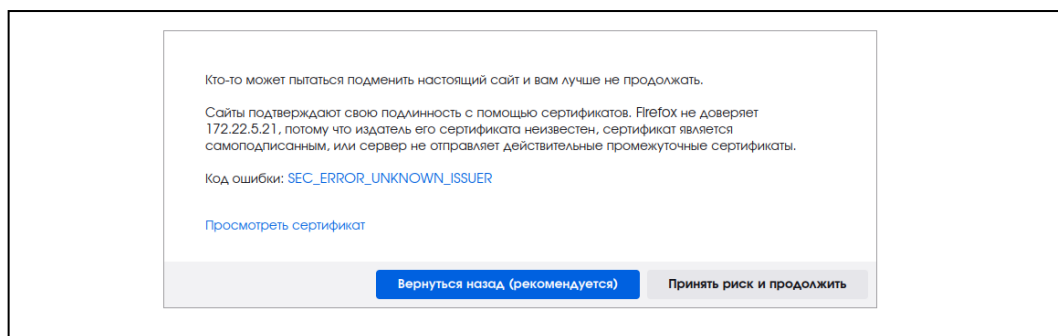


Рисунок 8 – Страница ошибки распознавания сертификата

- 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.

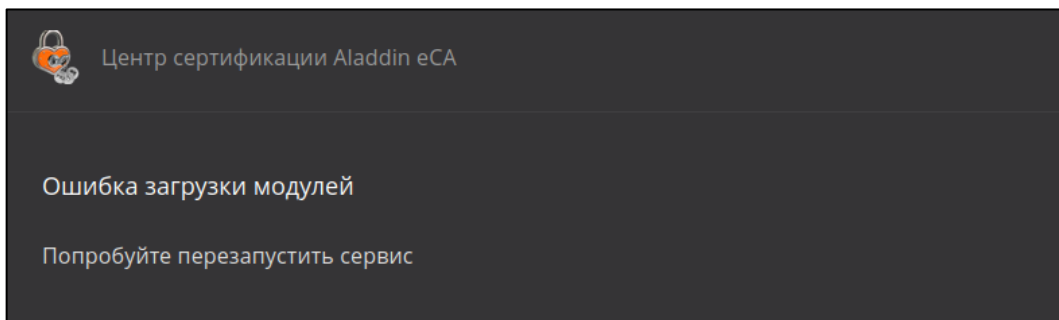


Рисунок 9 – Окно «Управление сертификатами»

- 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 перейдите 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>;

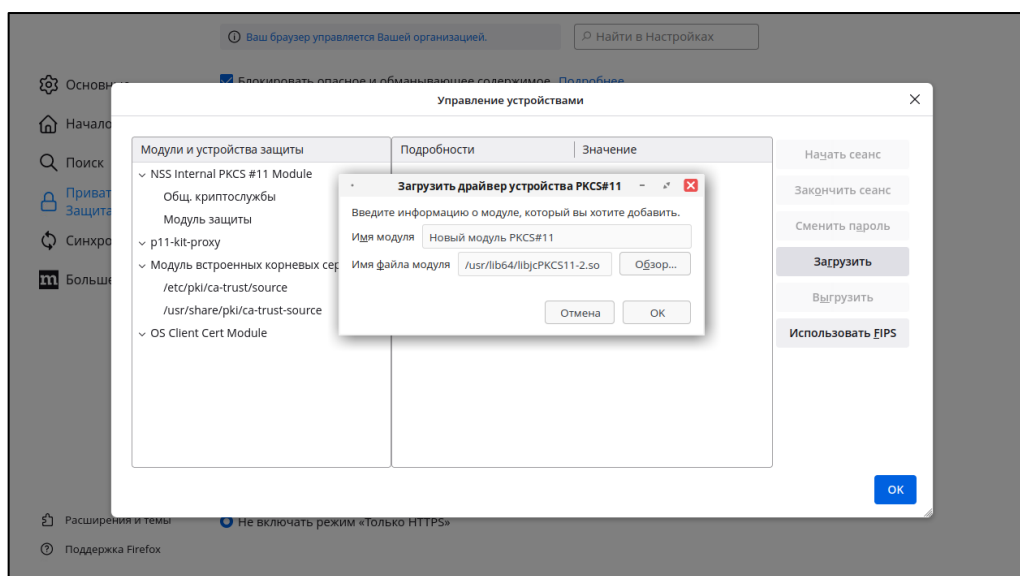


Рисунок 10 – Настройка браузера Firefox

- 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/libjсPKCS11-2.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://sub02.presale.aeca
```

- В появившемся окне введите PIN-код ключевого носителя.

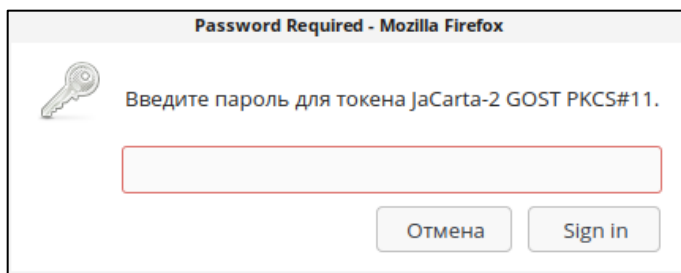


Рисунок 11 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

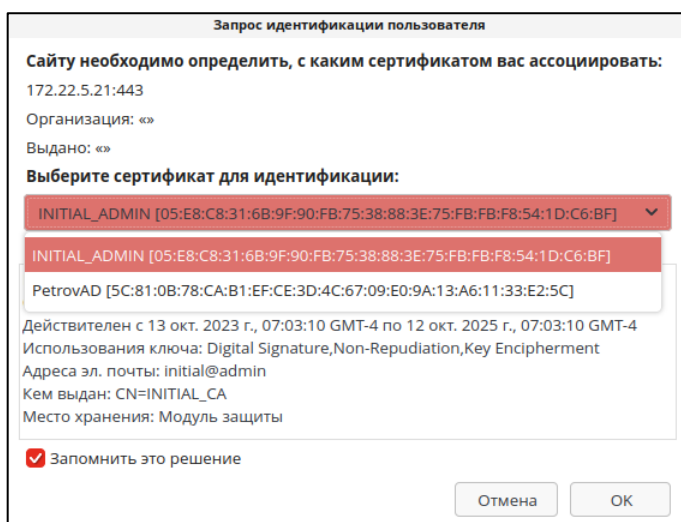


Рисунок 12 – Окно выбора сертификата пользователя для аутентификации на сервере

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»

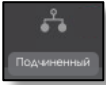


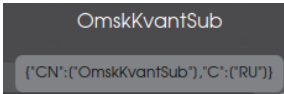
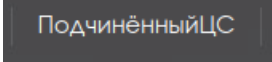

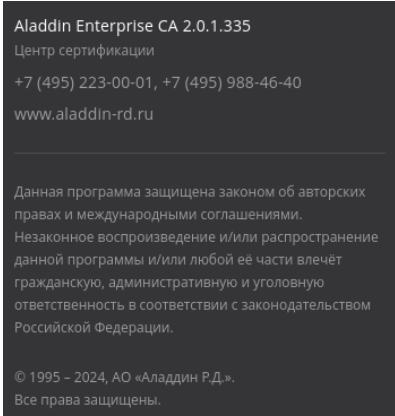
Верхняя панель (см. Рисунок 13) Центра сертификации фиксирована и отображается на любом шаге или переходе между вкладками.



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.

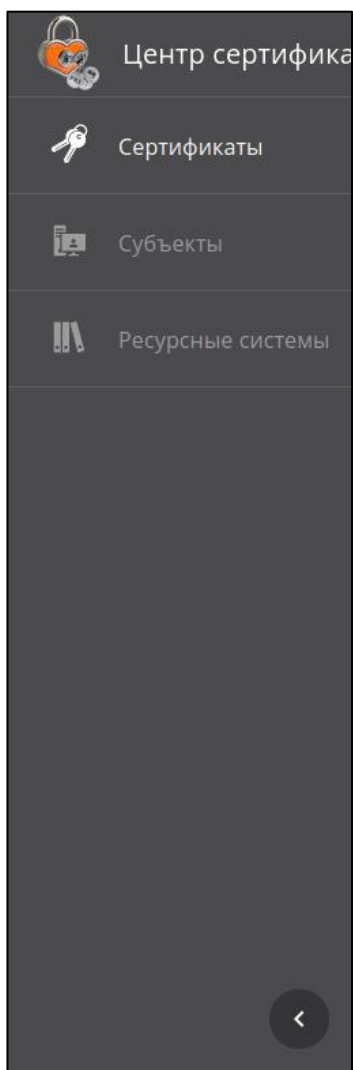


Рисунок 14 – Полный вид боковой панели



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.

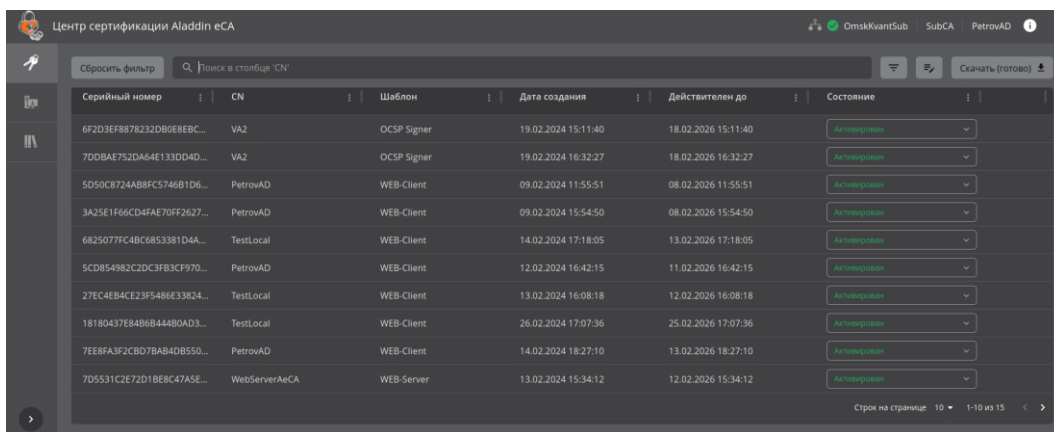
Далее в настоящем документе приводится полное описание доступных функций управления Центром сертификации для каждой вкладки.

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).



Серийный номер	CN	Шаблон	Дата создания	Действителен до	Состояние
6F2D3EF878232D80E8EBC...	VA2	OCSF Signer	19.02.2024 15:11:40	18.02.2026 15:11:40	Активирован
7DDBAE752DA64E133DD4D...	VA2	OCSF Signer	19.02.2024 16:32:27	18.02.2026 16:32:27	Активирован
5D50C8724AB8FC5746B1D6...	PetrovAD	WEB-Client	09.02.2024 11:55:51	08.02.2026 11:55:51	Активирован
3A25E1F66CD4FAE70FF2627...	PetrovAD	WEB-Client	09.02.2024 15:54:50	08.02.2026 15:54:50	Активирован
6825077FC4BC6853381D4A...	TestLocal	WEB-Client	14.02.2024 17:18:05	13.02.2026 17:18:05	Активирован
5CD854982C2DC3FB3CF970...	PetrovAD	WEB-Client	12.02.2024 16:42:15	11.02.2026 16:42:15	Активирован
27EC4EB4CE23P5486E33824...	TestLocal	WEB-Client	13.02.2024 16:08:18	12.02.2026 16:08:18	Активирован
18180437E84B684480AD3...	TestLocal	WEB-Client	26.02.2024 17:07:36	25.02.2026 17:07:36	Активирован
7EE8FA3FCBD78AB4DB550...	PetrovAD	WEB-Client	14.02.2024 18:27:10	13.02.2026 18:27:10	Активирован
7D5531C2E72D1B8EC47A5E...	WebServerAeCA	WEB-Server	13.02.2024 15:34:12	12.02.2026 15:34:12	Активирован

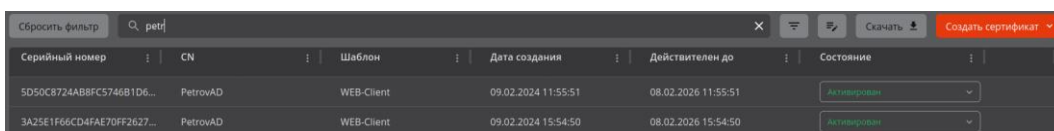
Рисунок 16 - Экран раздела меню «Сертификаты»

- 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 в формате .pem;
 - просмотр списка сертификатов с заданными критериями;
 - сброс всех применённых фильтров или выборочная отмена выбранного фильтра;
 - 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.




Серийный номер	CN	Шаблон	Дата создания	Действителен до	Состояние
5D50C8724AB8FC5746B1D6...	PetrovAD	WEB-Client	09.02.2024 11:55:51	08.02.2026 11:55:51	Активирован
3A25E1F66CD4FAE70FF2627...	PetrovAD	WEB-Client	09.02.2024 15:54:50	08.02.2026 15:54:50	Активирован

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.




Серийный номер	CN	Шаблон	Дата создания	Действителен до	Состояние
----------------	----	--------	---------------	-----------------	-----------

Рисунок 18 – Поля сортировки содержимого раздела «Сертификаты»

- Также отобразить в определённом порядке список сертификатов (отсортировать) в колонке возможно по нажатию кнопки  «Действия в колонке», выбрав и нажав в раскрывшемся меню «Сортировать...» (см. Рисунок 20).

4.3.3 Фильтрация сертификатов

4.3.3.1 Применение фильтров

• Для выборочного просмотра сертификатов на экране раздела «Сертификаты» возможно применение фильтров. Для отображения параметров фильтрации для всех колонок таблицы нажмите кнопку <Фильтр> , заголовки колонок экранной таблицы будут дополнены полями фильтра для каждой колонки (см. Рисунок 19):

- шаблон. Выберите шаблоны сертификатов для отображения списка сертификатов, которые были выпущены на основании выбранных шаблонов;
- дата создания. Выберите за какой период создания отобразить сертификаты на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
- действителен до. Выберите за какой период даты окончания действия отобразить сертификаты на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
- состояние. Выберите состояния сертификатов для отображения (активирован, приостановлен, отозван).

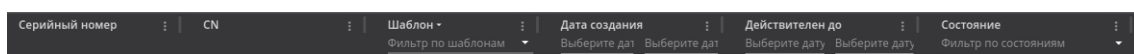



Рисунок 19 – Поля фильтра заголовков экранной таблицы


• Выберите одно или несколько значений фильтров, после выбора фильтр будет применён сразу автоматически.

• Повторное нажатие кнопки <Фильтр>  скроет поля выбора критериев фильтрации, но не отменяет применённые фильтры.

- Заголовки таблицы, для которых применён фильтр, будут отмечены знаком .

4.3.3.2 Сброс применённых фильтров

• Для очистки применённых фильтров для каждого заголовка колонки:

- нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 20);

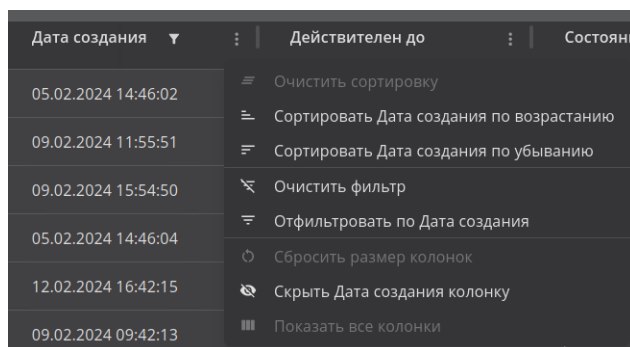
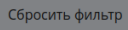



Рисунок 20 – Кнопка <Очистить> фильтр

• Для полной отмены всех применённых фильтров по всем колонкам воспользуйтесь кнопкой <Сбросить фильтр>  на экране раздела «Сертификаты».

4.3.4 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 21).

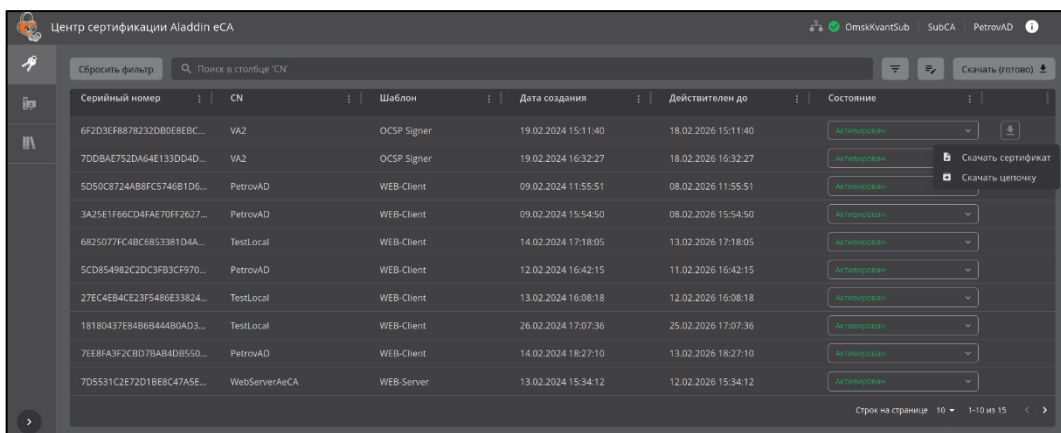


Рисунок 21 – Подменю «Скачать сертификат/цепочку»

4.3.5 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 22).

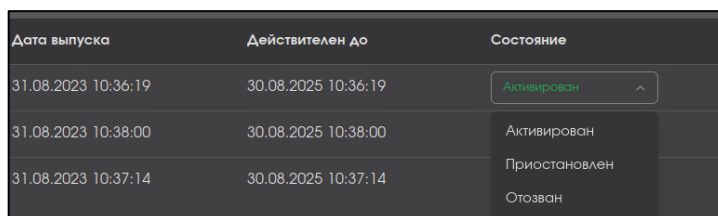


Рисунок 22 – Выпадающее меню смены состояния сертификата

- 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 23)

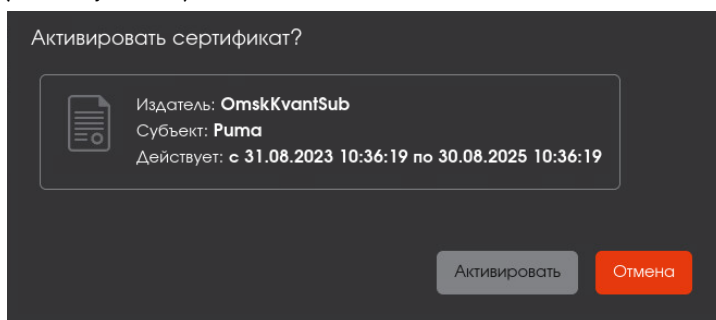


Рисунок 23 – Окно активации сертификата

- приостановка действия сертификата (см. Рисунок 24):

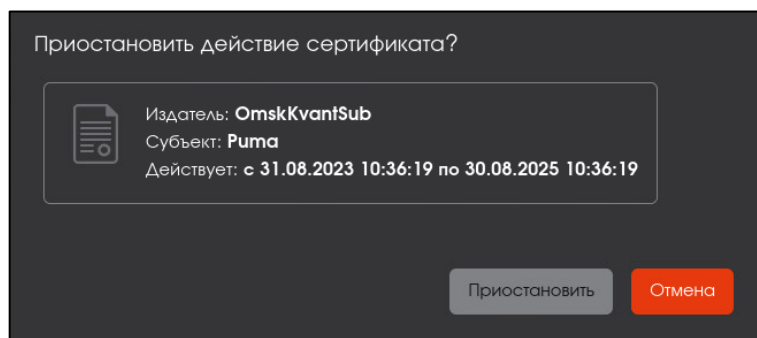


Рисунок 24 – Окно приостановки действия сертификата

- отзыв (см. Рисунок 25);

ВНИМАНИЕ! Данную операцию нельзя отменить.

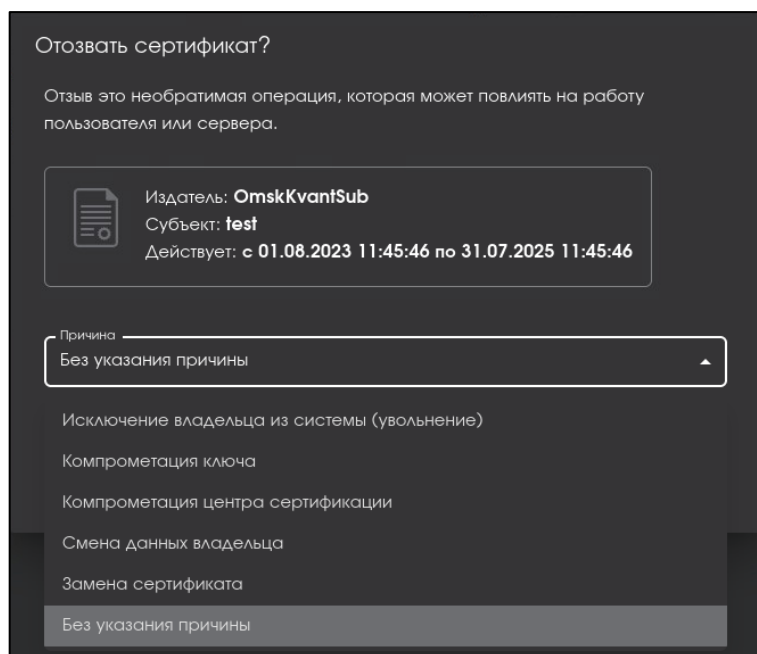


Рисунок 25 – Окно отзыва сертификата

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).

4.3.6 Карточка сертификата

- Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».
- Переход к экрану «Карточка сертификата» (см. Рисунок 26) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 16).

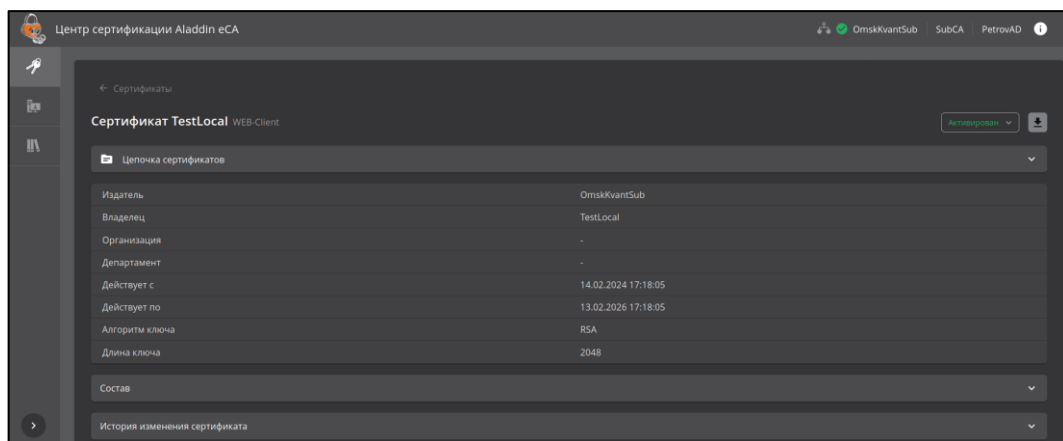






Рисунок 26 – Окно «Карточка сертификата»

- Оглавление карточки сертификата включает в себя (см. Рисунок 26):
 - тип (сертификат);
 - принадлежность (TestLocal);
 - шаблон сертификата (Web-Client).
- Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке  «Сертификаты»
- Для изменения статуса сертификата выбрать из выпадающего списка действие  «Активирован» в соответствии с Таблица 2 .
- Для скачивания сертификата наведите указатель мыши на кнопку , во всплывающем меню выберите <Скачать сертификат> субъекта или <Скачать цепочку> сертификатов.
- 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 27).

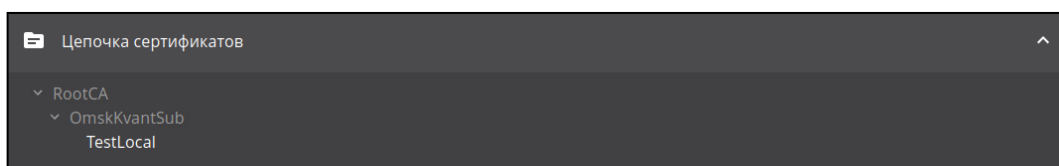



Рисунок 27 – Окно карточки сертификата. Вкладка «Цепочка сертификатов»

- «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 28):
 - серийный номер;
 - 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.

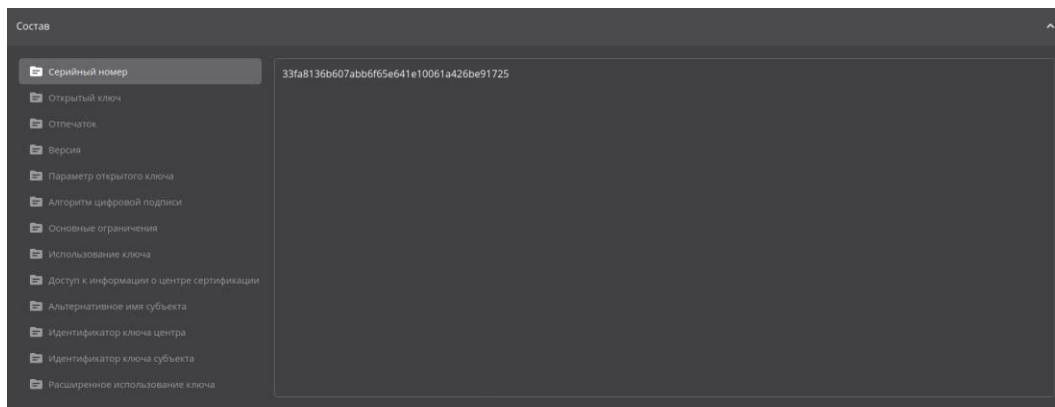



Рисунок 28 – Окно карточки сертификатов. Вкладка «Состав»

- «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 29):

- дата – дата совершенного действия;
- пользователь – учётная запись, под которой было совершено данное действие;
- событие – действие, совершённое над сертификатом.

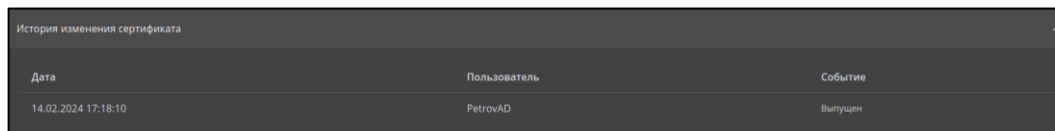

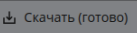


Рисунок 29 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

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

4.3.7 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> <Скачать все сертификаты в формате CSV>. Происходит формирование списка сертификатов, по завершению действия и готовности к выгрузке списка сертификатов кнопка переходит в состояние . Нажмите кнопку <Скачать (готово)> для сохранения подготовленного списка сертификатов.
- Сохранение списка сертификатов в виде zip-архива происходит по выбранному пути в открывшемся окне сохранения файла (см. Рисунок 30).

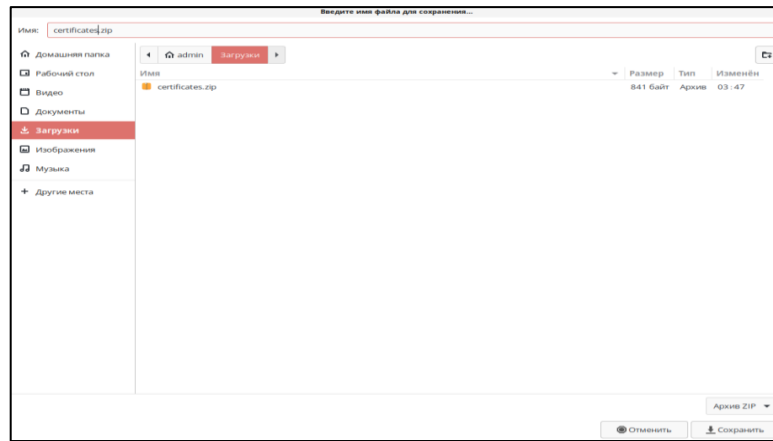


Рисунок 30 – Окно указания пути сохранения файла


• Выгруженный файл .csv представлен в текстовом формате для представления табличных данных, где строки текста содержат поля таблицы, разделенные запятыми. Сформированная таблица содержит следующие столбцы (см. Рисунок 31):

- 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	532af36b565670f83238c9d881	#####	#####	CN=SubCA242	02.09.2022 13:18	Revoked: Cessation c 77b28149a1e1	HOLD	CN=SubCA242	#####	SubCA242	null	OCSP Signer	RSA	2048
3	c32484f9822df0f83238c9d881	#####	#####	CN=SubCA242	31.08.2022 21:56	Revoked: Cessation c 29644f71ac7c6	HOLD	CN=DC	#####	DC	dnsNames=DC, gu Domain Cont	RSA		2048
4	5258bc09c20610f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 13:39	Suspended: Certifica	6996dc111ec1e	ACTIVE	CN=cheburger	#####	cheburger	rfc822Name=cheb Smartcard Lo	RSA	1024
5	47b18421e42f0f83238c9d881	#####	#####	CN=SubCA242	#####	Active	5110646ee2431	ACTIVE	CN=SubCA242	#####	SubCA242-web	dnsNames=SubCA WEB-Server	RSA	2048
6	7c13052621aff0f83238c9d881	#####	#####	CN=SubCA242	02.09.2022 10:42	Suspended: Certifica	67f2c7275957b	REVOKED	CN=OP1_242	#####	OP1_242	rfc822Name=op1g WEB-Client	RSA	2048
7	52f46cc9e30f6f0f83238c9d881	#####	#####	CN=SubCA242	31.08.2022 21:56	Suspended: Certifica	7987f39c5d53c	REVOKED	CN=OP2_242	#####	OP2_242	rfc822Name=op2g WEB-Client	RSA	2048
8	c411492e6140df0f83238c9d881	#####	#####	CN=SubCA242	31.08.2022 21:56	Suspended: Certifica	171a2506d320	REVOKED	CN=koltakova	#####	koltakov	rfc822Name=eaca Smartcard Lo	RSA	2048
9	f830f0cb22a0f0f83238c9d881	#####	#####	CN=SubCA242	04.09.2022 14:46	Revoked: Cessation c	659787b69d9f9	HOLD	CN=tushkan	#####	tushkan	rfc822Name=tushl Smartcard Lo	RSA	2048
10	dec1c1520014f0f83238c9d881	#####	#####	CN=SubCA242	31.08.2022 21:56	Revoked: Cessation c	6360503883063	HOLD	CN=SUBCA	#####	SUBCA	dnsNames=SUBCA Domain Cont	RSA	3072
11	110f1fbd7a61af0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 18:34	Suspended: Certifica	560f56c6f48609	REVOKED	CN=ttttttt	#####	ttttttt	rfc822Name=tt@ Smartcard Lo	RSA	2048
12	bd8e4c114e36f0f83238c9d881	#####	#####	CN=SubCA242	02.09.2022 10:42	Suspended: Certifica	09f6e09a614e1	REVOKED	CN=OP1_242	#####	OP1_242	rfc822Name=testg WEB-Client	RSA	2048
13	f9c9f3951e7c0f83238c9d881	#####	#####	CN=SubCA242	02.09.2022 10:03	Suspended: Certifica	54a9be9b4d1d1	REVOKED	CN=ushkan	#####	ushkan	rfc822Name=ushk Smartcard Lo	RSA	2048
14	8c32419620b0f0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 13:39	Suspended: Certifica	360c202d0731a	REVOKED	CN=tushkan	#####	tushkan	dnsName=tushka Domain Cont	RSA	2048
15	bed018256dbcf0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 12:38	Suspended: Certifica	6a607b1d27e71	REVOKED	CN=SUBCA	#####	SUBCA	rfc822Name=SUBCA Domain Cont	RSA	3072
16	9b301f0e9d9dc0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 12:37	Suspended: Certifica	3fdaa0b12fdb3f	REVOKED	CN=OCSP	02.09.2022 9:54	OCSP	rfc822Name=OCSP, Domain Cont	RSA	2048
17	3e352d5bf49cf0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 18:34	Suspended: Certifica	124f06965c59bc	REVOKED	CN=paukan	#####	paukan	rfc822Name=pauk Smartcard Lo	RSA	2048
18	4810c3f5cbbbf0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 13:28	Suspended: Certifica	35e5f0c041cc8	REVOKED	CN=testop	#####	testop	rfc822Name=pauk WEB-Client	RSA	1024
19	3614f6ce3245f0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 15:01	Suspended: Certifica	201f0e17d371d	REVOKED	CN=DC	#####	DC	dnsName=DC, gu Domain Cont	RSA	2048
20	4f2b63a93d73f0f83238c9d881	#####	#####	CN=SubCA242	#####	Active	762a8430c0356f	ACTIVE	CN=operator	#####	operator	rfc822Name=swsd WEB-Client	RSA	2048
21	8b5e6e050346f0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 17:30	Suspended: Certifica	7061a34d5576b	REVOKED	CN=operator	#####	operator	rfc822Name=testg WEB-Client	RSA	2048
22	0633097415bf0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 15:57	Suspended: Certifica	2d6f64eb41687	REVOKED	CN=paukan	#####	paukan	rfc822Name=pauk Smartcard Lo	RSA	2048
23	01f4daded2341f0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 16:37	Suspended: Certifica	124f06965c59bc	REVOKED	CN=Guest	#####	Guest	dnsName=Guest, Domain Cont	RSA	2048
24	0f7e0809ca0bf0f83238c9d881	#####	#####	CN=SubCA242	01.09.2022 17:49	Suspended: Certifica	5fa7b04816ce9	REVOKED	CN=test	#####	test	rfc822Name=testg Smartcard Lo	RSA	2048
25	fc8cd2875a1ef0f83238c9d881	#####	#####	CN=SubCA242	04.09.2022 12:03	Revoked: Cessation c	6ed38ad110d43	HOLD	CN=kruchinini	06.09.2022 0:37	kruchinina	rfc822Name=alexl Smartcard Lo	RSA	2048
26	ad3e9be8d5d1f0f83238c9d881	#####	#####	CN=SubCA242	04.09.2022 8:50	Suspended: Certifica	36612c14a79f9	ACTIVE	CN=C:PIP PIP	#####	C:PIP PIP	rfc822Name=swsd Smartcard Lo	RSA	2048
27	23421a1f5bdcf0f83238c9d881	#####	#####	CN=SubCA242	#####	Active	513cb4479c38c	ACTIVE	CN=OP2_242	#####	OP2_242	rfc822Name=swsd WEB-Client	RSA	2048
28	8defc2b24fd4f0f83238c9d881	#####	#####	CN=SubCA242	04.09.2022 12:02	Revoked: Cessation c	4d70ce1e01f42f	HOLD	CN=CLIENT2	#####	CLIENT2	dnsName=CLIENT Domain Cont	RSA	2048
29	9ba4eecd5179f0f83238c9d881	#####	#####	CN=SubCA242	05.09.2022 15:58	Active	666cb74489ed	ACTIVE	CN=OCSP	02.09.2022 9:54	OCSP	rfc822Name=OCSP, Domain Cont	RSA	2048
30	c7f85322bb4af0f83238c9d881	#####	#####	CN=SubCA242	#####	Active	17b0c9697f993c	ACTIVE	CN=OP1_242	#####	OP1_242	rfc822Name=op1g WEB-Client	RSA	2048
31	d41f61fba662f0f83238c9d881	#####	#####	CN=SubCA242	04.09.2022 12:03	Revoked: Cessation c	3c131d8839d6d	HOLD	CN=koltakova	#####	koltakov	rfc822Name=eaca Smartcard Lo	RSA	2048
32	88bb73a7ae71f0f83238c9d881	#####	#####	CN=SubCA242	05.09.2022 16:11	Revoked: Cessation c	7aae5b17f1c57	HOLD	CN=testuser2	#####	testuser2	rfc822Name=testu Smartcard Lo	RSA	2048

Рисунок 31 – Пример экспортированного файла списка выпущенных сертификатов.csv

4.3.8 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 32).

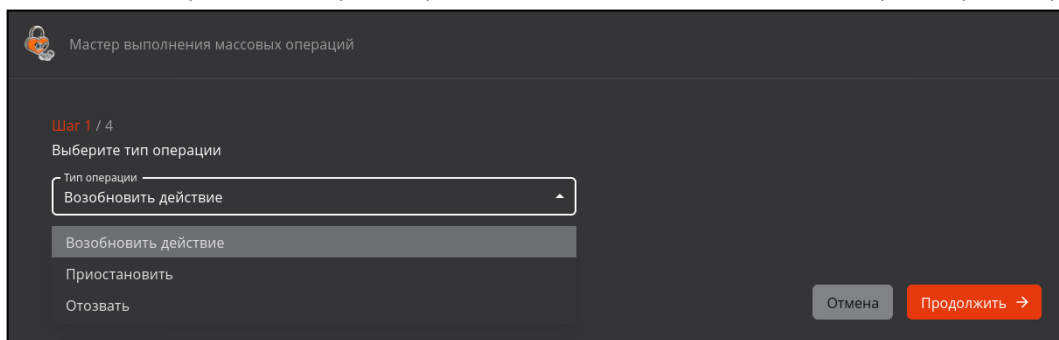




Рисунок 32 – Окно выполнения массовых операций. Шаг 1

- 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 33). 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.

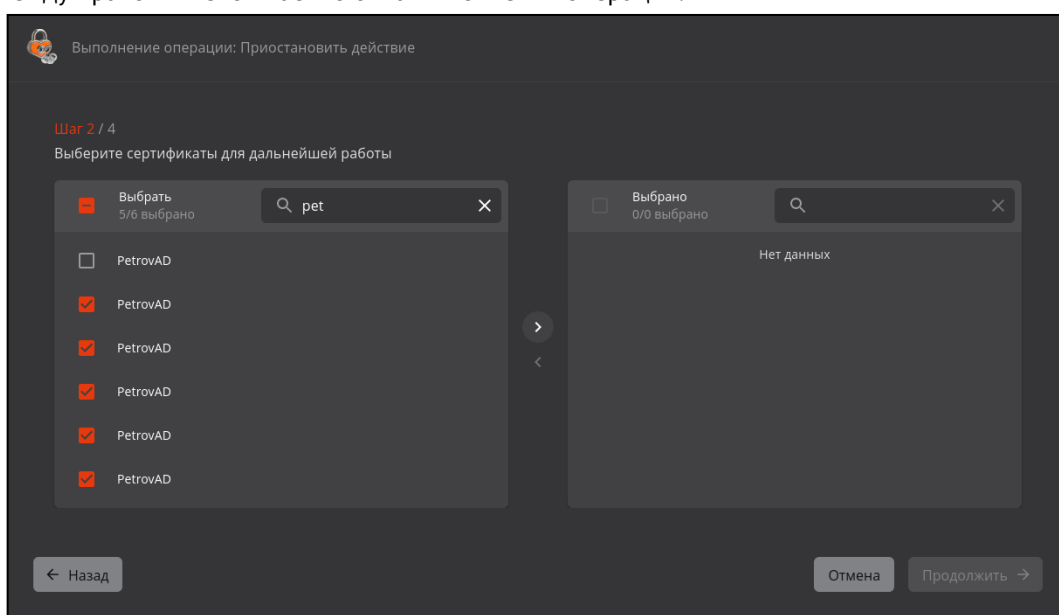



Рисунок 33 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

- 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 .

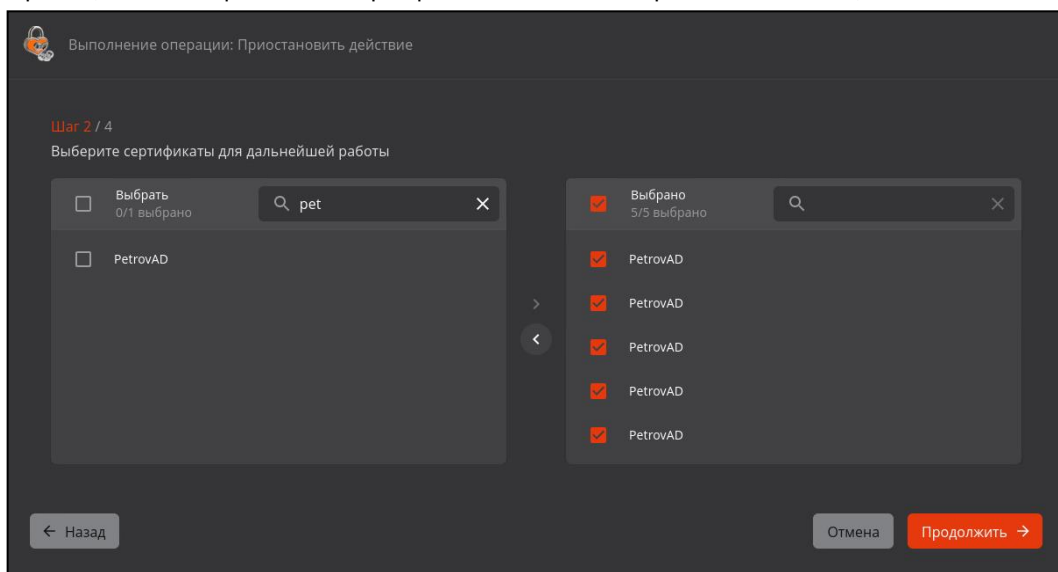


Рисунок 34 – Окно выполнения массовых операций. Шаг 2. Редактирование списка выбранных сертификатов

- Для перехода на следующий шаг нажмите кнопку <Продолжить>.
- В открывшемся окне подтвердите действие, нажав кнопку «Применить» (см. Рисунок 35).

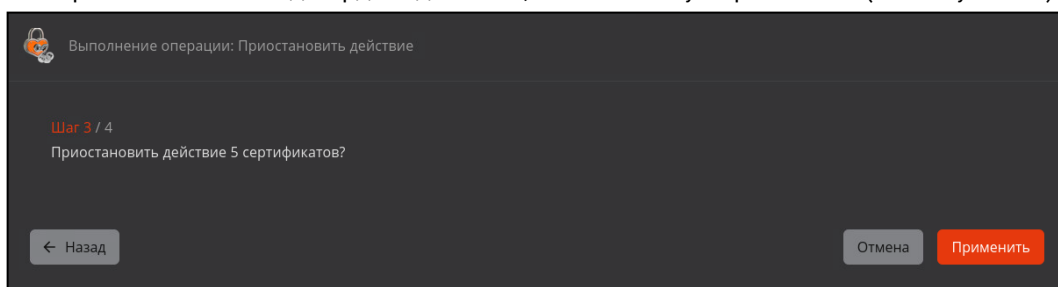


Рисунок 35 – Окно выполнения массовых операций. Шаг 3

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

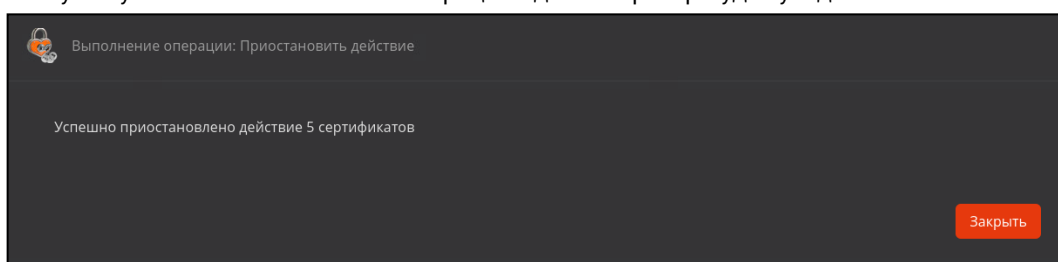


Рисунок 36 – Окно выполнения массовых операций. Шаг 4

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 37).

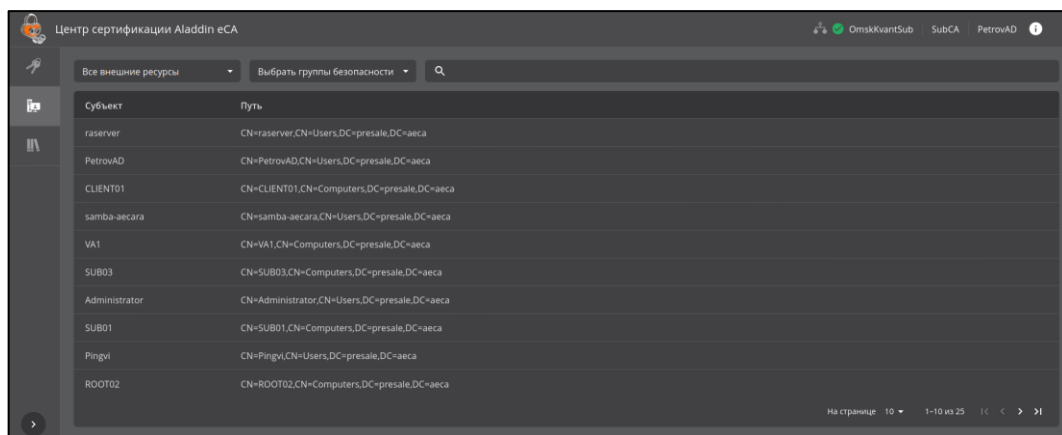


Рисунок 37 – Экран раздела меню «Субъекты». Подключенный ресурс

- Список субъектов на экране раздела отображается в виде таблицы с пагинацией и сортировкой по заголовку табличного поля экранной формы.
- 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).
- В разделе «Субъекты» доступны следующие действия:
 - просмотр субъектов подключенных ресурсных систем с выбором группы безопасности;
 - просмотр субъектов локальной ресурсной системы;
 - поиск субъекта;
 - создание нового субъекта локальной ресурсной системы;
 - редактирование значения атрибутов субъекта локальной ресурсной системы;
 - просмотр карточки субъекта;
 - просмотр списка сертификатов, выпущенных Центром сертификации для субъекта;
 - управление статусом сертификатов, выпущенных Центром сертификации для субъекта;
 - публикация сертификата субъекта в ресурсную систему;
 - экспорт сертификата субъекта;
 - создание сертификата для субъекта;
 - создание учётной записи для субъекта.
- Идентификация локальных и подключенных субъектов в Центре сертификации осуществляется по атрибуту UUID.

4.4.1 Просмотр субъектов ресурсных систем

- Просмотр субъектов осуществляется посредством выбора источника:
 - все внешние ресурсы – подключенные службы каталогов, на субъекты которых назначены права авторизованному оператору;
 - локальный ресурс – появляется в случае, если назначены права хот бы на один субъект в локальной базе данных Центра сертификации;
 - внешний ресурс, отображаемое имя которого соответствует имени контроллера домена.

- В разделе «Субъекты» в верхней панели расположены элементы выбора ресурса и фильтрации (см. Рисунок 38):

- поле «ресурсная система», по нажатию на которое в выпадающем меню выберите локальную ресурсную систему, подключенный ресурс или все внешние ресурсы для отображения всех субъектов внешних ресурсных систем;
- поле «Выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в выпадающем меню выберите необходимую группу. В случае если группа безопасности не выбрана, то будут отображены все субъекты выбранного источника. Для локального ресурса группы безопасности отсутствуют. 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.

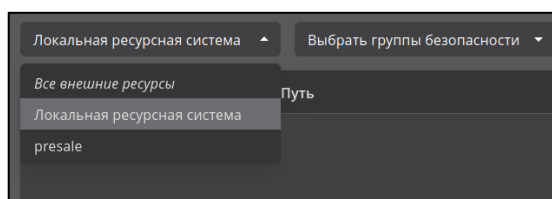


Рисунок 38 – Верхняя панель экранной формы вкладки «Субъекты»

4.4.2 Поиск субъектов

- В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 40):
 - 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.

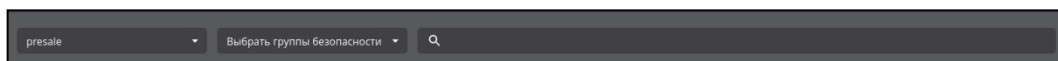


Рисунок 39 – Поле поиска субъектов


4.4.3 Фильтрация субъектов

- В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 38):
 - поле «Выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в развернутом 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;

4.4.4 Сортировка субъектов

Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 40):

- «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.

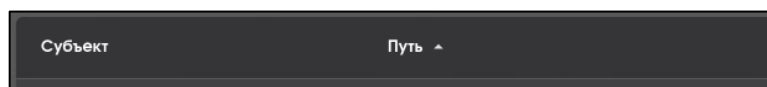


Рисунок 40 – Поля сортировки содержимого экрана раздела «Сертификаты»

4.4.5 Карточка субъекта

- Просмотра данных субъекта возможен посредством страницы «Карточка субъекта».
- Переход к экрану «Карточка субъекта» (см. Рисунок 41) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 37).

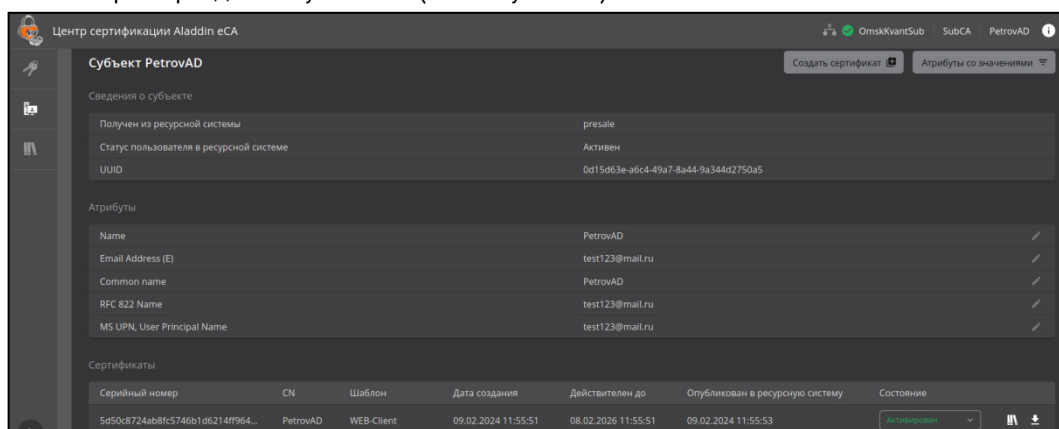
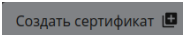


Рисунок 41 – Окно просмотра карточки субъекта (включено отображение «Атрибуты со значениями»)

- Карточка субъекта включает в себя следующие информационные поля:
 - сведения о субъекте:
 - из какой ресурсной системы получен субъект;
 - статус пользователя в ресурсной системе;
 - идентификатор UUID;
 - атрибуты SAN и SDN (см. Таблица 3);
 - сведения обо всех сертификатах субъекта, ранее выпущенных Центром сертификации:
 - серийный номер;
 - Common Name владельца сертификата;
 - шаблон;
 - дата создания;
 - дата окончания действия;
 - дата публикации в ресурсную систему;
 - состояние сертификата.
- Доступные действия в карточке субъекта:
 - создать сертификат для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку «Создать сертификат»  (см. п. 4.4.8, настоящего руководства);
 - выбрать набор атрибутов SDN и SAN, отображаемых в карточке субъекта, в выпадающем меню (см. Рисунок 42);

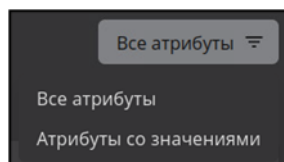


Рисунок 42 – Фильтрация отображаемых атрибутов в карточке субъекта



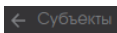
- опубликовать сертификат в ресурсную систему (только для подключенных субъектов). По нажатию на кнопку  происходит запись сертификата в формате LDIF в атрибут userCertification выбранного субъекта ресурсной системы, для которого выпущен сертификат. Если атрибут userCertification заполнен, то происходит перезапись содержимого;
- экспорт сертификата выбранного субъекта по указанному для сохранения файла по указанному пути по кнопке  «Скачать»;
- переход в карточку сертификата;
- изменить статус сертификатов, выпущенных для данного субъекта в поле сертификата «Состояние»;
- редактировать значения в полях атрибутов (только для локальных субъектов).

Таблица 3 – Атрибуты субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Сведения о субъекте			
Ресурсная система, к которой подключен субъект	Ресурсная система, к которой подключен субъект	resource: { id (UUID), commonName (string), name (string)}	Поле «Получен из ресурсной системы» в карточке субъекта Для локальных субъектов всегда отображается значение «Локальная ресурсная система».
Флаг подключения к РС	Субъект подключен к ресурсной системе (true)	"isConnected": true	Отображение субъекта в списке субъектов ресурсной системы, к которой он подключен.
	Локальный субъект (false)	"isConnected": false	Отображение субъекта в списке субъектов локальной ресурсной системы.
Флаг блокировки в РС	Для подключенных к РС субъектов: субъект заблокирован в РС (true) или субъект не заблокирован в РС (false)	"isBlocked"	Поле «Статус в ресурсной системе» в карточке субъекта. Для локальных субъектов всегда отображается символ «-».
	Для локальных субъектов: всегда false		
UUID	string(\$uuid)	"id"	Поле «UUID» карточки субъекта
Расположение субъекта в структуре РС	Строка	"distinguishedName"	Поле «Путь» в списке субъектов в разделе «Субъекты»

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Время обновления субъекта	Дата в формате ISO 8601	"updated"	-
Время создания субъекта	Дата в формате ISO 8601	"created"	-
Атрибуты SDN			
Common name	Список строк	"CN"	Поле «Common name» в карточке субъекта
Unique Identifier (UID)	Список строк	"UID"	Поле «Unique Identifier (UID)» в карточке субъекта
Email Address (E)	Список строк	"E"	Поле «Email Address (E)» в карточке субъекта
Email Address (Mail)	Список строк	"EMAILADDRESS"	Поле «Email Address (Mail)» в карточке субъекта
Mail	Список строк	"MAIL"	Поле «Mail» в карточке субъекта
Serial number	Список строк	"SN"	Поле «Serial number» в карточке субъекта
Given name	Список строк	"GIVENNAME"	Поле «Given name» в карточке субъекта
Initials	Список строк	"INITIALS"	Поле «Initials» в карточке субъекта
Surname	Список строк	"SURNAME"	Поле «Surname» в карточке субъекта
Organizational unit	Список строк	"OU"	Поле «Organizational unit» в карточке субъекта
Organization	Список строк	"O"	Поле «Organization» в карточке субъекта
Locality	Список строк	"L"	Поле «Locality» в карточке субъекта
State or province	Список строк	"ST"	Поле «State or province» в карточке субъекта
Domain component	Список строк	"DC"	Поле «Domain component» в карточке субъекта
Country	Список строк	"C"	Поле «Country» в карточке субъекта
Unstructured address	Список строк	"UNSTRUCTUREDADDRESS"	Поле «Unstructured address» в карточке субъекта
Unstructured name	Список строк	"UNSTRUCTUREDNAME"	Поле «Unstructured name» в карточке субъекта
Postalcode	Список строк	"POSTALCODE"	Поле «Postalcode» в карточке субъекта
Business category	Список строк	"BUSINESSCATEGORY"	Поле «Business category» в карточке субъекта
Telephone number	Список строк	"TELEPHONENUMBER"	Поле «Telephone number» в карточке субъекта
Pseudonym	Список строк	"PSEUDONYM"	Поле «Pseudonym» в карточке субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Postal address	Список строк	"POSTALADDRESS"	Поле «Postal address» в карточке субъекта
Street	Список строк	"STREET"	Поле «Street» в карточке субъекта
Name	Список строк	"NAME"	Поле «Name» в карточке субъекта
Title	Список строк	"T"	Поле «Title» в карточке субъекта
Domain Qualifier	Список строк	"DN"	Поле «Domain Qualifier» в карточке субъекта
Description	Список строк	"DESCRIPTION"	Поле «Description» в карточке субъекта
Атрибуты SAN			
MS GUID, Globally Unique Identifier	string(\$uuid)	"MS_GUID"	Поле «MS GUID, Globally Unique Identifier» в карточке субъекта
RFC 822 NAME	Список строк	"RFC822NAME"	Поле «RFC 822 NAME» в карточке субъекта
MS UPN, UserPrincipalName	Список строк	"MS_UPN"	Поле «MS UPN, UserPrincipalName» в карточке субъекта
DNS Name	Список строк	"DNS_NAME"	Поле «DNS Name» в карточке субъекта
IP address	Список строк	"IPADDRESS"	Поле «IP address» в карточке субъекта
Directory Name	Список строк	"DIRECTORY_NAME"	Поле «Directory Name» в карточке субъекта
Uniform resource identifier	Список строк	"UNIFORM_RESOURCE_ID"	Поле «Uniform resource identifier» в карточке субъекта
Registered identifier	Список строк	"REGISTERED_ID"	Поле «Registered identifier» в карточке субъекта
Kerberos KPN, Kerberos 5 Principal	Список строк	"KRB5PRINCIPAL"	Поле «Kerberos KPN, Kerberos 5 Principal» в карточке субъекта
Permanent identifier	Список строк	"PERMANENT_IDENTIFIER"	Поле «Permanent identifier» в карточке субъекта
Xmpp address	Список строк	"XMPP_ADDR"	Поле «Xmpp address» в карточке субъекта
Service Name	Список строк	"SRV_NAME"	Поле «Service Name» в карточке субъекта
Subject Identification Method	Список строк	"SUBJECT_IDENTIFICATION_METHOD"	Поле «Subject Identification Method» в карточке субъекта

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

4.4.5.1 Редактирование атрибутов субъекта

- Для субъектов локальной ресурсной системы доступно редактирование всех атрибутов SDN и SAN.

4.4.6 Субъекты локальной ресурсной системы

- Локальную базу субъектов формируют:
 - субъекты, созданные Администратором путём вызова метода API;
 - субъекты отключенной ресурсной системы (удалённой ранее зарегистрированной ресурсной системы), атрибут субъекта «isBlocked» принимает значение «false». В случае повторного подключения ресурсной системы связи субъектов с группами будут восстановлены, обновлены атрибуты в соответствии с данными из ресурсной системы;
 - субъекты, загруженные в базу данных Aladdin eCA при подключении ресурсной системы, но отсутствующие в списке субъектов, полученном по результатам выполнения полной синхронизации ресурсной системы. Атрибут субъекта «isBlocked» принимает значение «false».
- Локальный субъект отключенной ресурсной системы при подключении ресурсной системы, где существует данный субъект, будет перенесён из базы локальной ресурсной системы (атрибут субъекта «isConnected» примет значение «true»). При этом будет выполнено обновление атрибутов субъекта в соответствии с его атрибутами из ресурсной системы, остальные текущие атрибуты (то есть те, которые не были получены из ресурсной системы) не изменятся. Проверка субъектов осуществляется по атрибуту «id».

4.4.7 Субъекты внешнего ресурса

- Внешний (подключенный) ресурс формируется в результате регистрации службы каталогов доменных служб Samba DC, РЕД АДМ, ALD PRO, FreeIPA или MS Active Directory.
- Подключенный ресурс будет отображен только после регистрации ресурсной системы на вкладке «Ресурсная система».
- Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в пункте 4.5.1 настоящего руководства.
- После подключения внешней ресурсной системы, обновления и выбора источника в поле «Ресурсная система», субъекты будут отображены в виде списка в окне вкладки «Субъекты». Возможно настроить отображение определенной группы безопасности или вывести полный список, упорядочив субъекты в алфавитном порядке по имени (CommonName) (см. Рисунок 37).

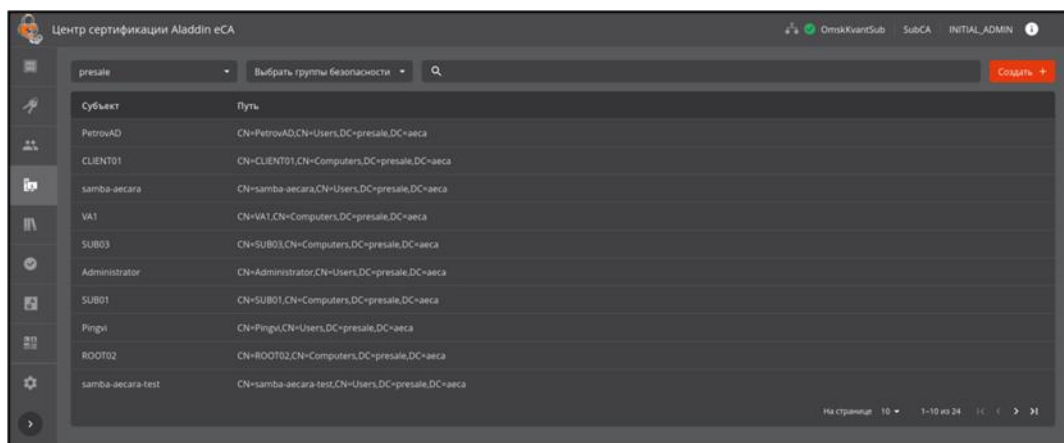


Рисунок 44 – Экран раздела меню «Субъекты». Подключенный ресурс

- Загрузка данных осуществляется из всей ресурсной системы, начиная с точки подключения, указанной в настройках подключения Корневого каталога.
- 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 7.

Таблица 5 – Преобразование данных субъектов ресурсной системы


Атрибут субъекта Aladdin eCA	Поле в базах Samba DC, MS AD, РЕД АДМ для типов субъектов		Поле в базах ALD PRO, FreeIPA для типов субъектов		
	Пользователь	Компьютер	Пользователь	Компьютер	Сервис
Id	ObjectGUID	ObjectGUID	ipaUniquelD	ipaUniquelD	ipaUniquelD
Common name	cn	cn	cn	cn	krbPrincipalName
			uid		
Initials	-	-	initials	-	-
Surname	sn	-	sn	-	-
Given Name	givenName	-	givenName	-	-
Organization	-	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Name	name	name	-	serverHostName	-
MS GUID	-	ObjectGUID	-	-	-
Domain Qualifier	distigushedName	distigushedName	entrydn	entrydn	
Description	description	-	-	-	-
DNS Name	-	dNSHostName	-	fqdn	-
Email Address (Mail)	mail	-	mail	-	-
	userPrincipalName		krbPrincipalName	krbPrincipalName	
RFC 822 NAME	mail	-	mail	-	krbPrincipalName
	userPrincipalName		krbPrincipalName	krbPrincipalName	
MS UPN	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Unique Identifier (UID)	-	-	uid	-	-
Kerberos KPN, Kerberos 5 Principal	-	-	-	krbPrincipalName	-

- Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.

- Идентификация подключенных субъектов в Центре сертификации осуществляется по атрибуту **UUID**.

4.4.8 Создание 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 45).

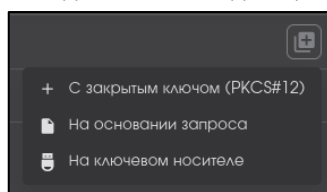


Рисунок 45 - Окно выпуска сертификата для субъекта ресурсной системы

4.4.8.1 Создание сертификата с закрытым ключом pkcs#12

- В открывшемся окне создания сертификата (см. Рисунок 46) 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. Для локальных субъектов данный чек-бокс выключен.

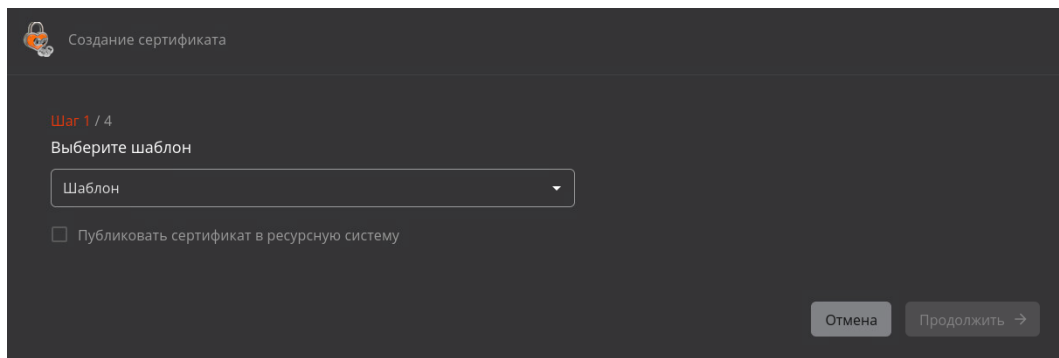




Рисунок 46 – Окно создания сертификата PKCS#12. Выбор шаблона

- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.
- Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.5 настоящего руководства) и изменению не подлежит.

В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить>  справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 47).

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля в карточке субъекта (см. п. 4.4.5.1 настоящего руководства).
- Необязательные поля могут оставаться незаполненными.
- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.

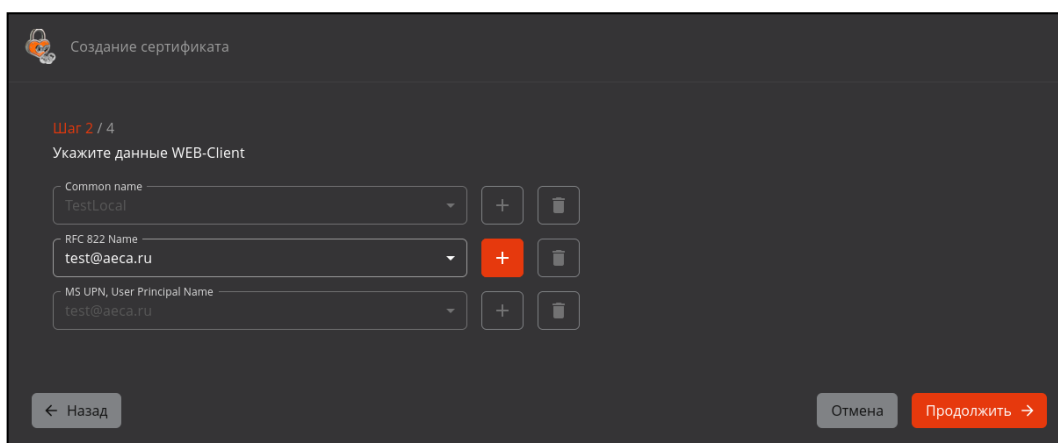



Рисунок 47 – Окно создания сертификата PKCS#12. Атрибуты сертификата

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 48). 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 48 – Окно создания сертификата PKCS#12. Задание пароля контейнера сертификата

- В следующем окне требуется определить параметры шифрования (см. Рисунок 49):
 - алгоритм ключа;
 - длину ключа.
- По умолчанию выбрано значение «RSA-2048».
- После выбора алгоритма нажмите кнопку <Создать сертификат>.

Рисунок 49 - Окно создания сертификата PKCS#12. Выбор параметров криптографии

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 54).

Внимание! Только в данном окне возможно скачать сертификат и закрытый ключ в контейнере pkcs#12, после закрытия окна скачать сертификат возможно только в формате .pem.

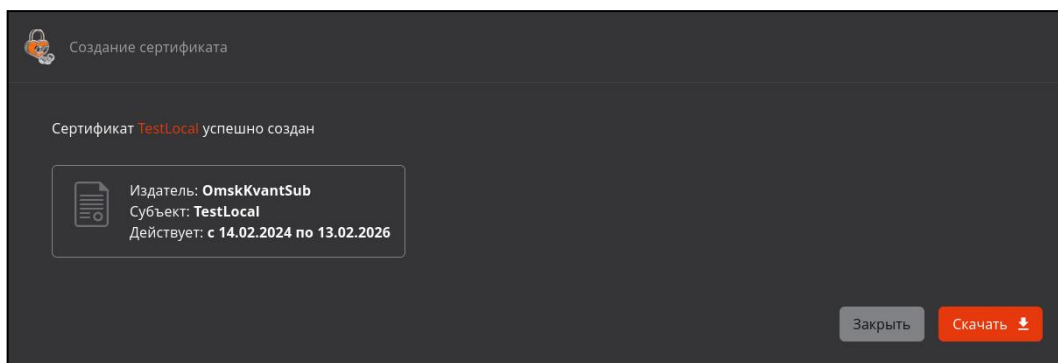


Рисунок 50 – Окно по результату успешного завершения создания сертификата PKCS#12

4.4.8.2 Создание 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 оператор заранее знает какой шаблон необходимо выбрать). По файлу запроса возможен только одноразовый выпуск сертификата.
 - Чек-бокс «Публиковать сертификат в ресурсную систему» доступен только при выпуске сертификата для субъектов внешних ресурсных систем, и активирован по умолчанию для публикации сертификата во внешнюю ресурсную систему путём добавления, а не перезаписи атрибута. Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат.
- При необходимости, возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке «Изменить».

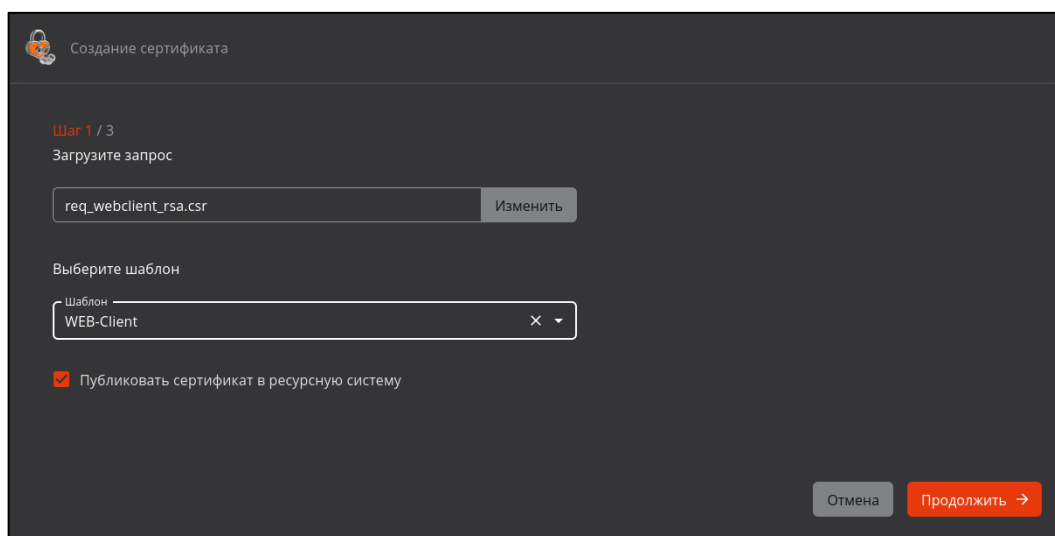


Рисунок 51 – Окно создания сертификата по запросу. Загрузка запроса и выбор шаблона

- После загрузки файла запроса и выбора шаблона нажмите активированную кнопку <Продолжить>.
- Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в Таблица 6.

Таблица 6 – Соответствие полей запроса шаблону выпускаемого сертификата

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Правила проверки соответствия SDN полей					
Есть, обязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, обязательное	Нет	Нет	Нет	-	Ошибка №1
Есть, обязательное	Есть	Есть	Да	Присутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4, если значение в запросе не соответствует значению атрибута субъекта
Есть, обязательное	Нет	Есть	Нет	-	Ошибка №1
Есть, необязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, необязательное	Нет	Нет	Да	Отсутствует	-
Есть, необязательное	Есть	Есть	Да	Присутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Отсутствует	-
Нет	Есть	Нет	Нет	-	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	-
Нет	Есть	Есть	Нет	-	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	-
Правила проверки соответствия SAN полей					
Есть, обязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, обязательное	Нет	Нет	Нет	-	Ошибка №1
Есть, обязательное	Есть	Есть	Да	Присутствует	1) Ошибка 2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка 4, если значение в запросе не соответствует значению атрибута субъекта Исправление указанных ошибок доступно на этапе переопределения значений для полей SAN, указанных в шаблоне.

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Есть, обязательное	Нет	Есть	Да	Присутствует	Ошибка №1 Исправление указанной ошибки доступно на этапе переопределения SAN (путем выбора значения для поля из атрибута субъекта).
Есть, необязательное	Есть	Нет	Да	Отсутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, необязательное	Нет	Нет	Да	Отсутствует	-
Есть, необязательное	Есть	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или Отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка 4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или Отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	-
Нет	Есть	Нет	Да	Отсутствует	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	-
Нет	Есть	Есть	Да	Отсутствует	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	-

• В случае выявления ошибки в запросе на сертификат доступа для субъекта возможны следующие сообщения:

- «Отсутствует обязательное поле» (ошибка №1);
- «Значение в поле не соответствует регулярному выражению: \"%s\"," где \"%s\"» (ошибка №2), регулярное выражение для валидации значений в соответствии с Приложением 1;
- «Поле отсутствует в шаблоне» (ошибка №3);
- «Значение в поле не соответствует значению атрибута в субъекте» (ошибка №4).

Если создание сертификата невозможно, то существует две возможности:

- вернуться на предыдущий шаг и сменить шаблон на подходящий;
- пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>.

• В результате успешной обработки запроса на сертификат субъекта на следующем шаге будут отображены (см. Рисунок 52):

- перечень полей, заданных в шаблоне (в столбце «Поля»);

- пиктограммы, отображающие обязательные и необязательные поля шаблона (в столбце «В шаблоне»). Пиктограмма «Галка» указывает на необязательность поля, а пиктограмма «Двойная галка» указывает на обязательность поля;
 - значения для полей, заданных шаблоном, полученные из запроса на сертификат (в столбце «Значение из запроса»);
 - значения, которые будут указаны в полях создаваемого сертификата (в столбце «Значение в сертификате»);
 - должна быть доступна кнопка «Продолжить» для перехода к следующему шагу;
 - должен быть предусмотрен возврат к предыдущему шагу (путем нажатия на кнопку «Назад») с возможностью изменения выбора запроса и/или шаблона сертификата;
 - должна быть доступна кнопка «Отмена» для завершения работы мастера создания сертификата без сохранения результатов.
- 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.

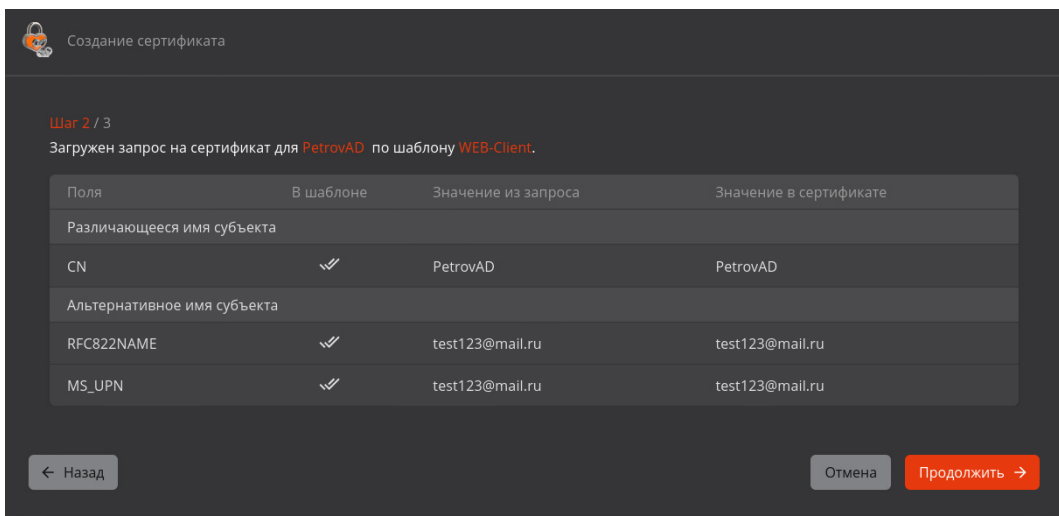


Рисунок 52 – Окно создания сертификата по запросу. Результат обработки запроса

- После успешной загрузки файла запроса нажмите кнопку «Продолжить» для продолжения процедуры выпуска сертификата для субъекта, кнопку «Отмена» для прекращения процедуры выпуска сертификата или кнопку «Назад» для возврата на предыдущий шаг.
- В окне следующего шага указаны атрибуты в соответствии с шаблоном сертификата (подробное описание полей шаблона приведено в Приложение 1. Описание полей шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.5 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки «Добавить» справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку «Добавить», она становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута (см. Рисунок 53).

- При отсутствии доступных для указания значений в поле обязательного атрибута будет отображаться ошибка «У субъекта отсутствует указанный атрибут».
- Необязательные поля могут оставаться незаполненными.

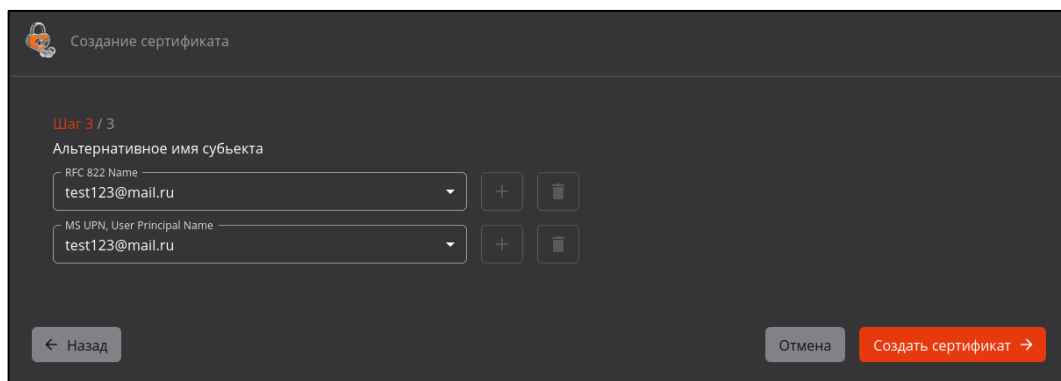


Рисунок 53 – Окно создания сертификата на основании запроса. Атрибуты сертификата

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 54).

Внимание! Только в данном окне возможно скачать сертификат и закрытый ключ в контейнере pkcs#12, после закрытия окна скачать сертификат возможно только в формате .pem.

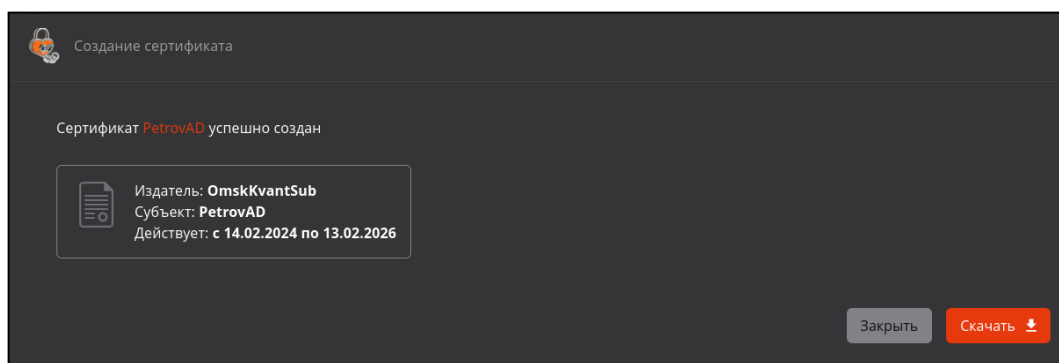


Рисунок 54 – Окно создания сертификата по запросу. Информирование об успешном создании сертификата

4.4.8.3 Создание 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 IC-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» запускает сценарий по созданию сертификата на ключевом носителе.
- В случае если электронный ключ успешно подключен, в открывшемся окне (см. Рисунок 55) необходимо выбрать ключевой носитель из выпадающего списка в поле «Устройство», ввести PIN-код пользователя ключевого носителя и указать шаблон для выпуска сертификата. При выпуске сертификата из раздела «Субъекты» шаблон будет определен по умолчанию и выбору не подлежит.
- Переход на следующий шаг осуществляется по ставшей активной кнопке <Продолжить> в случае ввода корректного PIN-кода электронного ключа и заполнения всех полей.

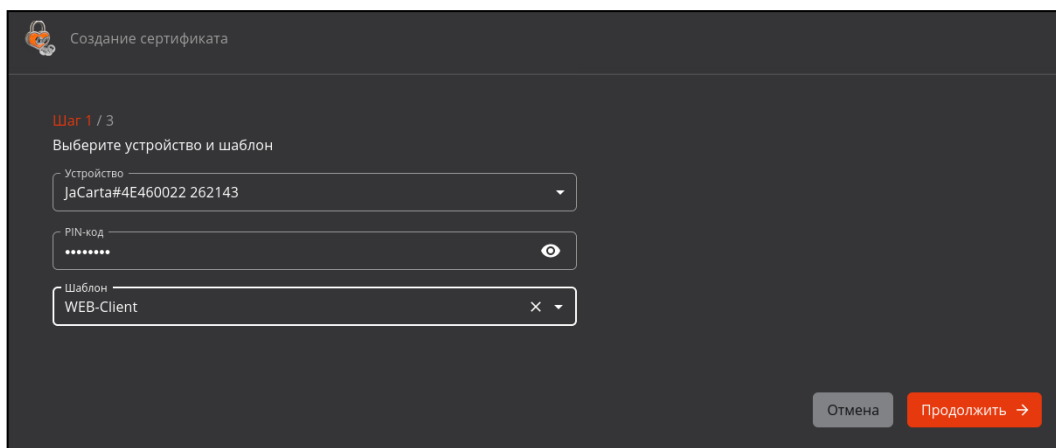




Рисунок 55 – Окно создания сертификата на электронном ключе. Шаг 1

- В окне Шага 2 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей шаблона приведено в Приложение 1. Описание полей шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.5 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить>  справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 56).

- Необязательные поля могут оставаться незаполненными.

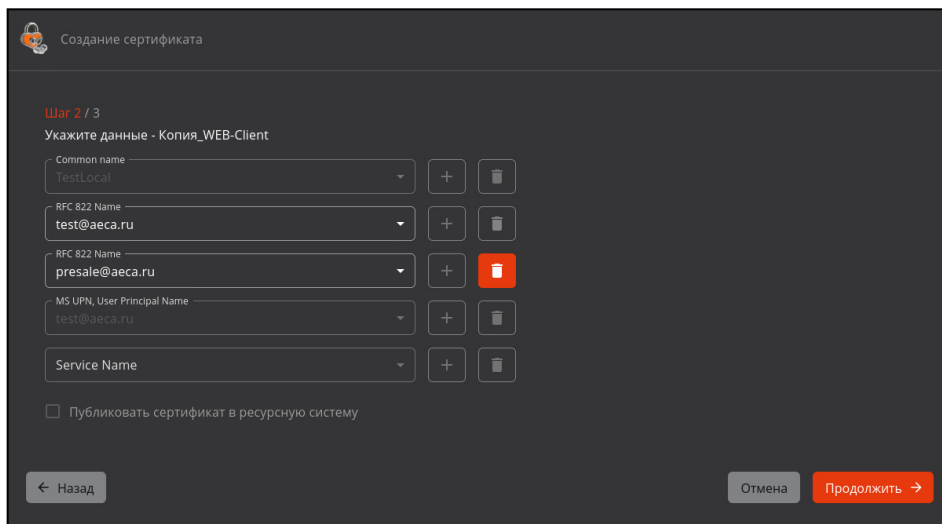


Рисунок 56 – Окно создания сертификата на электронном ключе. Шаг 2

- Далее необходимо выбрать параметры криптографии (см. Рисунок 57).
- После выбора алгоритма нажмите кнопку <Создать сертификат>.

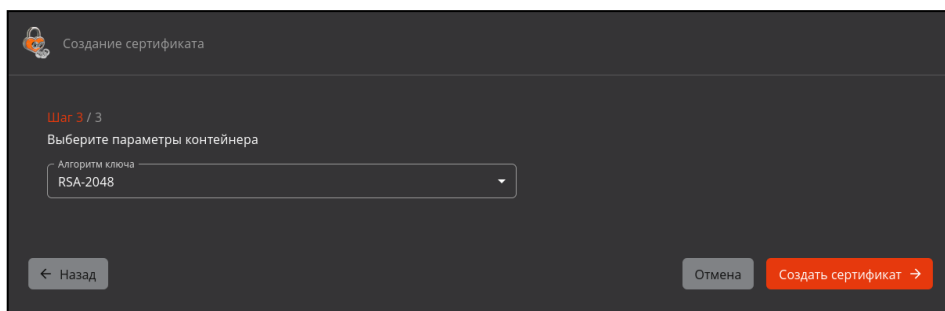


Рисунок 57 – Окно создания сертификата на электронном ключе. Шаг 3

- 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 58).

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!

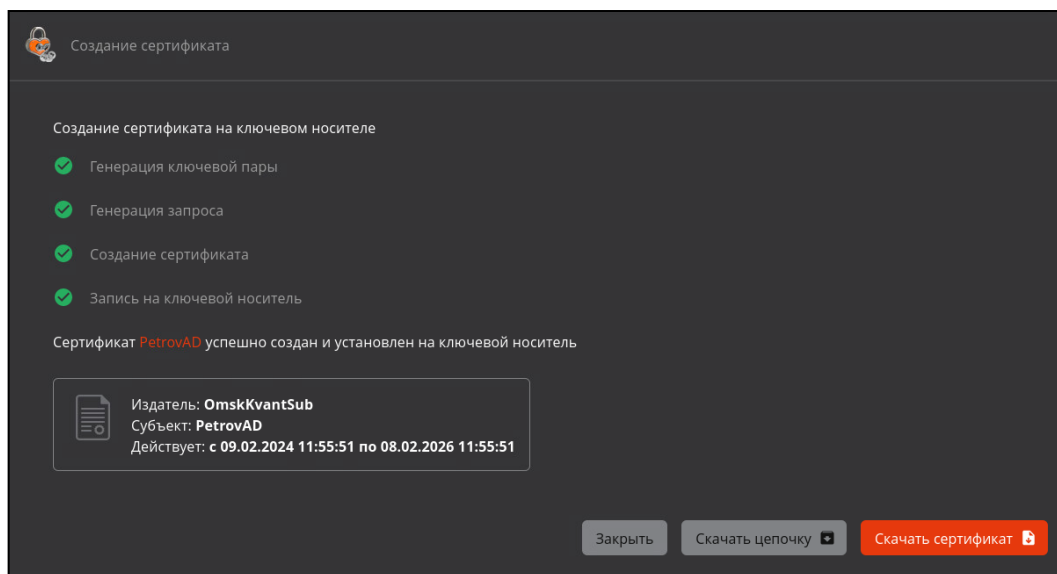


Рисунок 58 – Окно успешного создания сертификата субъекта на электронном ключе

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 59):

- 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.

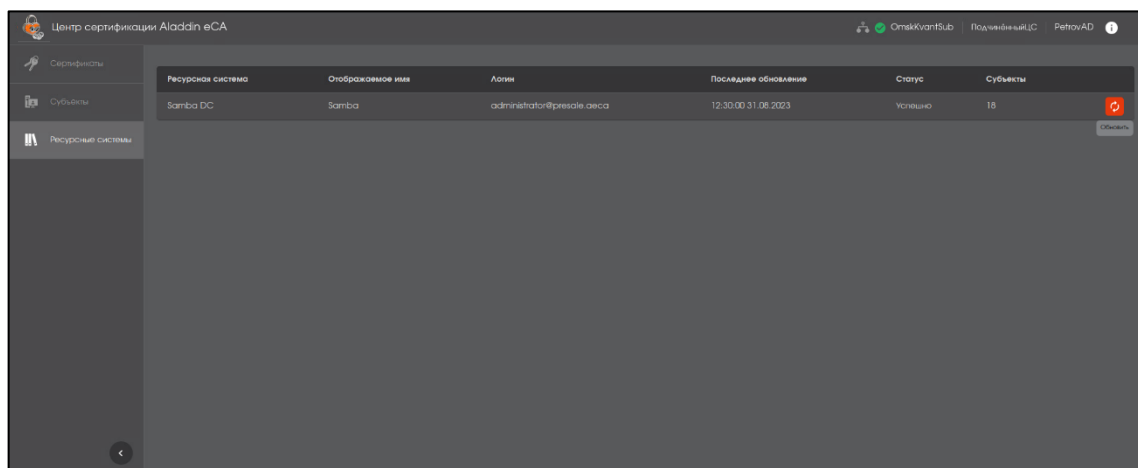



Рисунок 59 – Экран раздела «Ресурсная система»

- 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 частичная и полная синхронизация всех зарегистрированных точек подключения к ресурсным системам выполняется по расписанию в соответствии с заданным CRON-выражением администратором.
- Ручной запуск полной синхронизации 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 59) - осуществляется загрузка данных для каждого существующего субъекта из ресурсной системы:
 - список пользователей;
 - список ПК в домене;
 - список сервисов (только для ALD PRO и FreeIPA);
 - 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 7. Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.

Таблица 7 – 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	ipaUniqueID
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 8.

Таблица 8 – 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 1. 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				
CommonName	CommonName	имя контроллера домена	DC01	A-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел, ()
DNS Name	Domain Name System	FQDN (полное доменное имя вашего сервера)	dc1.presale.aeca	Только указанные символы: A-Я, а-я, A-Z, a-z, 0-9, ., -, *
MS GUID, Globally Unique Identifier	objectGUID / ipaUniqueID	<p>глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена</p> <p>Для получения значения идентификатора в среде РЕД ОС выполните команду:</p> <pre>samba-tool computer show <hostname> grep objectGUID</pre> <p>Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду:</p> <pre>ipa host-show <hostname> --all grep ipauniqueid</pre> <p>где [hostname] – короткое имя контроллера домена.</p>	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

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
алгоритм ключа	-	выберите значение из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите значение из выпадающего списка	-	1024,1536,2048,3072,4096,6144, 8192 192,224,256,384,521
ALD PRO Domain controller – шаблон сертификата контроллера домена ALD PRO				
CommonName	CommonName	имя контроллера домена ALD PRO	dc.ald.pro	A-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел, ()
Organization	-	организация	test	A-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
MS UPN, UserPrincipalName	objectGUID / ipaUniqueID	данные в формате «krbtgt/полное имя домена@полное имя домена»	krbtgt/ald.pro@ald.pro	Строка вида “text@text” A-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	A-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 192,224,256,384,521
Smartcard Logon ALD PRO – шаблон сертификата пользователя ALD PRO				
CommonName	CommonName	имя пользователя ALD PRO		A-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел, ()
Organization	-	организация	test	A-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: A-Я, а-я, A-Z, a-z, 0-9, ., @, /, _, -

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
MS UPN, UserPrincipalName	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	Строка вида "text@text" и только указанные символы: А-Я, а-я, А-Z, а-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 192,224,256,384,521
Smartcard Logon – шаблон сертификата пользователя				
CommonName	CommonName	имя пользователя	IvanovaAN	А-Я, а-я, А-Z, а-z, 0-9, ., _ , -, пробел, ()
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@ald.pro	Строка вида "text@text" А-Я, а-я, А-Z, а-z, 0-9, ., @, _ , -
MS UPN, UserPrincipalName	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@ald.pro	Строка вида "text@text" А-Я, а-я, А-Z, а-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 192,224,256,384,521

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
Web-client – шаблон сертификата учетной записи				
CommonName	CommonName	имя web-клиента	Operator01	A-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	Только указанные символы: A-Я, а-я, A-Z, a-z, 0-9, ., -, *
MS UPN, UserPrincipalName	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	Строка вида “text@text” A-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 192,224,256,384,521
Web-server – шаблон сертификата web-сервера				
CommonName	CommonName	имя web-сервера	Center01	A-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел, ()
DNS Name	Domain Name System	FQDN (полное доменное имя вашего сервера)	dc1.presale.aeca	Только указанные символы: A-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,

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
				8192 192, 224, 256, 384, 521
S/MIME – шаблон сертификата электронной почты				
CommonName	CommonName	имя пользователя	ivanova	A-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" A-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 192,224,256,384,521

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 токenu, 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

