



АКЦИОНЕРНОЕ ОБЩЕСТВО

«Аладдин Р.Д.»

УТВЕРЖДЕН

RU.АЛДЕ.03.01.020-01 32–ЛУ

ЦЕНТР СЕРТИФИКАТОВ ДОСТУПА

ALADDIN ENTERPRISE CA

Руководство администратора

RU.АЛДЕ.03.01.020-01 32

Листов 102

2022

Литера

# Содержание

1	О документе.....	6
1.1	Назначение документа .....	6
1.2	На кого ориентирован данный документ .....	6
1.3	Рекомендации по использованию документа.....	6
1.4	Соглашения по оформлению .....	6
1.5	Обозначения и сокращения.....	7
1.6	Ключевые слова.....	7
1.7	Авторские права, товарные знаки, ограничения .....	10
1.8	Лицензионное соглашение .....	11
2	Основные понятия.....	15
2.1	Назначение.....	15
2.2	Состав.....	15
2.3	Основные режимы работы .....	15
3	Системные требования.....	16
3.1	Требования к программному обеспечению .....	16
3.2	Требования к аппаратным средствам.....	16
4	Основные сведения.....	18
4.1	Комплект поставки .....	18
5	Подготовка к установке ПО Aladdin eCA .....	19
5.1	Подключение репозиторий и установка зависимостей.....	19
5.1.1	Подключение репозиторий .....	19
5.1.2	Установка Liberica JDK v.8.....	19
5.2	Настройке СУБД и подготовка базы данных .....	20
5.2.1	Предварительная установка и инициация БД на ОС RED OS.....	20
5.2.2	Предварительная установка и инициация БД на Astra Linux.....	22
5.3	Распаковка инсталляционного комплекта AeCA CA .....	24
5.4	Распаковка инсталляционного комплекта AeCA VA .....	27
6	Установка ПО Aladdin eCA .....	30
6.1	Установка ПО «Центр сертификации» Aladdin Enterprise CA.....	30
6.1.1	Инициализация процесса установки AeCA CA.....	30
6.1.2	Процесс установки AeCA CA .....	30
6.1.3	Дополнительные возможные действия при установке.....	32
6.2	Установка ПО «Центр валидации» Aladdin Enterprise CA.....	32
6.2.1	Инициализация процесса установки AeCA VA .....	32
6.2.2	Процесс установки AeCA VA.....	32

6.2.3	Дополнительные возможные действия при установке.....	34
7	Настройка ПО «Центр сертификации» Aladdin Enterprise CA.....	36
7.1	Первичная инициализация Alladin eCA CA.....	36
7.2	Описание верхней панели «Центра сертификации» .....	41
7.3	Описание вкладки «Центр сертификации».....	42
7.3.1	Вкладка «Свои сертификаты» .....	42
7.3.2	Вкладка «Сертификаты подчиненных центров».....	45
7.3.3	Создание корневого центра сертификатов.....	46
7.3.4	Создание подчиненного центра сертификатов .....	50
7.3.5	Подписание запроса на корневом ЦС.....	51
7.3.6	Импорт сертификата подчиненного ЦС .....	53
7.4	Описание вкладки «Сервис публикации» .....	55
7.4.1	Состав элементов вкладки «Сервис публикаций» .....	55
7.4.2	Моментальная публикация списков CRL .....	57
7.4.3	Настройка периода автообновления.....	57
7.4.4	Создания новых точек публикации CRL и AIA.....	58
7.5	Описание вкладки «Сертификаты доступа».....	59
7.5.1	Карточка сертификата.....	62
7.5.2	Создание сертификата для нового субъекта аутентификации .....	64
7.5.3	Создание сертификата для существующего субъекта аутентификации .....	67
7.5.4	Создание сертификата субъекта аутентификации по запросу.....	71
7.6	Описание вкладки «Сервисы OCSP».....	76
7.6.1	Добавление URL-адреса сервиса OCSP .....	77
7.6.2	Проверка наличия URL-адреса OCSP в атрибуте сертификата субъекта аутентификации .....	78
8	Настройка ПО «Центр валидации» Aladdin Enterprise CA.....	80
8.1	Первичная инициализация Alladin eCA VA.....	80
8.2	Вкладка «Сервисы OCSP» .....	85
8.2.1	Создание сервиса OCSP .....	86
8.2.2	Подписание запроса на сертификат для службы OCSP.....	90
8.2.3	Импорт сертификата службы OCSP.....	92
8.2.4	Карточка сервиса OCSP.....	95
8.2.5	Просмотр данных сервиса .....	96
8.2.6	Удаление сервиса OCSP .....	99
8.2.7	Редактирование сервиса OCSP .....	99
9	Удаление ПО Aladdin eCA.....	100

9.1 Удаление программного компонента «Центр сертификации» Aladdin Enterprise CA	
100	
9.1.1 Инициализация процесса удаления.....	100
9.1.2 Удаление установочного пакета.....	100
9.2 Удаление программного компонента «Центр валидации» Aladdin Enterprise CA ..	100
9.2.1 Инициализация процесса удаления.....	100
9.2.2 Удаление установочного пакета.....	101
10 Методы Rest API программного средства Aladdin ECA.....	102
10.1 Создать субъект аутентификации .....	102
10.2 Получить информацию о списке id всех существующих субъектов аутентификации, ассоциированных с активным ЦС .....	103
10.3 Получить информацию о конкретном субъекте аутентификации по его id .....	103
10.4 Получить список серийных номеров действующих сертификатов, выпущенных для субъекта аутентификации, по его id.....	104
10.5 Получить список серийных номеров сертификатов, выпущенных для субъекта аутентификации, отфильтрованных по статусу сертификатов .....	104
10.6 Получить список Id групп субъекта аутентификации.....	104
10.7 Получить список шаблонов сертификатов активного УЦ, доступных субъекту аутентификации .....	105
10.8 Изменить субъект аутентификации .....	105
10.9 Добавить субъект в заданную группу .....	106
10.10 Исключить субъект из заданной группы .....	106
10.11 Явно задать группы, в которых состоит субъект аутентификации.....	107
10.12 Удалить субъект аутентификации .....	107
10.13 Получить информацию о списке доступных групп субъектов аутентификации	108
10.14 Получить информацию о группе субъектов аутентификации по id.....	108
10.15 Получить список субъектов, состоящих в группе субъектов аутентификации	109
10.16 Получить список шаблонов сертификата, доступных текущему активному центру сертификации .....	109
10.17 Получить детальное описание шаблона сертификата субъекта аутентификации .....	109
10.18 Получить сертификат по CSR для нового субъекта аутентификации .....	112
10.19 Получить сертификат по CSR для заданного субъекта аутентификации .....	115
10.20 Получить состояние сертификата по его серийному номеру.....	117
10.21 Приостановить действие сертификата.....	117

10.22	Возобновить действие сертификата.....	118
10.23	Отозвать сертификат.....	118
11	Контакты .....	120
11.1	Офис (общие вопросы) .....	120
11.2	Техподдержка .....	120
	Лист регистрации изменений .....	121

# 1 О ДОКУМЕНТЕ

## 1.1 Назначение документа

Настоящий документ представляет собой руководство администратора Центра сертификатов доступа Aladdin Enterprise Certificate Authority.

## 1.2 На кого ориентирован данный документ

Документ предназначен для администраторов ПО "Центра сертификатов доступа Aladdin Enterprise Certificate Authority", регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств.

## 1.3 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве ознакомительного материала (подробного руководства по установке и настройке ПО «Центра сертификатов доступа Aladdin Enterprise Certificate Authority»), а также в качестве справочника при работе с ПО «Центра сертификатов доступа Aladdin Enterprise Certificate Authority».


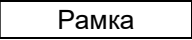
Документ рекомендован как для последовательного, так и для выборочного изучения.

## 1.4 Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 1.

Таблица 1 — Элементы оформления

[Поле]	Используется для выделения наименований полей, блоков, закладок экранных форм
<Кнопка>	Используется для выделения наименований кнопок
Меню:	Используется для выделения наименований пунктов меню
Ctrl+X	Используется для выделения сочетаний клавиш
<code>file.exe</code>	Используется для выделения имен файлов, каталогов, текстов программ
Термин	Используется для выделения первого и последующих вхождений определяемого в документе термина в тексте документа

<b>Выделение</b>	Используется для выделения отдельных значимых слов и фраз в тексте
Ссылка (Рисунок 5)	Используется для выделения перекрестных ссылок
 <i>Важно</i>	Используется для выделения информации, на которую следует обратить внимание
 Рамка	Используется для выделения важной информации, вывод, резюме

## 1.5 Обозначения и сокращения

Таблица 2 — Обозначения и сокращения

<b>ОС</b>	Операционная система.
<b>ПО</b>	Программное обеспечение.
<b>СУБД</b>	Система управления базами данных.
<b>УЦ</b>	Удостоверяющий центр.
<b>ЦС</b>	Центр сертификатов.
<b>АеСА, Aladdin eCA</b>	Центр сертификатов доступа Aladdin Enterprise Certificate Authority
<b>АеСА VA</b>	Aladdin Enterprise Certificate Authority Validation Authority
<b>CRL</b>	Certificate Revocation List
<b>AIA</b>	Authority Information Access
<b>URL</b>	Uniform Resource Locator

## 1.6 Ключевые слова

**Администратор безопасности** – сотрудник (специалист) и соответствующая роль в центре сертификации отвечающая за администрирование и управление настройками изделия. Физическое лицо (уполномоченный пользователь), имеющее роль «Администратор», должно быть указано в организационно-распорядительных документах организации, эксплуатирующей ПО.

**Администратор инициализации** – 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.

**Корневой ЦС** – экземпляр центра сертификации в информационной системе, имеющий абсолютное доверие со стороны всех участников процесса строгой

аутентификации. С точки зрения службы безопасности предприятия должен быть обеспечен максимальным уровнем защиты (отдельный ПК, отключённый от сети, с доступом ограниченного круга лиц). Корневой ЦС владеет само подписанным сертификатом, который должен распространяться доверенным способом в информационной системе.

**Крипто-токен** – 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.

**Подчиненный ЦС** – экземпляр центра сертификации в информационной системе, обладающий функцией управления политиками строгой аутентификации или функцией управления жизненным циклом сертификатов доступа субъектов информационной системы. Подчиненный ЦС владеет сертификатом, выданным вышестоящим ЦС (корневым или другим подчиненным), который используется для проверки всей цепочки доверия сертификатов доступа.

**Права доступа** – набор возможных действий, которые субъекты доступа могут выполнять над субъектами доступа в конкретной среде функционирования.

**Сервис валидации** – служба, составная часть Центра сертификации, отвечающая за предоставление информации о действительности сертификатов доступа. Предоставляет сервисы CRL DP, OCSP.

**Сервис регистрации** – служба, составная часть Центра сертификации, отвечающая за обработку запросов на выдачу сертификатов от субъектов информационной системы.

**Сервис сертификатов** – служба, составная часть Центра сертификации, непосредственно отвечающая за жизненный цикл сертификатов доступа (выдача, отзыв).

**Сертификат или сертификат доступа** – 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.

**Событие безопасности** – идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности.

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

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

**Центр сертификации** – комплекс средств, задача которых заключается в обеспечении жизненного цикла сертификатов доступа пользователей и устройств информационной системы, а также в создании инфраструктуры для обеспечения



процессов идентификации и строгой аутентификации в информационной системе. Центр сертификации является частью Центра сертификатов доступа.

**Шаблон субъекта** – шаблон, на основании которого необходимо создавать субъекты аутентификации. 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.).

**OCSP (Online Certificate Status Protocol)** – онлайн протокол получения статуса сертификата, RFC2560.

## 1.7 Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является субъектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р.Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р.Д.» обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р.Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

### Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р.Д.» без предварительного уведомления.

АО «Аладдин Р.Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р.Д.» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р.Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО «Аладдин Р.Д.» НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р.Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

### Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

## 1.8 Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в АО «Аладдин Р.Д.», удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) — конечным пользователем (далее "Пользователь") — и АО «Аладдин Р.Д.» (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

### Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

### Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуально, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного Соглашения:

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;
- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;
- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;
- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-

либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

### Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (<http://developer.aladdin-rd.ru/>).

### Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;
- встраивать ПО любым способом в продукты и решения Пользователя;
- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникнуть в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);
- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

### Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

### Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

### Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению,

если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелегальным программным обеспечением.

#### **Ограничение возмещения**

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;
- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

#### **Исключение косвенных убытков**

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного ПО, даже если компания письменно уведомлена о возможности подобных убытков.

#### **Ограничение ответственности**

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами АО «Аладдин Р.Д.» за это ПО.

#### **Прекращение действия соглашения**

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;
- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

#### **Применимое законодательство**

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или

Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

#### **Разное**

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ. Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ. ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

## 2 ОСНОВНЫЕ ПОНЯТИЯ

### 2.1 Назначение

ПО «Центр сертификатов доступа Aladdin Enterprise Certificate Authority» (далее - Aladdin eCA) предназначено для защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации для организации процессов идентификации и аутентификации субъектов и субъектов доступа в автоматизированной системе.

### 2.2 Состав

Центр сертификатов доступа Aladdin Enterprise Certificate Authority является программным комплексом и включает:

- компоненты Aladdin Enterprise Certificate Authority, реализующие и представляющие функции доверенной третьей стороны для обеспечения идентификации и аутентификации субъектов и субъектов доступа;
- компонент Программный токен, реализующий криптографические механизмы для строгой аутентификации;
- база данных.

### 2.3 Основные режимы работы

ПО Aladdin eCA поддерживает следующие режимы работы:

- Оператор. Оператору доступны действия:
  - просмотра субъектов (база данных субъектов и групп накапливается путем синхронизации базы с взаимодействующими информационными системами);
  - выпуска сертификатов для субъектов.

Для конкретного «Оператора» можно определить перечень групп субъектов, над которыми он может осуществлять свои ролевые права.

- Администратор. Администратор имеет неограниченные права. Также кроме доступа к функциональным задачам, администратор получает доступ к функциям управления учетными записями. Учетные записи могут быть созданы, отредактированы, удалены или заблокированы администратором.

## 3 СИСТЕМНЫЕ ТРЕБОВАНИЯ

### 3.1 Требования к программному обеспечению

Для работы ПО Aladdin Enterprise Certificate Authority на компьютере требуется предустановленное программное обеспечение:

- сервер приложений WildFly v.18;
- набор спецификаций Java EE v.5 или v.8;
- среда исполнения Java Liberica JDK v.7 или v.8;
- браузер Firefox Browser v. 75.18.0esr (64-битный) и выше;
- СУБД:
  - PostgreSQL 12.9 для RED OS;
  - PostgreSQL 11.10 (Debian 11.10-astra.se5) для ASTRA LINUX;
- ОС Linux:
  - Astra Linux 1.7 Смоленск;
  - RED OS 7.3.

### 3.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования ПО:

- свободное дисковое пространство – не менее 40 Гб;
- доступная оперативная память – не менее 4 Гб;
- процессор с архитектурой x86, x64 (кроме архитектур IA-32, IA-64; процессоров AMD до Athlon 64; процессоров Intel до Pentium; архитектур VIA C3; архитектур Transmeta Crusoe);
- VGA-совместимый видеоадаптер;
- монитор с поддерживаемым разрешением экрана:
  - 1920x1080 16:9 HD 1080;
  - 1366x768 HD
  - 1536x864
  - 1440x900 8:5 WSXGA
  - 2560x1440;
  - 1280x720 16:9 HD 720
  - 1600x900 16:9 HD+ 900p

- 1680x1050 8:5 WSXGA+;
- 1280x1024 5:4 SXGA;
- 1280x800 8:5 WXGA;
- 1920x1200 8:5 WUXGA;
- устройства взаимодействия с пользователем:
  - клавиатура;
  - мышь;
- usb 2.0 тип А или совместимые.

## 4 ОСНОВНЫЕ СВЕДЕНИЯ

### 4.1 Комплект поставки

4.1.1 Комплект поставки включает в себя:

- центр сертификации Aladdin eCA (rpm-пакет для установки на ОС RED OS 7.3 и deb-пакет для установки на Astra 1.7 Smolensk);
- центр валидации Aladdin eCA (rpm-пакет для установки на ОС RED OS 7.3 и deb-пакет для установки на Astra 1.7 Smolensk).

4.1.2 Комплект поставки должен быть развернут на одной из предварительно установленной ОС:

- RED OS 7.3 (5.10.29-1.el7.x86\_64)
- Astra 1.7 Smolensk (5.4.0-54-generic) в конфигурации “Минимальный сервер” с опцией SSH-сервер и уровнем безопасности «Базовая защита».

4.1.3 Комплект поставки содержит пакеты следующего формата:

• <name>	- название изделия;
• <major_version>	- мажорная версия Изделия;
• <minor_version>	- минорная версия Изделия;
• <release>	- номер релиза Изделия;
• <build_number>	- номер сборки;
• <arch>	- целевая архитектура.



## 5 ПОДГОТОВКА К УСТАНОВКЕ ПО ALADDIN ECA

### 5.1 Подключение репозитория и установка зависимостей

#### 5.1.1 Подключение репозитория

Перед началом установки изделия необходимо установить пути нахождения всех необходимых репозитория.

5.1.1.1 Для ОС **RedOS 7.3** репозитории настроены по умолчанию для скачивания из сети Интернет. Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС, выполнив команды:

```
sudo yum install -y git wget ant psmisc bc patch java-1.8.0-openjdk-devel  
sudo yum install tar unzip
```

При ошибке следует проверить наличие интернет-соединения.

5.1.1.2 Для ОС **AstraLinuxSE 1.7** репозитории настроены по умолчанию для скачивания DVD-диска. Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС, выполнив команды:

```
sudo apt install -y git wget ant psmisc bc patch java-1.8.0-openjdk-devel  
sudo apt install tar unzip
```

В процессе установки может потребоваться вставить и заменить диск на нужный диск с репозиторием (“диск 1”, “диск 2”, “develop”).

#### 5.1.2 Установка Liberica JDK v.8

Помимо загруженных зависимостей должен быть установлен компонент Liberica JDK v.8 (не входит в состав установочного комплекта, предоставляется отдельно).

##### 5.1.2.1 Установка Liberica JDK v.8 для **RedOS 7.3**

- Выполните настройку репозитория:

```
echo | sudo tee /etc/yum.repos.d/bellsoft.repo > /dev/null << EOF  
[BellSoft]  
name=BellSoft Repository  
baseurl=https://yum.bell-sw.com  
enabled=1  
gpgcheck=1  
gpgkey=https://download.bell-sw.com/pki/GPG-KEY-bellsoft  
priority=1  
EOF
```

- Обновите репозитории, выполнив команду:

```
sudo yum update
```

- Установите Liberica JDK из предоставленного файла, выполнив команду:

```
sudo yum install bellsoft-java8
```

После чего компоненты Liberica JDK будут установлены в каталог **/usr/lib/jvm/bellsoft-java8-amd64**.

#### 5.1.2.2 Установка Liberica JDK v.8 для **AstraLinuxSE 1.7**

- Перед установкой Liberica JDK нужно произвести добавление GPG-ключа и настройку репозитория, выполнив команды:

```
wget -q -O - https://download.bell-sw.com/pki/GPG-KEY-bellsoft | sudo apt-key add -  
echo "deb [arch=amd64] https://apt.bell-sw.com/ stable main" | sudo tee  
/etc/apt/sources.list.d/bellsoft.list
```

- Обновите репозитории, выполнив команду:

```
sudo apt-get update
```

- Установите Liberica JDK из предоставленного файла, выполнив команду:

```
sudo dpkg -i bellsoft-jdk8u312+7-linux-amd64.deb
```

После чего компоненты Liberica JDK будут установлены в каталог **/usr/lib/jvm/bellsoft-java8-amd64**.

## 5.2 Настройка СУБД и подготовка базы данных

Требования к настройке предварительно установленной СУБД PostgreSQL (для RED OS – версия 12.9, для ASTRA LINUX – версия 11.10):

- создание пользователя, от имени которого будет осуществляться всё взаимодействие с СУБД;
- создание базы данных, используемой Изделием в процессе работы;
- созданному пользователю должны быть назначены полные права доступа к созданной базе данных.

Возможно использование локальной СУБД или удаленной, доступной для подключений.

### 5.2.1 Предварительная установка и инициация БД на ОС RED OS

Для стабильной работы приложения на ОС RED OS должна быть установлена СУБД PostgreSQL версия 12.9.

- 5.2.1.1 Для установки СУБД PostgreSQL выполнить команду:

```
sudo dnf install postgresql-server
```

5.2.1.2 Произвести инициализацию БД, выполнив команду:

```
sudo postgresql-setup --initdb
```

5.2.1.3 Для успешного локального подключения пользователя к базе данных нужно отредактировать файл `/var/lib/pgsqli/data/pg_hba.conf` и изменить параметры:

```
sudo nano /var/lib/pgsqli/data/pg_hba.conf
```

В открывшемся файле `pg_hba.conf` сделать замены согласно Таблица 3:

Таблица 3 – Выдержка из файла `pg_hba.conf` для редактирования

<code>local all all peer</code>	на	<code>local all all trust</code>
<code>host all all 127.0.0.1/32 ident</code>	на	<code>host all all 127.0.0.1/32 password</code>
<code>host all all ::1/128 ident</code>	на	<code>host all all ::1/128 password</code>

После вышеуказанных изменений строки должны иметь следующий вид:

```
local          all          all          trust

#IPv4 local connection:

host          all          all          127.0.0.1/32 password

#IPv6 local connection:

host          all          all          ::1/128     password
```

5.2.1.4 Сохранить изменения.

5.2.1.5 Для запуска PostgreSQL выполнить команду:

```
sudo systemctl start postgresql
```

5.2.1.6 Для добавления запуска PostgreSQL в автозагрузку выполнить команду:

```
sudo systemctl enable postgresql
```

5.2.1.7 Далее необходимо зайти под пользователем «postgres» в PostgreSQL, выполнив команду:

```
sudo -i -u postgres
```

5.2.1.8 Создать пользователя, выполнив команды:

```
psql
CREATE USER aeca;
```

Здесь и далее, для примера, задан пользователь «аеса».

5.2.1.9 Задать пароль пользователю, выполнив команды:

```
ALTER USER aeca WITH PASSWORD 'aeca';
```

Здесь и далее, для примера, задан пароль «аеса».

5.2.1.10 Создать базу данных, выполнив команды:

```
CREATE DATABASE aecatest;
```

Здесь и далее, для примера, задано название базы данных «aecatest».

5.2.1.11 Назначить владельцем созданной базы данных «aecatest» созданного пользователя «аеса», выполнив команду:

```
ALTER DATABASE aecatest OWNER TO aeca;
```

5.2.1.12 Наделить пользователя «аеса» полными правами доступа к созданной базе «aecatest», выполнив команду:

```
GRANT ALL PRIVILEGES ON DATABASE aecatest TO aeca;
```

5.2.1.13 Назначить пользователя аеса суперпользователем и завершить действия, выполнив команды:

```
ALTER USER aeca SUPERUSER;
```

```
\q
```

5.2.1.14 Далее необходимо завершить работу под пользователем «postgres» и выйти из терминала, выполнив команду:

```
exit
```

5.2.1.15 Перезапустить СУБД PostgreSQL, выполнив команду:

```
sudo systemctl restart postgresql
```

## 5.2.2 Предварительная установка и инициация БД на Astra Linux

Для стабильной работы приложения на ОС Astra Linux должна быть установлена СУБД PostgreSQL версия 11.10.

5.2.2.1 Для установки СУБД PostgreSQL выполнить команду в окне (см. Рисунок 1):

```
sudo apt update
```

```
sudo apt install postgresql-11
```

```

user@astrastandaloneca:~$ sudo apt update
Сущ:1 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 devel-2 DVD 1.7_x86-64 InRelease
Сущ:2 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 devel-1 DVD 1.7_x86-64 InRelease
Игн:3 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 DVD 1.7_x86-64 InRelease
Сущ:4 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 DVD 1.7_x86-64 Release
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.

```

Рисунок 1 – Окно ввода команды установки СУБД

5.2.2.2 Для создания пользователя СУБД PostgreSQL, который не назначен в ОС Astra Linux, откройте файл **/etc/parsec/mswitch.conf** и **измените параметр:**

zero\_if\_notfound: no    на    zero\_if\_notfound: yes

После вышеуказанных изменений строки должны иметь следующий вид:

zero\_if\_notfound: yes

5.2.2.3 Для вступления изменений в силу, произвести перезапуск СУБД PostgreSQL, выполнив последовательно команды:

```

sudo systemctl start postgresql
sudo systemctl enable postgresql

```

5.2.2.4 Для успешного локального подключения пользователя к базе данных нужно отредактировать файл **/etc/postgresql/11/main/pg\_hba.conf** и изменить параметры:

local all all peer    на    local all all trust

5.2.2.5 Сохранить изменения и выполнить перезапуск СУБД PostgreSQL для вступления изменений в силу, выполнив команду:

```

sudo systemctl restart postgresql

```

5.2.2.6 Далее необходимо зайти под пользователем «postgres» в СУБД PostgreSQL, выполнив команду:

```

sudo -i -u postgres

```

5.2.2.7 Создать пользователя и задать пароль пользователю аеса, выполнив команды:

```

psql
CREATE USER aeca;
ALTER USER aeca WITH PASSWORD 'aeca';
CREATE DATABASE aecatest;

```

5.2.2.8 Назначить пользователя аеса суперпользователем, выполнив команды:

```

ALTER DATABASE aecatest OWNER TO aeca;

```

```
GRANT ALL PRIVILEGES ON DATABASE aecatest TO aeca;  
  
ALTER USER aeca SUPERUSER;  
  
\q
```

5.2.2.9 Далее необходимо завершить работу под «суперпользователем» и выйти из терминала, выполнив команду:

```
exit
```

## 5.3 Распаковка инсталляционного комплекта AeCA CA

**Внимание!** Перед установкой необходимо подключить репозиторий компании для подгрузки зависимостей программного продукта.

Необходимые для корректной установки зависимости (git, wget, tar, unzip, ant, psmisc, bc, patch, java-1.8.0-openjdk-devel) будут загружены из репозитория целевой ОС из сети Интернет и установлены автоматически. Помимо загруженных зависимостей должен быть скачен компонент Liberica JDK v.8 и установлен в директорию /usr/lib/jvm/bellsoft-java8-amd64.

### 5.3.1 Подготовка к установке Изделия

- **на ОС RED OS** необходимо выполнить следующую команду, находясь в папке, где расположен пакет .rpm (см. рисунок 3):

```
sudo dnf install ./ <наименование пакета>.rpm;
```

Например:

```
sudo dnf install ./aeca-CA-0.0-0.x86_x64.rpm;
```

- **на ОС ASTRA LINUX** необходимо выполнить следующую команду (см. Рисунок 2):

```
sudo apt install ./ <наименование пакета>.deb;
```

Например:

```
sudo apt install ./aeca-CA-0.0-0.x86_x64.deb;
```

```

user@astrastandaloneca:~/Загрузки$ sudo apt install ./aeca_1.1.0.101_amd64.deb
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Заметьте, вместо «./aeca_1.1.0.101_amd64.deb» выбирается «aeca»
Будут установлены следующие дополнительные пакеты:
  ant ant-optional ca-certificates-java default-jre-headless java-common
  openjdk-11-jre-headless
Предлагаемые пакеты:
  ant-doc antlr javacc junit junit4 jython libactivation-java libbccl-java libbsf-java
  libcommons-logging-java libcommons-net-java libmail-java libjaxp1.3-java libjdepend-java
  libjsch-java liblog4j1.2-java liboro-java libregexp-java libxalan2-java
  libxml-commons-resolver1.1-java libxz-java default-jre libnss-mdns fonts-dejavu-extra
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei fonts-indic
Следующие NOBBIE пакеты будут установлены:
  aeca ant ant-optional ca-certificates-java default-jre-headless java-common
  openjdk-11-jre-headless
Обновлено 0 пакетов, установлено 7 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов н
е обновлено.
Необходимо скачать 0 В/341 МВ архивов.
После данной операции объём занятого дискового пространства возрастёт на 175 МВ.
Хотите продолжить? [Д/н] y
Смена носителя: Вставьте диск с меткой
«OS Astra Linux 1.7.0 1.7_x86-64 devel-1 DVD»
В устройство «/media/cdrom/» и нажмите [Enter]

```

Рисунок 2 – Окно установки

### 5.3.2 Инсталляционный комплект будет автоматически распакован в директорию:

```
/opt/ <наименование пакета>
```

Например:

```
/opt/aeca-0.0-0/
```

5.3.3 В выбранном каталоге (далее в качестве примера будет использоваться значение `/opt/aeca-0.0-0/`) будет размещён установочный комплект Изделия. Структура установочного комплекта Изделия приведена в Таблица 4.

Таблица 4 – Структура установочного комплекта Изделия

Структурный элемент	Назначение элемента
../dist	установочный комплект Изделия, а также используемых дополнительных инструментов
../dist/aeca_plugins.tar.gz	архив, содержащий плагин центра сертификации AeCA
../dist/db_connectors.tar.gz	архив, содержащий набор драйверов, необходимых для работы WildFly с различными СУБД
../dist/sql	автоматически выполняемые при установке наборы SQL-запросов для подготовки БД
../dist/wildfly	автоматически развёртываемые при установке файлы конфигурации WildFly
../dist/ejbca_ce_7_4_3_2.tar.gz	архив, содержащий оригинальный установочный комплект EJBCA 7.4.3.2
../dist/wildfly-18.0.0.Final.tar.gz	архив, содержащий оригинальный установочный комплект WildFly 18

Структурный элемент	Назначение элемента
<code>../properties</code>	шаблоны файлов настроек
<code>../scripts</code>	установочные скрипты, которые необходимо выполнить пользователю при установке Изделия
<code>../scripts/auxiliary_aeca_setup.sh</code>	скрипт установки AeCA
<code>../scripts/auxiliary_aeca_database_setup.sh</code>	скрипт подготовки структуры БД для AeCA
<code>../scripts/auxiliary_ejbca_database_setup.sh</code>	скрипт подготовки структуры БД для EJBCA
<code>../scripts/auxiliary_aeca_database_cleanup.sh</code>	скрипт очистки структуры БД для AeCA перед повторной установкой
<code>../scripts/auxiliary_ejbca_database_cleanup.sh</code>	скрипт очистки структуры БД для EJBCA перед повторной установкой
<code>../scripts/auxiliary_default_properties_setup.sh</code>	скрипт конфигурирования файлов настроек EJBCA из шаблонов
<code>../scripts/auxiliary_ejbca_setup.sh</code>	скрипт установки EJBCA
<code>../scripts/auxiliary_wildfly_setup.sh</code>	скрипт установки Wildfly
<code>../scripts/config.sh</code>	скрипт установки параметров
<code>../scripts/install.sh</code>	скрипт установки «Центра сертификации AeCA»
<code>../scripts/uninstall.sh</code>	скрипт удаления «Центра сертификации AeCA»

Владельцем распакованных файлов будет являться пользователь «root», другие пользователи не будут иметь прав доступа к инсталляционному комплекту.

5.3.4 Отредактировать конфигурационный файл `/opt/aeca-CA-0.0-0/scripts/config.sh`, выполнив команду:

```
sudo nano /opt/aeca-CA-0.0-0/scripts/config.sh
```

В случае, если база данных установлена на другое ПК, то изменить значение в поле `[aeca_httpsserver_hostname]` на «host».

В поле `[aeca_httpsserver_hostname]` указывается сетевое имя машины, на которую производится установка AeCA CA.

В Таблица 5 приводится описание параметров конфигурации.

Таблица 5 – Описание параметров конфигурации



Параметр	Значение параметра по умолчанию	Описание
aeca_httpserver_hostname	"localhost"	Имя, которое будет использовать веб-сервер
aeca_install_directory	"/opt/aeca"	Директория, в которую будет осуществляться установка Изделия
aeca_user	"aeca"	Имя пользователя, от имени которого будет функционировать Изделие (пользователь будет создан в процессе установки)
aeca_database_type	"postgres "	Тип используемой СУБД
aeca_database_username	"ejbca"	Имя пользователя СУБД, используемого для работы Изделия
aeca_database_password	"ejbca"	Пароль пользователя СУБД используемого для работы Изделия
aeca_database_host	"localhost"	Сетевой адрес СУБД
aeca_database_port	"5432"	Порт, используемый для подключения к базе данных
aeca_database_name	"ejbcatest"	Имя используемой Изделием базы данных в указанной СУБД
aeca_BASE_DN	"O=Aladdin test AECA CA,C=RU"	Базовое назначаемое имя, где: O=наименование организационной единицы C=страна
aeca_superuser_cn	"InitialAdmin"	Наименование первоначально создаваемого администратора инициализации
aeca_ca_name	"ManagementTestCA"	Наименование первоначально создаваемого центра сертификации

## 5.4 Распаковка инсталляционного комплекта AeCA VA

**Внимание!** Перед установкой необходимо подключить репозиторий компании для подгрузки зависимостей программного продукта.

Необходимые для корректной установки зависимости (git, wget, tar, unzip, ant, psmisc, bc, patch, java-1.8.0-openjdk-devel) будут загружены из репозитория целевой ОС из сети Интернет и установлены автоматически. Помимо загруженных зависимостей должен быть скачен компонент Liberica JDK v.8 и установлен в директорию /usr/lib/jvm/bellsoft-java8-amd64.

### 5.4.1 Подготовка к установке Изделия:

- на **ОС RED OS** необходимо выполнить следующую команду, находясь в папке, где расположен пакет .rpm (см. рисунок 3):

```
sudo dnf install ./ <наименование пакета>.rpm;
```

Например:

```
sudo dnf install ./aeca-VA-0.0-0.x86_x64.rpm;
```

- на ОС **ASTRA LINUX** необходимо выполнить следующую команду (см. **Рисунок 2**):

```
sudo apt install ./<наименование пакета>.deb;
```

Например:

```
sudo apt install ./aeca-VA-0.0-0.x86_x64.deb;
```

5.4.2 Инсталляционный комплект будет автоматически распакован в директорию:

```
/opt/ <наименование пакета>
```

Например:

```
/opt/aeca-va-0.0-0/
```

5.4.3 В выбранном каталоге (далее в качестве примера будет использоваться значение `/opt/aecaVA/`) будет размещён установочный комплект Изделия. Структура установочного комплекта Изделия приведена в Таблица 6.

Таблица 6 – Структура установочного комплекта Изделия

Структурный элемент	Назначение элемента
../dist	установочный комплект Изделия, а также дополнительно используемых инструментов
../dist/aeca_plugins.tar.gz	архив, содержащий плагин центра валидации AeCA
../dist/db_connectors.tar.gz	архив, содержащий набор драйверов, необходимых для работы WildFly с различными СУБД
../dist/sql	автоматически выполняемые при установке наборы SQL-запросов для подготовки БД
../dist/wildfly	автоматически развёртываемые при установке файлы конфигурации WildFly
../dist/ejbca_ce_7_4_3_2.tar.gz	архив, содержащий оригинальный установочный комплект EJBCA 7.4.3.2
../dist/wildfly-18.0.0.Final.tar.gz	архив, содержащий оригинальный установочный комплект WildFly 18
../properties	шаблоны файлов настроек
../scripts	установочные скрипты, которые необходимо выполнить пользователю при установке Изделия
../scripts/auxiliary_aeca_setup.sh	скрипт установки AeCA
../scripts/auxiliary_aeca_database_setup.sh	скрипт подготовки структуры БД для AeCA
../scripts/auxiliary_ejbca_database_setup.sh	скрипт подготовки структуры БД для EJBCA

Структурный элемент	Назначение элемента
<code>../scripts/auxiliary_aeca_database_cleanup.sh</code>	скрипт очистки структуры БД для AeCA перед повторной установкой
<code>../scripts/auxiliary_ejbca_database_cleanup.sh</code>	скрипт очистки структуры БД для EJBCA перед повторной установкой
<code>../scripts/auxiliary_default_properties_setup.sh</code>	скрипт конфигурирования файлов настроек EJBCA из шаблонов
<code>../scripts/auxiliary_ejbca_setup.sh</code>	скрипт установки EJBCA
<code>../scripts/auxiliary_wildfly_setup.sh</code>	скрипт установки Wildfly
<code>../scripts/config.sh</code>	скрипт установки параметров
<code>../scripts/install.sh</code>	скрипт установки «Центра валидации AeCA»
<code>../scripts/uninstall.sh</code>	скрипт удаления «Центра валидации AeCA»

Владельцем распакованных файлов будет являться пользователь «root», другие пользователи не будут иметь прав доступа к инсталляционному комплекту.

5.4.4 Отредактировать конфигурационный файл `/opt/aecaVa/scripts/config.sh`, выполнив команду:

```
sudo nano /opt/aecaVA/scripts/config.sh
```

В случае, если база данных установлена на другое ПК, то изменить значение в поле `[aeca_httpsserver_hostname]` на `[host]`.

## 6 УСТАНОВКА ПО ALADDIN ECA

### 6.1 Установка ПО «Центр сертификации» Aladdin Enterprise CA

#### 6.1.1 Инициализация процесса установки AeCA CA

Для инициализации процесса установки Изделия необходимо запустить скрипт с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo bash /opt/aecaCa/scripts/install.sh
```

В случае запуска от имени пользователя, не имеющего соответствующих привилегий, будет выведено сообщение, после которого работа инсталлятора завершится:

```
"This script must be run as root!"
```

#### 6.1.2 Процесс установки AeCA CA

**ВНИМАНИЕ! В процессе установки все действия подтверждаются выбором пункта ([Yes], [No] или [Cancel]) посредством нажатия соответствующей цифры ( 1, 2 или 3 соответственно).**

После инициализации процесса установки интерактивный инсталлятор запущен автоматически выполняются действия, описанные в шагах 6.1.2.1 – 6.1.2.7.

##### 6.1.2.1 Автоматическая проверка на наличие установленного компонента – Liberica JDK v.8.

В случае, если компонент Liberica JDK v.8 отсутствует, пользователь будет уведомлен о невозможности продолжить установку. Процесс установки будет прекращен.

6.1.2.2 Создание системного пользователя (если не существует) и соответствующей группы, от имени которых будет функционировать Изделие. Будет создана systemd-служба `aeca.service`, функционирующая от имени заданного пользователя.

6.1.2.3 Пользователю будет предложено сформировать файлы конфигурации пакета ПО центра сертификации EJBCA из шаблонов в `/opt/aeca-CA-0.0-0/properties` на основе значений, заданных в пункте 5.3.4 в `/opt/aeca-CA-0.0-0/scripts/config.sh`.

Для более тонкой настройки EJBCA возможно ручное редактирование данных файлов в соответствии с руководствами по эксплуатации EJBCA. Автоматически будут заменены только параметры со значением CHANGEIT:

- при выборе пункта `[Yes]` будет осуществлена замена CHANGEIT на значения из конфигурационного файла `/opt/aeca-CA-0.0-0/scripts/config.sh`;
- при выборе пункта `[No]` будут использоваться файлы конфигурации в неизменном виде;

**ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеются корректно сформированные `.properties` файлы конфигурации EJBCA, которые должны быть скопированы в каталог `/opt/aeca-CA-0.0-0/properties` с заменой существующих файлов.**

- при выборе пункта `[Cancel]` установка будет прекращена.

6.1.2.4 Пользователю будет предложено установить сервер приложений Java EE:

- при выборе пункта [Yes] будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки сервера приложений Java EE Wildfly-18.0.0.Final с подробным выводом процесса установки и конфигурирования сервера приложений в консоль пользователя;
- при выборе пункта [No] установка сервера приложений Java EE будет пропущена;

**ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеется корректно настроенный сервер приложений, функционирующий по пути, указанному в параметре `aesa_appserver_home` скрипта конфигурации `/opt/aesa-CA-0.0-0/scripts/config.sh`**

- При выборе пункта [Cancel] установка будет прекращена.

6.1.2.5 Пользователю будет предложено установить пакет ПО центра сертификации EJBCA CE 7.4.3.2:

- при выборе пункта [Yes] будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки пакета ПО EJBCA CE 7.4.3.2 с подробным выводом процесса установки и конфигурирования в консоль пользователя;
- при выборе пункта [No] установка EJBCA будет пропущена;

**ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеется корректно настроенный EJBCA CE 7.4.3.2, функционирующий по пути, указанному в параметре `aesa_ejbsa_home` скрипта конфигурации `/opt/aesa-CA-0.0-0/scripts/config.sh`**

- при выборе пункта [Cancel] установка будет прекращена.

6.1.2.6 Пользователю будет предложено установить центр сертификатов доступа Aladdin eCA соответствующей версии:

- при выборе пункта [Yes] будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки Aladdin eCA;
- при выборе пункта [No] установка Aladdin eCA будет пропущена;
- при выборе пункта [Cancel] установка будет прекращена.

6.1.2.7 После завершения установки в директории, выбранной в качестве пути для установки, будут содержаться:

- файл «`generated_passwords.txt`» (по умолчанию, расположен по пути `/opt/aesa/generated_passwords.txt`), содержащий все созданные и используемые пароли;
- каталог «`p12`» (по умолчанию, расположен по пути `/opt/aesa/p12/superadmin.p12`), содержащий сертификат "Администратора Инициализации", необходимый для дальнейшей аутентификации через Web. Более подробно шаги по аутентификации через Web описаны в пункте 7.1 настоящего руководства.

6.1.2.8 В процессе установки в случае возникновения ошибки установка будет прекращена, сообщение об ошибке будет выведено в консоль пользователя.

### 6.1.3 Дополнительные возможные действия при установке

6.1.3.1 Так как предусмотрен модульный процесс установки, возможны различные варианты установки:

- возможно использование заранее подготовленных файлов настроек пакета ПО центра сертификации EJBCA;
- если в каталоге «properties» уже находятся файлы конфигурации, необходимые пользователю, то при установке возможно пропустить шаг их формирования, ответив отрицательно за запрос инсталлятора;
- возможно использование заранее подготовленного и корректно настроенного существующего сервера приложений WildFly. Для этого путь, по которому он размещён, должен соответствовать пути, описанному в config.sh. При установке возможно пропустить данный шаг, ответив отрицательно на запрос инсталлятора;
- возможно использование заранее подготовленного и корректно настроенного установленного пакета ПО EJBCA, если путь, по которому он размещён, соответствует пути, описанному в config.sh. При установке возможно пропустить данный шаг, ответив отрицательно за запрос инсталлятора.
- каждый шаг установки можно выполнить отдельно или повторно, запустив соответствующий скрипт:

```
auxiliary<наименование_действия>.sh;
```

6.1.3.2 В случае отсутствия config.sh или наличие ошибок в config.sh каждый скрипт установки содержит определённые по умолчанию значения, достаточные для его автономной работы.

## 6.2 Установка ПО «Центр валидации» Aladdin Enterprise CA

### 6.2.1 Инициализация процесса установки AeCA VA

Для инициализации процесса установки Изделия необходимо запустить скрипт с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo bash /opt/aecaVA/scripts/install.sh
```

В случае запуска от имени пользователя, не имеющего соответствующих привилегий, будет выведено сообщение, после которого работа инсталлятора завершится:

```
"This script must be run as root!"
```

### 6.2.2 Процесс установки AeCA VA

**ВНИМАНИЕ! В процессе установки все действия подтверждаются выбором пункта ([Yes], [No] или [Cancel]) посредством нажатия соответствующей цифры ( 1, 2 или 3 соответственно).**

После инициализации процесса установки интерактивный инсталлятор запущен автоматически выполняются действия, описанные в шагах 6.2.2.1 – 6.2.2.7.

#### 6.2.2.1 Автоматическая проверка на наличие установленного компонента – Liberica JDK v.8.

В случае, если компонент Liberica JDK v.8 отсутствует, пользователь будет уведомлен о невозможности продолжить установку. Процесс установки будет прекращен.

6.2.2.2 Создание системного пользователя (если не существует) и соответствующей группы, от имени которых будет функционировать Изделие. Будет создана systemd-служба `aeca.service`, функционирующая от имени заданного пользователя.

6.2.2.3 Пользователю будет предложено сформировать файлы конфигурации пакета ПО центра сертификации EJBCA из шаблонов в `/opt/aeca-VA-0.0-0/properties` на основе значений, заданных в пункте 5.4.4 в `/opt/aeca-VA-0.0-0/scripts/config.sh`.

Для более тонкой настройки EJBCA возможно ручное редактирование данных файлов в соответствии с руководствами по эксплуатации EJBCA. Автоматически будут заменены только параметры со значением CHANGEIT:

- при выборе пункта `[Yes]` будет осуществлена замена CHANGEIT на значения из конфигурационного файла `/opt/aeca-VA-0.0-0/scripts/config.sh`;
- при выборе пункта `[No]` будут использоваться файлы конфигурации в неизменном виде;

**ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеются корректно сформированные `.properties` файлы конфигурации EJBCA, которые должны быть скопированы в каталог `/opt/aeca-VA-0.0-0/properties` с заменой существующих файлов.**

- при выборе пункта `[Cancel]` установка будет прекращена.

6.2.2.4 Пользователю будет предложено установить сервер приложений Java EE:

- при выборе пункта `[Yes]` будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки сервера приложений Java EE Wildfly-18.0.0. Final с подробным выводом процесса установки и конфигурирования сервера приложений в консоль пользователя;
- при выборе пункта `[No]` установка сервера приложений Java EE будет пропущена;

**ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеется корректно настроенный сервер приложений, функционирующий по пути, указанному в параметре `aeca_appserver_home` скрипта конфигурации `/opt/aeca-VA-0.0-0/scripts/config.sh`**

- При выборе пункта `[Cancel]` установка будет прекращена.

6.2.2.5 Пользователю будет предложено установить пакет ПО центра сертификации EJBCA CE 7.4.3.2:

- при выборе пункта `[Yes]` будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки пакета ПО EJBCA CE 7.4.3.2 с подробным выводом процесса установки и конфигурирования в консоль пользователя;
- при выборе пункта `[No]` установка EJBCA будет пропущена;

**ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеется корректно настроенный EJBCA CE 7.4.3.2, функционирующий**

по пути, указанному в параметре `aesa_ejbca_home` скрипта конфигурации `/opt/aesa-VA-0.0-0/scripts/config.sh`

- при выборе пункта `[Cancel]` установка будет прекращена.

6.2.2.6 Пользователю будет предложено установить центр сертификатов доступа Aladdin eCA соответствующей версии:

- при выборе пункта `[Yes]` будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки Aladdin eCA;
- при выборе пункта `[No]` установка Aladdin eCA будет пропущена;
- при выборе пункта `[Cancel]` установка будет прекращена.

6.2.2.7 После завершения установки в директории, выбранной в качестве пути для установки, будут содержаться:

- файл «`generated_passwords.txt`» (по умолчанию, расположен по пути `/opt/aesa/generated_passwords.txt`), содержащий все созданные и используемые пароли;
- каталог «`p12`» (по умолчанию, расположен по пути `/opt/aesa/p12/superadmin.p12`), содержащий сертификат "Администратора Инициализации", необходимый для дальнейшей аутентификации через Web. Более подробно шаги по аутентификации через Web описаны в пункте 8.1 настоящего руководства.

6.2.2.8 В процессе установки в случае возникновения ошибки установка будет прекращена, сообщение об ошибке будет выведено в консоль пользователя.

### 6.2.3 Дополнительные возможные действия при установке

6.2.3.1 Так как предусмотрен модульный процесс установки, возможны различные варианты установки:

- возможно использование заранее подготовленных файлов настроек пакета ПО центра сертификации EJBCA;
- если в каталоге «`properties`» уже находятся файлы конфигурации, необходимые пользователю, то при установке возможно пропустить шаг их формирования, ответив отрицательно за запрос инсталлятора;
- возможно использование заранее подготовленного и корректно настроенного существующего сервера приложений WildFly. Для этого путь, по которому он размещён, должен соответствовать пути, описанному в `config.sh`. При установке возможно пропустить данный шаг, ответив отрицательно на запрос инсталлятора;
- возможно использование заранее подготовленного и корректно настроенного установленного пакета ПО EJBCA, если путь, по которому он размещён, соответствует пути, описанному в `config.sh`. При установке возможно пропустить данный шаг, ответив отрицательно за запрос инсталлятора.
- каждый шаг установки можно выполнить отдельно или повторно, запустив соответствующий скрипт:



```
auxiliary<наименование_действия>.sh;
```

6.2.3.2 В случае отсутствия config.sh или наличие ошибок в config.sh каждый скрипт установки содержит определённые по умолчанию значения, достаточные для его автономной работы.

6.2.3.3 Проверить наличие службы и ее статус, выполнив команду:

```
sudo systemctl status aeca.service
```

После установки существует служба `aeca.service` и имеет статус `active`.

## 7 НАСТРОЙКА ПО «ЦЕНТР СЕРТИФИКАЦИИ» ALADDIN ENTERPRISE CA

В результате установки Программного компонента «Центр Сертификации Aladdin eCA» в консоли ОС отобразится информация о конфигурации установленного приложения, а также учетные данные администратора (логин и пароль для первого входа в приложение).

### 7.1 Первичная инициализация Alladin eCA CA

7.1.1 Только для ОС **RED OS 7.3** при необходимости произвести установку браузера Mozilla Firefox, выполнив команду:

```
sudo dnf install firefox
```

7.1.2 Открыть браузер Firefox.

7.1.2 Для импортирования пакета .p12 в браузер из директории [директория\_хранения\_пакета\_p12] выберете меню приложения «Настройки»;

7.1.3 Выбрать вкладку "Приватность и защита", нажать кнопку <Просмотр сертификатов> (см. **Рисунок 3**).

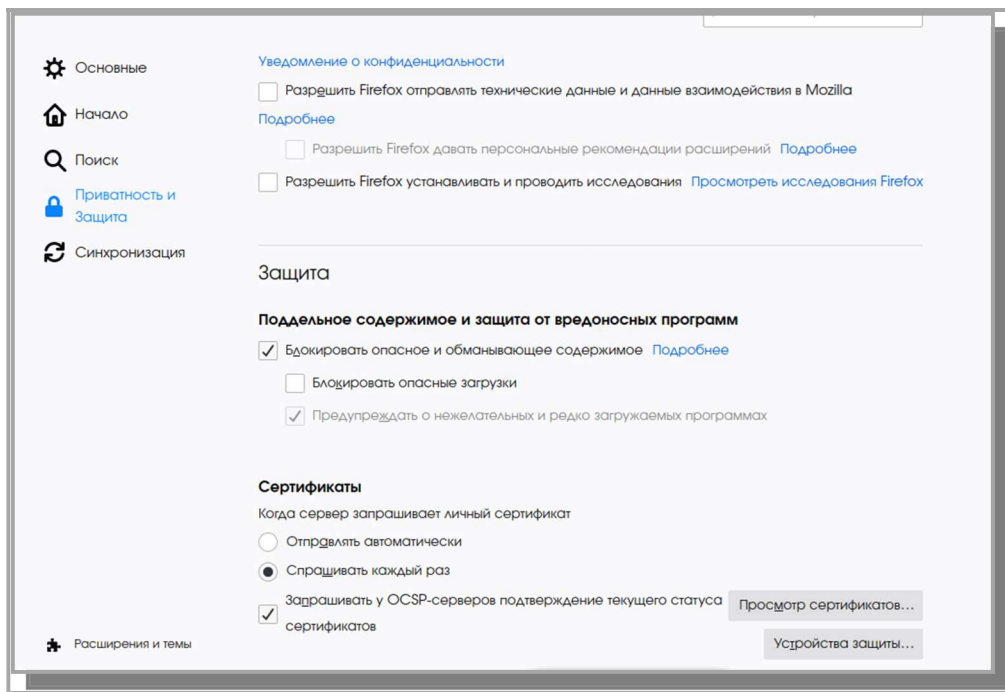


Рисунок 3 – Окно настроек браузера

7.1.4 Выбрать вкладку «Ваши сертификаты», в открывшейся вкладке нажать кнопку <Импортировать> (см. **Рисунок 4**).

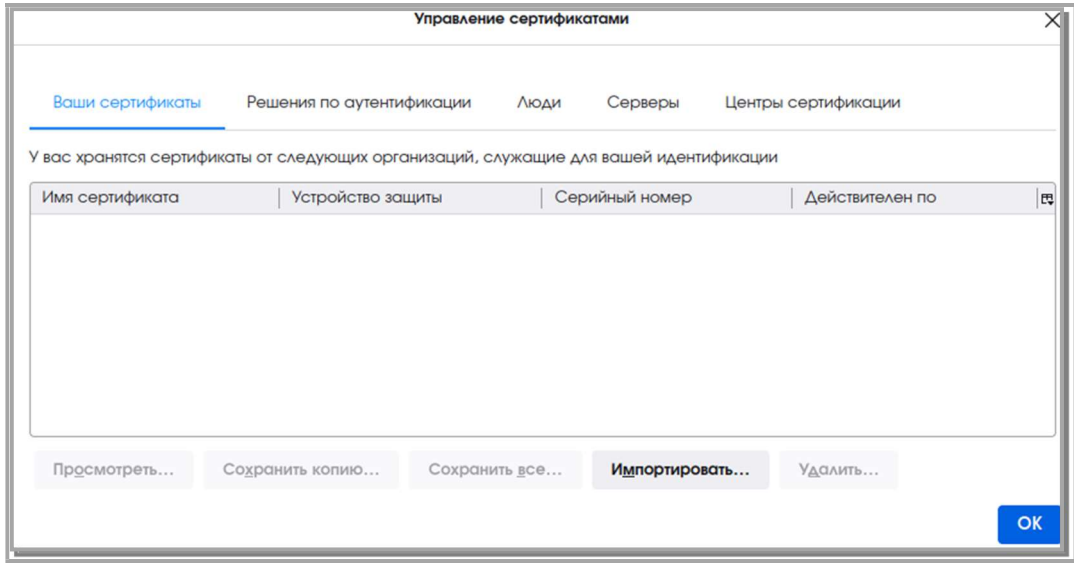


Рисунок 4 – Окно управления сертификатами

7.1.5 В директории хранения пакета. p12 найти созданный на этапе установки файл сертификата `/opt/aeca/p12/superadmin.p12`. Нажать кнопку <Открыть> (см. **Рисунок 5**).

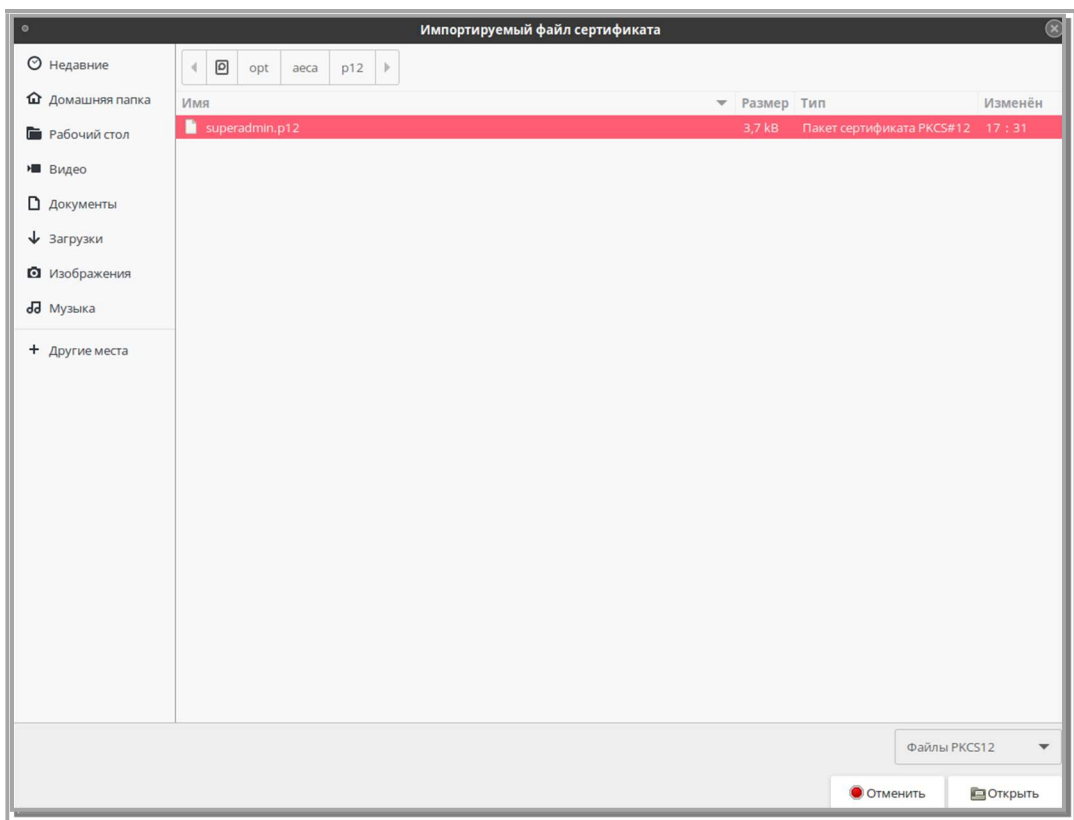


Рисунок 5 – Окно выбора импортируемого файла сертификата

7.1.6 В открывшемся окне (см. Рисунок 6) ввести пин-код сертификата (данные предоставляются по завершению установки, а также доступны в директории установленного приложения `opt\aeca\p12\generated_passwords.txt` – см. **Рисунок 7**). Нажать кнопку <Ок>.

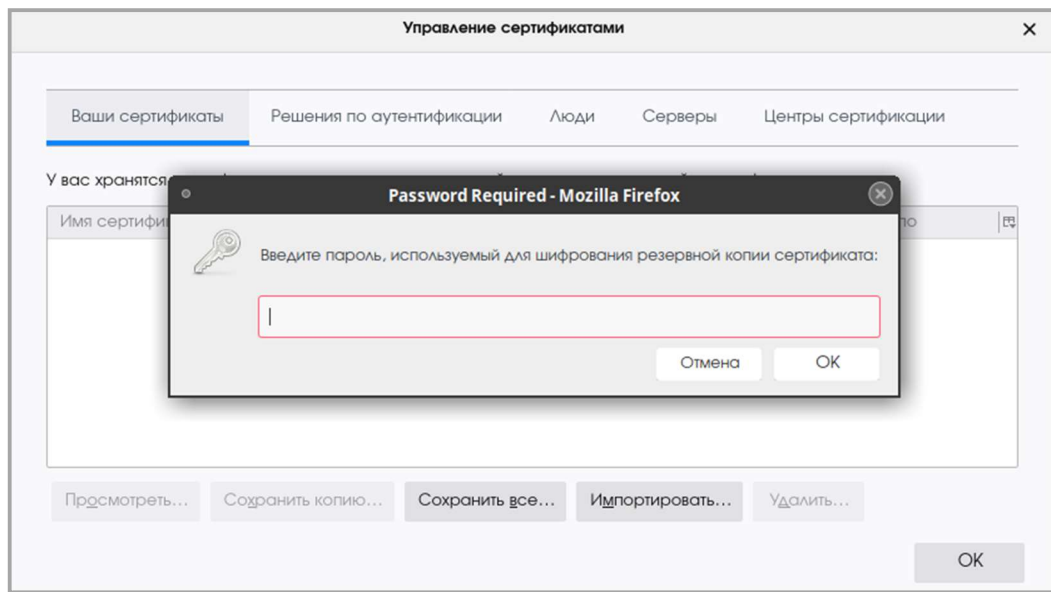


Рисунок 6 – Окно ввода пин-кода сертификата

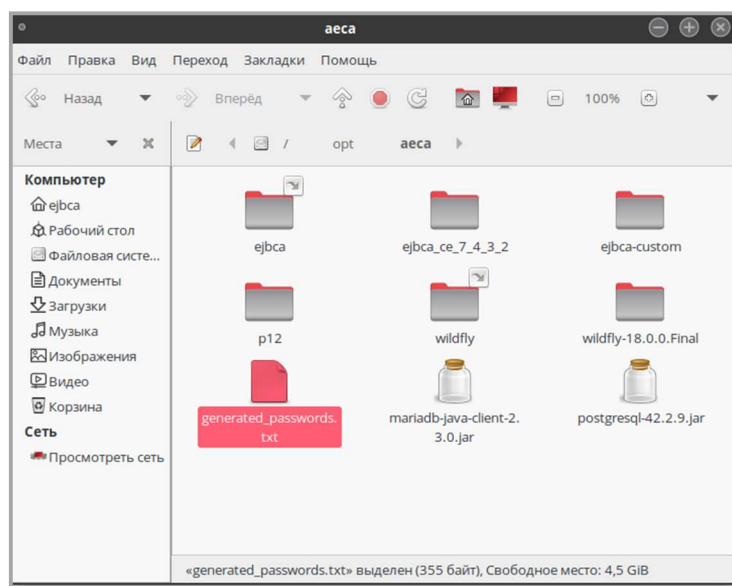


Рисунок 7 – Папка расположения файла с пин-кодом

7.1.7 В качестве пин-кода необходимо использовать данные строки `superadmin_password` из файла `generated_passwords.txt` (см. **Рисунок 8**).

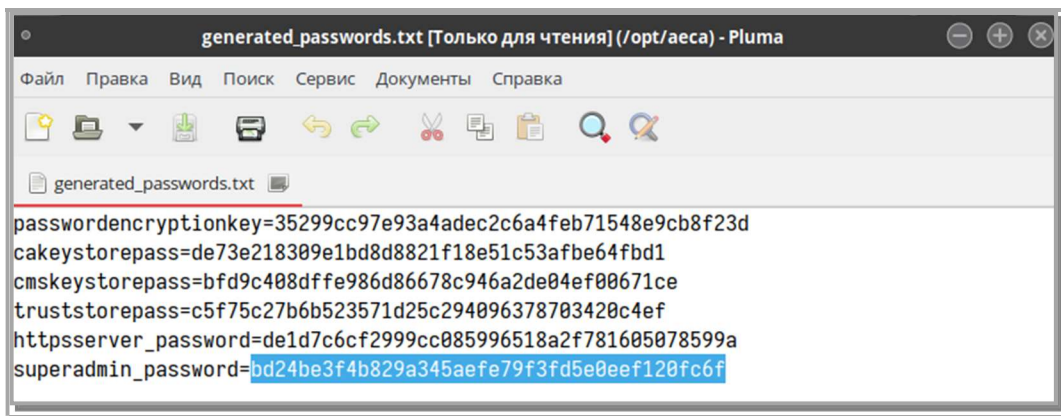


Рисунок 8 – Окно файла generated\_passwords.txt

7.1.8 В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 9). Нажать кнопку <OK>.

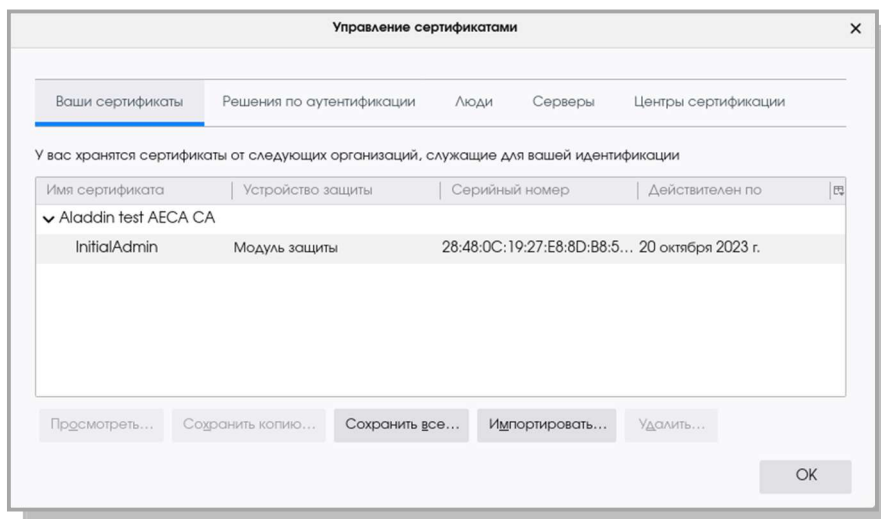


Рисунок 9 – Окно «Управление сертификатами»

7.1.9 В адресную строку браузера ввести URL-адрес в формате <адрес\_хоста\_развертывания\_продукта>:<порт>/<aecaCa>/.

Например:

```
https://localhost:8888/aecaCa/
```

- Если сертификат пользователя не импортирован, то откроется страница с сообщением об ошибке (см. Рисунок 10).

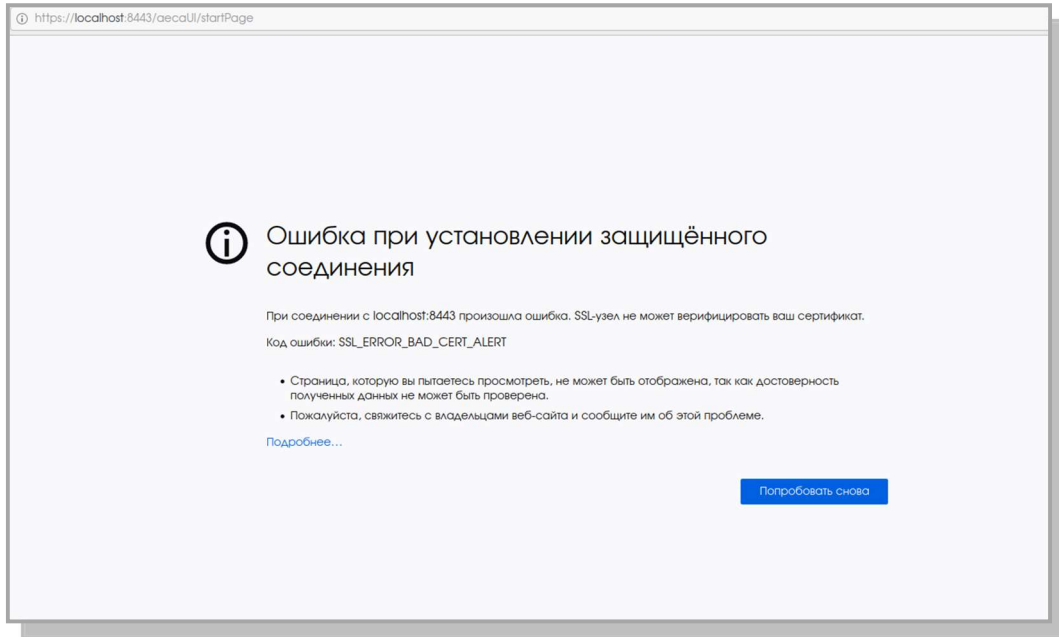


Рисунок 10 – Страница с сообщением об ошибке

- В случае успешной установки сертификата откроется страница с предупреждением системы безопасности (см. **Рисунок 11**). Нажать кнопку <Advanced>.

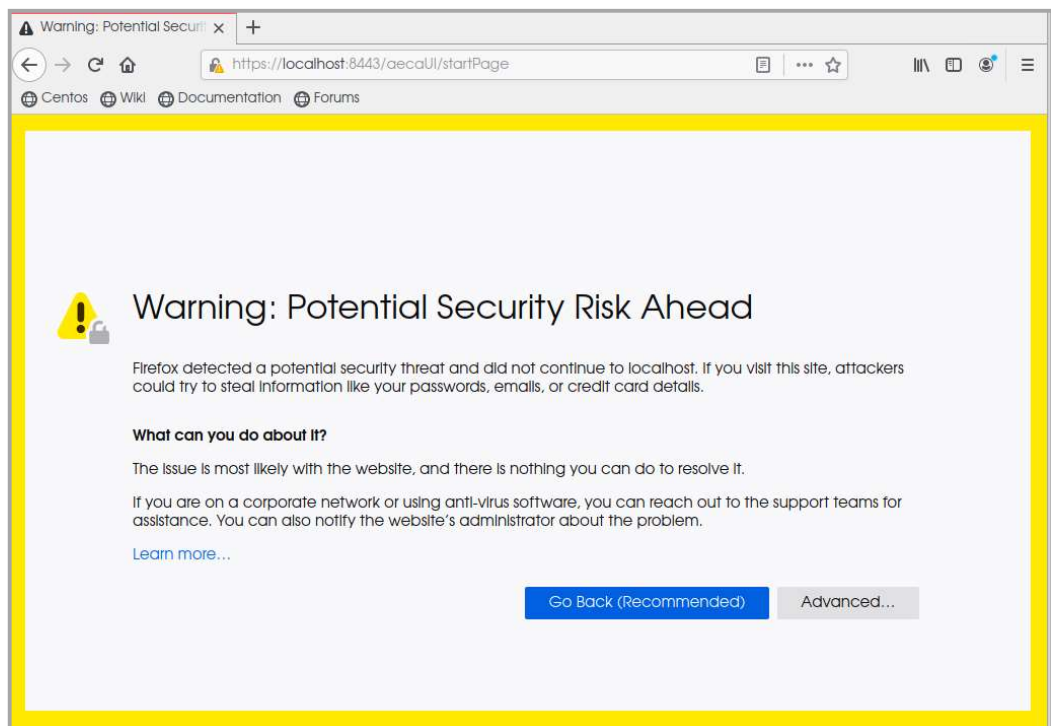


Рисунок 11 – Страница с предупреждением системы безопасности

7.1.10 По нажатию кнопки <Advanced> на странице предупреждения системы безопасности (см. **Рисунок 11**) осуществляется переход на страницу ошибки распознавания сертификата (см. **Рисунок 12**). Нужно принять риски, нажав кнопку <Accept the Risk and Continue> на текущей странице.

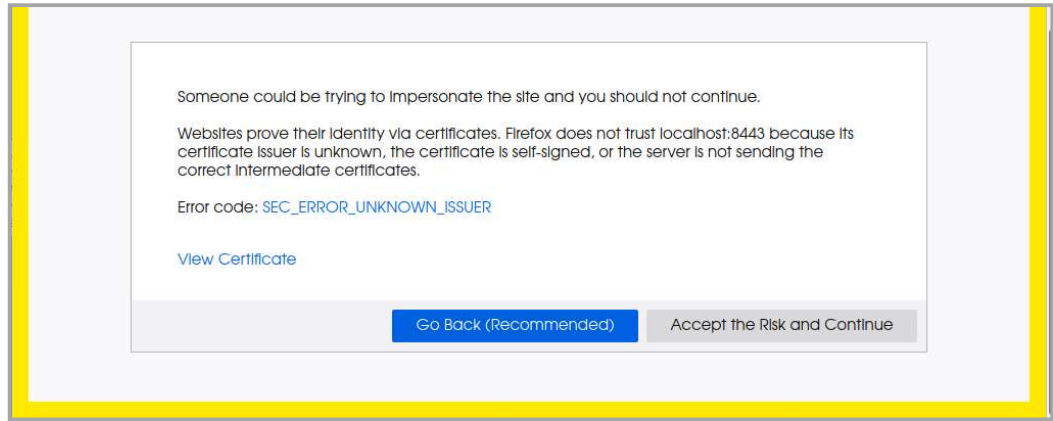


Рисунок 12 – Страница ошибки распознавания сертификата

7.1.11 Далее, при первом запуске AeCA CA разворачивается Мастер инициализации центра сертификации для создания центра сертификации (процедура создания корневого ЦС описана в пункте 7.2.3 настоящего документа).

Процедуру создания корневого ЦС можно выполнить позже.

7.1.12 Установка и предварительный ввод в эксплуатацию Изделия завершены, все компоненты центра сертификатов доступа Aladdin eCA установлены и готовы к работе.

## 7.2 Описание верхней панели «Центра сертификации»




Во всех окнах и вкладках «Центра сертификации» отображается верхняя панель (см. Рисунок 13).




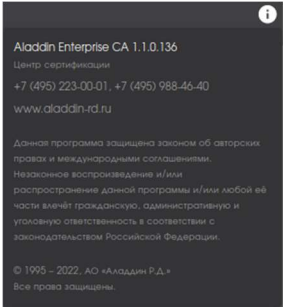
Рисунок 13 – Верхняя панель окна «Центра сертификации»

При наведении курсора на каждую иконку панели всплывает 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 желтому цвету иконки, «истек срок действия сертификата» - соответствует оранжевому цвету иконки, «истек срок действия лицензии» - соответствует красному цвету иконки);

- 

LocalService01  
CN=LocalService01,OU=Development  
Department=Ost\_C=RU
  - 

Aladdin Enterprise CA 1.1.0.136  
Центр сертификации  
+7 (495) 223-00-01, +7 (495) 988-46-40  
www.aladdin-rd.ru

Данная программа защищена законом об авторских правах и международными соглашениями. Незаконное воспроизведение и/или распространение данной программы и/или любой её части влечёт гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

© 1995 – 2022, АО «Алладин Р.Д.»  
Все права защищены.
- имя текущего активного ЦС (при наведении курсора всплывают заданные значения суффикса различающегося имени);
- сведения о текущей версии ПО и контактная информация разработчика.

### 7.3 Описание вкладки «Центр сертификации»

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

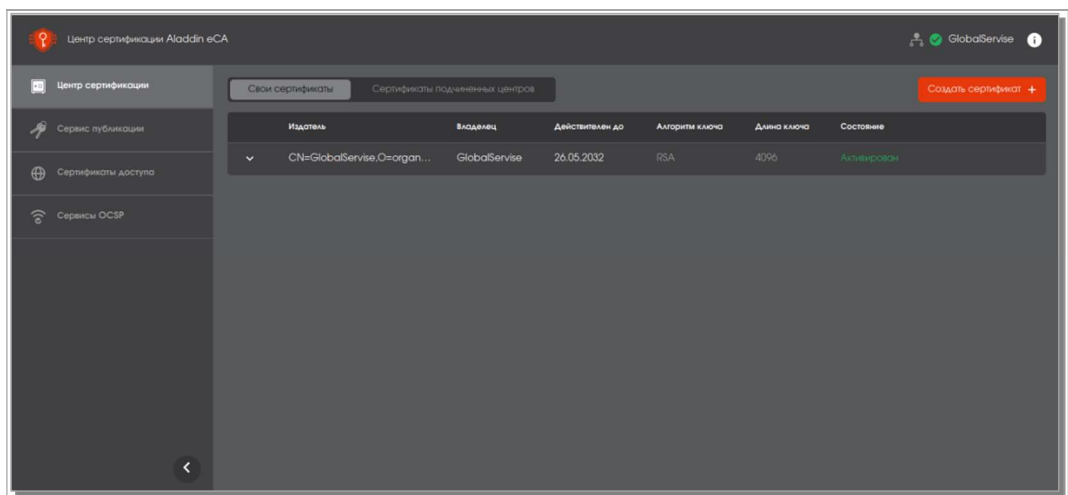


Рисунок 14 - Экран раздела меню "Центр сертификации"

#### 7.3.1 Вкладка «Свои сертификаты»

Вкладка «Центр сертификации» управления центром сертификации в правом поле экрана содержит вкладки «Свои сертификаты» (управление собственными Корневыми и Подчиненными ЦС) и «Сертификаты подчиненных центров» (работа с Подчиненными ЦС нижнего уровня).

7.3.1.1 Для сертификата ЦС АСeА из категории «Свои сертификаты», имеющего статус «активный», доступны настройки, в том числе создание и перенастройка сервисов публикации CRL DP.

7.3.1.2 Для сертификата ЦС AeCA из категории «Свои сертификаты», имеющего статус «не активирован», не доступны настройки, в том числе создание и перенастройка сервисов публикации CRL DP и работа с сертификатами доступа.

7.3.1.3 В обычном состоянии, без наведения указателя, управляемые элементы сертификатов не отображаются.



7.3.1.4 При наведении указателя мыши, кнопки управления сертификатами начинают отображаться (см. **Рисунок 15**).

Издатель	Владелец	Действует с	Действует по	Алгоритм ключа	Длина ключа	Состояние
CN=GlobalService,OU=D...	GlobalService	16.05.2022	17.05.2047	RSA	2048	Активирован
CN=High Global,O=Acti...	High Global	16.05.2022	17.05.2047	RSA	2048	Не активирован
CN=GlobalService,OU=D...	Local Service 02	16.05.2022	17.05.2047	RSA	2048	Запрос
CN=GlobalService,OU=D...	Local Service 01	16.05.2022	17.05.2047	RSA	2048	Запрос

Рисунок 15 - Экран "Свои сертификаты"


7.3.1.5 Информационные элементы вкладки «Свои сертификаты»:

- Неуправляемые (табличные поля):
  - издатель;
  - владелец;
  - действует с (дата);
  - действует по (дата);
  - алгоритм ключа;
  - длина ключа;
  - состояние (варианты состояния: активирован, не активирован, запрос, отозван, истёк срок).
- Управляемые поля – в соответствии с состоянием сертификата при помощи кнопок управления, расположенных на табличных полях (управление сертификатами также доступно через REST), возможны действия над сертификатами, приведенные в Таблица 7.

Таблица 7 – Действия над «своими» сертификатами

Состояние сертификата	Функции управления сертификатами			
	скачать	удалить	активировать	импорт
активирован	+	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
не активирован	+	+	+	<input type="checkbox"/>
запрос	+	+	<input type="checkbox"/>	+
отозван	+	+	<input type="checkbox"/>	<input type="checkbox"/>
истек срок	+	+	<input type="checkbox"/>	<input type="checkbox"/>

- Функции управления сертификатами:
  - «Активировать» – включение сертификата, как текущего Основного (рабочий сертификат), на базе которого происходит работа с остальными сертификатами. Активирование производится с последующим подтверждением;
  - Удалить – удаление через подтверждение;
  - Отозвать – отзыв через подтверждение;
  - Скачать – скачивание (без подтверждения);
  - Импорт – импорт сертификата.

7.3.1.6 Для каждого сертификата возможно просмотреть цепочку сертификатов (см. Рисунок 16), нажав кнопку  в строке слева от имени сертификата, и скачать цепочку сертификатов по нажатию кнопки <Скачать цепочку>, формирующей chain-файл.


Издатель	Владелец	Действителен до	Алгоритм ключа	Длина ключа	Состояние
▼ CN=GlobalService,O=org...	GlobalService	26.05.2032	RSA	4096	Не активирован
▲ CN=GlobalService,O=org...	LocalService01	26.05.2032	RSA	2048	Активирован
▼ CN=GlobalService,O=organization / 26.05.2032 / Действителен CN=LocalService01,OU=Development Department,O=Ost,C=RU.					Скачать цепочку 

Рисунок 16 – Просмотр цепочки сертификатов

### 7.3.1.7 Пояснения к экрану «Карточка сертификата»

Переход к экрану «Карточка сертификата» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты».

Варианты отображения экрана «Карточка сертификата»:

- Состояние «Активирован» (см.
- Рисунок 18);
- Состояние «Не активирован» (см. Рисунок 17).



← Центр сертификации	
GlobalService Action/Development Department <span style="color: red;">Не активирован</span>	
Скачать  Удалить  Активировать	
☰ Цепочка сертификатов ▼	
Издатель	GlobalService
Владелец	GlobalService
Организация	Action
Департамент	Development Department
Действует с	16.05.2022
Действует по	17.05.2047
Алгоритм ключа	RSA
Длина ключа	2048
Состав ▼	

Рисунок 17 - Состояние «Не активирован»

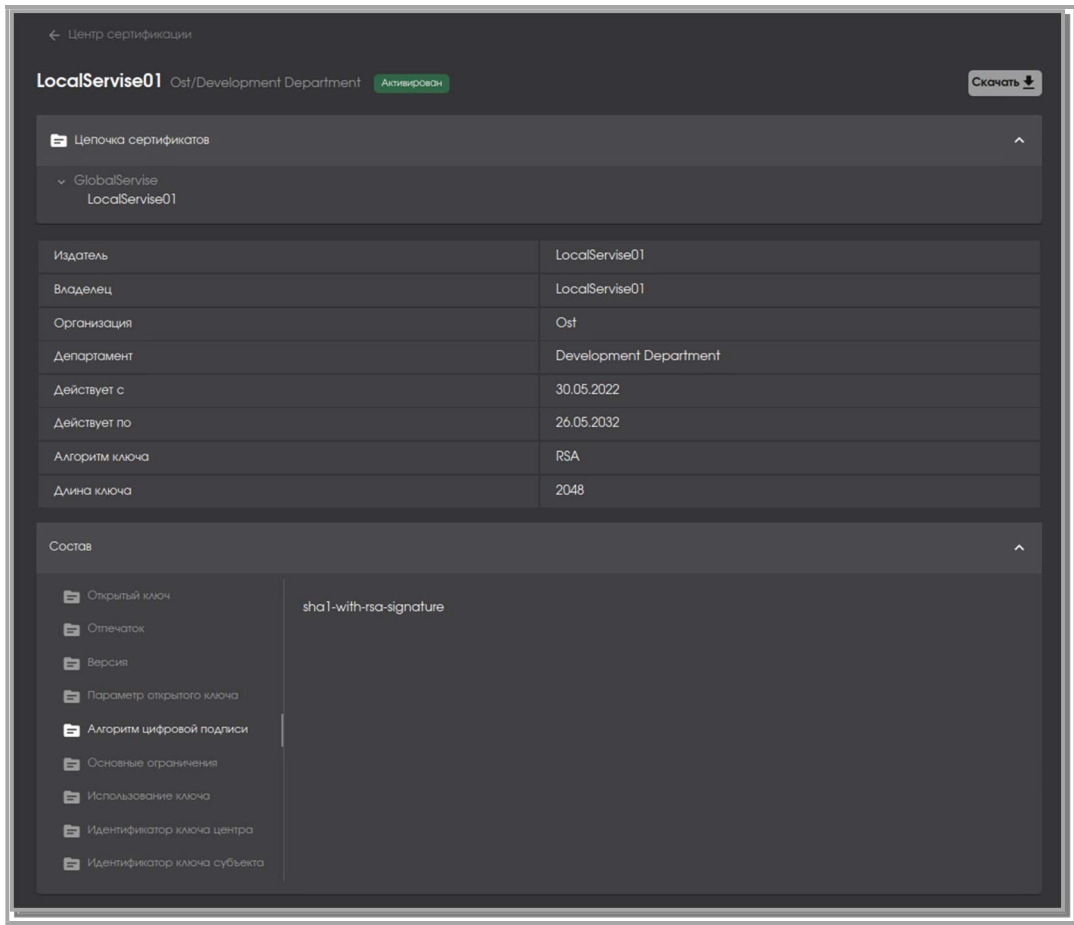


Рисунок 18 - Состояние «Активирован»

- Действия, возможные в карточке сертификата, аналогичны действиям, описанным в Таблица 7, в зависимости от состояния сертификата.
- При просмотре карточки сертификата из раздела «Сертификаты подчиненных центров» доступны те же команды, что и в списке сертификатов ЦС категории «Сертификаты подчиненных центров».

### 7.3.2 Вкладка «Сертификаты подчиненных центров»

Вкладка «Сертификаты подчиненных центров» (см. на Рисунок 19) предназначена для работы с Сертификатами Подчиненных ЦС нижнего уровня, сертификаты которых подписаны ЦС из категории «Свои сертификаты».

Варианты состояния и возможных операций над сертификатами из категории «Сертификаты подчиненных центров» с учетом наведенного указателя мыши и без приведены в Таблица 8.

7.3.2.1 Нажатие на кнопку <Подписать запрос> запускает сценарий подписи запроса подчиненного ЦС из категории «Сертификаты подчиненных центров».

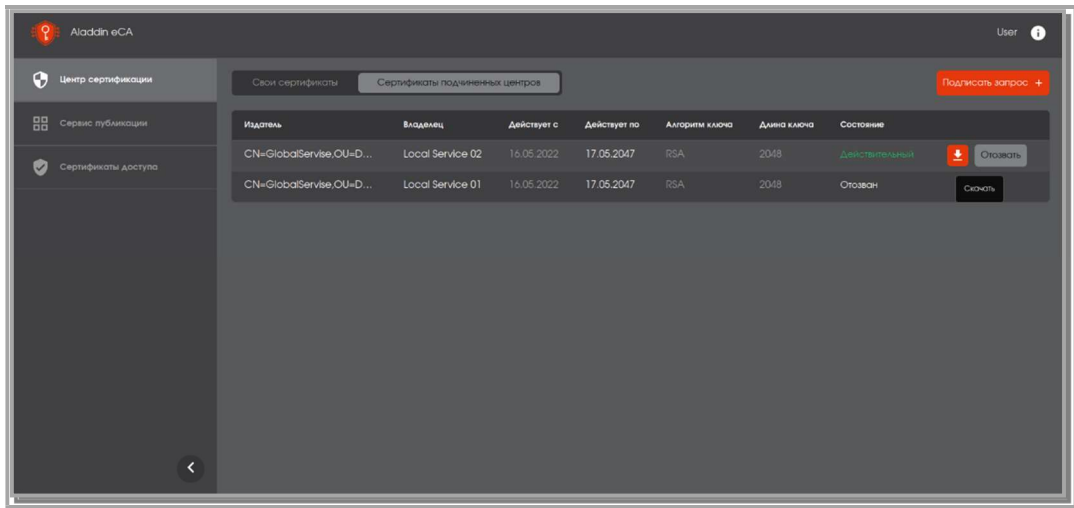


Рисунок 19 - Экран «Сертификаты подчиненных центров»

### 7.3.2.2 Информационные элементы экрана «Сертификаты подчиненных центров»:

- Неуправляемые табличные поля:
  - издатель;
  - владелец;
  - действует с (дата);
  - действует по (дата);
  - алгоритм ключа;
  - длина ключа;
  - состояние (варианты состояний: действительный, отозван, истёк срок).
- Управляемые поля – в соответствии с состоянием подчиненного сертификата при помощи кнопок управления, расположенных на табличных полях, возможны действия, приведенные в Таблица 8.

Таблица 8 – Действия над сертификатами подчиненных центров

Состояние сертификата	Функции управления сертификатами		
	скачать	удалить	отозвать
действительный	+	<input type="checkbox"/>	+
отозван	+	+	<input type="checkbox"/>
истек срок	+	+	<input type="checkbox"/>

- Функции управления подчиненными сертификатами:
  - скачать – скачивание сертификата (без подтверждения);
  - удалить – удаление сертификата с подтверждением;
  - отозвать – отзыв сертификата с подтверждением.

### 7.3.3 Создание корневого центра сертификатов

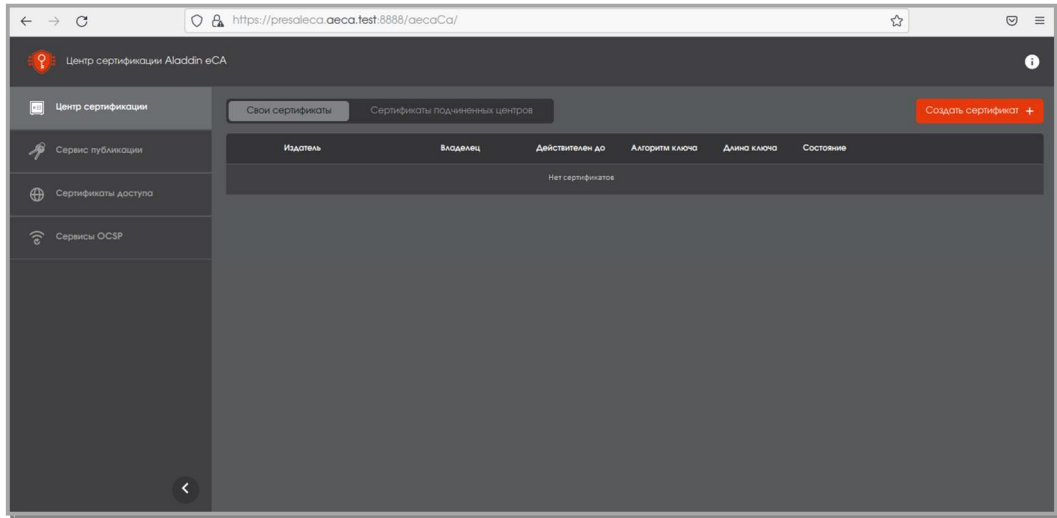
#### 7.3.3.1 Открыть браузер и перейти по адресу веб-приложения в формате:

<адрес\_хоста\_развертывания\_продукта>:<порт>/<аесаСа>/.

Например:

`https://localhost:8888/aecaCa/`

7.3.3.2 В открывшемся окне «Центр сертификации» в разделе «Свои сертификаты» нажать кнопку <Создать сертификат+> (см. **Рисунок 20**).



**Рисунок 20 – Окно главного экрана АЕСА**

7.3.3.3 В результате нажатия кнопки <Создать сертификат+> в появившемся окне (см. Рисунок 21) задать:

- наименование центра сертификации – ввод имени ЦС. Имя ЦС не должно содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами – запятые и запятые с пробелами, ограничение на длину вводимого имени – 250 байт;
- суффикс различающегося имени – ввод суффикса различающегося имени ЦС. Суффикс различающегося имени не должен содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами – запятые и запятые с пробелами, ограничение на длину вводимого имени – 250 байт. Поддерживаемые варианты атрибутов суффикса различающегося имени приведены в Таблица 9;
- тип ЦС (на данном этапе выбираем корневой ЦС).

Таблица 9 – Поддерживаемые атрибуты суффикса различающегося имени

Наименование атрибута	Описание атрибута
E=	// E-mail address(электронная почта)
UID=	//Unique Identifier(уникальный идентификатор)
SN=	//Serial number(серийный номер)
GIVENNAME=	//Given name (first name – имя)

## RU.АЛДЕ.03.01.020-01 32

Наименование атрибута	Описание атрибута
INITIALS=	//First name abbreviation(инициалы)
SURNAME=	//Surname (фамилия)
T=	//title(заглавие)
OU=	//Organizational Unit(отдел(организации))
O=	//Organization(организация)
L=	//Locality(район)
ST=	//State or Province(область, край, республика)
DC=	//Domain Component(first)(первый доменный компонент, если вводить второй раз, добавит во второй)
C=	// C, Country (страна, вводить согласно - ISO 3166)
UNSTRUCTUREDADDRESS=	//IP address(IP-адрес)
UNSTRUCTUREDNAME=	//Domain name(доменное имя - FQDN)
POSTALCODE=	//postalCode(почтовый индекс)
BUSINESSCATEGORY=	//Organization type(категория(тип) организации)
DN=	//DN Qualifier
POSTALADDRESS=	//postalAddress(почтовый адрес)
TELEPHONENUMBER=	// telephoneNumber(телефонный номер)
PSEUDONYM=	//pseudonym(псевдоним)
STREET=	//streetAddress(адрес - улица)
NAME=	//name(дополнительное имя)
DESCRIPTION=	//Description(краткое описание)

Мастер инициализации центра сертификации

1. Имя и тип

Имя центра сертификации  
GlobalService

Суффикс различающегося имени  
O=Action, OU=Development Department, C=RU  
Лимит: 168 байт

Выберите тип ЦС для инициализации

Корневой

Подчиненный

Отмена Продолжить →

Введите имя, используя только латинские буквы, цифры, символы и пробел.

Формат ввода: C=organization, OU=Department, L=City, DC=Component, C=RU...

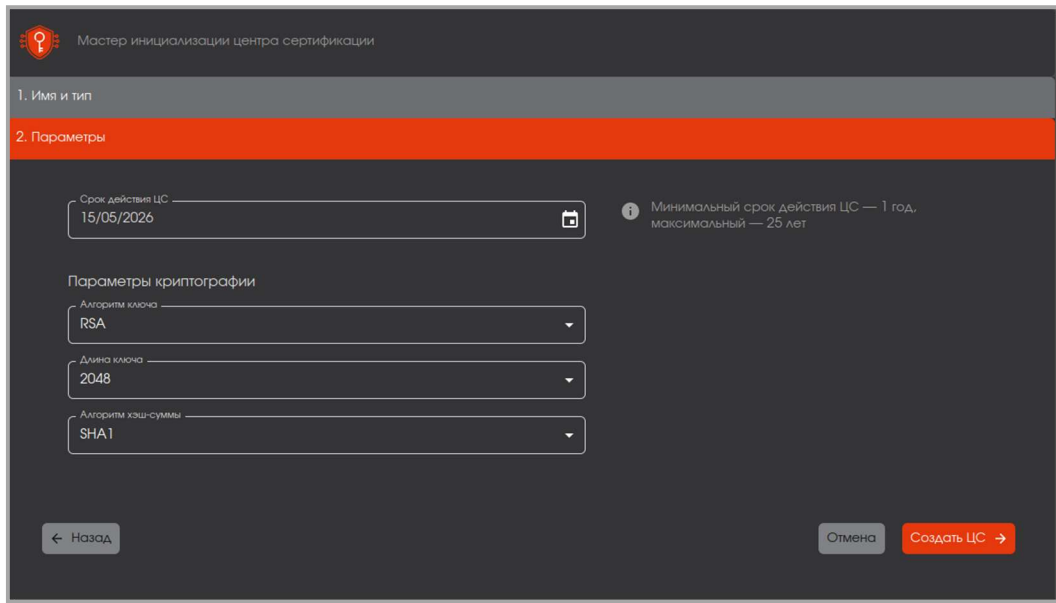
Рисунок 21 – Окно задания наименования ЦС и суффикса различающегося имени

- После задания имени, суффикса различающегося имени и выбора типа ЦС нажать кнопку <Продолжить>.

7.3.3.4 В открывшемся окне (см. **Рисунок 22**) в соответствующих полях установить:

- срок действия сертификата (по умолчанию – 15 лет). Ввод осуществляется вручную или выбором даты окончания действия сертификата в открывшемся календаре;
- параметры шифрования:
  - алгоритм ключа;
  - длина ключа;
  - алгоритм хэш-суммы.

После задания значений нажать кнопку <Создать ЦС>.



Мастер инициализации центра сертификации

1. Имя и тип

2. Параметры

Срок действия ЦС  
15/05/2026

Минимальный срок действия ЦС — 1 год,  
максимальный — 25 лет

Параметры криптографии

Алгоритм ключа  
RSA

Длина ключа  
2048

Алгоритм хэш-суммы  
SHA1

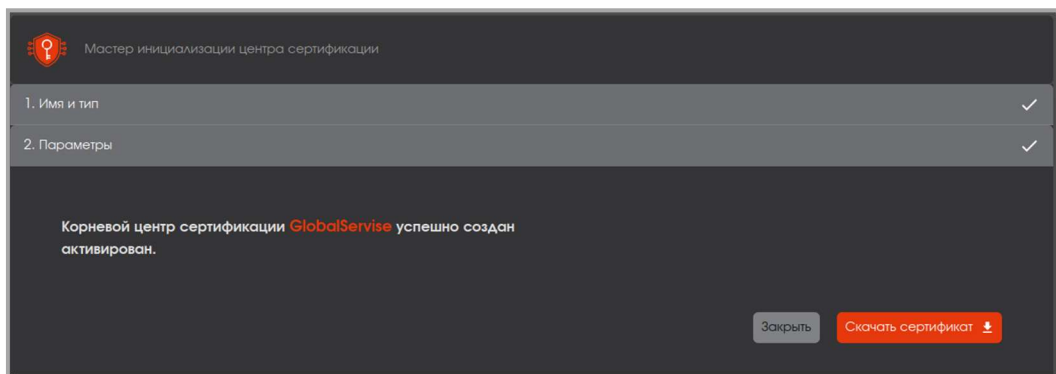
← Назад

Отмена

Создать ЦС →

Рисунок 22 – Окно ввода параметров криптографии и срока действия ЦС

7.3.3.5 При успешном создании корневого ЦС и завершении мастера инициализации центра сертификации администратор видит соответствующее сообщение (см. Рисунок 23). Возможно скачать сертификат созданного корневого ЦС и открыть карточку ЦС (см. пункт 7.2.1.6).



Мастер инициализации центра сертификации

1. Имя и тип ✓

2. Параметры ✓

Корневой центр сертификации **GlobalService** успешно создан  
активирован.

Закрыть

Скачать сертификат ↓

Рисунок 23 – Окно завершения работы мастера инициализации по созданию корневого ЦС

### 7.3.4 Создание подчиненного центра сертификатов

7.3.4.1 Процедура создания подчиненного центра сертификатов повторяет процедуру создания корневого центра сертификатов.

7.3.4.2 Для создания подчиненного центра сертификатов проделать шаги, описанные в пунктах:

- 7.3.3.1;
- 7.3.3.2;
- 7.3.3.3;
- 7.3.3.4 На этом шаге требуется выбрать «Тип ЦС для инициализации» - подчиненный;



- 7.3.3.5.

7.3.4.3 При успешном создании подчиненного ЦС и завершении мастера инициализации центра сертификации администратор видит соответствующее сообщение (см. Рисунок 24). Возможна отмена текущего прогресса, можно загрузить сертификат для активации подчиненного ЦС.

На данном этапе подчиненный ЦС создан, отображается на вкладке «Свои сертификаты» и имеет статус «Запрос».

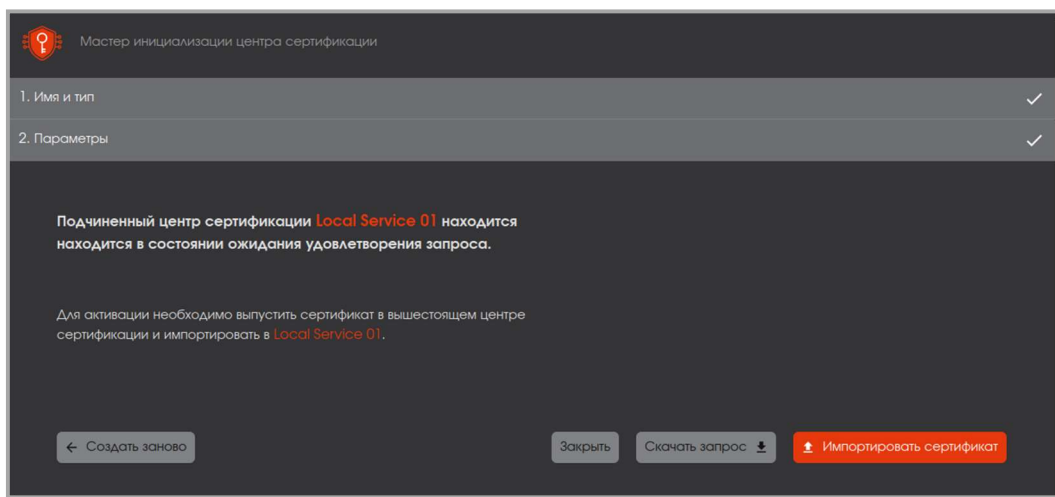



Рисунок 24 – Окно завершения работы мастера инициализации по созданию подчиненного ЦС

7.2.4.4 Для перевода ЦС в состояние «Не активирован», при котором становится доступна активация ЦС, необходимо выполнить подписание запроса на корневом ЦС (пункт 7.3.5) и загрузку подписанного сертификата подчиненного ЦС (пункт 7.3.6).

### 7.3.5 Подписание запроса на корневом ЦС

7.3.5.1 На вкладке «Свои сертификаты» выбрать созданный подчиненный ЦС в состоянии «Запрос».

7.3.5.2 Нажать появившуюся в строке выбранного ЦС кнопку  и скачать запрос в формате .csr.

7.3.5.3 При активном корневом ЦС, от имени которого будет выдан сертификат, на вкладке «Сертификаты подчиненных центров» нажать кнопку <Подписать запрос+> (см. Рисунок 25)

**Внимание! Подписание файл-запроса и выдача подписанного сертификата производится от ЦС в состоянии «Активирован» на вкладке «Свои сертификаты».**

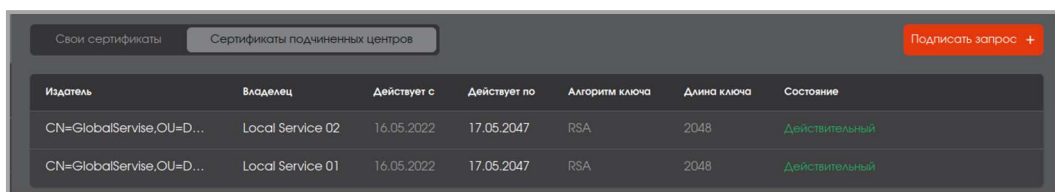


Рисунок 25 – Окно «Сертификаты подчиненных ЦС»

7.3.5.4 Далее загрузите запрос в формате .csr, скачанный на шаге 7.2.5.2, нажав кнопку <Выбрать файл> (см. Рисунок 26).

На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку <Изменить> (см. Рисунок 27).

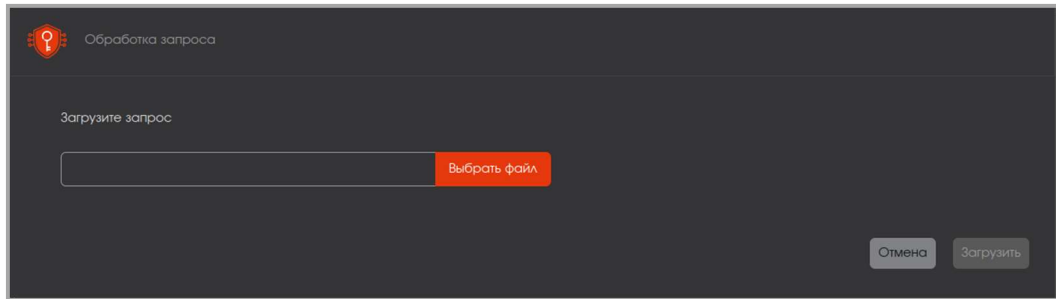


Рисунок 26 – Окно выбора файла запроса

Нажмите ставшую активной кнопку <Загрузить> (см. Рисунок 27).



Рисунок 27 – Окно загрузки файла запроса

При нажатии кнопки <Загрузить> происходит загрузка файл запроса в Корневой ЦС (текущий активный корневой ЦС из категории «Свои сертификаты»).

7.3.5.5 Далее администратор видит уведомление о том, что сертификат подчиненного ЦС успешно сформирован и подписан корневым ЦС (см. Рисунок 28).

Необходимо скачать файл сформированного сертификата в формате .pem, нажав кнопку <Скачать сертификат> в окне Обработки запроса на данном шаге.

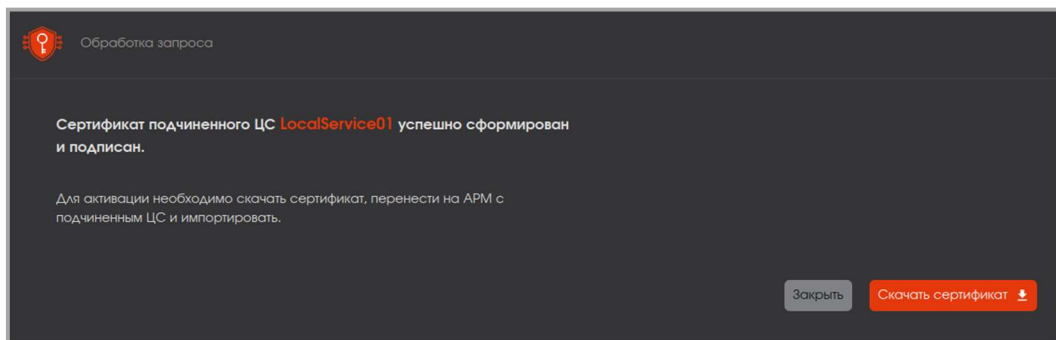



Рисунок 28 – Окно успешного формирования и подписи сертификата

Скачать сформированный и подписанный сертификат можно позднее, открыв вкладку «Сертификаты подчиненных центров», выбрав нужный сертификат и нажав появившуюся кнопку  для скачивания сертификата (см. Рисунок 29).

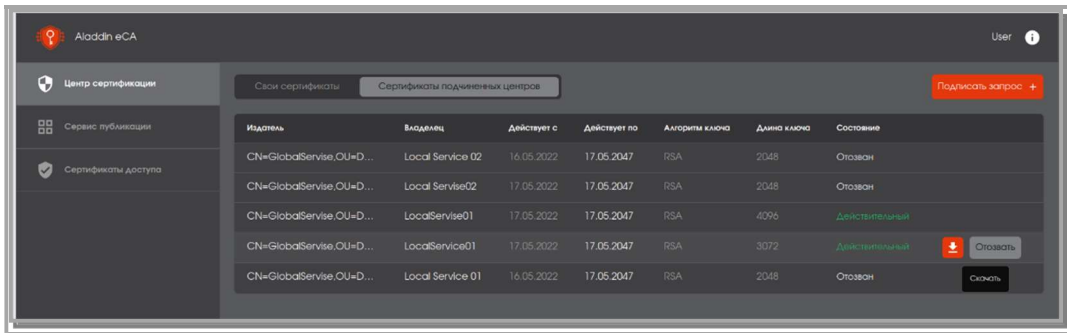



Рисунок 29 – Окно вкладки «Сертификаты подчиненных центров» с выбранным сертификатом

7.3.5.6 Нажать кнопку <Закрыть> для завершения работы Мастера обработки запроса.

### 7.3.6 Импорт сертификата подчиненного ЦС

**ВНИМАНИЕ!** Сценарий является контекстным и используется только для ЦС со статусом «Запрос».

7.3.6.1 На вкладке «Свои сертификаты» выбрать подчиненный ЦС (см. Рисунок 30) в состоянии «Запрос», по запросу которого был сформирован сертификат формата .pem в подразделе 7.2.5 данного руководства. Нажать кнопку  <Загрузить>.

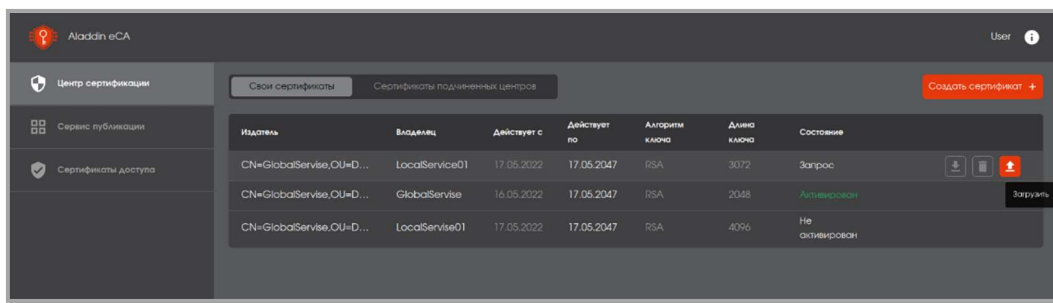
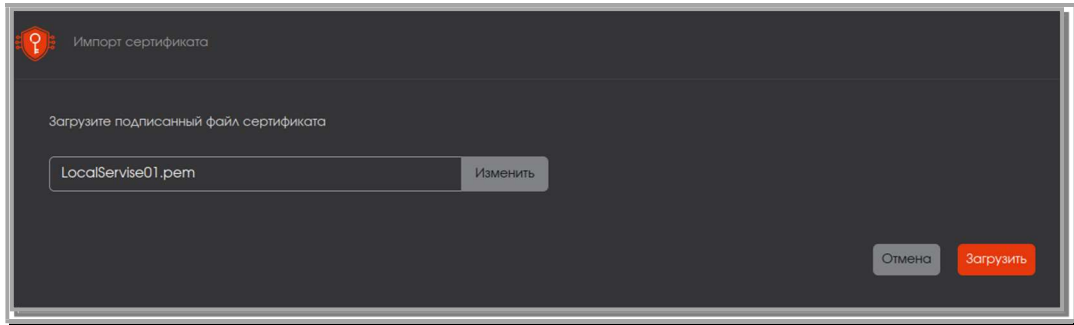


Рисунок 30 – Окно выбора подчиненного ЦС в состоянии «Запрос» на вкладке «Свои сертификаты»

7.3.6.2 Далее в появившемся окне импорта сертификата (см. Рисунок 31) выбрать подписанный ранее файл сертификата для загрузки в формате .pem. После выбора файла сертификата для подчиненного ЦС, не переходя к следующему шагу, есть возможность переопределить файл сертификата, нажав кнопку <Изменить>.

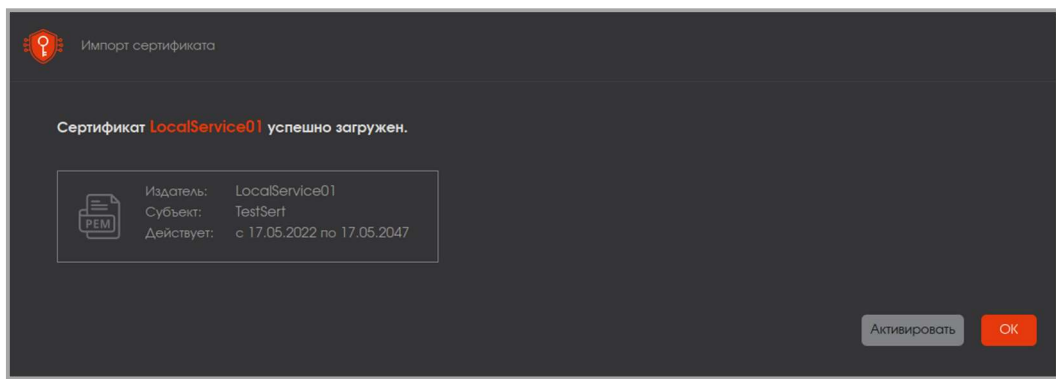
Далее нажать кнопку <Загрузить>, активированную после выбора файла сертификата.



**Рисунок 31 - Окно импорта сертификата**

7.3.6.3 После успешной загрузки сертификата открывается окно с уведомление об успешной загрузке сертификата (см. **Рисунок 32**) и отображается следующая информация:

- издатель;
- субъект;
- срок действия сертификата.



**Рисунок 32 – Окно уведомления об успешной загрузке сертификата**

На данном этапе подчиненный ЦС, для которого был импортирован сертификат, возможно перевести в состояние «Активный», нажав кнопку <Активировать>.

По нажатию на кнопку <Ок> сертификат присваивается подчиненному ЦС, и работа мастера импорта сертификата завершается, но ЦС не активируется.

7.3.6.4 После нажатия на кнопку <Ок> (см. Рисунок 32) и завершения работы мастера импорта сертификата, на вкладке «Свои сертификаты» состояние подчиненного ЦС, для которого произведена загрузка подписанного сертификата, измениться с первоначального «Запрос» (см. Рисунок 30) на «Не активирован» (см. Рисунок 33). Активация возможна по кнопке <Активировать>, которая появляется при выборе строки подчиненного ЦС в состоянии «Не активирован».

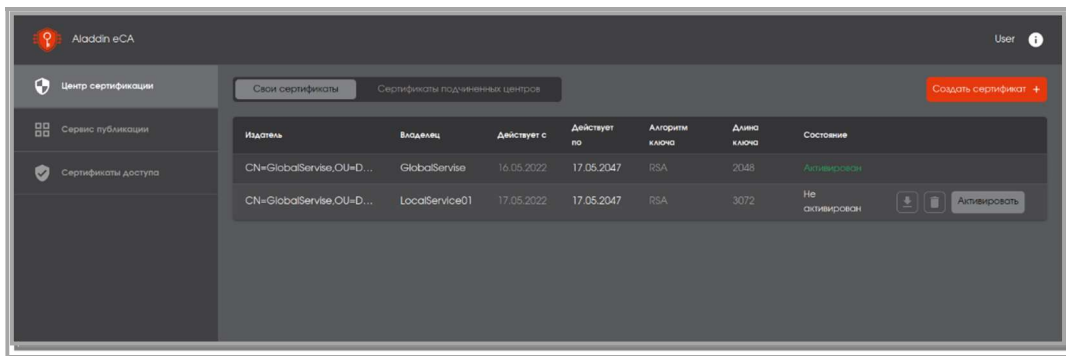


Рисунок 33 – Окно вкладки «Свои сертификаты» с загруженным сертификатом для подчиненного ЦС

7.3.6.5 Для Центра Сертификатов в состоянии «Активирован» доступно выполнение сценариев на вкладке «Сервис публикации».

## 7.4 Описание вкладки «Сервис публикации»

### 7.4.1 Состав элементов вкладки «Сервис публикаций»

Переход на вкладку «Сервис публикации» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 14).

На основном экране сервиса публикации отображены информационные элементы (см. Рисунок 34).

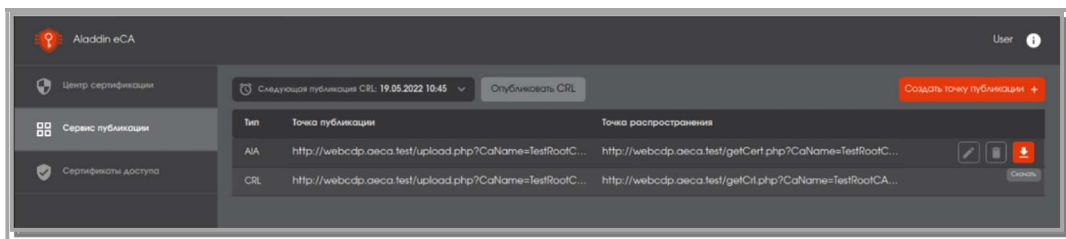



Рисунок 34 - Экран "Сервис публикации"

- Чтобы не ждать наступление времени публикации, указанного в элементе «Следующая публикация» можно нажать кнопку «Опубликовать CRL» Неуправляемые (табличные поля):
  - Тип. В графе экранной таблицы «Тип» отображается возможный тип точки публикации CRL, AIA;
  - Точка публикации. В графе экранной таблицы «Точка публикации» отображается url-адрес публикации;
  - Точка распространения. В графе экранной таблицы «Точка распространения» отображается url-адрес распространения.

Ограничение количества строк экранной таблицы – 15, при полном заполнении новую точку публикации задать будет невозможно.

• Управляемые поля – кнопки управления, которые отображаются при наведении указателя мыши на существующую точку публикации в таблице (см. Рисунок 34). Доступные действия:

- Редактирование . При нажатии на иконку <Редактировать> строки типа CRL открывается окно с возможностью перенастройки точки публикации CRL (см. Рисунок 35) и для строки типа AIA окно с возможностью перенастройки точки публикации AIA (см. Рисунок 36).

Ввод точки распространения и точки публикации осуществляется в соответствии с примером.

Для сохранения изменений нажать кнопку <Сохранить изменения>, в противном случае, после закрытия браузера или перехода на шаг назад средствами браузера, изменения будут утеряны.

При нажатии на кнопку <Отмена> изменения не сохраняются.

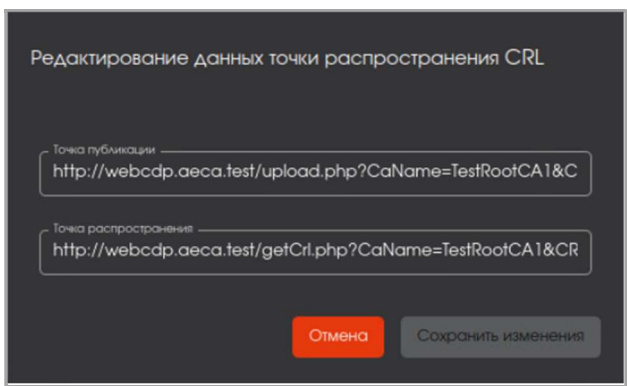


Рисунок 35 - Окно редактирования CRL

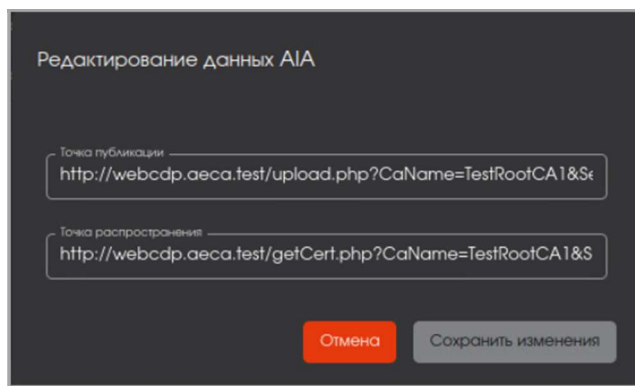




Рисунок 36 - Окно редактирования AIA

- удаление  точки публикации;
- скачивание  CRL или AIA.

В обычном состоянии, без наведения указателя, управляемые элементы точек публикации не отображаются.

Работа с разделом «Сервис публикации» предусматривает выполнение следующих сценариев использования:

- моментальная публикация списков CRL через точки публикации (окно с подтверждением);
- создание точки публикации CRL или AIA (окно с подтверждением);
- редактирование точки публикации (окно с подтверждением);
- удаление точки публикации (с подтверждением);
- скачивание артефакта (скачать CRL или AIA);
- изменение периода авто-обновления точек публикации CRL для текущего активного сертификата (с подтверждением).

Описание особенностей и процедур данных сценариев представлено далее.

#### 7.4.2 Моментальная публикация списков CRL

Для того, чтобы не ждать наступление времени публикации, указанного в элементе «Следующая публикация» можно нажать кнопку «Опубликовать CRL» (см. Рисунок 37). При нажатии на кнопку «Опубликовать CRL» публикуется внеплановый список отзыва, при этом таймер публикации списка отзыва сбрасывается и начинается новый отсчет времени публикации.

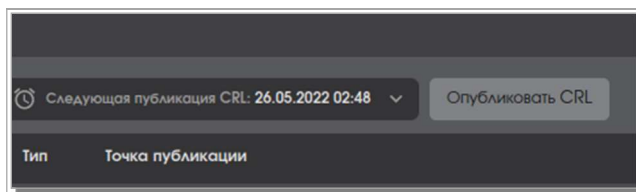


Рисунок 37 – Кнопка «Опубликовать CRL»

#### 7.4.3 Настройка периода автообновления

- Поле «Следующая публикация CRL» на экране «Сервис публикации» содержит дату и время следующей публикации в формате «дд.мм.гггг чч.мм» (24-часовой формат), раскрывающееся подменю с возможностью просмотреть дату и время предыдущей публикации и изменить период публикации (см. Рисунок 38).

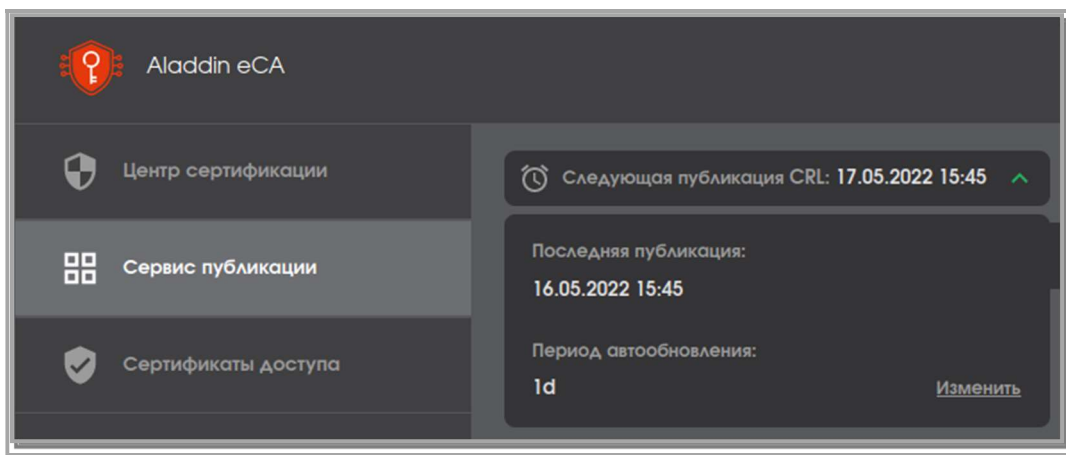


Рисунок 38 - Подменю "Следующая публикация"

При нажатии на ссылку «Изменить» (см. Рисунок 38) открывается окно, предоставляющее возможность перенастройки периода обновления публикации CRL (см. Рисунок 39).

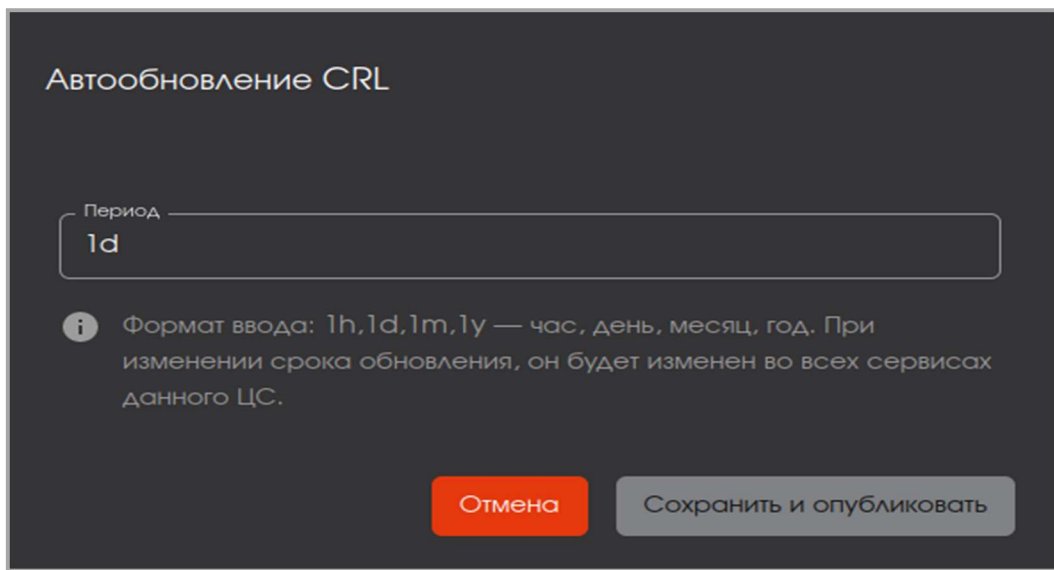


Рисунок 39 - Экран "Авто-обновление CRL"

**ВНИМАНИЕ!** При перенастройке периода точки публикации текущего сертификата перенастраивается время публикации всех точек публикации CRL текущего сертификата. Время публикации CRL синхронизировано по времени публикации при настройке периода публикации, при создании новой точки публикации, при публикации по команде (включая REST) и одинаково для всех точек публикации текущего сертификата.

- При нажатии

#### 7.4.4 Создания новых точек публикации CRL и AIA

- На экране «Сервис публикации» (см. Рисунок 34) нажать кнопку , инициировав старт сценария создания новой точки публикации.

**ВНИМАНИЕ!** Сервисы публикации создаются для активного сертификата ЦС раздела «Свои сертификаты».

- При нажатии на кнопку <Создать точку публикации> появляется окно мастера создания сервиса публикации (см. Рисунок 40). Выбор типа сервиса публикации осуществляется посредством радиокнопок.

При выборе пункта CRL (см. Рисунок 40) или AIA (см. Рисунок 41) доступны два поля для заполнения параметров сервиса публикации:

- в строке <Точка публикации> вводится адрес точки публикации, например: 192.168.111.192/upload.php;
- в строке <Точка распространения> вводится адрес точки распространения, например: 192.168.111.192/getCrl.php

**ВНИМАНИЕ!** Формат ввода «getCrl...» обязателен, ввод типа «getcrl...» работать не будет.

В данном окне имеются кнопка <Отмена> для закрытия окна без сохранения изменений, и кнопка <Создать>, которая неактивна до заполнения всех полей окна мастера создания сервиса публикации.



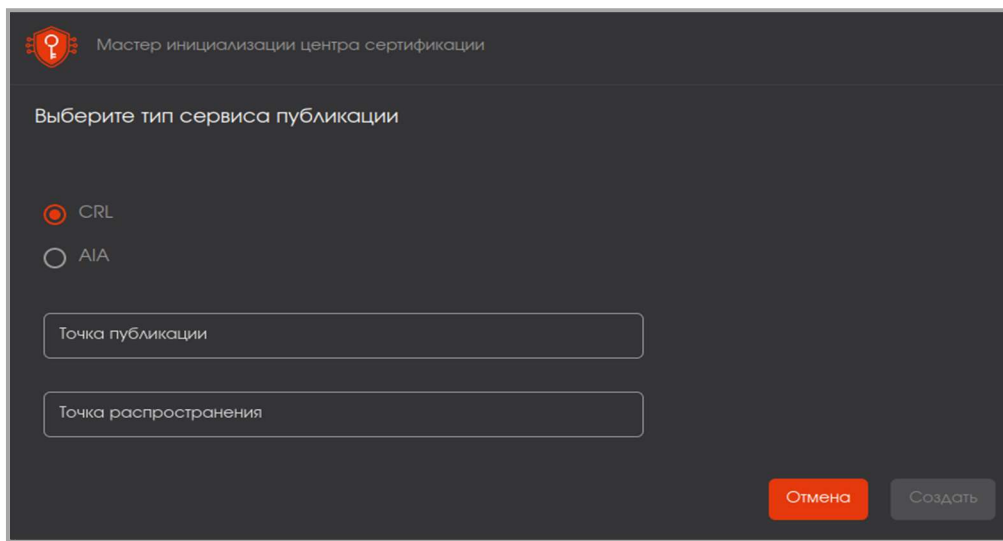


Рисунок 40 - Сценарий настройки точки публикации CRL

**ВНИМАНИЕ!** Изначально срок обновления введен в графе «Срок обновления» и соответствует настроенному сроку обновления точек публикации выбранного сертификата. При смене данного параметра нужно задать срок обновления для всех точек обновления сертификата – дата следующей публикации.

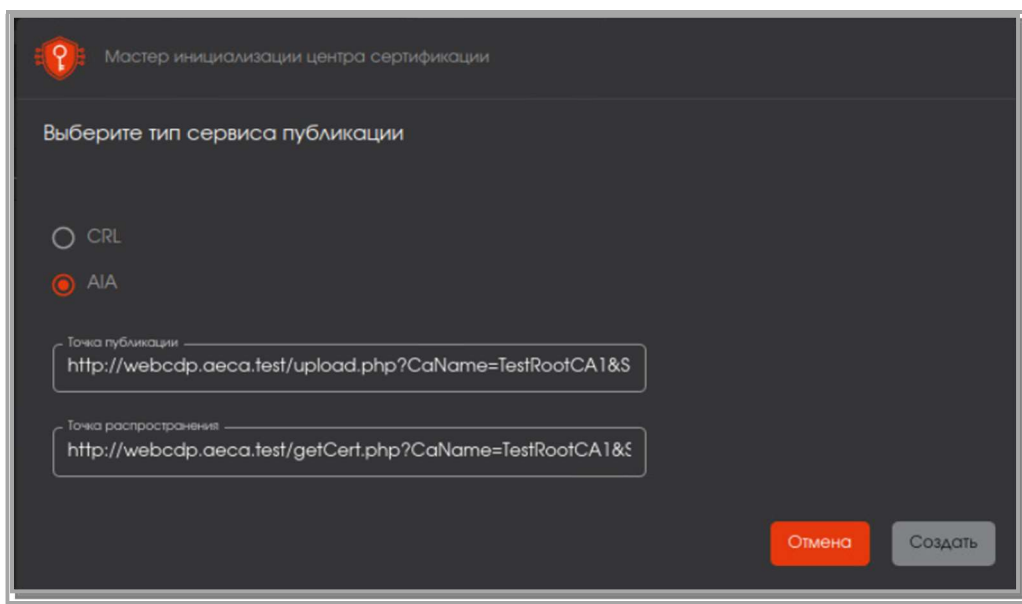


Рисунок 41 - Сценарий настройки точки публикации AIA

- После заполнения всех полей окна мастера создания сервиса публикации нажать ставшую активной кнопку <Создать>.
- Новый сервис публикации CRL или AIA создан и отображается на главном экране сервиса публикации.

## 7.5 Описание вкладки «Сертификаты доступа»

Переход на экран управления центра сертификации осуществляется по выбору вкладки «Сертификаты доступа» бокового меню, расположенного слева на главном экране (см. Рисунок 42).

На данном экране отображаются все созданные сертификаты пользователей, контроллеров домена, web-серверов.

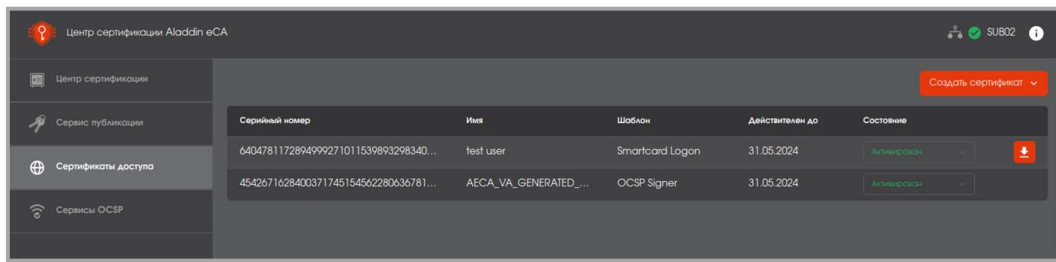


Рисунок 42 - Экран раздела меню "Сертификаты доступа"

На основном экране сервиса публикации отображены информационные элементы:


- Неуправляемые (табличные поля):
  - серийный номер (сертификата);
  - имя (субъекта аутентификации);
  - шаблон (тип шаблона категории сертификата);
  - действует с (дата выдачи сертификата);
  - действует до (дата срока окончания действия сертификата).
- Управляемые поля:
  - кнопка управления <Скачать>, которая отображается при наведении указателя мыши на существующий сертификат на экранной таблице. Для скачивания сертификата наведите указатель мыши на выбранный сертификат и скачайте по нажатию появившейся кнопки  <Скачать сертификат> (см. Рисунок 42).
  - состояние – возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в Таблица 10. Смена состояния сертификата производится посредством выбора нужного значения из выпадающего меню (см. Рисунок 43).

Таблица 10 – Доступные действия над сертификатами в зависимости от состояния

Состояние сертификата	Доступные действия		
	активация	приостановка	отзыв
активирован	<input type="checkbox"/>	<b>+</b>	<b>+</b>
приостановлен	<b>+</b>	<input type="checkbox"/>	<b>+</b>
отозван	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Действует с	Действует по	Состояние
16.05.2022	15.05.2024	Приостановлен
16.05.2022	15.05.2024	Активирован

Активирован  
Приостановлен  
Отозван

Рисунок 43 – 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 44);

**ВНИМАНИЕ!** Данную операцию нельзя отменить.

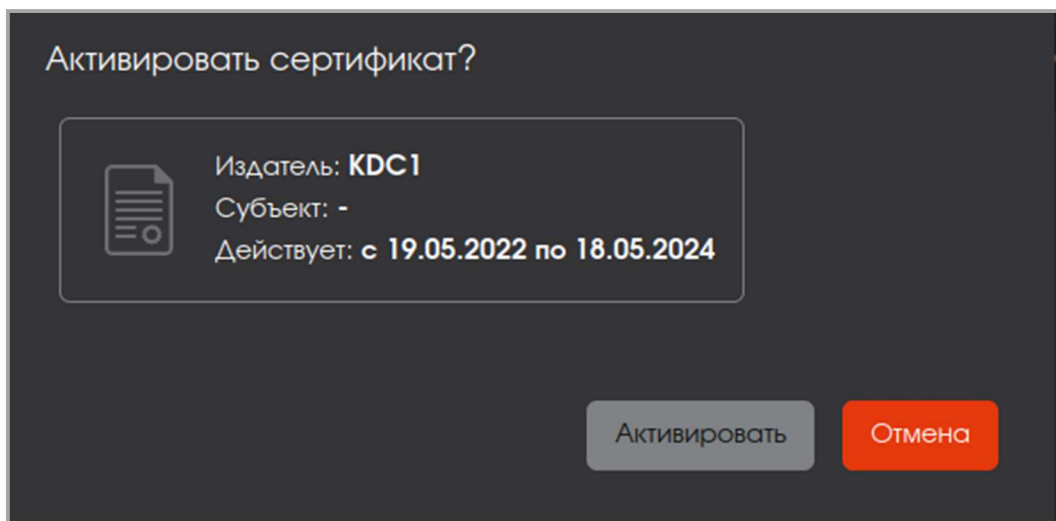


Рисунок 44 – Окно активации сертификата

- отзыв (см. Рисунок 45);

**ВНИМАНИЕ!** Данную операцию нельзя отменить.

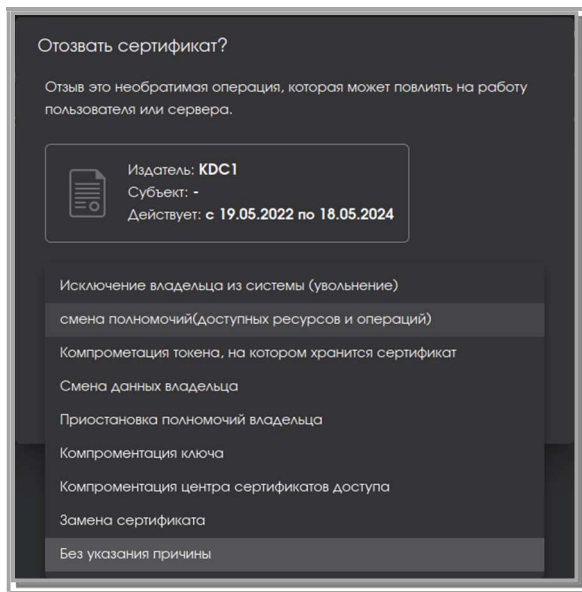


Рисунок 45 – Окно отзыва сертификата

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

- неиспользуемый (unused) – исключение владельца из системы/увольнение;
  - компрометация ключа (keyCompromise);
  - компрометация центра сертификации (cACompromise);
  - принадлежность изменена (affiliation Changed) – смена данных владельца;
  - заменен (сертификат) – заменен на иной сертификат;
  - приостановка полномочий владельца сертификата (certificateHold);
  - без указания причины (unspecified).
- Приостановка действия сертификата (см. Рисунок 46):

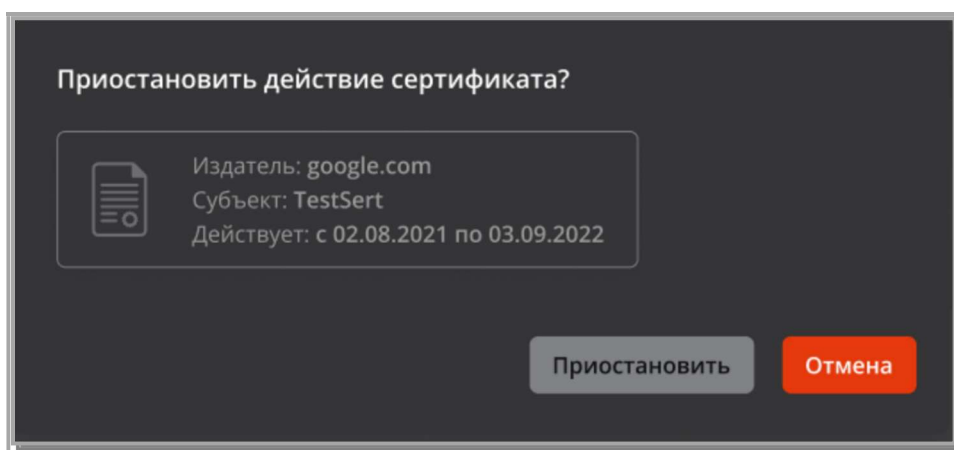


Рисунок 46 – Окно приостановки действия сертификата

### 7.5.1 Карточка сертификата

- Просмотра данных сертификата возможен посредством страницы «Карточка сертификата».

- Переход к экрану «Карточка сертификата» (см. Рисунок 47) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты доступа» (см. Рисунок 42).

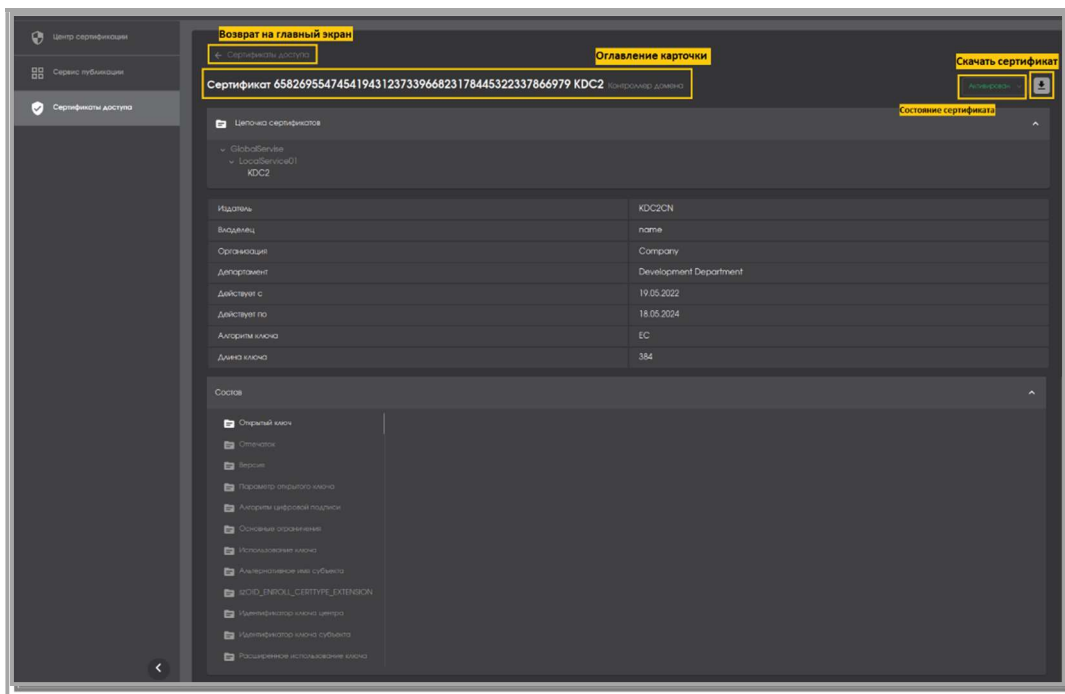




Рисунок 47 – Окно «Карточка сертификата»

- Оглавление карточки сертификата включает в себя:
  - тип-сертификат;
  - серийный номер;
  - принадлежность;
  - тип субъекта аутентификации.
- Для возврата на главный экран раздела «Сертификаты доступа» проследовать по стрелке  «Сертификаты доступа».
- Для изменения состояния сертификата выбрать из выпадающего списка действие в соответствии с Таблица 10.
- Для скачивания сертификата наведите указатель мыши на выбранный сертификат и скачайте по нажатию появившейся кнопки  «Скачать сертификат».
- Выход из карточки сертификата осуществляется по кнопке «Возврат» и по кнопкам вкладки главного меню.

### 7.5.2 Создание сертификата для нового субъекта аутентификации

- Нажатие кнопки <Создать сертификат +> на главном экране раздела «Сертификаты доступа» запускает сценарий по созданию сертификата для нового субъекта аутентификации (см. Рисунок 48).

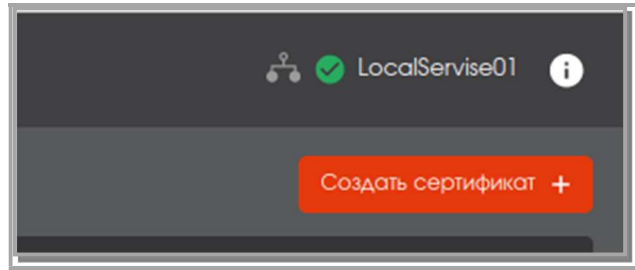


Рисунок 48 - Кнопка «Создать сертификат +»

- Для нового пользователя осуществляется выбор по радиокнопке <Создать нового пользователя или устройство> (см. Рисунок 49).

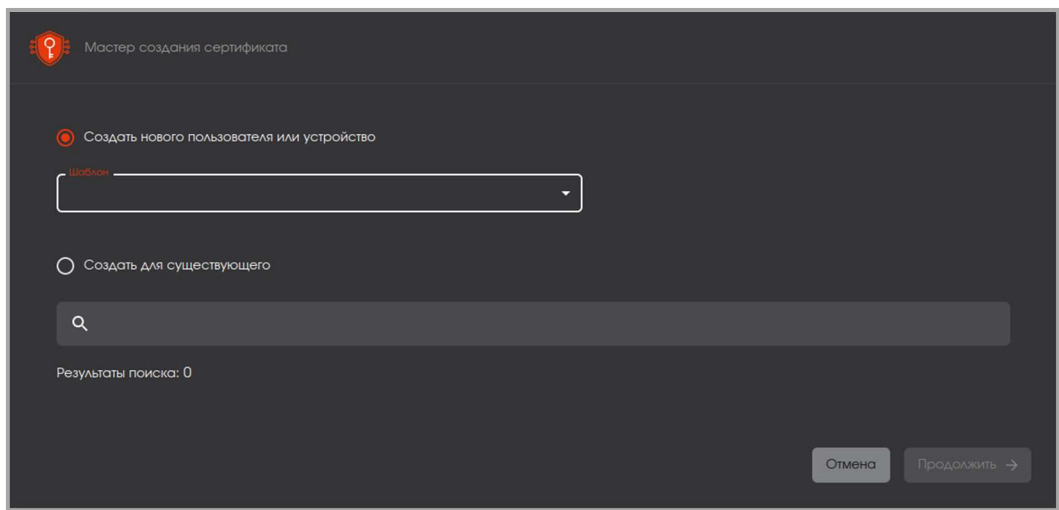


Рисунок 49 - Окно создания сертификата

- Далее из выпадающего списка администратор выбирает шаблон вида субъекта аутентификации (см. Рисунок 50) и по ставшей активной кнопке <Продолжить> переходит к следующему шагу.

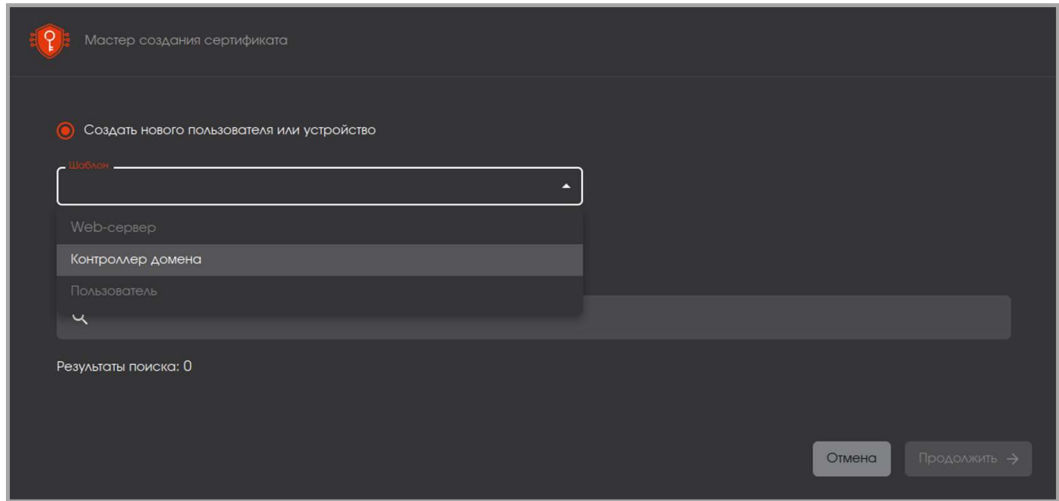


Рисунок 50 - Окно выбора шаблона

- После выбора шаблона для субъекта аутентификации открывается окно ввода данных для шаблона (см. Рисунок 51). После ввода всех данных кнопка «Продолжить» становится активной.

Вводимые данные не должны содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами.

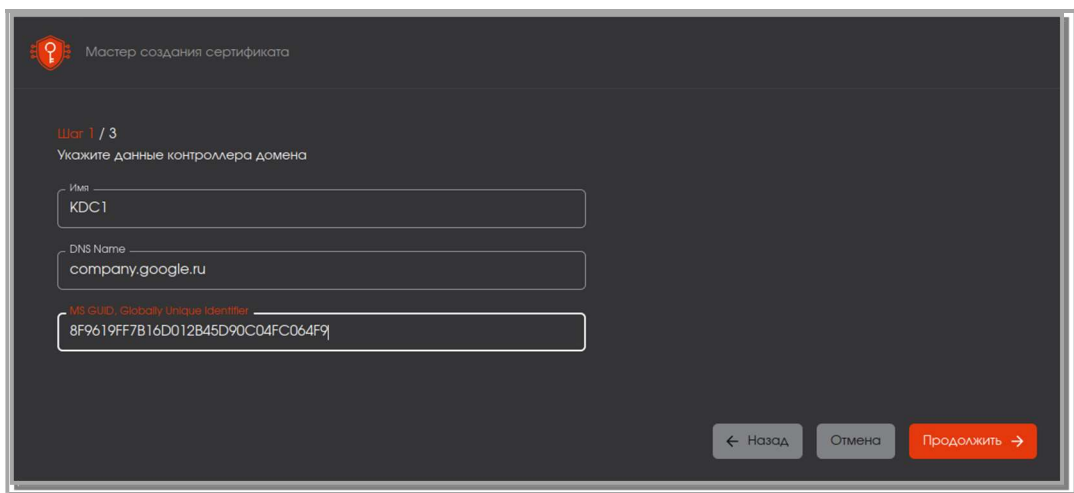



Рисунок 51 - Окно ввода данных для шаблона

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 52).

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.

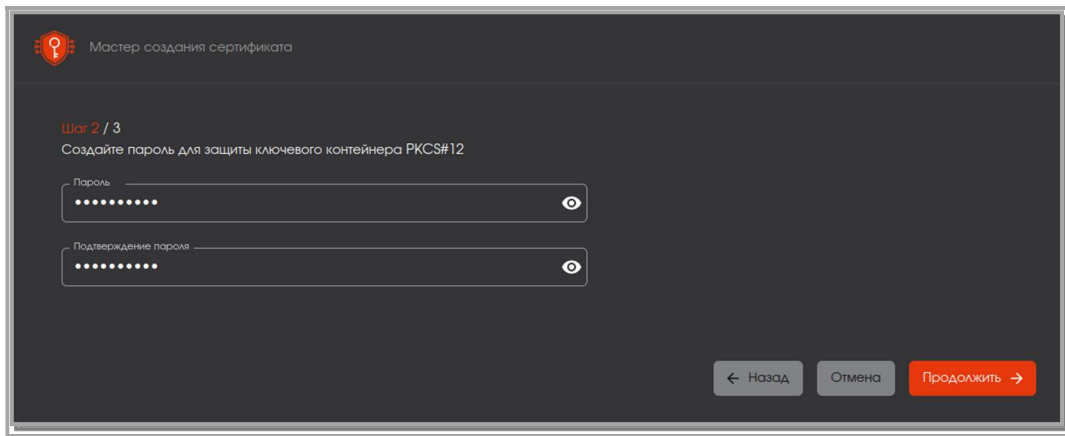


Рисунок 52 – Окно создания пароля с подтверждением

- В следующем окне требуется определить параметры шифрования:
  - алгоритм ключа;
  - длину ключа;
  - хэш-алгоритм.

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

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



Рисунок 53 - Задание параметров криптографии

- По завершению работы мастера создания сертификата субъекта аутентификации администратор видит окно, изображенное на Рисунок 54. В окне отображена общая информация о созданном сертификате (издатель, субъект, срок действия).



Существует возможность скачать созданный сертификат.

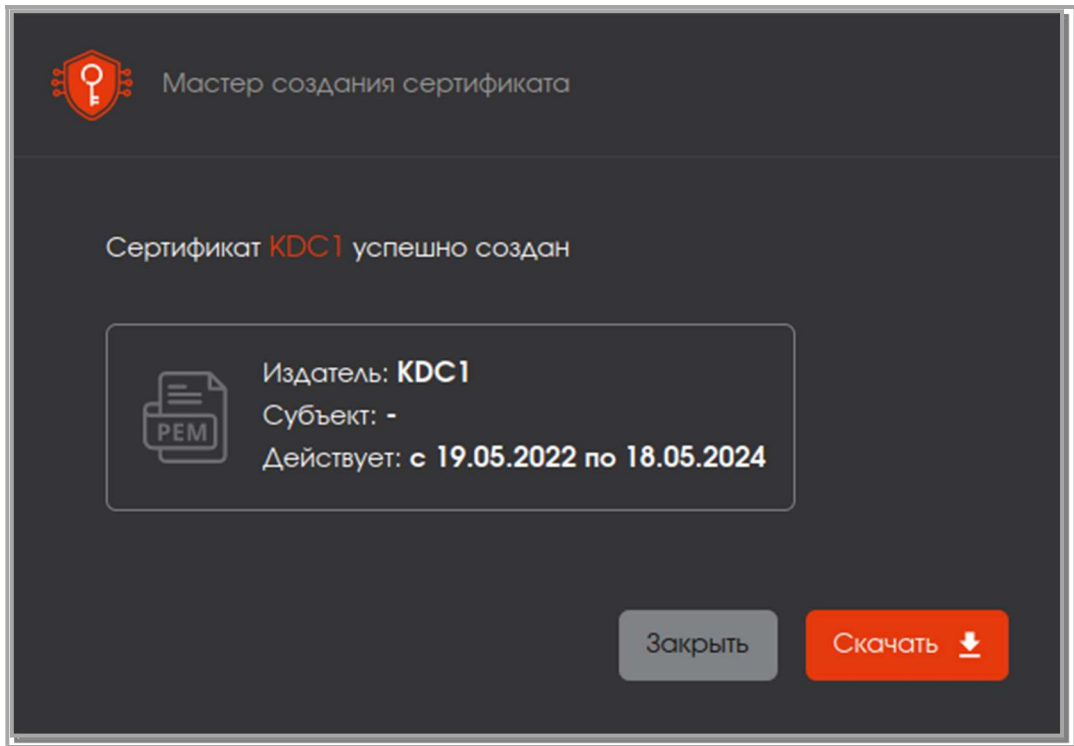


Рисунок 54 – Окно по результату успешного завершения создания сертификата

### 7.5.3 Создание сертификата для существующего субъекта аутентификации

- Нажатие кнопки «Создать сертификат +» на главном экране раздела «Сертификаты доступа» запускает сценарий по созданию сертификата для существующего субъекта аутентификации (см Рисунок 55).

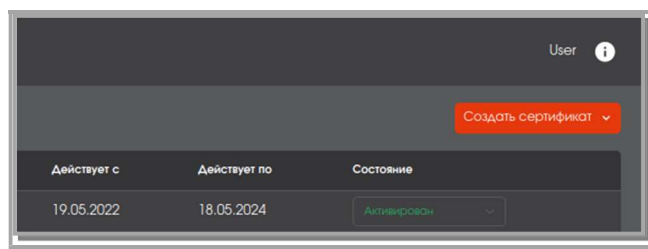


Рисунок 55 - Кнопка «Создать сертификат +»

- Далее необходимо выбрать вариант «Создать для существующего» (см. Рисунок 56).
- После выбора поля активируется строка поиска для субъекта.

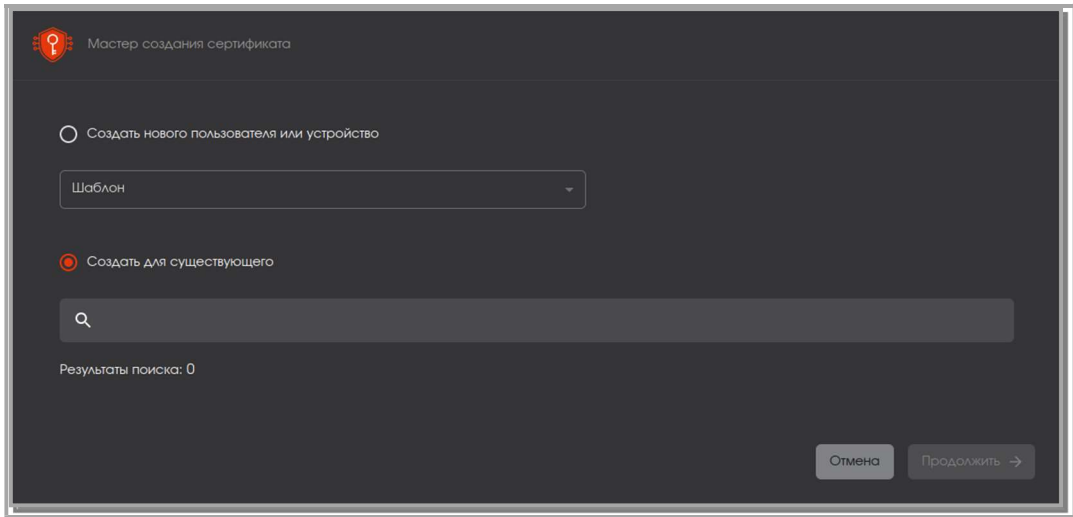


Рисунок 56 - Экран с выбранным значением «Создать для существующего»

- Поиск осуществляется путем ввода части известного параметра субъекта (id, имени, суффикса дополнительного имени), далее нажать на клавишу ENTER. При условии, что найдено не более трех субъектов, открывается страница с отображением результатов упрощенного поиска (см. Рисунок 57). Из которых возможно выбрать нужный субъект аутентификации.

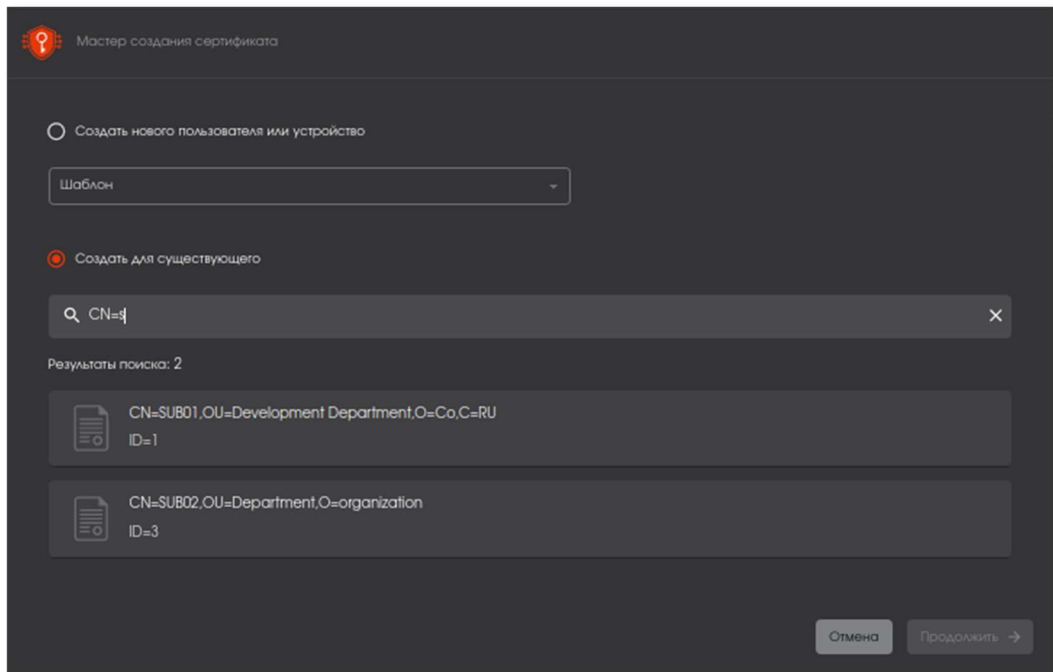


Рисунок 57 - Окно результатов поиска не более 3-х субъектов аутентификации

- Если количество найденных субъектов более трех, то система предлагает перейти к расширенному поиску (поиск по полям в формате SN=\*\*\*\*\*, DN=\*\*\*\*\*, OU=\*\*\*\*\*, O=\*\*\*\*\*, UID=\*\*\*\*\*, DC=\*\*\*\*\*, C=\*\*\*\*\*) (см. Рисунок 58).

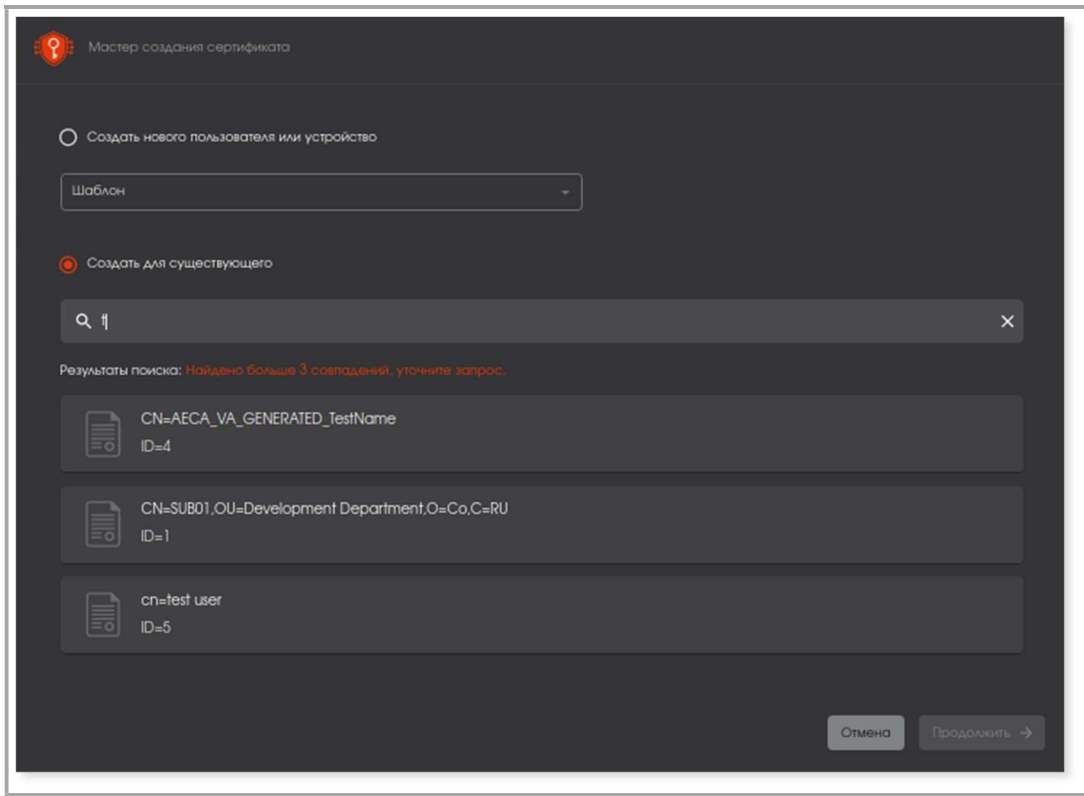


Рисунок 58 - Окно результатов поиска более 3-х субъектов аутентификации

- После поиска и выбора необходимого субъекта активизируется мастер создания сертификата.

Выполнить следующие шаги:

- выбрать шаблон сертификата из списка доступных (см. Рисунок 59). После выбора шаблона нажать активировавшуюся кнопку <Продолжить> и перейти к следующему шагу;

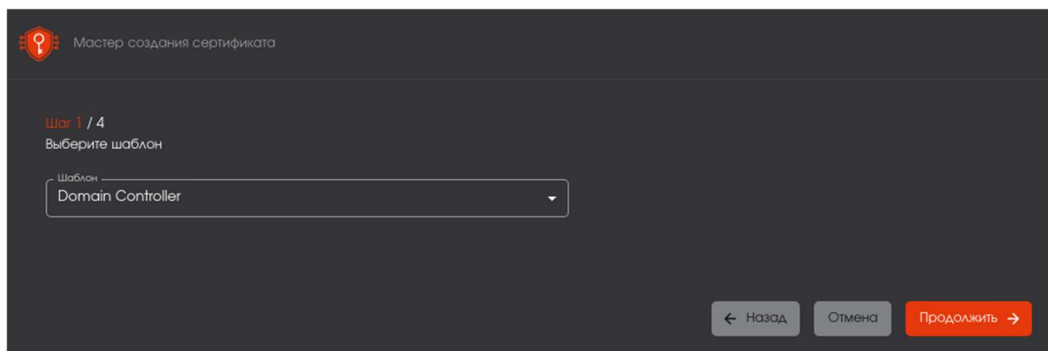


Рисунок 59 - Мастер создания сертификата. Выбор шаблона

- ввести данные из шаблона сертификата (см. Рисунок 60). Поля уже заполнены в соответствии с имеющимися данными о субъекте из имеющегося сертификата. Данные можно изменять в соответствии с поставленными задачами.

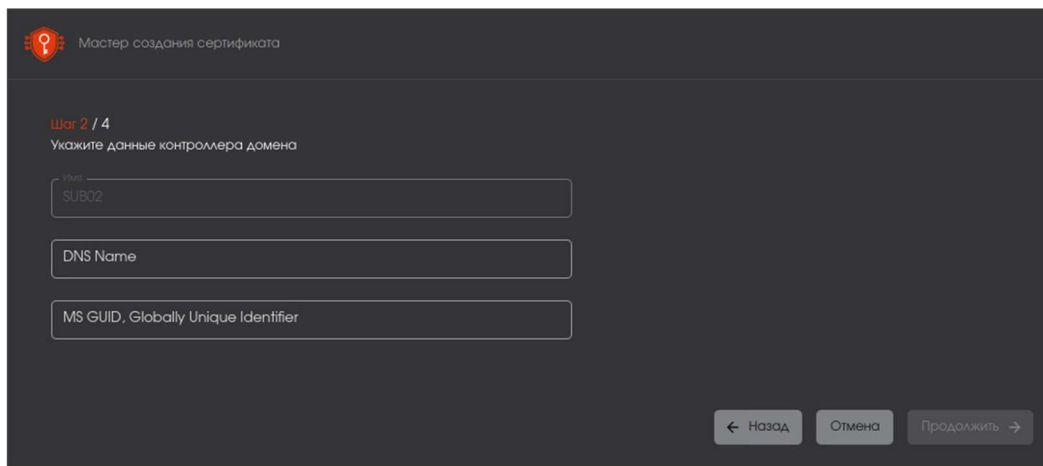



Рисунок 60 – Окно мастера создания сертификата. Ввод данных

- создать пароль с подтверждением (см. Рисунок 61) в соответствии с правилами ввода пароля.

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.

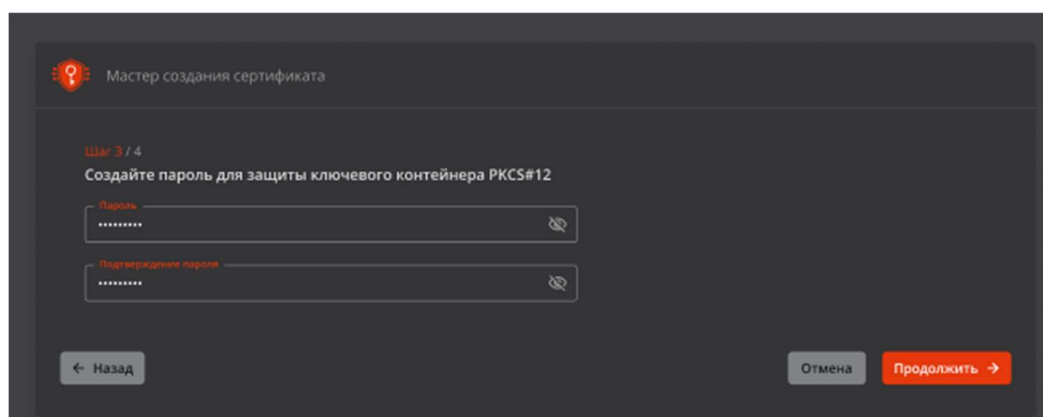


Рисунок 61 – Окно мастера создания сертификата. Задание пароля

- указать параметры шифрования (алгоритм ключа, длину ключа и хэш-алгоритм) (см. Рисунок 62).

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

Кнопка <Создать сертификат> доступна после выбора всех параметров.

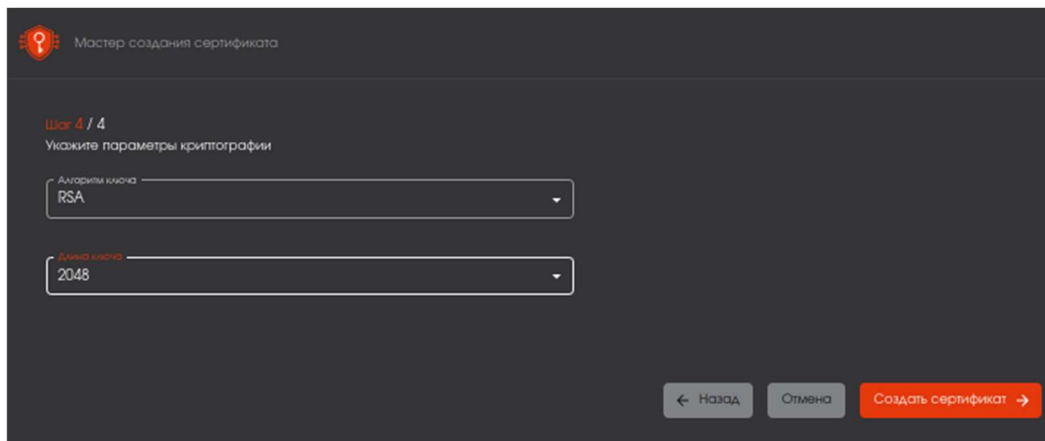


Рисунок 62 – Окно мастера создания сертификата. Задание параметров криптографии

– по завершению работы мастера создания сертификата субъекта аутентификации администратор видит окно, изображенное на Рисунок 63. В окне отображена общая информация о созданном сертификате (издатель, субъект, срок действия).

Существует возможность скачать созданный сертификат.

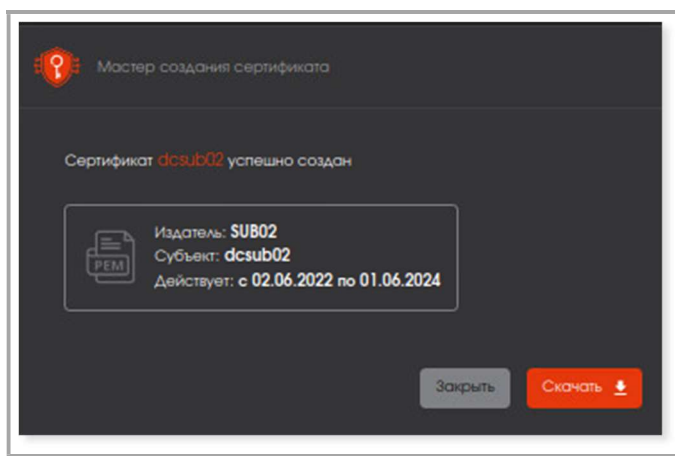


Рисунок 63 – Окно уведомления о успешном создании сертификата

#### 7.5.4 Создание сертификата субъекта аутентификации по запросу

##### 7.4.5.1 Предварительные условия выполнения сценария:

- файл-запрос для субъекта аутентификации должен быть подготовлен заранее на стороннем ЦС (например, на базе Openssl);
- расширение файл-запроса не имеет существенного значения, но предполагается, что оно будет «\*\*\*.csr» или «\*\*\*.pem»;
- файл-запрос должен быть сформирован с учетом известных данных шаблона EJBCA.

Например, для «контроллера домена» данные шаблона должны соответствовать следующим параметрам End Entity Profile – новый «Domain Controller» со следующими отличиями от значений по умолчанию:

Компоненты Subject Alt Name:

- DNS Name (required=0, modifiable=1, validation=0);
- MS GUID (required=0, modifiable=1, validation=0);
- Available certificate profile = «Domain Controller»;
- Default CA = созданный ЦС;
- Available CA = созданный ЦС (AnyCA);
- Number of allowed requests = Use, 5.

7.4.5.2 Нажатие кнопки «Создать сертификат +» на главном экране раздела «Сертификаты доступа» запускает сценарий по созданию сертификата по запросу (см. Рисунок 64) посредством мастера создания сертификата доступа по запросу.

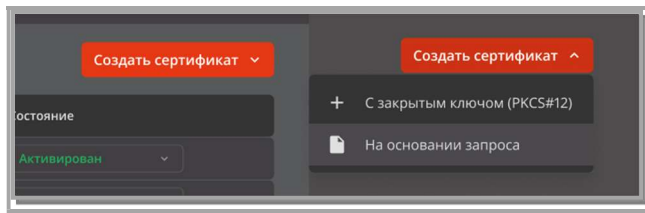


Рисунок 64 - Кнопка создания сертификата

- В открывшемся окне (см. Рисунок 65) необходимо выбрать и загрузить файл-запрос, а также выбрать шаблон сертификата в соответствии с запросом (предполагается, что администратор АЕСА заранее знает для какого субъекта загружается файл-запрос и какой шаблон необходимо выбрать).

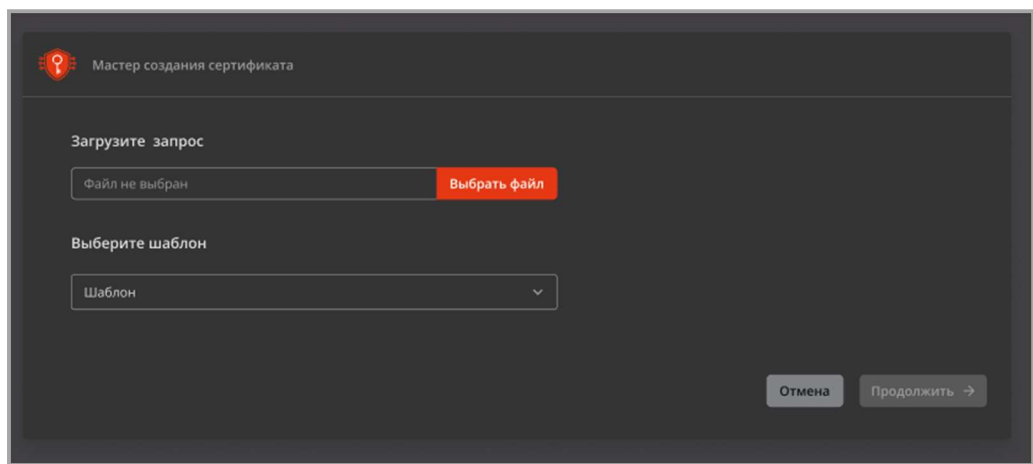


Рисунок 65 – Окно мастера по созданию сертификата. Загрузка запроса и выбор шаблона

После загрузки файла запроса и выбора шаблона нажать активировавшуюся кнопку «Продолжить» (см. Рисунок 66).

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

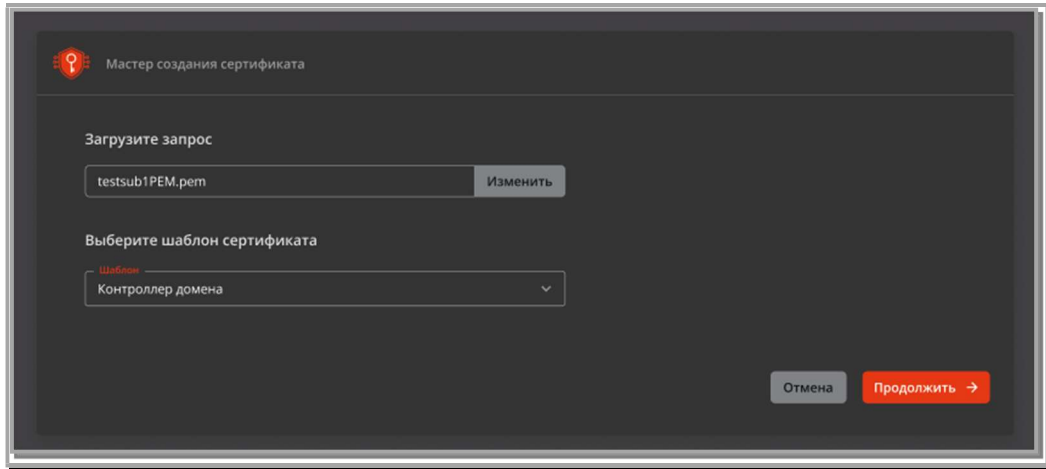


Рисунок 66 – Окно мастера по созданию сертификата. Загруженный файл-запрос

- Приложение проверяет запрос на наличие субъекта аутентификации:
  - в случае обнаружения ошибок в файле запроса см. пункт 7.4.5.3;
  - если субъект не обнаружен – создается новый субъект аутентификации, для которого выдается сертификат (см. Рисунок 67).

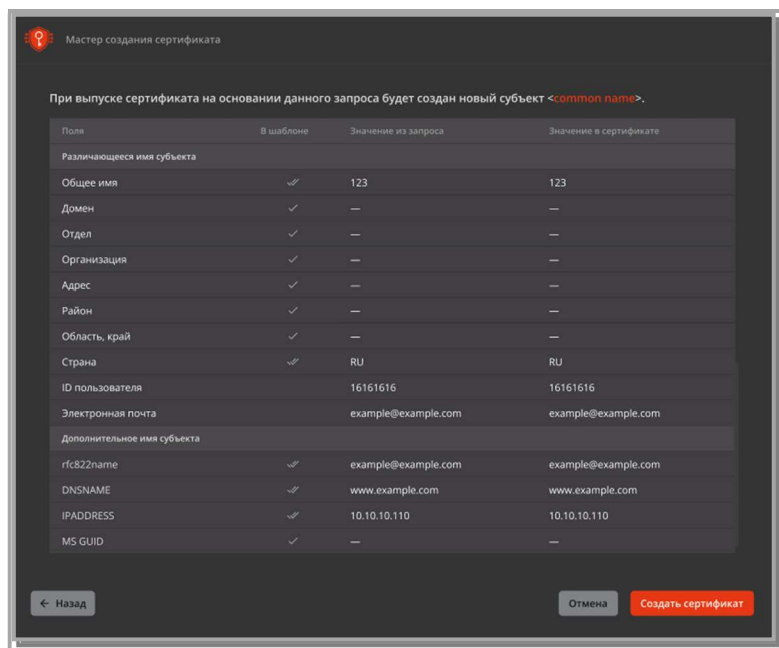


Рисунок 67 – Окно мастера создания сертификата для нового субъекта

- при соответствии данных запроса и выбранного шаблона открывается окно с данными шаблона и принятыми данными из файла запроса (см. Рисунок 68).

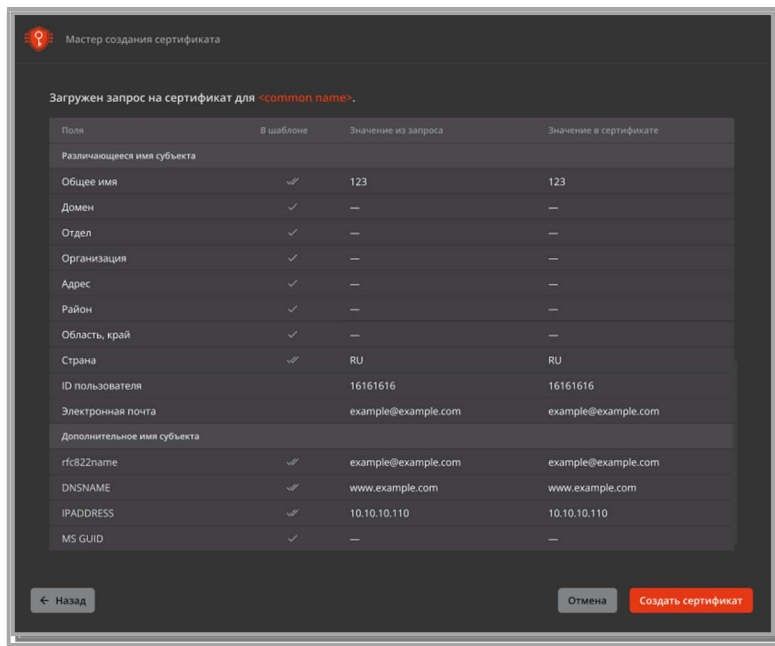


Рисунок 68 – Окно мастера создания сертификата для существующего субъекта

**ВНИМАНИЕ!** Окно с данными шаблона на Рисунок 67 и Рисунок 68 приведено в ознакомительных целях, количество и наименование полей зависят от выбранного шаблона.

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

В окне мастера создания сертификата для существующего и нового субъектов обозначены:

- обязательные к заполнению поля шаблона, отмеченные знаком  и необязательные поля шаблона, отмеченные знаком ;
- значения запроса, соответствующие полям шаблона сертификата;
- финальное представление данных, попадающих в сертификат доступа.

Отображение данных в окне мастера создания сертификата для существующего и нового субъектов разделены на две основные части:

- различающееся имя субъекта (Subject DN)
- дополнительное имя субъекта (Subject AltName).

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

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно мастера создания сертификатов доступа и отображается краткая информация о созданном сертификате (см. Рисунок 69).

Существует возможность скачать сертификат доступа.



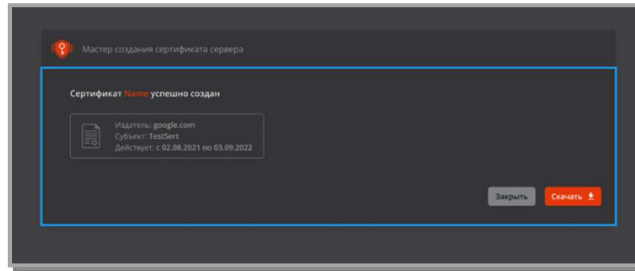


Рисунок 69 - Финальное окно мастера создания сертификатов

7.4.4.3 В случае обнаружения ошибок или несоответствия обязательных полей параметров шаблона в файле запроса при проверке мастером создания сертификата в таблице сравнения появляется ошибка:

- для нового субъекта (см. Рисунок 70);

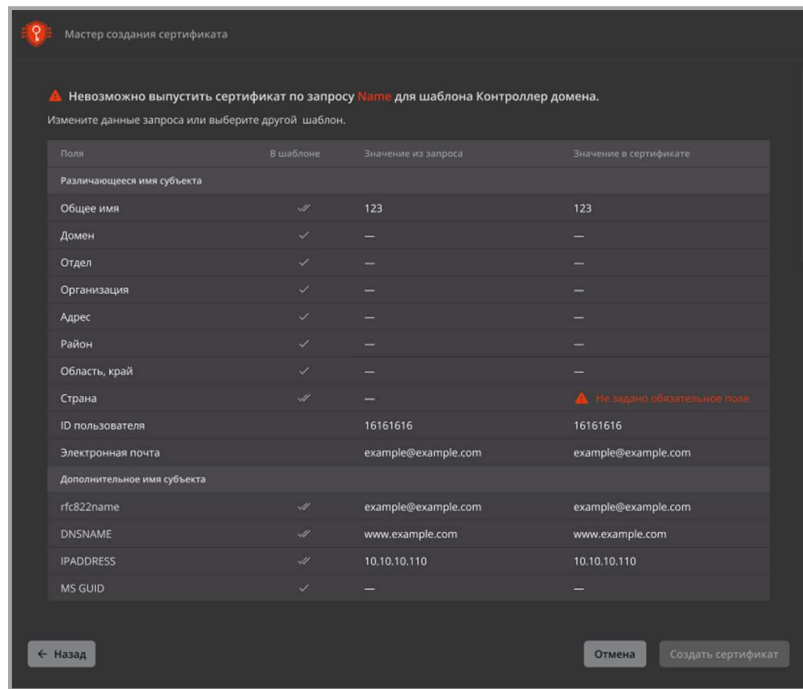


Рисунок 70 - Экран ошибки для нового субъекта аутентификации

- для существующего субъекта (см. Рисунок 71).

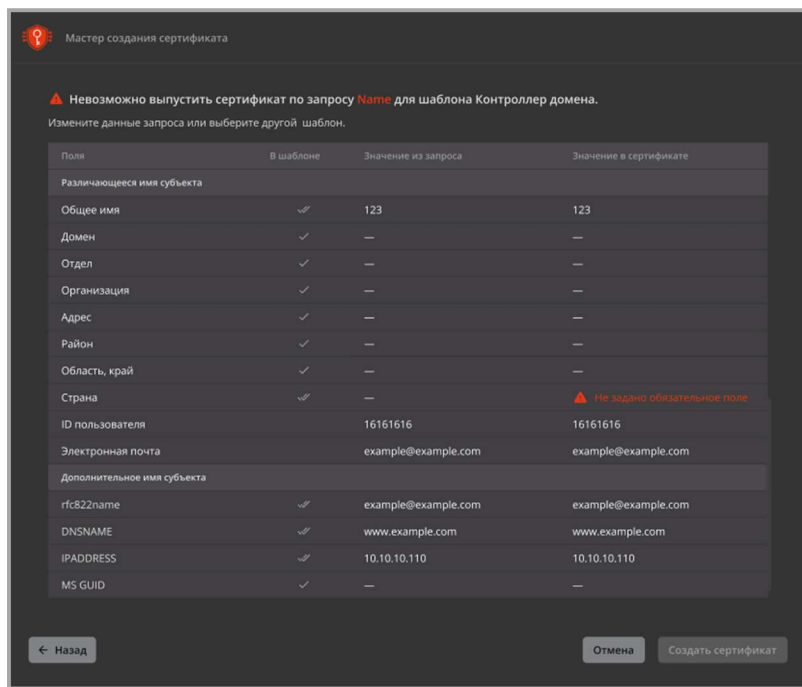


Рисунок 71 - Экран ошибки для существующего субъекта аутентификации

- В таком случае создание сертификата невозможно и 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 в АЕСА.

## 7.6 Описание вкладки «Сервисы OCSP»

Переход на вкладку «Сервисы OCSP» осуществляется через боковое меню, расположенное слева на главном экране (см. [Рисунок 72](#) [Рисунок 14](#)).

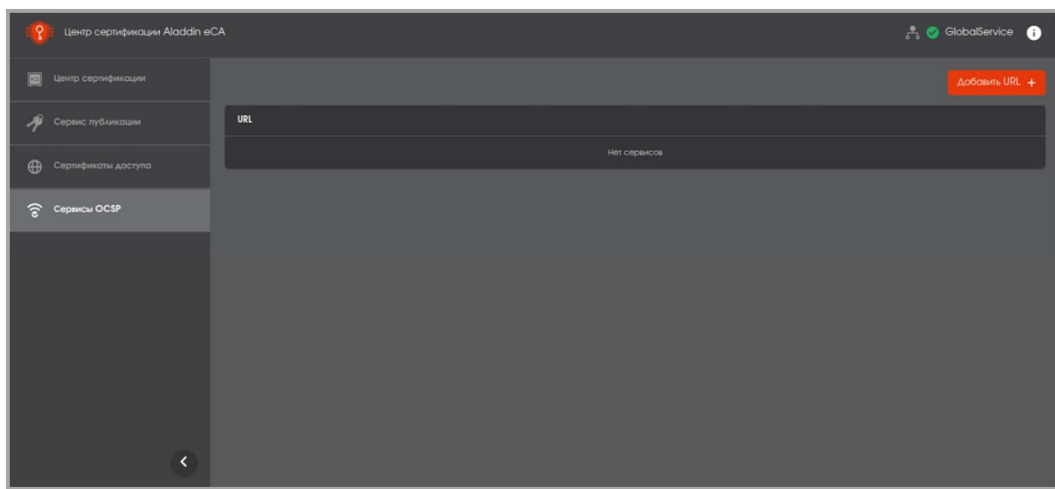


Рисунок 72 – Экран раздела меню "Сервисы OCSP"

На данном экране отображаются добавленные URL-адреса сервисов OCSP, созданных в «Центре валидации AeCA» для текущего активного ЦС.

### 7.6.1 Добавление URL-адреса сервиса OCSP

Для автоматического задания атрибута сертификата, содержащего адрес службы OCSP необходимо:

- предварительно скопировать URL-адрес OCSP в «Центре валидации AeCA» для текущего активного ЦС (см. п. 8.2.2) и передать его в «Центр сертификации AeCA» на APM активного ЦС;
- нажать кнопку <Добавить URL+> (см. Рисунок 73);

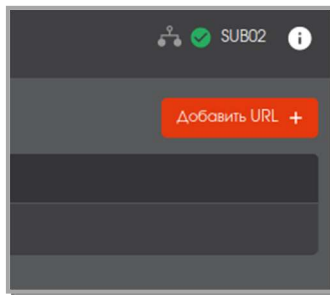


Рисунок 73 – Кнопка <Добавить URL+>

- в появившемся окне (см. Рисунок 74) ввести скопированный URL-адрес сервиса OCSP, соответствующий текущему активному ЦС;

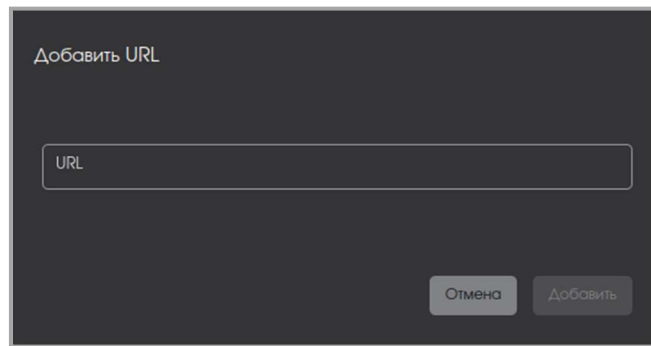


Рисунок 74 – Добавление URL-адреса

- нажать ставшую доступной кнопку <Добавить>;
- URL-адрес сервиса OCSP успешно добавлен! (см. Рисунок 75).

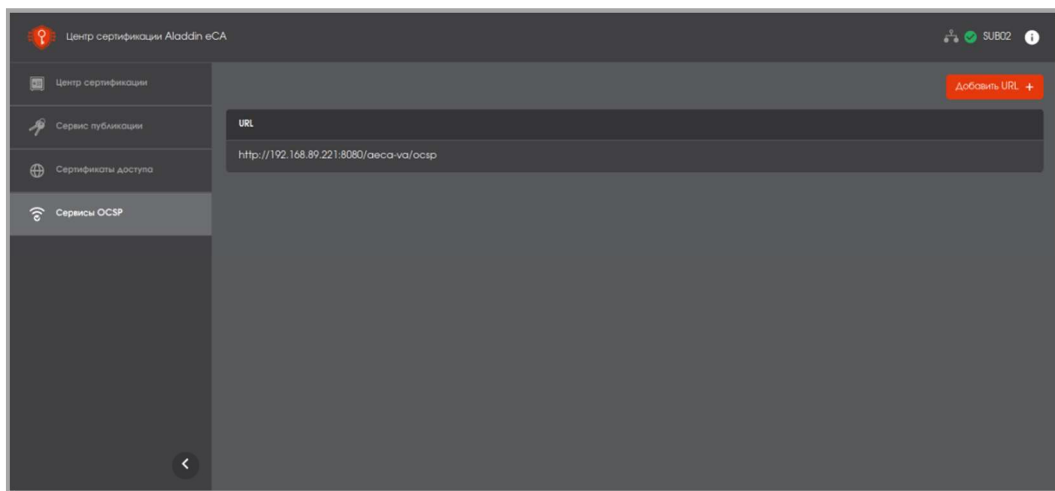


Рисунок 75 – Окно экрана Сервисы OCSP с добавленным URL-адресом сервиса OCSP

## 7.6.2 Проверка наличия URL-адреса OCSP в атрибуте сертификата субъекта аутентификации

7.6.2.1 Проверка сертификата доступа выполняется при необходимости и не является обязательной процедурой.

- В ПО «Центр сертификации AeCA» скачать нужный сертификат доступа.
- В терминале ОС перейти в папку с сохраненным сертификатом доступа формата .pem, выполнив команду:

```
cd {имя папки} /
```

- Для вывода и просмотра содержимого файла сертификата в командной строке, выполнить команду:

```
cat {имя сертификата}.pem
```

- Для проверки наличия в сертификате URL-адреса OCSP, выполнить команду:

```
openssl x509 -noout -ocsp_uri -in ./{имя сертификата}.pem
```

Пример успешного ответа:

```
http://192.168.89.221:8080/aeca-va/ocsp
```

- Скопировать ответ сервера для использования в следующем шаге.
- С помощью команды OpenSSL отправить запрос OCSP:

```
openssl ocsf -issuer {имя ЦС*}.pem -CAfile {имя ЦС*}.pem -url {URL OCSP} -cert {имя сертификата}.pem -no_nonce
```

где {имя ЦС\*} - имя ЦС, выпустившего проверяемый сертификат доступа; {URL OCSP} – ранее скопированный адрес сервиса OCSP.


- Получить текстовый результат и убедиться, что сертификат содержит URL-адрес OCSP:

```
Response verify OK
```

```
{имя сертификата}.pem: good
```

```
    This Update: {месяц} {число} {время} {год} GMT
```

7.6.2.2 Значение данного атрибута также можно увидеть в карточке сертификата (см. п. 7.5.1) для этого:

- перейти на вкладку бокового меню Сертификаты доступа;
- щелкнуть мышью по строке с сертификатом;
- в открывшейся карточке сертификата раскрыть подменю «Состав», нажав кнопку ;
- в открывшемся меню выбрать поле «Доступ к информации о центре сертификации»;
- убедиться, что в правой части экрана отображена информация для доступа к службе актуальных статусов сертификатов в онлайн-режиме.

## 8 НАСТРОЙКА ПО «ЦЕНТР ВАЛИДАЦИИ» ALADDIN ENTERPRISE CA

В результате установки Программного компонента «Центр Валидации Aladdin eCA» в консоли ОС отобразится информация о конфигурации установленного приложения, а также учетные данные администратора (логин и пароль для первого входа в приложение).

### 8.1 Первичная инициализация Alladin eCA VA

8.1.1 Только для **RED OS 7.3**, при необходимости произвести установку браузера Mozilla Firefox, выполнить команду:

```
sudo dnf install firefox
```

8.1.2 Открыть браузер Firefox.

8.1.2 Для импортирования пакета .p12 в браузер из директории <директория\_хранения\_пакета\_p12> выберете меню приложения «Настройки»;

8.1.3 Выбрать вкладку "Приватность и защита", нажать кнопку «Просмотр сертификатов» (см. Рисунок 76).

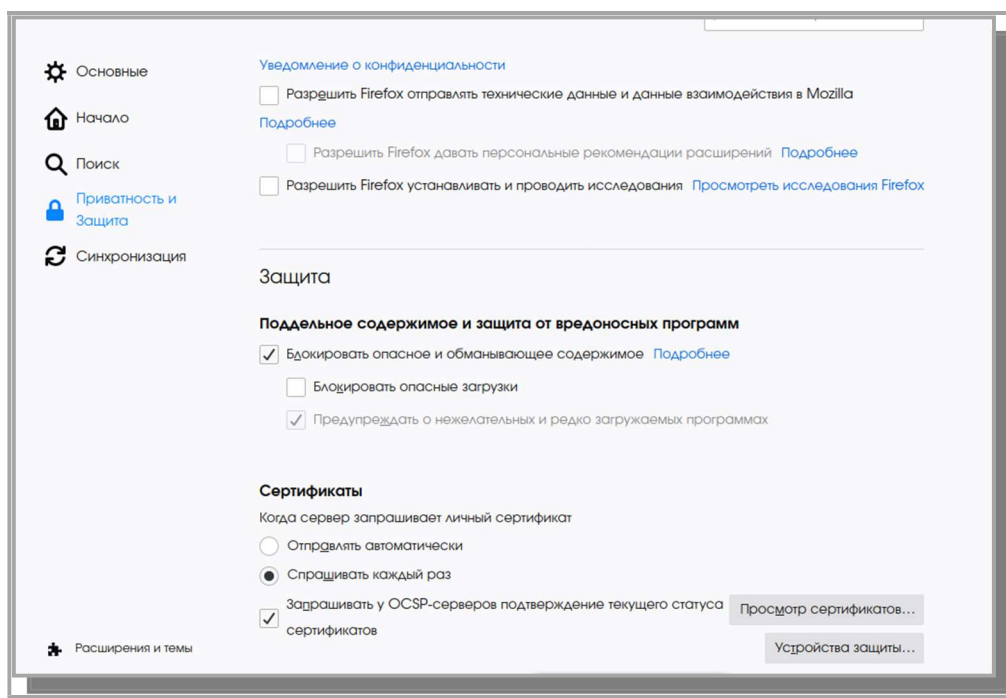


Рисунок 76 – Окно настроек браузера

8.1.4 Выбрать вкладку «Ваши сертификаты», в открывшейся вкладке нажать кнопку «Импортировать» (см. Рисунок 77).

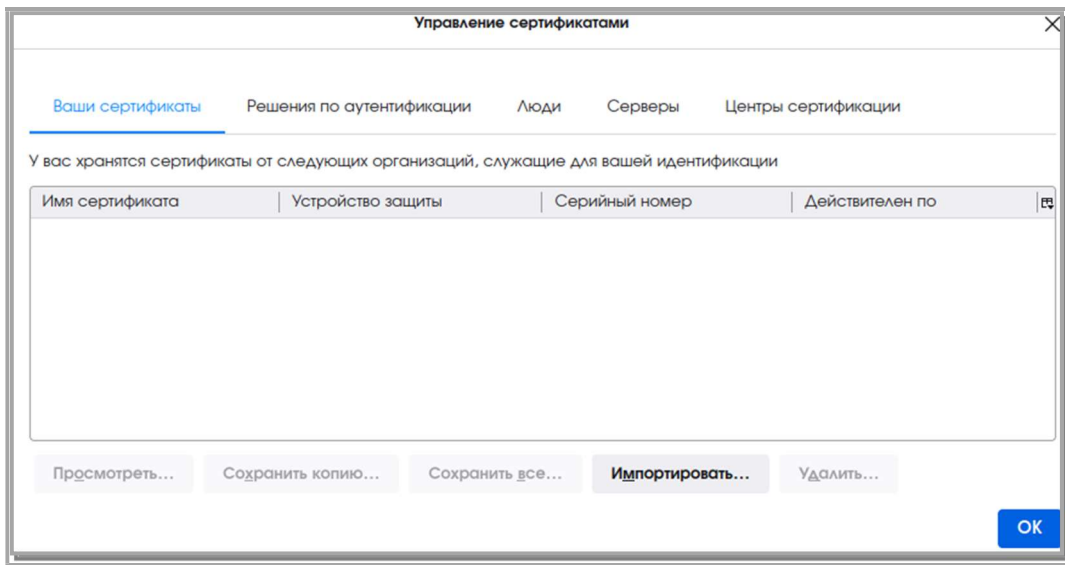


Рисунок 77 – Окно управления сертификатами

8.1.5 В директории хранения пакета. p12 найти созданный на этапе установки файл сертификата `/opt/aeca/p12/superadmin.p12`. Нажать кнопку <Открыть> (см. Рисунок 78).

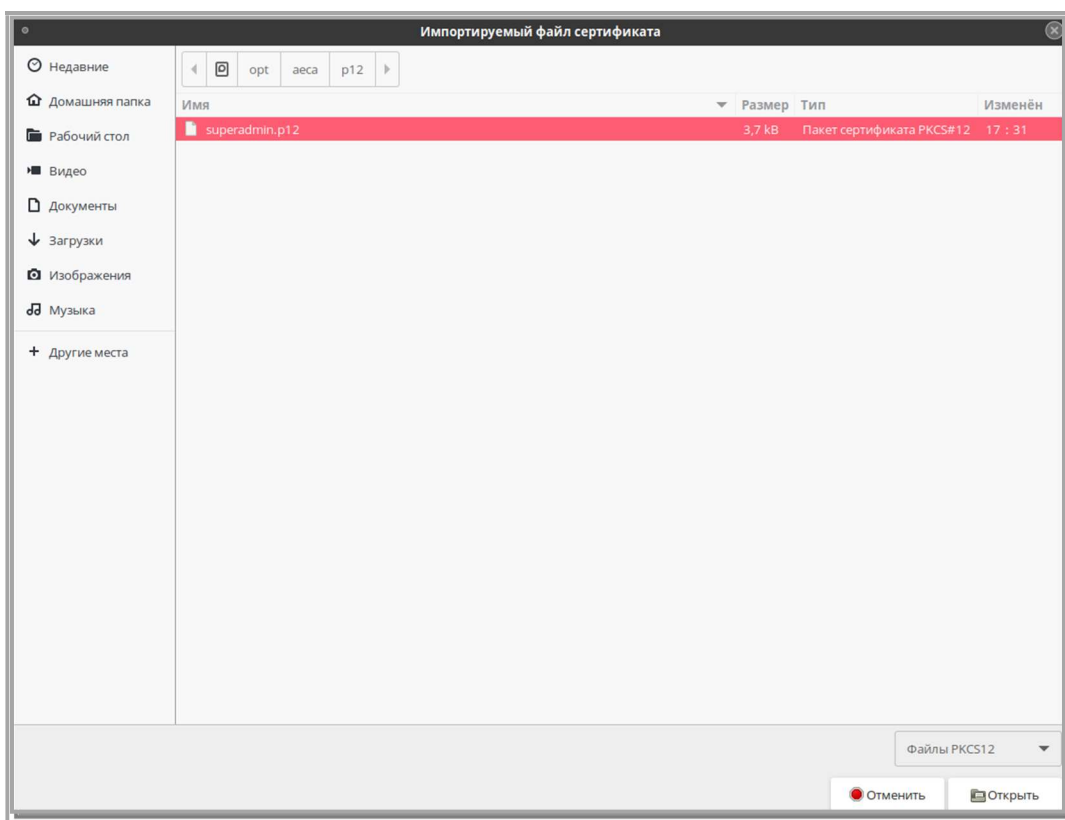


Рисунок 78 – Окно выбора импортируемого файла сертификата

8.1.6 В открывшемся окне (см. Рисунок 79) ввести пин-код сертификата (данные предоставляются по завершению установки, а также доступны в директории установленного приложения `opt/aeca/p12/generated_passwords.txt` – см. Рисунок 80). Нажать кнопку <Ок>.

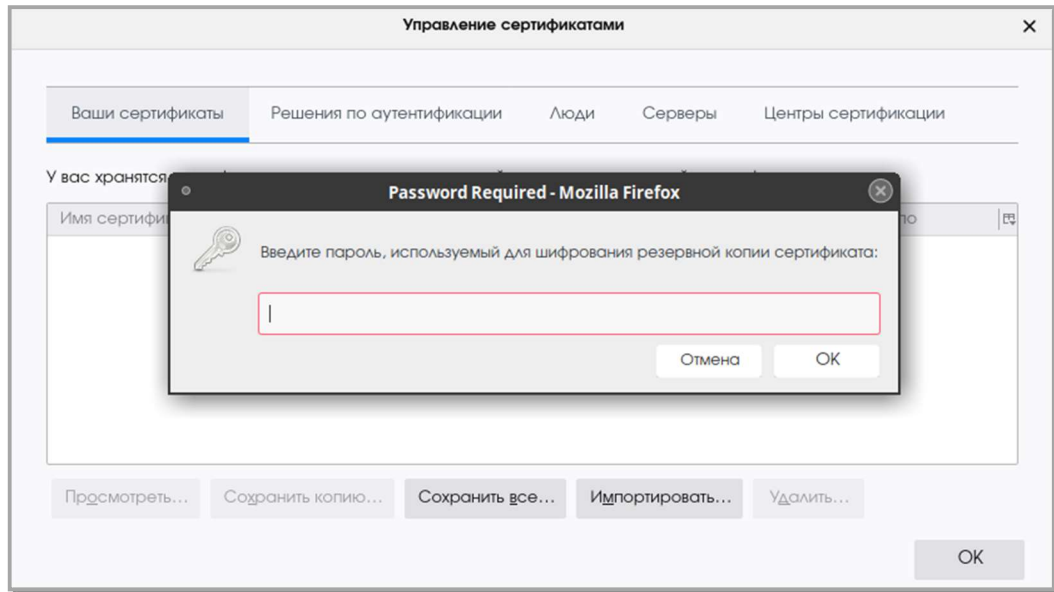


Рисунок 79 – Окно ввода пин-кода сертификата

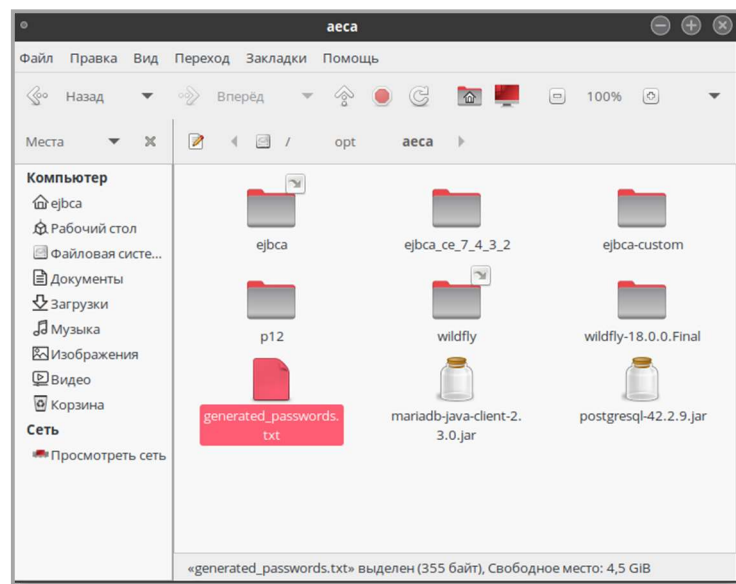


Рисунок 80 – Папка расположения файла с пин-кодом

8.1.7 В качестве пин-кода необходимо использовать данные строки `superadmin_password` из файла `generated_passwords.txt` (см. **Рисунок 8**).



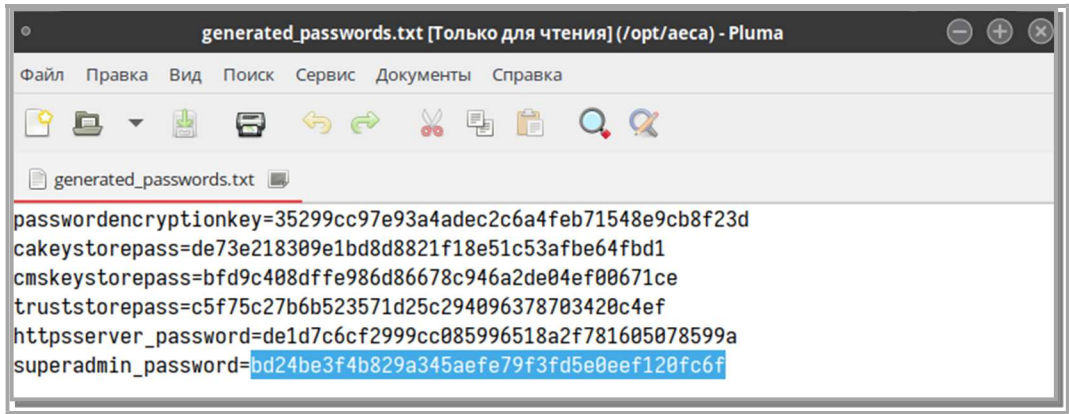


Рисунок 81 – Окно файла generated\_passwords.txt

8.1.8 В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 82). Нажать кнопку <ОК>.

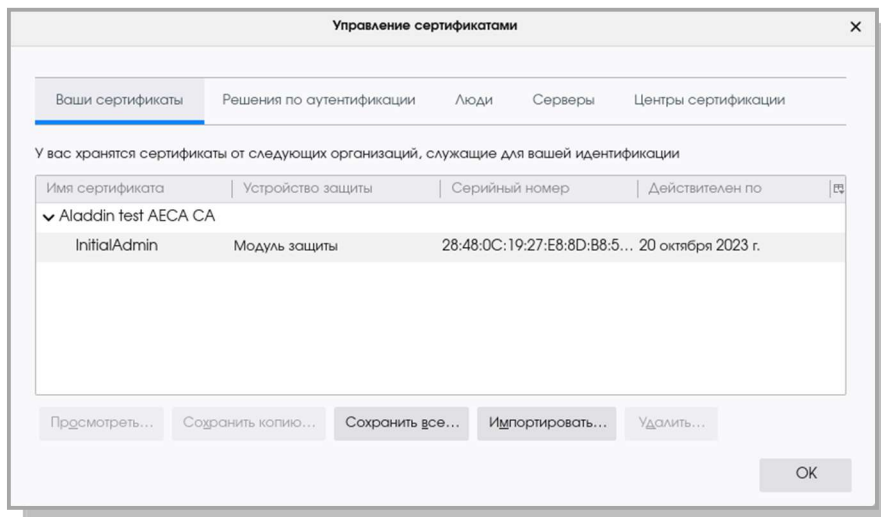


Рисунок 82 – Окно «Управление сертификатами»

8.1.9 В адресную строку браузера ввести URL в формате `<адрес_хоста_развертывания_продукта>:<порт>/<aecaVa>/`.

Например:

```
https://localhost:8888/aecaVa/
```

- Если сертификат пользователя не импортирован, то откроется страница с сообщением об ошибке (см. Рисунок 83).

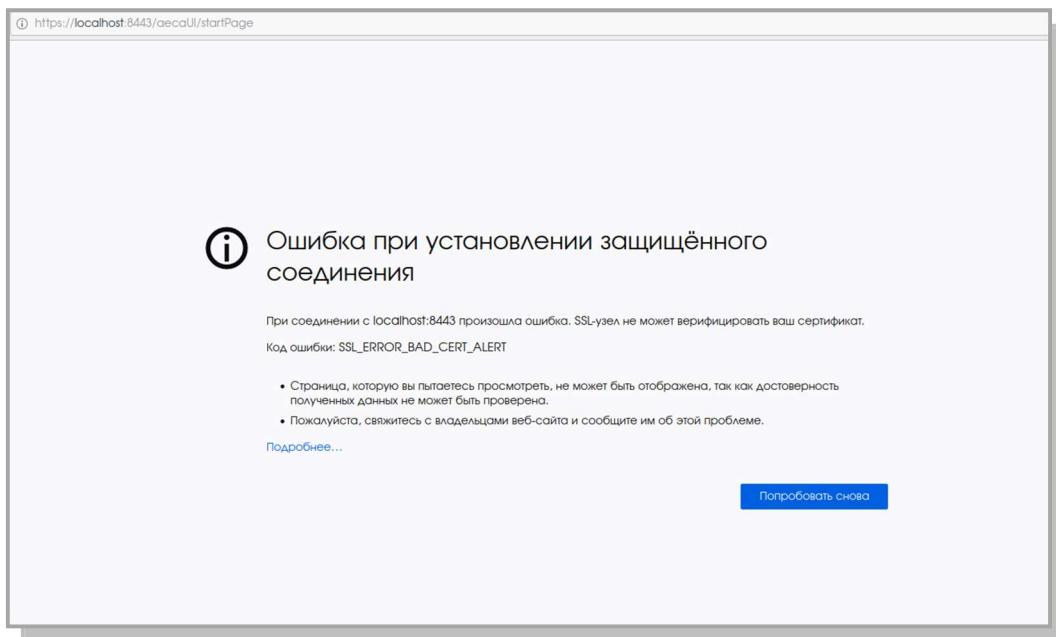


Рисунок 83 – Страница с сообщением об ошибке

- В случае успешной установки сертификата откроется страница с предупреждением системы безопасности (см. Рисунок 84). Нажать кнопку <Advanced>.

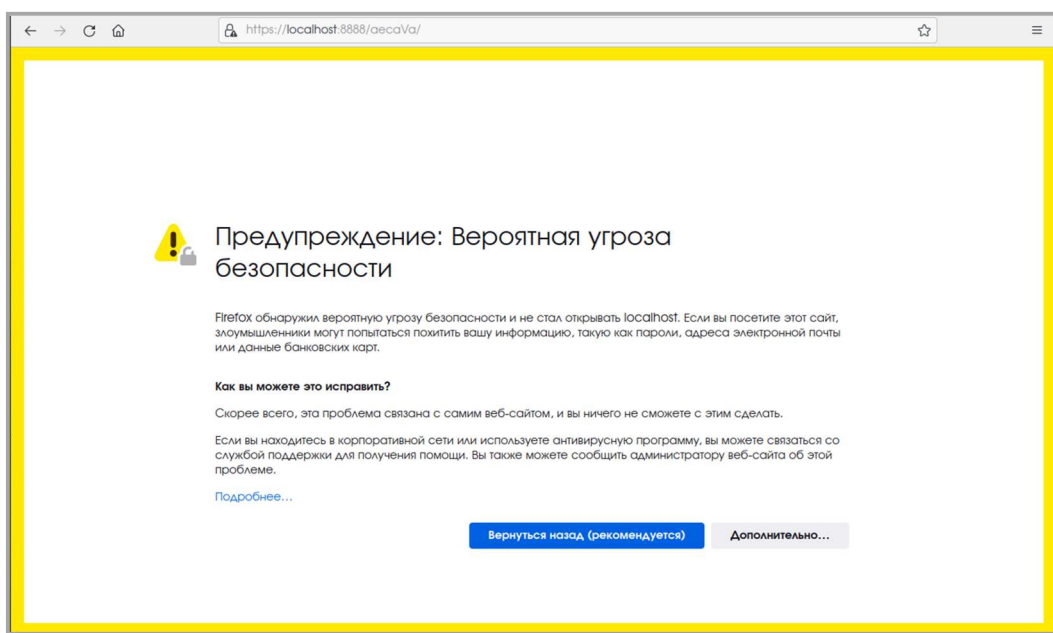
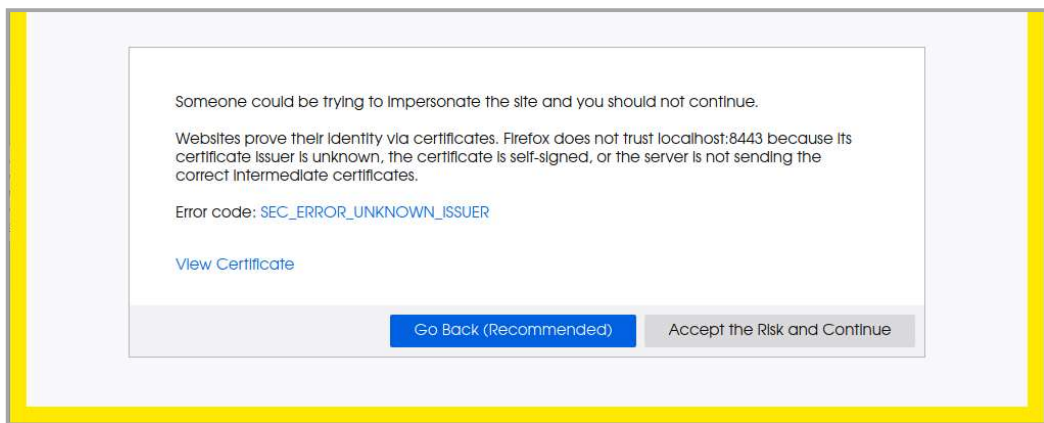


Рисунок 84 – Страница с предупреждением системы безопасности

8.1.10 По нажатию кнопки <Advanced> на странице предупреждения системы безопасности (см. Рисунок 84) осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 85). Нужно принять риски, нажав кнопку <Accept the Risk and Continue> на текущей странице.



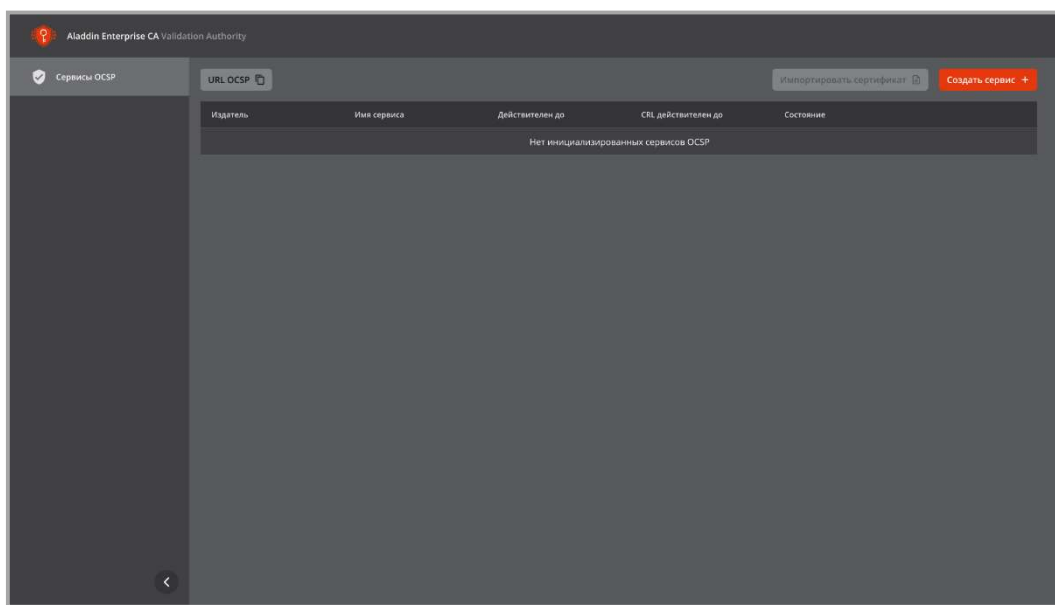
**Рисунок 85 – Страница ошибки распознавания сертификата**

8.1.11 Далее осуществляется переход на страницу Центра валидации AeCA (см. Рисунок 86).

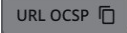
8.1.12 Установка и предварительный ввод в эксплуатацию Изделия завершены, все компоненты центра валидации Aladdin eCA установлены и готовы к работе.

## 8.2 Вкладка «Сервисы OCSP»

8.2.1 При первом старте администратору доступен экран управления сервисами OCSP (см. Рисунок 86).



**Рисунок 86 - Главный экран управления сервисами OCSP**

8.2.2 По нажатию кнопки на главном экране управления сервисами OCSP  происходит копирование URL службы OCSP (по этому URL будет доступен каждый OCSP) (см. Рисунок 87).

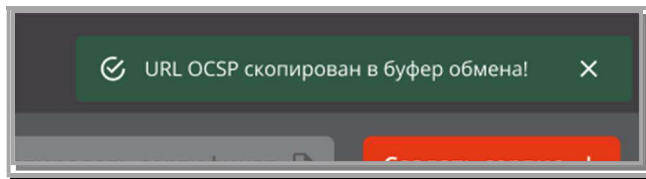


Рисунок 87 - Уведомление об успешном копировании URL службы OCSP

8.2.3 По нажатию кнопки на главном экране управления сервисами OCSP происходит запуск сценария создания сервиса OCSP.

Создать сервис +

Кнопка **Импортировать сертификат** будет доступной при наличии сервисов на главном экране управления сервисами OCSP в состоянии «Ожидает сертификат».

8.2.4 С помощью Службы актуальных статусов сертификатов вы можете в онлайн-режиме проверять статус сертификатов на основе протокола OCSP (Online Certificate Status Protocol).

Для настройки параметров доступа к службе необходимо выполнить нижеописанные процедуры.

### 8.2.1 Создание сервиса OCSP

Перед созданием сервиса OCSP требуется предварительно:

- скачать цепочку сертификатов ЦС, согласно п.7.3.1.6, для которого создаем сервис OCSP и перенести цепочку сертификатов на АРМ, на котором происходит настройка «Центра валидации».
- настроить сервис публикации центра сертификации, для которого создаем сервис OCSP и передать на АРМ, на котором происходит настройка «Центра валидации», указатель ресурса точки распространения CRL.

8.2.1.1 На экране управления сервисами OCSP по нажатию на кнопку <Создать сервис +> открывается окно мастера создания сервиса OCSP.

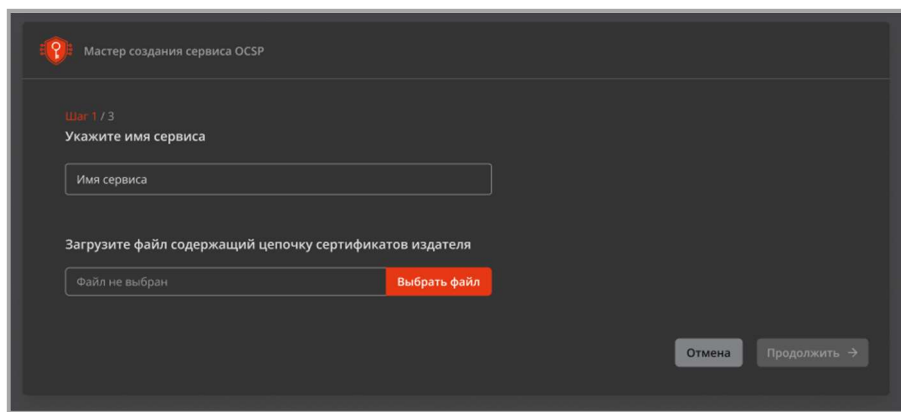


Рисунок 88 – Окно мастера создания сервиса OCSP. Шаг 1

8.2.1.2 В открывшемся окне заполнить следующие поля:

- имя сервиса – имя, которое должно попасть в Common Name запроса на сертификат службы OCSP и соответствующего сертификата службы OCSP;
- указать файл формата .pem, содержащий цепочку сертификатов;

Пример заполнения полей на данном шаге приведен на Рисунок 89.

Возможные ошибки, которые могут привести к завершению создания сервиса:

- файл неверного формата. Загрузите, пожалуйста, файл в формате PEM;
- сертификат не действителен. Загрузите, пожалуйста, файл, содержащий валидную цепочку сертификатов.

В рамках данного сценария не проверяется валидность CRL.

После выбора файла и нажатия кнопки <Продолжить> файл импортируется.

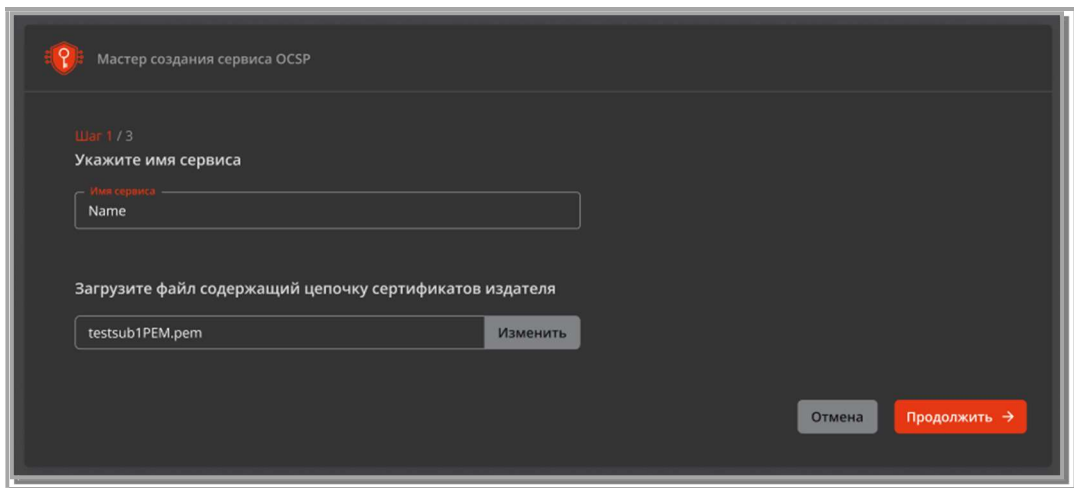


Рисунок 89 - Пример заполнения полей на шаге 1

8.5.1.3 В случае успешного импорта файла, администратор переходит на следующий экран мастера создания сервиса OCSP (см. Рисунок 90).

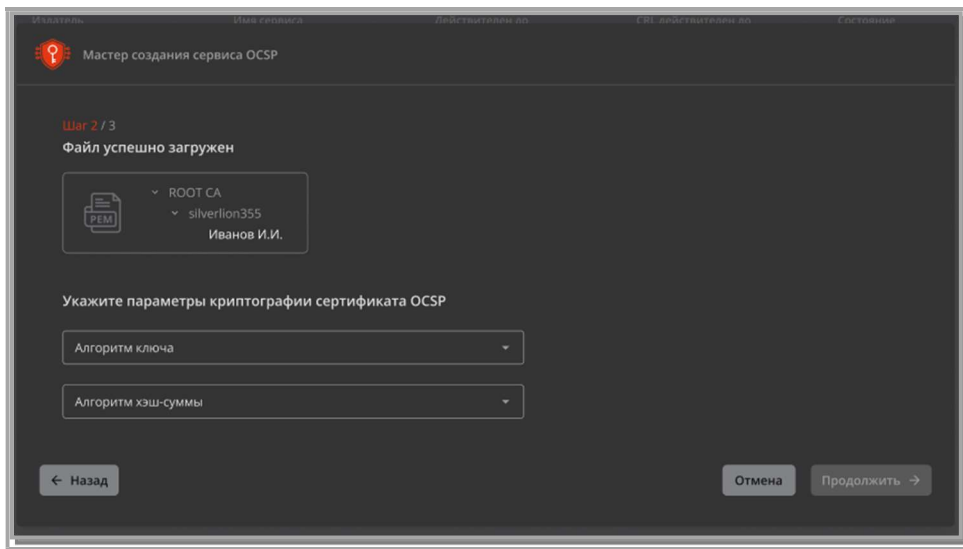


Рисунок 90 – Окно мастера создания сервиса OCSP. Шаг 2

На экране появится подтверждение успешной загрузки с отображением полной цепочки сертификатов, а также полей с выпадающими списками, где администратор указывает параметры криптографии создаваемого сервиса:

- алгоритм ключа;
- алгоритм хэш-суммы.

Пример заполнения полей на данном шаге приведен на Рисунок 91.

После указания параметров криптографии создаваемого сервиса нажать кнопку <Продолжить>.

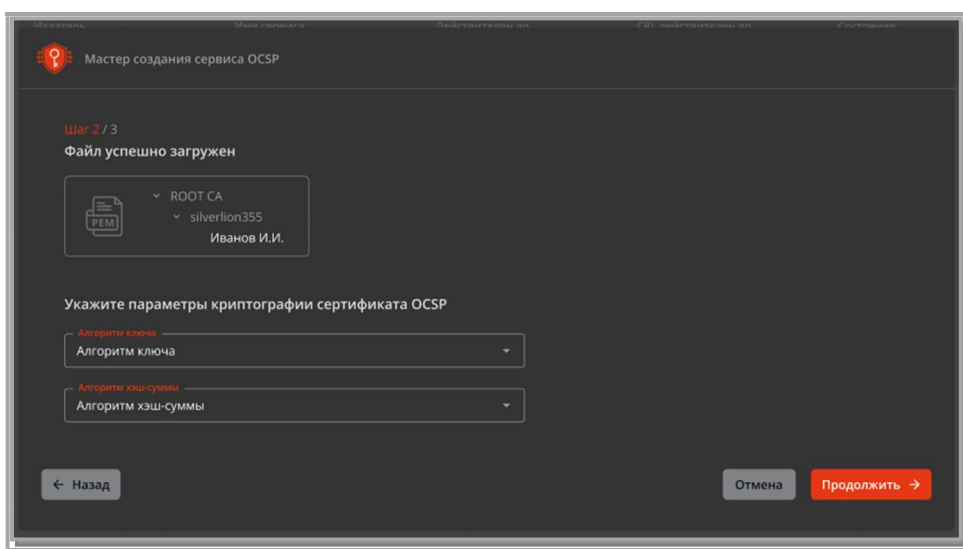


Рисунок 91 - Пример заполнения полей на шаге 2

8.5.1.4 Следующим шагом является задание параметров CRL на экране мастера создания сервиса OCSP (см. Рисунок 92).

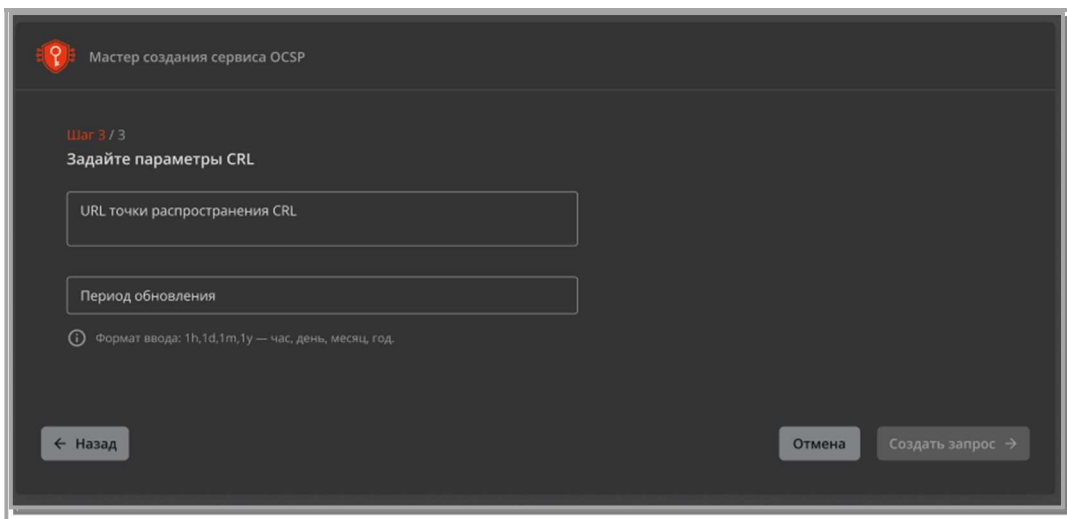


Рисунок 92 – Окно мастера создания сервиса OCSP. Шаг 3

В открывшемся окне заполнить следующие поля:

- <URL точки распространения CRL> – указать путь скачивания CRL того ЦС, статус сертификатов которого будет проверяться;
- <Период обновления> - задание периода опроса CRL DP. Формат ввода: 1h,1d,1m,1y — час, день, месяц, год.

На каждом шаге создания сервиса OCSP администратору доступны кнопки:

- <Назад> - для возврата на предыдущий шаг;
- <Отмена> - для прекращения процесса создания сервиса.

После указания параметров CRL нажать ставшую активной кнопку <Создать запрос>.

8.5.1.5 Финальным шагом является экран с результатом успешного создания запроса на сертификат для службы OCSP, где администратору доступны кнопки (см. Рисунок 93):

- <Скачать> - для скачивания сформированного запроса на сертификат;
- <Закреть> - мастер закрывается и происходит возврат в главное окно. В списке сервисов появляется запись в состоянии «Ожидание сертификата».

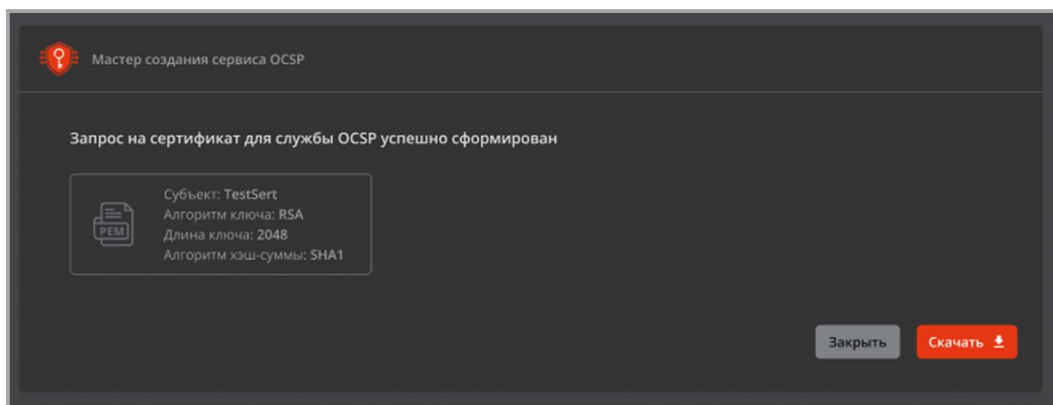


Рисунок 93 - Окно мастера создания сервиса OCSP. Шаг 4

Созданный сервис отобразится в списке сервисов OCSP на главном экране «Сервисы OCSP» в состоянии «Нужно импортировать сертификат сервиса» (см. Рисунок 94).

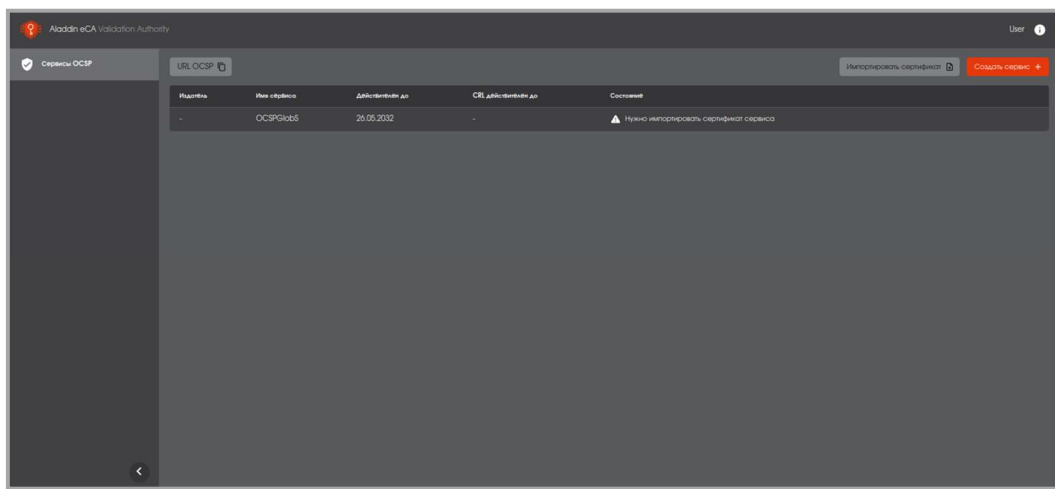




Рисунок 94 – Главный экран. Список сервисов OCSP

При наведении на строку с нужным сервисом будут доступны иконки  «Скачать» и  «Удалить».

8.5.1.6 Для дальнейшего подписания запроса на сертификат для службы OCSP необходимо скачать созданный запрос и перенести его на АРМ ЦС, для которого создается сервер-OCSP.

## 8.2.2 Подписание запроса на сертификат для службы OCSP

Для подписания запроса:

- открыть «Центр сертификации» AeCA;
- на вкладке «Свои сертификаты» убедиться, что ЦС, для которого создается сервер-OCSP, находится в состоянии «Активирован»;
- на левой боковой панели окна «Центра сертификации» нажать на меню «Сертификаты доступа»;
- Нажать радиокнопку «Создать сертификат», в открывшемся подменю выбрать «На основании запроса» (см.

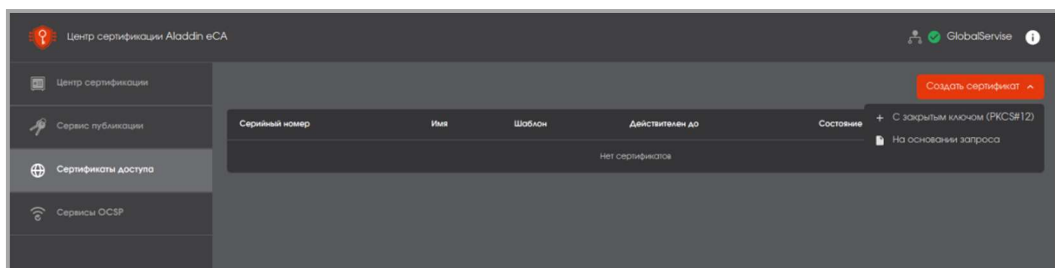


Рисунок 95 – Экран «Сертификаты доступа» - кнопка «Создать сертификат»

- В появившемся окне Мастера создания сертификатов необходимо:



- загрузить созданный и перенесенный запрос, нажав кнопку <Выбрать файл> (см. Рисунок 96). На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку <Изменить>;

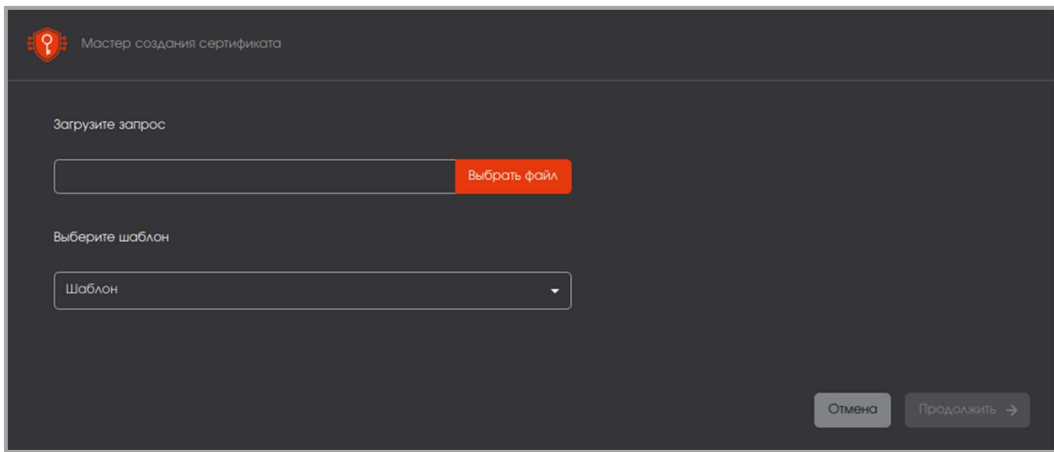



Рисунок 96 – Мастер обработки запросов

- в поле «Шаблон» по нажатию на  из раскрывающегося списка выбрать шаблон «OCSP Signer»;
- нажать ставшую активной после заполнения всех полей кнопку <Продолжить> (см. Рисунок 97)

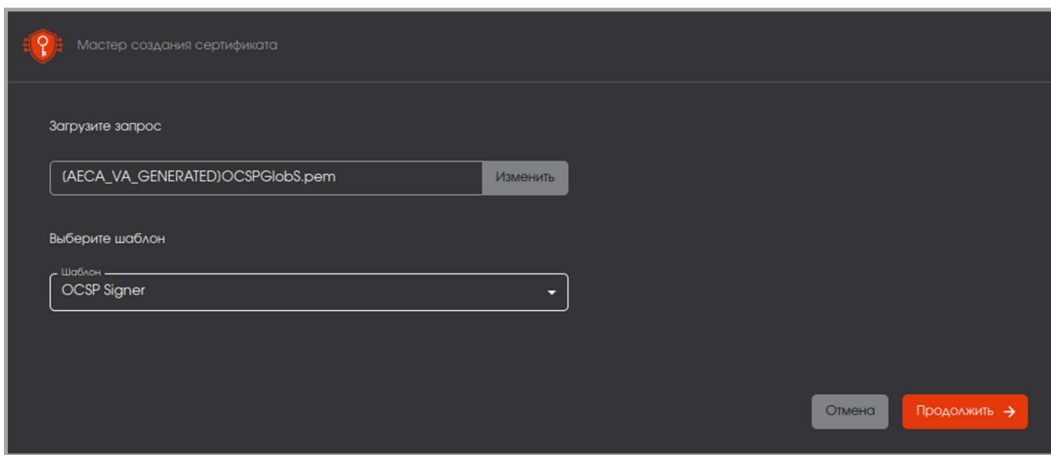


Рисунок 97 – Окно мастера создания сертификата. Загрузка запроса и выбор шаблона

- далее следует окно уведомления о загрузке запроса на сертификат (см. Рисунок 98). На данном этапе возможна отмена всех предыдущих действий по созданию сертификата на сервер OCSP, по нажатию кнопки <Отмена> или возврат к предыдущему шагу загрузки запроса и выбора шаблона, по нажатию кнопки <Назад>;
- нажать кнопку <Создать сертификат>;

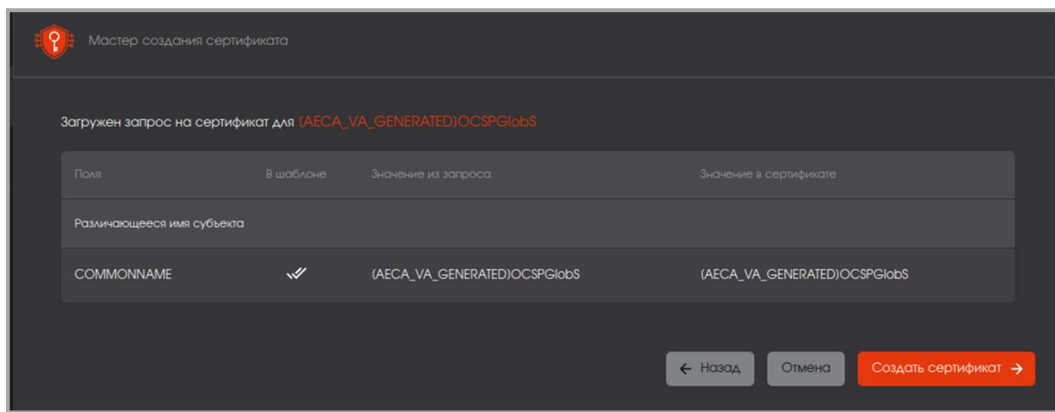


Рисунок 98 – Окно мастера создания сертификатов. Создание сертификата

- далее администратор видит уведомление о том, что сертификат на сервер OCSP успешно создан (см. Рисунок 99).

Сертификат подписан отображаемым на экране издателем (активным ЦС) для субъекта (OCSP сервера, чей запрос был подписан) с указанием периода действия выпущенного сертификата.

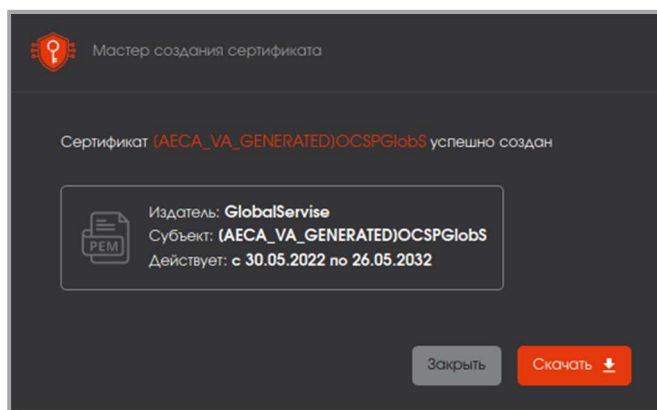


Рисунок 99 – Мастер создания сертификата. Успешное создание сертификата

- Далее необходимо скачать файл сформированного сертификата в формате .pem, нажав кнопку <Скачать>.
- Перенести созданный сертификат на APM «Центра валидации», для которого был выпущен данный сертификат.
- Произвести импорт сертификата сервиса OCSP.

### 8.2.3 Импорт сертификата службы OCSP

#### 8.5.2.1 Импорт сертификата инициируется по нажатию на кнопку

Импортировать сертификат

<Импортировать сертификат> на главном экране «Сервисы OCSP» (см. Рисунок 94).

Если есть сервисы в состоянии «Ожидает сертификат», то кнопка «Импортировать сертификат» доступна в карточке сервиса со статусом «Ожидает сертификат» и на главном экране раздела.

Если нет сервисов в состоянии «Ожидает сертификат», то кнопка «Импортировать сертификат» не доступна (disabled).

8.5.2.2 По нажатию на кнопку <Импортировать сертификат> открывается окно для загрузки файла сертификата (см. Рисунок 100). Прием файла осуществляется в формате .PEM.

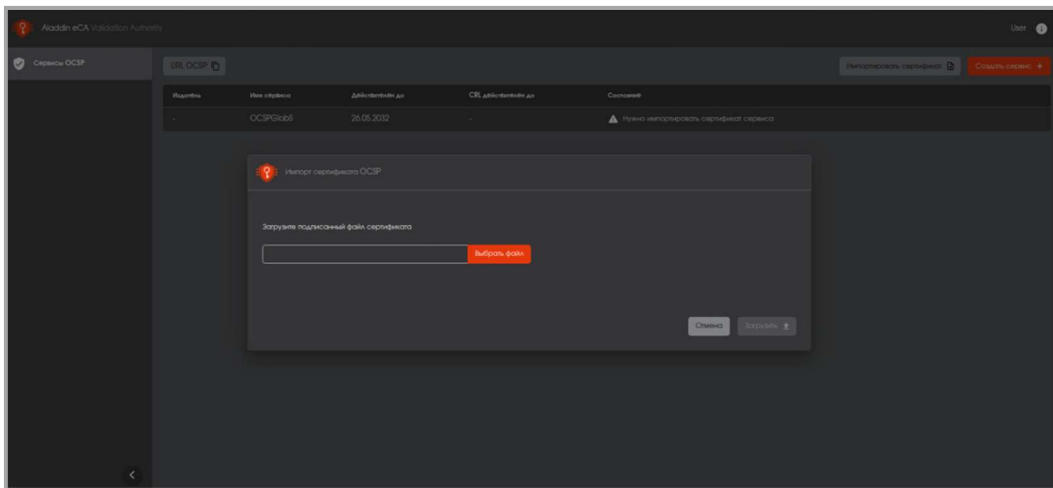


Рисунок 100 – Окно импорта сертификата OCSP

При необходимости, возможно перезагрузить подписанный файл сертификата через кнопку <Изменить>.

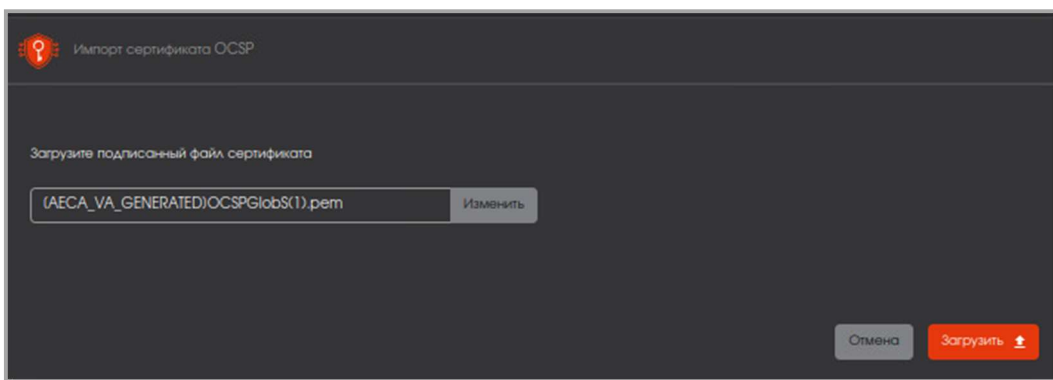


Рисунок 101 – Окно импорта сертификата OCSP. Состояние с загруженным файлом

После того, как будет выбран сформированный файл сертификата, нажать на кнопку <Загрузить>.

8.5.2.3 Если загрузка файла сертификата была произведена с ошибкой, то администратору будет выведено уведомление с ошибкой (см. Рисунок 102, Рисунок 103).

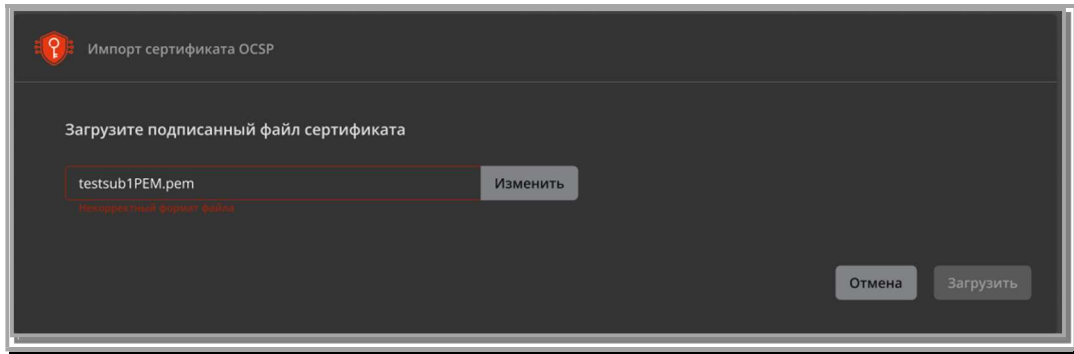


Рисунок 102 - Окно импорта сертификата OCSP. Ошибка импорта. Некорректный формат файла

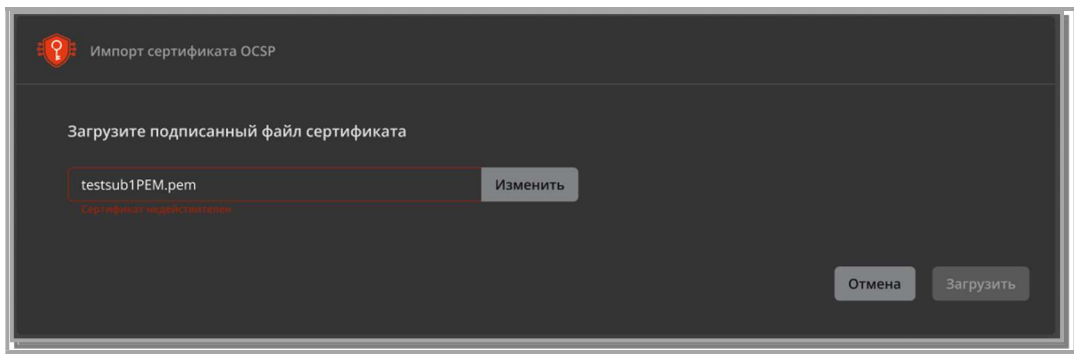


Рисунок 103 - Окно импорта сертификата OCSP. Ошибка импорта. Недействительный сертификат

В случае успешной загрузки откроется окно с результатом (см. Рисунок 104).



Рисунок 104 - Окно импорта сертификата OCSP. Успешная загрузка файла

После успешного импорта по нажатию на кнопку <Импортировать и запустить> происходят следующие действия:

- запускается сервис OCSP;
- запускается служба CRL updater (служба обновления CRL).

#### 8.2.4 Карточка сервиса OCSP

Для просмотра карточки созданного сервиса, необходимо выбрать нужный сервис в списке и дважды кликнуть по выбранной строке (см. Рисунок 105). В открывшемся окне администратору доступны:

- кнопка <Импортировать сертификат> для сервиса в состоянии запроса (более подробно в пункте 8.2.3);
- кнопка <Удалить> для удаления сервиса через подтверждение действия (более подробно в пункте 8.2.6);
- кнопка <Настроить> (более подробно в пункте 8.2.7);
- имя сервиса, заданное при создании;
- ссылка <Скачать запрос> для скачивания запроса без подтверждения (для сервиса в состоянии запроса);
- состояние (для сервисов в состоянии ожидания сертификата, будет значение <Нужно импортировать сертификат сервиса>)
- поле <Алгоритм подписи ответа> по умолчанию:
  - RSA для алгоритма сертификата RSA;
  - ECDSA для алгоритма сертификата ECDSA.
- поле <Адрес загрузки CRL> и <Период обновления> для отображения значений, заданных в мастере создания;
- поле <Следующее обновление CRL> показывает дату следующего обновления по таймеру;
- данные в полях <Номер текущего CRL> и «CRL действителен до» (Next Update) отображаются в случае, если удалось скачать сертификат по указанному адресу загрузки;
- Расширения OCSP, заданные в настройках сервиса (все галочки по умолчанию заданы):
  - статус неизвестных сертификатов GOOD (для любого сертификата не указанного в CRL ответ: good; для любого сертификата не указанного в CRL ответ: unknown (off));
  - галочки <Включать цепочку сертификатов...> и <Включать сертификат подписи...> определяют включать или нет сертификат подписи (сертификат OCSP) в ответ и включать ли его цепочку.

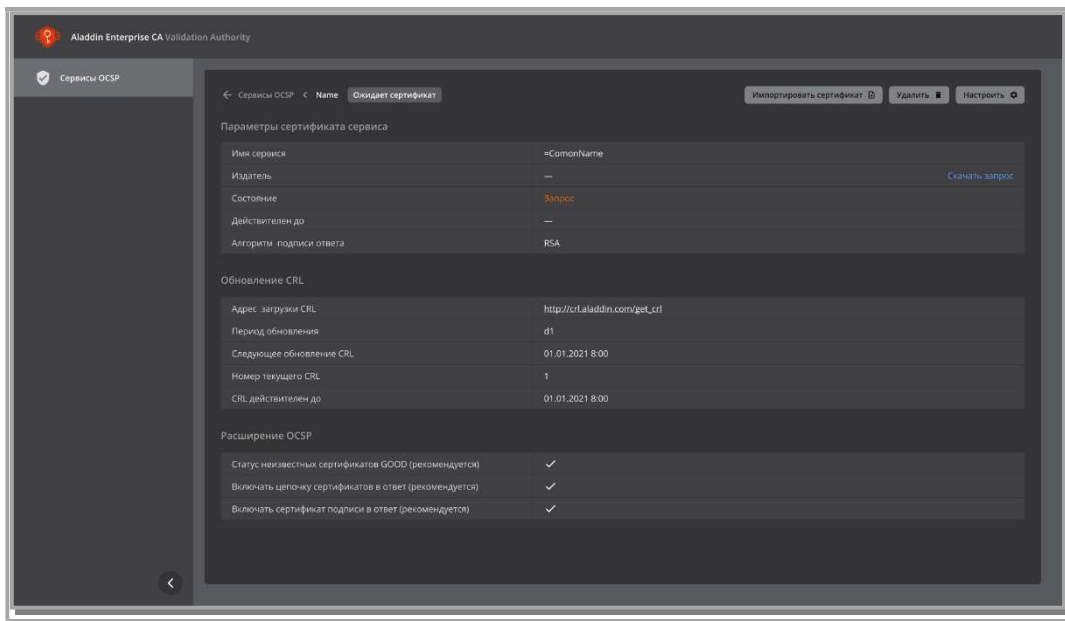


Рисунок 105 - Отображение карточки сервиса в состоянии «Ожидает сертификат»

## 8.2.5 Просмотр данных сервиса

### 8.2.3.1 Сервис в состоянии «Запущен».

После успешного импорта сертификата сервис переходит в состояние «Запущен» (см. Рисунок 106).

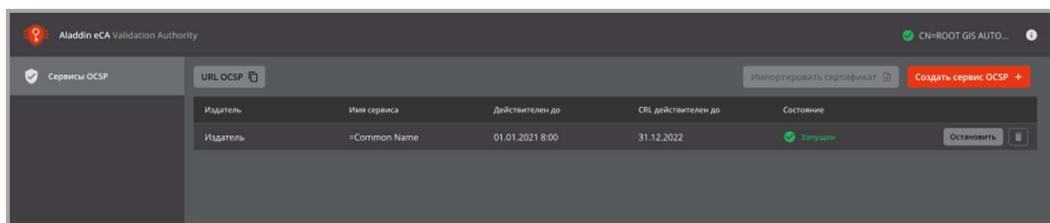


Рисунок 106 - пример сервиса в состоянии "Запущен"

После скачивания CRL, если он валиден, сервис OCSP будет отвечать на запросы о статусе сертификата ЦС, подписавшего сертификат этого сервиса, в соответствии с настройками.

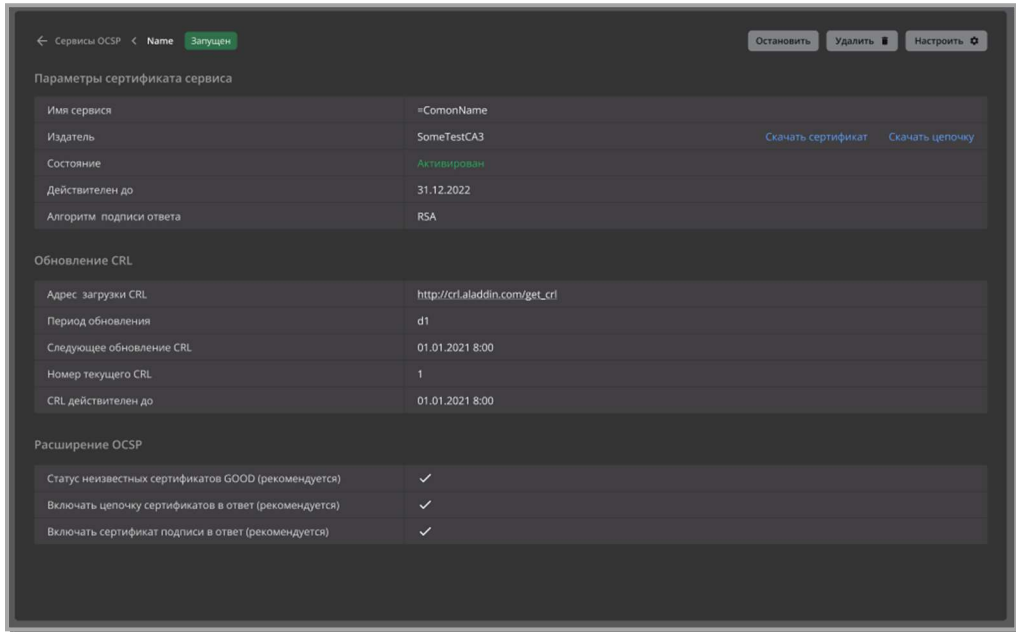


Рисунок 107 - карточка сервиса в состоянии "Запущен"

### 8.5.3.2 Сервис в состоянии «Остановлен».

В состоянии «Остановлен» сервис не работает (см. Рисунок 108). Обновление CRL не происходит. Остановленный сервис может перейти в состояние «Запущен» по нажатию на кнопку <Запустить>. После нажатия кнопки <Запустить> производятся следующие действия:

- запускается сервис OCSP;
- запускается служба CRL updater;
- осуществляет отображение «Запущен» в столбце «Состояние».

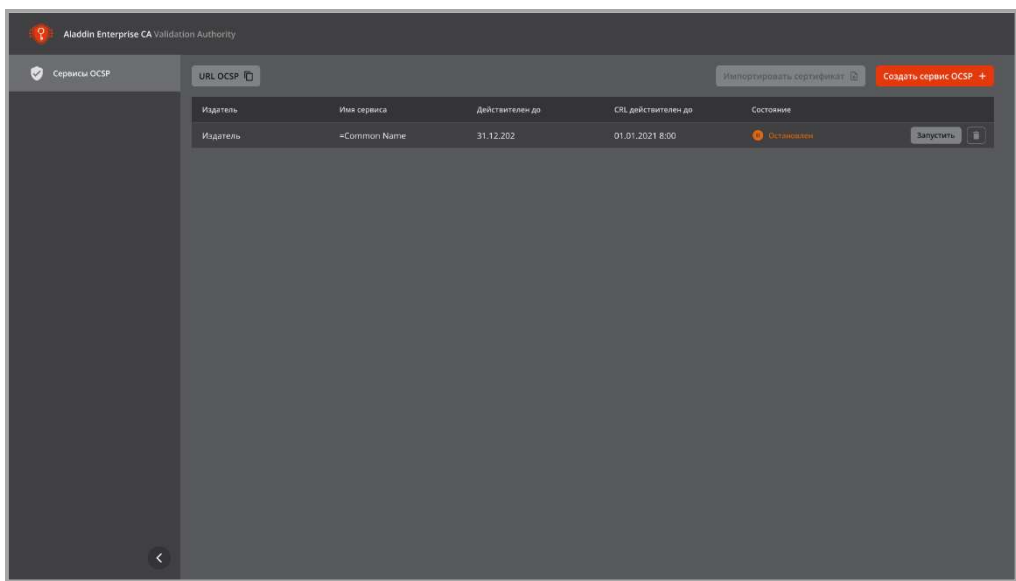


Рисунок 108 - Сервис в состоянии "Остановлен"

### 8.5.3.3 Работа сервиса в состоянии «Ошибка CRL»

В это состояние сервис переходит, если по указанному URL-адресу CRL недоступен, просрочен или не валиден (см. Рисунок 109).

В этом состоянии сервис отвечает на запросы OCSP ошибкой: `interlaError(2)` или `tryLater(3)` в соответствии с <https://datatracker.ietf.org/doc/html/rfc6960#section-4.2>

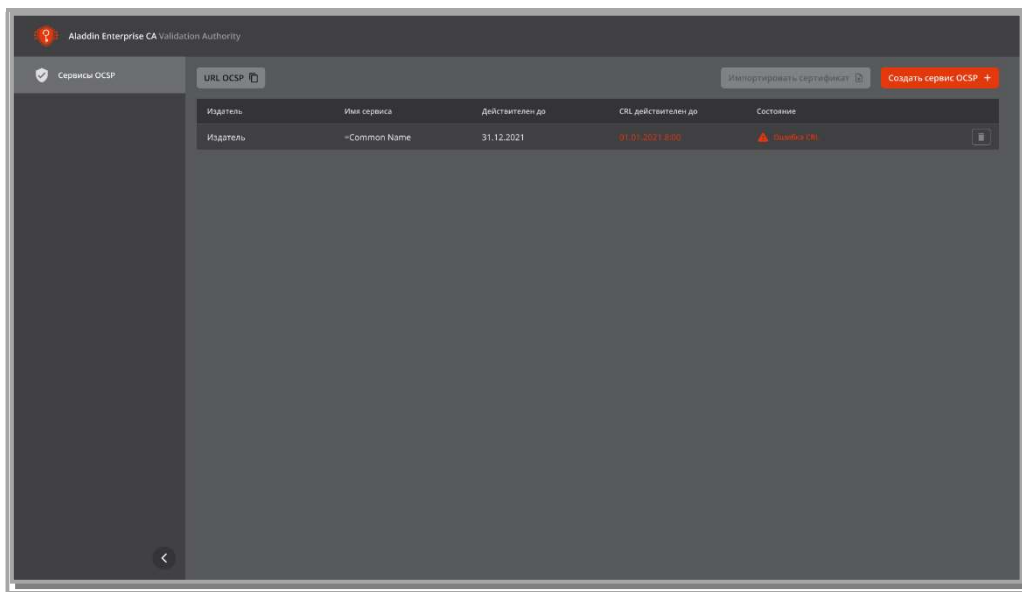


Рисунок 109 - Сервис в состоянии «Ошибка CRL»

Служба обновления CRL продолжает работать и, если CRL обновился и валиден, то сервис автоматически переходит в состояние «Запущен».

#### 8.5.3.4 Сервис в состоянии «Недействителен».

В этом состоянии сервис можно только удалить через подтверждение (см. Рисунок 110).

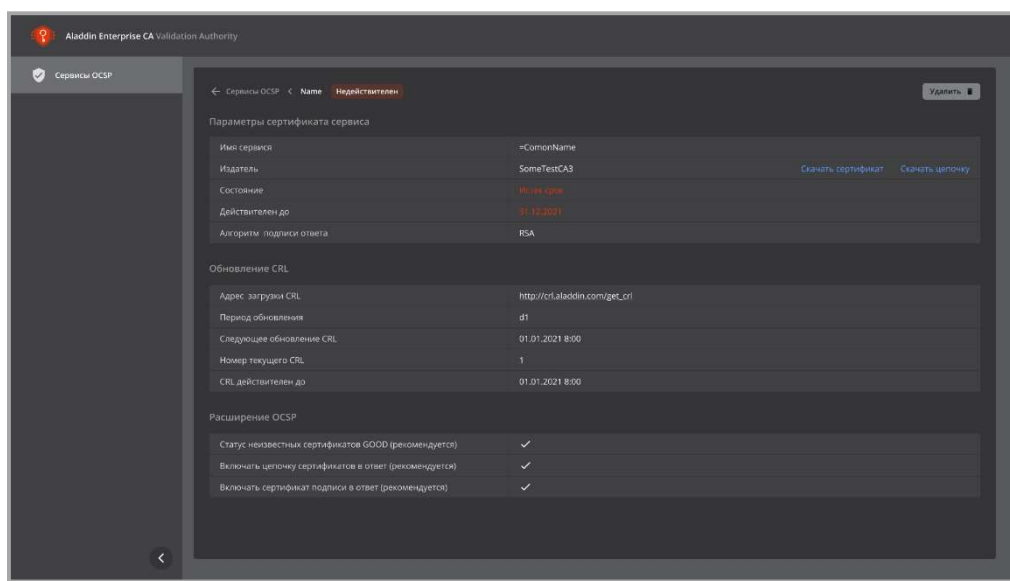


Рисунок 110 - Сервис в состоянии «Недействителен»



### 8.2.6 Удаление сервиса OCSP

Удаление сервиса доступно на главном экране по клику на иконку <Удалить> в соответствующей строке с сервисом (см. Рисунок 94), а также по нажатию на кнопку <Удалить> в карточке просмотра сервиса (см. Рисунок 105).

При клике на кнопку <Удалить> будет запрошено подтверждение действия (см. Рисунок 111).

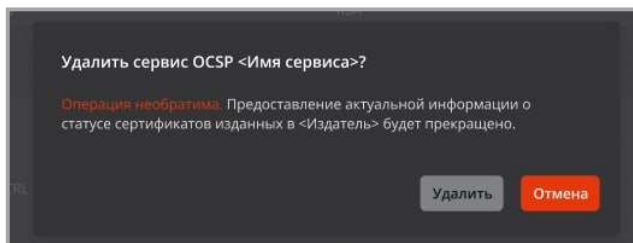


Рисунок 111 – Окно подтверждения удаления сервиса

### 8.2.7 Редактирование сервиса OCSP

Сценарий редактирования сервиса инициируется по нажатию кнопки <Настроить> (см. Рисунок 112) в карточке сервиса (см. Рисунок 105).

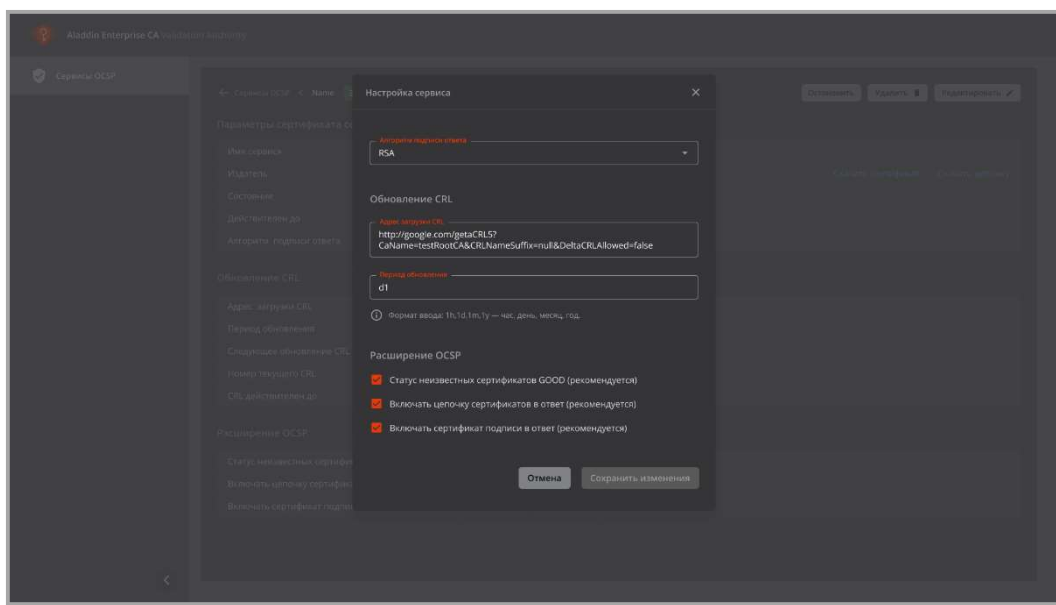


Рисунок 112 – экран с настройками сервиса OCSP

По умолчанию проставлены все галочки в блоке «Расширение OCSP».

При необходимости администратор может внести изменения в поля:

- алгоритм подписи ответа;
- адрес загрузки CRL;
- период обновления;
- статус неизвестных сертификатов GOOD (рекомендуется);
- включать цепочку сертификатов в ответ (рекомендуется);
- включать сертификат подписи в ответ (рекомендуется).

## 9 УДАЛЕНИЕ ПО ALADDIN ECA

### 9.1 Удаление программного компонента «Центр сертификации» Aladdin Enterprise CA

#### 9.1.1 Инициализация процесса удаления

Для инициализации процесса удаления необходимо выполнить команду с правами суперпользователя (root или sudo):

```
sudo bash /opt/aeca-0.0-0/scripts/uninstall.sh.
```

В результате выполнения данного действия будут полностью уничтожены:

- все добавленные при установке Изделия системные службы;
- все добавленные при установке Изделия пользователи и группы;
- все добавленные при установке Изделия файлы и структура каталогов.

Все внесённые изменения будут выведены в консоль. Удаление затронет только те изменения, которые были внесены скриптами установки, но не затронет установочный комплект в каталоге `/opt/aeca-0.0-0`.

#### 9.1.2 Удаление установочного пакета

Удаление пакета повлечёт за собой удаление установочного комплекта в каталоге `/opt/aeca-0.0-0/`.

- Для удаления на ОС **RED OS** необходимо выполнить следующую команду:

```
sudo dnf remove aeca-0.0-0
```

- Удаление на ОС **ASTRA LINUX** возможно выполнить двумя способами:

– *удаление пакета AECA:*

```
sudo apt remove aeca-0.0-0
```

– *удаление пакета AeCA вместе с конфигурационной информацией:*

```
sudo apt purge aeca-0.0-0
```

### 9.2 Удаление программного компонента «Центр валидации» Aladdin Enterprise CA

#### 9.2.1 Инициализация процесса удаления

Для инициализации процесса удаления необходимо выполнить команду с правами суперпользователя (root или sudo):

```
sudo bash /opt/aeca-0.0-0/scripts/uninstall.sh.
```

В результате выполнения данного действия будут полностью уничтожены:

- все добавленные при установке Изделия системные службы;
- все добавленные при установке Изделия пользователи и группы;
- все добавленные при установке Изделия файлы и структура каталогов.

Все внесённые изменения будут выведены в консоль. Удаление затронет только те изменения, которые были внесены скриптами установки, но не затронет установочный комплект в каталоге `/opt/aeca-0.0-0`.

### 9.2.2 Удаление установочного пакета

Удаление пакета повлечёт за собой удаление установочного комплекта в каталоге `/opt/aecaVa/`.

- Для удаления на ОС **RED OS** необходимо выполнить следующую команду:

```
sudo dnf remove aeca-va-0.0-0.rpm
```

- Удаление на ОС **ASTRA LINUX** возможно выполнить двумя способами:

– *удаление пакета АЕСА:*

```
sudo apt remove aeca-0.0-0
```

– *удаление пакета АеСА вместе с конфигурационной информацией:*

```
sudo apt purge aeca-0.0-0
```

## 10 МЕТОДЫ REST API ПРОГРАММНОГО СРЕДСТВА ALADDIN ECA

Доступ к методам REST API осуществляется через точку:

```
https://host:8888/aeca/api
```

где host - адрес вычислительной машины, на которой развернуто ПО АЕСА-СА

Перед использованием следует подготовить сертификат и ключ для работы по протоколу HTTPS.

Далее в примерах указаны:

`https.key.pem` - сертификат открытого ключа

`https.crt.pem` - сертификат закрытого ключа

Ключи можно получить из контейнера p12, используя утилиту openssl:

```
openssl pkcs12 -in superadmin.242.p12 -out https.key.pem -nocerts -nodes
openssl pkcs12 -in superadmin.242.p12 -out https.crt.pem -clcerts -nokeys
```

Примечание. При описании методов приведены примеры выполнения запросов с использованием утилиты `curl`, входящей в дистрибутив целевой ОС.

### 10.1 Создать субъект аутентификации

#### 10.1.1 Формат запроса:

```
PUT /subjects/create
```

В теле запроса нужно передать json-объект, содержащий поля:

- `[subjectDN]` - указать строку описания полей раздела `[subjectDN]`;
- `[subjectAltName]` - указать строку описания полей раздела `[subjectAltName]`;
- `[groupIds]` - указать массив идентификаторов групп (см. п. 10.13).

#### 10.1.2 Пример запроса:

```
curl -X PUT -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/subjects/create" -d '{"subjectDN": "cn=BL", "subjectAltName": "dnsname=bl.ru, guid=f022222222222222222211111111111444", "groupIds": [100000]}' -H 'Content-Type: application/json'
```

#### 10.1.3 Формат ответа:

- При успешной обработке запроса – статус 200 и число - идентификатор созданного субъект.
- При ошибке запроса – статус 400, 401, 403, 501 и строка с описанием ошибки.

#### 10.1.4 Примеры ответов

- Пример ответа при успешной обработке запроса:



## 10.4 Получить список серийных номеров действующих сертификатов, выпущенных для субъекта аутентификации, по его id

### 10.4.1 Формат запроса:

```
GET /subjects/info/{id}/certificates
```

где {id} - идентификатор субъекта (см. п. 10.2).

### 10.4.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM  
"https://192.168.111.242:8888/aeca/api/subjects/info/2/certificates"
```

### 10.4.3 Формат ответа – массив целых чисел.

### 10.4.4 Пример ответа:

```
["550594305716314482602807924022737971996383683366"]
```

## 10.5 Получить список серийных номеров сертификатов, выпущенных для субъекта аутентификации, отфильтрованных по статусу сертификатов

### 10.5.1 Формат запроса

```
GET /subjects/info/{id}/certificates/{filter}
```

где {id} – идентификатор субъекта (см. п. 10.2); {filter} – статус сертификатов, которые надо получить; может иметь одно из значений CERT\_UNASSIGNED, CERT\_INACTIVE, CERT\_ROLLOVERPENDING, CERT\_ACTIVE, CERT\_NOTIFIEDABOUTEXPIRATION, CERT\_REVOKED, CERT\_ARCHIVED.

### 10.5.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM  
"https://192.168.111.242:8888/aeca/api/subjects/info/2/certificates/CERT_ACTIVE"
```

### 10.5.3 Формат ответа – массив целых чисел.

### 10.5.4 Пример ответа:

```
["550594305716314482602807924022737971996383683366"]
```

## 10.6 Получить список Id групп субъекта аутентификации

### 10.6.1 Формат запроса:

```
GET /subjects/info/{id}/groups
```

где {id} - идентификатор субъекта (см. п. 10.2).

#### 10.6.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM
"https://192.168.111.242:8888/aeca/api/subjects/info/2/groups"
```

#### 10.6.3 Формат ответа – массив целых чисел.

#### 10.6.4 Пример ответа:

```
[100000]
```

## 10.7 Получить список шаблонов сертификатов активного УЦ, доступных субъекту аутентификации

#### 10.7.1 Формат запроса:

```
GET /subjects/info/{id}/certificatetemplates
```

где {id} - идентификатор субъекта (см. п. 10.2).

#### 10.7.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM
"https://192.168.111.242:8888/aeca/api/subjects/info/2/certificatetemplates"
```

#### 10.7.3 Формат ответа – массив целых чисел.

#### 10.7.4 Пример ответа:

```
[100001,100000,100002,100004]
```

## 10.8 Изменить субъект аутентификации

#### 10.8.1 Формат запроса:

```
POST /subjects/edit
```

В теле запроса нужно передать json-объект содержащий поля:

- [subjectId] - указать идентификатор субъекта (см. п. 10.2);
- [subjectDN] - указать строку описания полей раздела subjectDN;
- [subjectAltName] - указать строку описания полей раздела subjectAltName.

#### 10.8.2 Пример запроса:

```
curl -X POST -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-
type PEM "https://192.168.111.242:8888/aeca/api/subjects/edit" -d '{"id":
2,"subjectDN":
"cn=AL","subjectAltName":"dnsname=al.ru,guid=f0222222222222222222111111111111333"}' -H
'Content-Type: application/json'
```

### 10.8.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

### 10.8.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz": "NullPointerException", "message": null}
```

## 10.9 Добавить субъект в заданную группу

### 10.9.1 Формат запроса:

```
PUT /subjects/addgroup
```

В теле запроса нужно передать json-объект, содержащий поля:

- [subjectId] - указать идентификатор субъекта (см. п. 2);
- [groupId] - указать идентификатор группы (см. п. 10.13).

### 10.9.2 Пример запроса:

```
curl -X PUT -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/subjects/addgroup" -d '{"subjectId":2, "groupId":100000}' -H 'Content-Type: application/json'
```

### 10.9.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

### 10.9.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz": "NotAllowedException", "message": "RESTEASY003650: No resource method found for PUT, return 405 with Allow header"}
```

## 10.10 Исключить субъект из заданной группы

### 10.10.1 Формат запроса:

```
DELETE /subjects/removegroup
```

В теле запроса нужно передать json-объект содержащий поля:

- [subjectId] - указать идентификатор субъекта (см. п. 10.2);



- `[groupId]` - указать идентификатор группы (см. п. 10.13).

#### 10.10.2 Пример запроса:

```
curl -X DELETE -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/subjects/removegroup" -d '{"subjectId":2, "groupId":100000}' -H 'Content-Type: application/json'
```

#### 10.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

#### 10.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz":"NotAllowedException","message":"RESTEASY003650: No resource method found for PUT, return 405 with Allow header"}
```

## 10.11 Явно задать группы, в которых состоит субъект аутентификации

### 10.11.1 Формат запроса

```
PUT /subjects/setgroups
```

В теле запроса нужно передать json-объект содержащий поля:

- `[subjectId]` - указать идентификатор субъекта (см. п. 10.2);
- `[groupId]` - указать идентификатор группы (см. п. 10.13).

### 10.11.2 Пример запроса:

```
curl -X PUT -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/subjects/setgroups" -d '{"subjectId":2, "groupIds":[100000]}' -H 'Content-Type: application/json'
```

#### 11.3 Формат ответа

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

#### 11.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz":"NotAllowedException","message":"RESTEASY003650: No resource method found for PUT, return 405 with Allow header"}
```

## 10.12 Удалить субъект аутентификации

### 10.12.1 Формат запроса

```
DELETE /subjects/delete/{id}
```

где {id} - идентификатор субъекта (см. п. 10.2)

10.12.2 Пример запроса:

```
curl -X DELETE -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/subjects/delete/25"
```

10.12.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

10.12.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz": "NumberFormatException", "message": "For input string: \"aa\""} 
```

## 10.13 Получить информацию о списке доступных групп субъектов аутентификации

10.13.1 Формат запроса:

```
GET /groups/all
```

10.13.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/groups/all"
```

10.13.3 Формат ответа – массив целых чисел.

10.13.4 Пример ответа:

```
[100000]
```

## 10.14 Получить информацию о группе субъектов аутентификации по id

10.14.1 Формат запроса:

```
GET /groups/info/{id}
```

где {id} - идентификатор группы (см. п. 10.13).

10.14.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/groups/info/100000"
```

10.14.3 Формат ответа – JSON-объект с полями, которые сохранены для выбранной группы субъектов.

10.14.4 Пример ответа:

```
{  
  "id":100000,  
  "name":"default",  
  "authSubjectsIds":[1,2,3,4,5,6,8],  
  "certificateTemplatesIds":[100001,100000,100002,100004]  
}
```

## 10.15 Получить список субъектов, состоящих в группе субъектов аутентификации

### 10.15.1 Формат запроса

```
GET /groups/info/{id}/subjects
```

где {id} - идентификатор группы (см. п. 10.13).

### 10.15.2 Пример запроса

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM  
"https://192.168.111.242:8888/aeca/api/groups/info/100000/subjects"
```

10.15.3 Формат ответа – массив целых чисел.

10.15.4 Пример ответа:

```
[1,2,3,4,5,6,8]
```

## 10.16 Получить список шаблонов сертификата, доступных текущему активному центру сертификации

10.16.1 Формат запроса:

```
GET /certificates/certificatetemplates
```

10.16.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM  
"https://192.168.111.242:8888/aeca/api/certificates/certificatetemplates"
```

10.16.3 Формат ответа – массив целых чисел.

10.16.4 Пример ответа:

```
[100001,100000,100003,100002,100004]
```

## 10.17 Получить детальное описание шаблона сертификата субъекта аутентификации

10.17.1 Формат запроса:

```
GET /certificates/certificatetemplates/{id}
```

где {id} - номер шаблона (см. п. 10.16).

#### 10.17.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM  
"https://192.168.111.242:8888/aeca/api/certificates/certificatetemplates/100001"
```

#### 10.17.3 Формат ответа – JSON-объект с полями входящими в шаблон.

#### 10.17.4 Пример ответа:

```
{  
  "id":100001,  
  "certificateProfileId":100002,  
  "name":"Smartcard Logon",  
  "useSubjectDnSubset":false,  
  "subjectDnSubset":[],  
  "useBasicConstraints":true,  
  "basicConstraintsCritical":true,  
  "useAuthorityKeyIdentifier":true,  
  "authorityKeyIdentifierCritical":false,  
  "useSubjectKeyIdentifier":true,  
  "subjectKeyIdentifierCritical":false,  
  "useQcetSignatureDevice":false,  
  "useCertificatePolicies":false,  
  "certificatePoliciesCritical":false,  
  "certificatePolicies":[],  
  "useSubjectAlternativeName":true,  
  "subjectAlternativeNameCritical":false,  
  "useIssuerAlternativeName":true,  
  "issuerAlternativeNameCritical":false,  
  "useSubjectDirAttributes":false,  
  "useNameConstraints":false,  
  "useCrlDistributionPoint":true,  
  "useDefaultCrlDistributionPoint":true,
```

```
"crlDistributionPointCritical":false,
"crlDistributionPointUri":"","
"crlIssuer":"","
"useFreshestCrl":false,
"useCaDefinedFreshestCrl":false,
"freshestCrlUri":"","
"useAuthorityInformationAccess":true,
"useDefaultOcspServiceLocator":true,
"ocspServiceLocatorUri":"","caIssuers":[],
"useDefaultCaIssuer":true,
"usePrivKeyUsagePeriodNotBefore":false,
"usePrivKeyUsagePeriod":true,
"usePrivKeyUsagePeriodNotAfter":true,
"privKeyUsagePeriodStartOffset":0,
"privKeyUsagePeriodLengthInSeconds":63072000,
"useExtendedKeyUsage":true,
"extendedKeyUsage":["1.3.6.1.5.5.7.3.2","1.3.6.1.5.5.7.3.4"],
"availableCA":[-1],
"endEntityProfileId":100003,
"profileName":"Smartcard Logon",
"rowVersion":0,
"rowProtection":null,
"endEntityAvailableCA":[1],
"defaultCA":496012993,
"availableCertificateProfile":["Smartcard Logon"],
"numberOfAllowedRequestsString":"use",
"numberOfAllowedRequestsInt":5,
"dnsName":{
  "modifiable":0,
  "required":0,
  "validation":0
},
"msUPN":{
```

```

"modifiable":1,
"required":0,
"validation":0
},
"guid":{
"modifiable":0,
"required":0,
"validation":0
},
"rfc822Name":{
"use entity email":1,
"modifiable":1,
"required":0
}
}
}

```

## 10.18 Получить сертификат по CSR для нового субъекта аутентификации

### 10.18.1 Формат запроса:

```
PUT /certificates/create-and-enroll
```

В теле запроса нужно передать json-объект содержащий поля:

- [groupId] - указать идентификатор группы (см. п. 10.13);
- [certificateTemplateId] - указать идентификатор шаблона (см. п. 10.16);
- [subjectAltName] - указать строку описания полей раздела subjectAltName (см. п. 10.1);
- [file] - указать строку, содержащуюся в csr-файла (текст запроса в формате Base64);

### 10.18.2 Пример запроса:

```

curl -X PUT -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-
type PEM "https://192.168.111.242:8888/aeca/api/certificates/create-and-enroll" -d
'{"groupId":100000,"certificateTemplateId":100004,"subjectAltName":"dnsname=cl.ru,gui
d=f02222222222222221111111111555","file":"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNUL
S0tLS0KTU1JQnpUQ0NBVF1DQVFBd0p6RWxNQ01HQTFVRUF3d2NRVVZEUVVY5V1FwoUhsVTpGVWtGVVJVVmZWA0
UzTVVOQgpVekkwTWpDQm56QU5CZ2txaGtpRz13MEJBUEVVGQUFPQmpRQXdnWWtDZ11FQXdQbm5SLy9Rd1E4S0x
CZnhpbHhZSmlwR3JlcjE3dDQ0d5bWdyVVFVZXZ1FwSlNpUmVCVm1lweUd1dEJZTVpQsZiIwL1Z2UTRoVV1pTWhVOVFaSFJIT1p5ODRtL1h3T1ZlU
S9oOHg5UGNsNApWUXp1RjFFMjF6Rm1VUVV1wgcTROyklURUNBd0VBUWFjQVU1HUUdDU3FHU01lM0RRRUUpEakZYTU

```

```
ZVd0hRWURWUjBPCkJCWUVGQVBoNGVIRkJnQmR0cm5xMETBeDdFVXFGeEVBtUE0R0ExVWREd0VCL3dRRUF3SUh
nREFUQmdOVkhTVUUKRERBS0JnZ3JCZ0VGQlFjRENUQVBCZ2tyQmdFRkJKRY3dBUVVfQWdVQU1BMEdDU3FHU01i
M0RRRUJCQVVBQTRHQPpBS2pDamNoNTdqTjhYRXVvMEIvUUsvc3pVZUZKYUFQdlJPQVNiREEyRGRZSXkrCDJRT
nRrRnRNdHF1b2dwYUNQCk02UER5YUJXZE5JQVR5cjRaaTJKeTEvZxc3VU9nSzgyV3UvVDZadXFPNVI5RThKNV
FIcjFQTVFySXFbMnBzUGQKS3dvbVdyL1ZpTldPRWZybmXTQUs0MXhqaVZBMEpJcFp1Q093UX1SckdaQnEKL50
tLS1FTkQgQ0VSVElGSUNBVEUgUkVRVUVTVc0tLS0tCg=="}' -H 'Content-Type: application/json'
```

### 10.18.3 Формат ответа

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

### 10.18.4 Пример ответа

Пример ответа при успешном исполнении запроса:

```
{
"subjectId":27,
"name":"AECA_VA_GENERATED_VA71CAS242",
"subjectDN":"CN=AECA_VA_GENERATED_VA71CAS242",
"subjectAltName":null,
"issuerDN":"CN=SubCenter,OU=Subdepart L,O=Suborg,C=RU",
"validity":1716988805000,
"created":1653916806000,
"cert":"U3ViamVjdDogQ049QUVDQV9WQV9HRU5FUkFURURfVke3MUNBUzI0MgpJc3N1ZXI6IENOPVN1Ykn1b
nRlcixPVT1TdWJkZXBhcnQgTCxPPVN1Ym9yZyxDPVJVCi0tLS0tQkVHSU4gQ0VSVElGSUNBVEUtLS0tLQpNSU
1EQVRDQ0FlbWd0L0cQWdJVUdpwJg2MzZYTmNvcEZ4NEEzTTFwbzJzMzJxc3dEUUV1KS29aSWH2Y05BUUVGCKJ
RQXdTREVTtUJBR0ExVUVBd3dKVTNwaVEyVnVkr1Z5TVJRd0VnWURWUvFMREF0VGRXSmtaWEJoY25RZ1RERVAK
TUEwR0ExVUVDZ3dHVtNwaWiZSm5NUXN3Q1FzRFZRUUdFd0pTV1RBZUZ3MH1NakExTXpBeE16SXdnRFphRncwe
QpOREEeTWpreE16SXdnRFZhtUNjeEpUQWpCZ05WQkFNTUhfRkZrMEZmVmtGZlIwVkr9SVkpcVkvVWRVgxWkJOek
ZEC1FWTXlOREl3Z1o4d0RRWUpLb1pJaHJzTkFRRUJCUEFEZ1kwQU1JR0pBb0dCQU1ENTUwZi8wTUVQQ213WDh
ZcGIKNVpxUnEzcXkvQkd1L0pzamJFdXFsYTVocGc3VWlUeWZMY0JzcG9LMUVGbjBLU1Vva1hnV1llaW1sWUg2
QlQ1WgpIeWFaZ0NtcDZTMW1LY2hyclFXREdUeXR0TDFiME9JVkdJaklWUFVHUjBSeldjdk9KdJE4RFZYa1A0Z
k1mVDNKcmVGVU03aGRStNRjeFpTMEdLYXVEV31KeEFnTUJBQUdqZ11jd2dZUXdEQV1EV1IwVEFRSC9CQU13QU
RBZkJnTlYKSFNNRUdEQVdnQ1JuSFBuejZXT0JurHozOCTUOV1NQULodzViWmpBUEJna3JCZ0VGQlFjZ0FRVUV
BZ1VBTUJNRwpBMVVsSlFRtU1Bb0dDQ3NHQVFVRkZ3TUUpNQjBHQTFVZERnUVdCQ1FENGVIaHhRWUFYyME1NnRD
Z01leEZLaGNSCkFEQU9CZ05WSFE4QkFmOEVCQU1DQjRBD0RRWUpLb1pJaHJzTkFRRUZCUUFEZ2dFQkFMbWcvZ
StQT1BLblRMcnUKRv1QQVhDb1ZYn1FFMktXSWU3WWtmSURMMytKtGVwa00yTFZac2k2ZXhMZ3pWTFdkeTMyeV
JtRnBQWH12SXZSZgo4ZmhUSVhiWEJ6NFntOUZ1VkrNw1INWpSQ0dMz1lZSF1hWnFTWVvINTHQN3FZM2I2MV1
SOTgxv2xmS3pnY0ZnckVQZE1qZE1CZ2NFcG1wZ111SkRLYmNCSDNLeGsyOEhkQ1hvbXpZUjU5bDhaSUVraVBI
bTk3VTdIL3pyVjY4ZWsKNkFDUXNIM3QxVDJZwitpb3gxcGNmcGhMT1I4YXdDRI9BRzZ6Q1NSRmlNT0hKa3NMQ
1hWUnFzNnVJY11vU1JkUAp1b01UYm0xVkiXvXhwbVYxv2dwalJxMktJNXJWaVZQdjFmNk5Oa0QwazcrM052Zj
Nkd0sldUVVK1RLaEkrMFZECmcvOVJuUXc9Ci0tLS0tRU5EIEENFU1RJRklDQVRFLS0tLS0KU3ViamVjdDogQ04
```

9U3ViQ2VudGVyLE9VPVN1YmRlcGFydCBMLE89U3Vib3JnLEM9U1UKSXNzdWVyoibDTj10ZXN0LE9VPURlcGFy  
dG1lbnQsTz1vcmdhbm16YXRpb24sTD1DaXR5LEM9U1UKLS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JS  
URrRENDQW5pZ0F3SUJBZ01VZXQvUGxJRFRQNXhYbXFYUWk2N29YWVNXdkVRd0RRWUpLb1pJaHZjTkFRRUYKQ1  
FBd1Z6RU5NQXNHQTFVRUF3d0Vkr1Z6ZERFVE1CRUdBMVVFQ3d3S1JHVndZWEowY1dWdWRERVZVNQk1HQTFVRQp  
DZ3dNYjNKb1lXNXBlbUYwYVc5dU1RMhdDd1lEVlFRSERBUkRhWFI1TVFzd0NRWURWUVFHRXdKU1ZUQWVGdzB5  
Ck1qQTFNekF4TWpBNU5UTmFGdzB6TWpBMU1qY3dNREF3TURCYU1FZ3hFakFRQmdOVk1JBTU1DVk4xWWtObGJuU  
mwKY2pFVU1CSUdBMVVFQ3d3TFUzVmlaR1Z3WVhKME1Fd3hEekFOQmdOVkJBb01CbE4xWW05eVp6RUxNQWtHQ  
FVRQpCaE1DVWxVd2dnRW1NQTBHQ1Nxr1NjYjNEUUVUVCQVVFVQUE0SUJEd0F3Z2dFS0FvSUJBUUQwbThMdmMwY3l  
hU01PClUwc25jaktGUy81K0JnNTFSbWpyTkViclZwNUdLZnE0b1pjOEk1Rm5CNmUvMFYrbkVZb0c4OE9vYTF0  
cEZMaWoKa2tJNVVWRct0RVc3b2ZBS3dTNERRc2lCSXJtMWNZUTVMakxUcmR2YzNhRDVGbU5NNTZrbm1GZE5TV  
1FVRnZVcwp1ejRRN1k1NWJEN2Y5Yk8rOUdrL0g4VEZ6NXhRRVczTEppRzJheDM2TmxabTc5UmYwR1VrdzFMRn  
pldS9yb3NlCkExRctQSnlsaVv1WTRKblZKR0NmcnpSQW5RS2ZyYVY5aDlWUVJnRGNxa3NjY3FBa0NHVDRyZV1  
Mc280dlpJY2oKc0p1WStGeTd4dU9yUWlZVGHpeDhibUHVU3FrTWVBCERZMkFueHZ5SzbJQkhuclhKNHivTG13  
R0Eza1RrNGxaaAoyNW9UV3RkWEFntUJBJQudqWXPcaE1BOEdBMVVKRXdfQi93UuzNQU1CQWY4d0h3WURWUjBqQ  
kJnd0ZvQVU1czFyCnlUckh5NUdJaEhNSjhoZVBjRGp1RUFbd0hRWURWUjBPQkJZRUZHY2MrZ1BwWTRHY1BQZn  
o1UDFnd0FpSERsdG0KTUE0R0ExVWRED0VCL3dRRUF3SUJoakFOQmdrcWhraUc5dzBCQVFRkFBT0NBuUVRkKJ  
aUmtFbXBveVNHOFrYNgpaM0JKQTRiA1RjZzF0WUpDUkZzd3JMMnRldU9HbXhnUFhoaVYyREhZdnYxMi9DaFJ6  
Y3NBVHlPYmlMcjhiSy93CjZ3eU1zQ0MvWTNTbngyYklMwXpXcnorZVRIQTdSWWg2dmVuSktYzZnyUnB4eU5XM  
UhBcFpJUHKxT2JTaFzqZVEKRHVkZFlrdkNyb1N5VDFWk1JRK3JqSGhVRWdXK0MyN1djKzRCbk43MjgwaW05SW  
JuODRRVTlWWTNQNE5nU3YyZApMNxhoa0NLe1ZMMzNuRfPtCe9Lb2wzelNzRXJKZHv0eE1renRBVmhDMUZBYjh  
ETFREK3RubXhjYnNYTHVBV3owCjJ3L2VtbFY5d2N3cGJZUEFKZXFJclg3QXVuaUlWamVEcjd6dlhsZEpFdWVL  
ZjBxc2hKcDRsR0d2VExud2M2cisKVXJvZ1JnPT0KLS0tLS1FTkQgQ0VSVE1GSUNBVEUtLS0tLQpTdWJqZWN0O  
iBDTj10ZXN0LE9VPURlcGFydG1lbnQsTz1vcmdhbm16YXRpb24sTD1DaXR5LEM9U1UKSXNzdWVyoibDTj10ZX  
N0LE9VPURlcGFydG1lbnQsTz1vcmdhbm16YXRpb24sTD1DaXR5LEM9U1UKLS0tLS1CRUdJTiBDRVJUSUZJQ0F  
URS0tLS0tCk1JSURuekNDQW9lZ0F3SUJBZ01VSEhCQjBzcVZDN1dSbWkvSkRIY0hubVI1ck5Nd0RRWUpLb1pJ  
aHZjTkFRRUYKQ1FBd1Z6RU5NQXNHQTFVRUF3d0Vkr1Z6ZERFVE1CRUdBMVVFQ3d3S1JHVndZWEowY1dWdWRER  
VZVNQk1HQTFVRQpDZ3dNYjNKb1lXNXBlbUYwYVc5dU1RMhdDd1lEVlFRSERBUkRhWFI1TVFzd0NRWURWUVFHRX  
dKU1ZUQWVGdzB5Ck1qQTFNamN4TWpRMk16QmFGdzB6TWpBMU1qY3dNREF3TURCYU1GY3hEVEFMQmdOVk1JBTU1  
CSFJsYzNReEV6QVIKQmdOVkJBc01Da1JsY0dGeWRHMWxiBlF4R1RBVEJnTlZCQW9NREc5eVoyRnVhWHBoZEds  
dmJqRU5NQXNHQTFVRQpCd3dFUTJsmGVURUxNQWtHQTFVRUJoTUNVbFV3Z2dFaU1BMEddU3FHU01im0RRRUJBU  
VVBQTRJQkr3QXdnZ0VLCkFvSUJBUUNVOG9ka1NQSHB6a0NtbfJqNjIyM0NzTUx0L00vZUJLa1F4OE1ydFFZnK  
9pUmXTOXQwaE5kRnQ0SHEKOFB6L0loYnlZUU9wNkhHWnV2RXQ5ODdTcEZMemdiSXN3d3puNk5ya3c5a3pEb3p  
zWFFSSHVscmhtcKvjcxV0bwp4S21GRzZVUFQ0SXE2a052djRoRHRyUDJxN1cwOU9Pa1BtTitRdno1b3RLbW5s  
eGh2NCtxTEx5ZjM2Rm9Ud2VRCndhUVI4WG9ZbGZYzmkvK3R6S3ZKT2J6Z1dFRm55S0RPckRsUlFVb05wWlFTN  
3NNNVVTdzFQVudXais3cy9VU2IKQi9MLzJJZmdQTWdqREzWmJozTlJM3JORK5JUEZGNXVYeGY3Wt1xWkrQb0  
JKOXJCNmxyNVVtaGxYN2J6R0JIVgpxT1VXYkpsQXlyN1hNbGNBUUlzc1pNREdmNnduQWdNQkFBR2pZekJoTUE  
4R0ExVWRFd0VCL3dRRk1BTUJBJzh3Ckh3WURWUjBqQkJnd0ZvQVU1czFyEVRyShk1R01oSE1KOGh1UGNEanVF  
QUF3SFFZRFZSME9CQ1lFRk9iTeE4azYKeDh1Um1JUUnPDzk1YajNBNDdoQUFNQTRHQTFVZER3RUIvd1FFQXdJQ  
mhqQU5CZ2txaGtpRzl3MEJBUVVGQUFpQwpBUUVBQ3NyS0p4NTI0ME94eGRxcGJPck1uUlRoZWtyZVIyYRfPqVU  
FvVWNKT3VVOEkwV2gyY1FMZVhHaC8vM1VICkwwQW1TbFFQZE12Ym44bHdHeFF1TkpkDK09sej1sMkVsU0Z5aW1  
UVkpsc0xYTUQwYWhPSktnY1E3eUxjUVFoVmgKVW1UUXZnWDhFSnF3RU9mbTRnWmc2Y21zWnI4cXJ3L2tsU3dj  
V3JjWVpvVklQbWZwanNleU01dmhUcmdzaENmSgpIZ3FNd1NhTW80TWplUHBtTHRwcZCS2phVMMrLzRnbzRST



```
HIyOENhV2JnTklQaVJnd0tIQVVYUHB2czdhV0JjClZhVXl0TjVORFVPL0lWN0dablB6UmY3VWUwNVNtZk1lT1
VVVEhaRWlSZ2hFaWlydm9TRnlFKzJmRTRzbHB4bisKY3QvL3A2MUNnVTV0UkRtYkpzZk81N3NmY1E9PQotLS0
tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg=="
}
```

Пример ответа при ошибке на запрос:

```
{"clazz":"AecaRuntimeException","message":"Произошла ошибка создания субъект
SubjectDN=CN=AECA_VA_GENERATED_VA71CAS242 уже используется или группа не
существует."}
```

## 10.19 Получить сертификат по CSR для заданного субъекта аутентификации

### 10.19.1 Формат запроса:

```
PUT /certificates/enroll
```

В теле запроса нужно передать json-объект содержащий поля:

- `[authSubjectId]` – указать идентификатор субъекта (см. п. 10.1, п. 10.18);
- `[certificateTemplateId]` – указать идентификатор шаблона (см. п. 10.16);
- `[file]` – указать строку, содержащуюся в csr-файла (текст запроса в формате Base64).

### 10.19.2 Пример запроса:

```
curl -X PUT -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-
type PEM "https://192.168.111.242:8888/aeca/api/certificates/enroll" -d
'{"authSubjectId":27,"certificateTemplateId":100004,"file":"LS0tLS1CRUdJTiBDRVJUSUZJQ
0FURSBSRVFVRVNULS0tLS0KTU1JQnpUQ0NBVFlDQVFBd0p6RWxNQ01HQTFVRUF3d2NRVVZEUVY5V1FWOUhSVT
VGVWtGVVJVUmZwa0UzTVVOQgpVekkwTWpDQm56QU5CZ2txaGtpRz13MEJBUUVGQUFPQmpRQXdnWWtDZ1lFQXd
Qbm5SLy9RdlE4S0xCZnhpbHZsCm1wR3Jlckw4RVo3OG15TnNTNnFWcm1HbUR0U0pQSjh0d0d5bWdyVVFhZlFw
SlNpUmVCVmg2S0tWZ2ZvRlBsa2YKSnBtQUthbnBMV1lweUd1dEJZTVpQSZIwdlZ2UTRoVl1pTWhVOVFaSFJIT
lp5ODRtL1h3TlZlUS9oOHg5UGNsNApWUXp1RjFFMjF6RmRmMUUvLWcTROYkluRlUNBd0VBQWFCbU1HUUdDU3FHU0
liM0RRRUpeakZYTUZVd0hRWURWUjBPCkJKUUVGQVBoNGVIRklnQmR0cm5xMEtBeDdFVXFGGeEVBtUE0R0ExVWR
Ed0VCL3dRRUF3SUhnREFUQmdOVkhTVUUKRERBS0JnZ3JCZ0VGQ1FjRENUQVBCZ2tyQmdFRkJKRY3dBVVVFQWdV
QU1BMEdDU3FHU0liM0RRRUJCQVVBQTRHOGpBS2pDamNoNTdqTjhYRXVvMEIvUUsvc3pVZUZKYUFQdlJPQVNiR
EEyRGRZSXkrcDJRtRrRnRNdHFib2dwYUNQc0k0UER5YUJXZE5JQVR5cjRaaTJKeteEvZxc3VU9nSzgyV3UvVD
ZadXFPNVI5RThKNVFIcFQTVFySXFBNBzUGQKS3dvdVdyL1ZpTldPRWZybmxtQSU0MXhqaVZBMEpJcFp1Q09
3UXlScldaQnEKLS0tLS1FTkQgQ0VSVElGSUNBVEUgUkVVRVUUVTV0tLS0tCg=="}' -H 'Content-Type:
application/json'
```

### 10.19.3 Формат ответа

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

### 10.19.4 Пример ответа

Пример ответа при успешном исполнении запроса:

```
{
  "subjectId":27,
  "name":"AECA_VA_GENERATED_VA71CAS242",
  "subjectDN":"CN=AECA_VA_GENERATED_VA71CAS242",
  "subjectAltName":null,
  "issuerDN":"CN=NEWCASROOTTEST,OU=Department,O=organization,L=City,C=RU",
  "validity":1716989431000,
  "created":1653917517000,
  "cert":"U3ViamVjdDogQ049QUVDQV9WQV9HRU5FUkFURURfVke3MUNBUzI0MgpJc3N1ZXI6IENOPU5FV0NBU
1JPT1RURVNULE9VPURlcGFydG1lbnQsTz1vcmdhbml6YXRpb24sTD1DaXR5LEM9U1UKLS0tLS1CRUdJTtIBDRV
JUSUZJQ0FURS0tLS0tCk1JSURHakNDQWdLZ0F3SUJBZ01VTVRYZn1jbFJNaTF6NnRWM0JveU4vUy9BK21Zd0R
RWUpLb1pJaHJjTkFRRUYKQlFBd11URVhNQ1VHQTFVRUF3d09Ua1ZYUTBGVfVrOVBWR1JGVTFReEV6QVJCZ05W
QkFzTUNrUmXjR0Z5ZEcxbApib1F4R1RBVEJnTlZCQW9NREc5eVoyRnVhWHBoZEEdsdmJqRU5NQXNHQTFVRUJ3d
0VRMmwZVRfTE1Ba0dBMVVFcKJoTUNVbFV3SGhjTk1qSXdOVE13TVRNek1UVTNXaGNOTWpRd05USTVNVE16TU
RNeFdqQW5NU1V3SXdzRFZRUUQKREJ4Q1JVTk1JYmVpCWBdkR1RrV1NRV1JGUkY5V1FUY3hRMEZUTWpReU1JR2Z
NQTBHQ1NxR1NJYjNEUUVCCQVFVQpBNEdoQURDQmlRS0JnUURBK2VkSC85REJEd29zRi9HS1crV2FrYXQ2c3Z3
Um52eWJmMnhMcXBXdVlhWU8xSWs4Cm55M0FiS2FDdFJCWj1Da2xLSkY0RldIb29wV0IrZ1UrV1I4bW1ZQXBxZ
Wt0WmluSWE2MEZneGs4cmJTOVc5RGkKR1JpSXLGVDFCa2RFYzFuTHppYjlmQTFWNUQrSHpIMD15WGhWRE80WF
VUY1hNV1V0Qmltcmcxc21jU1EUVFBQgpnVEDITU1HRU1Bd0dBMVVkrXdfQi93UUNNQVF3SHdzRFZSMGpCQmd
3Rm9BVVc3M1I2S3RFR21CQ3daV1pPNWVICjhTMjFTNUF3RHdZSkt3WUJCUVVIUUFRRk1JBSUZBREQUmdOVkhT
VUVEREFLOmdncKJnRUZCUWNEQ1RBZEJnTlYKSFE0RUZnUUVVBK0hoNGNVR0FGMjJ1ZXJRb0Rlc1JTB1hFUUF3R
GdZRFZSMFBBUUGvQkFRREFnZUFNQTBHQ1NxRwptSWIzRFFfQk1RVUFBNE1CQVFCCXJSUWlia11Jck5ZUVNRak
kxeitJS1ZyM3RhN3gvN01ZR2R3ZjI4bXhqTE1HCk1JITzVYVDQrM0ZkNVVpK1dSNktoazFkVVBYNVFUSTdYUET
jMD10Z1QrZTJOa3l3VmhvZ0Fna2pGMUhhY0o4dTcKd1MwaXNjNmhmY2FJbnRYTU0UwMUNVYkhFclU5ejFlVXFJ
dFlwYW0wci9XMDdoZ0F2dHRESzBMQUJuYzRXTWhMMaPia2ZzB0doMn1QKzF3T1RBQ1BPMzhNenZSMDBRZTJMq
kFzekhteUo5VXpnRFFKRVEuUDJMcUxJUW9MMmtVb2htCnZLL3BIQXpjOFdxbmhFRXpvcmeZwGs2OFVRdXh6K2
tOUVhxaGxZNUJXdkd4OEprOTBjaFdoWnlpSjZ2Y1JCK0UKRj13aT1VQ01DcUpMSnJYdWloVDJ3WnpocE5TUFF
3Y09SY3hXMDhuagotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tC1N1YmplY3Q6IENOPU5FV0NBU1JPT1RURVNU
LE9VPURlcGFydG1lbnQsTz1vcmdhbml6YXRpb24sTD1DaXR5LEM9U1UKSXNzdWVYoiBDTj1ORVdDQVNST09UV
EVTVCxPVT1EZXBhcnRtZW50LE89b3JnYW5pemF0aW9uLEw9Q210eSxDPVJVCi0tLS0tQkvH5U4gQ0VSVE1GSU
NBVEUtLS0tLQpNSU1Ec3pDQ0FwdWdBd01CQWdJVWRhTmJHbVdJM2VBcTY2aDAyNGk1TEZMQ0JHRXdeUUV1KS29
aSWWh2Y05BUUVGcKJRQXdZVEVYTUJVR0ExVUVBd3dPVGtWFFEWrlRvazlQVkvZSR1UxUXhFekFSQmdOVk1Jc01D
a1JsY0dGeWRHMWwKYm5ReEzUQVRCZ05WQkFvTURHOXlaMkZ1YVhwaGRhbHziakVOTUFzR0ExVUVVc3dFUTJSM
GVURUxNQWtHQTFVRUQpCaE1DVWxVd0hoY05Nak13T1RNd01UTXpNVFUzV2hjTk16SXdOVE13TURBd01EQXdXak
JoTVJjd0ZRWURWUVFECkRBNU9SVmREUVZOU1QwOVVVRVZUVkRFVE1CRUdBMVVfQ3d3S1JHVndZWEowYldWdWR
ERVZNQk1HQTFVRUNnd00KYjNkbl1XNXBlbUYyWVc5dU1RMHdDd11EV1FRSERBUkRhWFI11TVFzd0NRWURWUVFH
RXdkU1ZUQ0NBU013RFFZSgpLb1pJaHJjTkFRRUJCUUFEZ2dFUEFEQ0NBWU9DZ2dFQkFOTFBvOXNscompTNXVUQ
2JPMG85an1EMVBuZExNamJqCmtkS0ozeEFuN0h2OWphTHh6eFdBWnNvQVQvUEVUV291V3FYWjBBWmpISkY0aF
```

```
ZaSHBZZUg5NHBwd25RUTBQeFYKZ2U0RTZYS3JWek41WXdqTFJWK1phaTVzeXh4bTJyaVhTSzNmR0lQbz1LdHh
kdE52SDc1Wlg2TDB0VtySTBreAp1dDZoYTFvc3pzR05uR0lyaHNWTi9tNnE0SWxQVHVOOXhuVTdsdTBXZDRL
d1NUTGw0V1ZkL2xKY3lmZThqQkRaCnByYU1RRTN1d0M5SWJFOVB2RkphUWp5UzFCb1VjUG1vc1B6cGZ3aTBZM
FpaVVE2VExmN1RPRHE5R3g1enowRXEKbGU3ZjgyU3N3U1Y2Yj1ZMnJnQ111RkY3NHRRU2FDYW9XWm10NUU4NE
hYaG1TS1Rxa1QyOFZ5VUNBd0VBQWFOagpNR0V3RHdZRFZSMFRBUUgVqkFVd0F3RUIvekFmQmdOVkhTTUVHREF
XZ0JSYnZaSG9xMFFhWUVMQmxaazdsNGZ4CkxiVkxrREFkQmdOVkhrNEVGZ1FVVzcyUjZLdEVHbUJdd1pXWk81
ZUg4UzIxUzVBd0RnWURWUjBQQVFIL0JBUUQKQWdHR01BMEdDU3FHU01iM0RRRUJCUVVBQTRJQkFRQitPU2hEa
kRtbUNiU1NjVEdiQ0szYmRzZnlETFN0ancvMApZeJewTjVrUS9pWWQ4WDE2YzJxS3NwWTExa2xYYV1sVVFPL2
V2dDFLSXV5VWVydi94My9Yd2ZudGYzd3ZKv1pUCnJYeTBxekhsaDIzbURYWndpV1hOYU5EMWdyQVZqUzE2bWJ
NcnBVTtljkdNaYVdkKzY2RmpZSkVLa1JYYm41RVIKYZxc3YyZDNqRVp0SFFLSWFkTGthSlh2Zk43Ni9rK2FV
Q2dHdFzFMVjvcEgyS25TNmlTL0NQK0QrMVZuRXZNeQppbVRqWU14UnJTSW9yRjFuSEgxT0ttduFqTHNRdzhoS
nhzUHpTdUppeU1IQXVyV3UxamRVsmlDG14M2dVVFVxCnA3WTN1bldjRjZydGkxdGdnenNnZDNtNXJUUXV1UE
5DQ11CMi9IM2RZemh6eEk4VzBKZTYKLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo="
}
```

Пример ответа при ошибке на запрос:

```
{"clazz": "AecaRuntimeException", "message": "Произошла ошибка создания субъект
SubjectDN=CN=AECA_VA_GENERATED_VA71CAS242 уже используется или группа не
существует."}
```

## 10.20 Получить состояние сертификата по его серийному номеру

### 10.20.1 Формат запроса:

```
GET /certificates/status/{serialNumber}
```

где {serialNumber} - номер серийный номер сертификата (см. п. 10.4, п. 10.5).

### 10.20.2 Пример запроса:

```
curl -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM
"https://192.168.111.242:8888/aeca/api/certificates/status/55059430571631448260280792
4022737971996383683366"
```

10.20.3 Формат ответа – строка со статусом сертификата. Возможные варианты статуса сертификата: ACTIVE, SUSPEND, REVOKED.

### 10.20.4 Пример ответа:

```
"ACTIVE"
```

## 10.21 Приостановить действие сертификата

### 10.21.1 Формат запроса:

```
POST /certificates/suspend
```

В теле запроса нужно передать json-объект с полем [certSerialNumber], в котором указать серийный номер сертификата (см. п. 10.4, п. 10.5).

#### 10.21.2 Пример запроса:

```
curl -X POST -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/certificates/suspend" -d '{"certSerialNumber":550594305716314482602807924022737971996383683366}' -H 'Content-Type: application/json'
```

#### 10.21.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

#### 10.21.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz":"NullPointerException","message":null}
```

## 10.22 Возобновить действие сертификата

#### 10.22.1 Формат запроса:

```
POST /certificates/reactivate
```

В теле запроса нужно передать json-объект с полем "certSerialNumber", в котором указать серийный номер сертификата (см. п. 10.4, п. 10.5).

#### 10.22.2 Пример запроса:

```
curl -X POST -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/certificates/reactivate" -d '{"certSerialNumber":550594305716314482602807924022737971996383683366}' -H 'Content-Type: application/json'
```

#### 10.22.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

#### 10.22.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz":"NullPointerException","message":null}
```

## 10.23 Отозвать сертификат

#### 10.23.1 Формат запроса:

```
POST /certificates/revoke
```

В теле запроса нужно передать json-объект, содержащий поля:

- [certSerialNumber] - указать номер серийный номер сертификата (см. п. 10.4, п. 10.5);
- [revocationReason] - указать причину отзыва, одну из UNSPECIFIED, KEY\_COMPROMISE, CA\_COMPROMISE, AFFILIATION\_CHANGED, SUPERSEDED, CESSATION\_OF\_OPERATION, CERTIFICATE\_HOLD, PRIVILEGES\_WITH\_DRAWN, AA\_COMPROMISE.

10.23.2 Пример запроса:

```
curl -X POST -k --cert ./https.crt.pem --cert-type PEM --key ./https.key.pem --key-type PEM "https://192.168.111.242:8888/aeca/api/certificates/revoke" -d '{"certSerialNumber":"550594305716314482602807924022737971996383683366","revocationReason" : "UNSPECIFIED" }' -H 'Content-Type: application/json'
```

10.23.3 Формат ответа:

- при успешном ответе на запрос – статус 200;
- при ошибке – статус 400, 401, 403, 500 с описанием ошибки.

10.23.4 Пример ответа

Пример ответа при ошибке на запрос:

```
{"clazz":"NullPointerException","message":null}
```

## 11 КОНТАКТЫ

### 11.1 Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: [aladdin@aladdin-rd.ru](mailto:aladdin@aladdin-rd.ru) (общий)

Web: <https://www.aladdin-rd.ru>

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

### 11.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

[www.aladdin-rd.ru/support/index.php](http://www.aladdin-rd.ru/support/index.php).

---

## Коротко о компании

Компания "Аладдин Р.Д." основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

### Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

### Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.

