Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition

Руководство получателя сертификатов

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 34 02
Версия	2.2.1
Листов	62
Дата	17.06.2025

Авторские права, товарные знаки, ограничения

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.

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.), подтверждённые или включённые 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 индивидуальное, 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 возникать 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 нелицензионным 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 УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

АННОТАЦИЯ

Настоящий документ представляет собой руководство пользователя с ролью «Получатель сертификатов» (далее – получатель сертификатов) программного комплекса «Центр регистрации Aladdin Enterprise Registration Authority [1]» (входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»[2]), предназначенного для заведения и обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов), выпускаемых в программном комплексе «Центр сертификации Aladdin Enterprise Certification Authority» [3] (входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»).

Получатели сертификатов являются субъектами ресурсной системы [4] (доменной службы каталогов), подключенной как к Центру регистрации eRA, так и к Центру сертификации eCA.

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

Перед эксплуатацией программы рекомендуется внимательно ознакомиться с настоящим руководством.

[1] Далее по документу – программа, Центр регистрации Aladdin eRA.
[2] Далее по документу –Центр сертификатов доступа Aladdin eCA CE.
[3] Далее по документу - Центр сертификации Aladdin eCA.
[4] Далее по документу – РС.

Содержание

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Область применения

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

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

1.2 Состав программы

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

- Программный компонент «Серверная часть Центра регистрации.

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

- Программный компонент «Клиентская часть Центра регистрации».

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

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

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

[7] Далее по документу – сертификаты.

1.3 Функции программы

Основные функции Центра регистрации Aladdin eRA, доступные получателю сертификатов:

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

1.4 Уровень подготовки пользователя

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

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

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Поддерживаемые веб-браузеры

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

2.2 Поддерживаемые ключевые носители

Поддерживаемые модели электронных ключей (ключевых носителей):

- JaCarta PKI.
- JaCarta PRO.
- JaCarta-2 PKI/ГОСТ.
- JaCarta-2 ГОСТ.

2.3 Режим функционирования программы

Центр регистрации Aladdin eRA функционирует в следующих режимах:

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

Основным режимом функционирования Центра регистрации Aladdin eRA является штатный режим.

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

3 ДОСТУП К ПРОГРАММЕ

3.1 Подключение к веб-интерфейсу

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

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

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

Получатели сертификатов (субъекты РС) (пользователи с доменными учётными записями [9]) могут проходить идентификацию и аутентификацию в Центре регистрации Aladdin eRA по комбинации доменного имени и пароля или по Kerberos-билету. Для успешной аутентификации в веб-браузере должна быть настроена Kerberos-аутентификации (инструкция по настройке приведена в разделе 3.2). Информация о домене отображена в окне авторизации в поле «Домен».

Порядок подключения к веб-интерфейсу Центра регистрации Aladdin eRA:

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

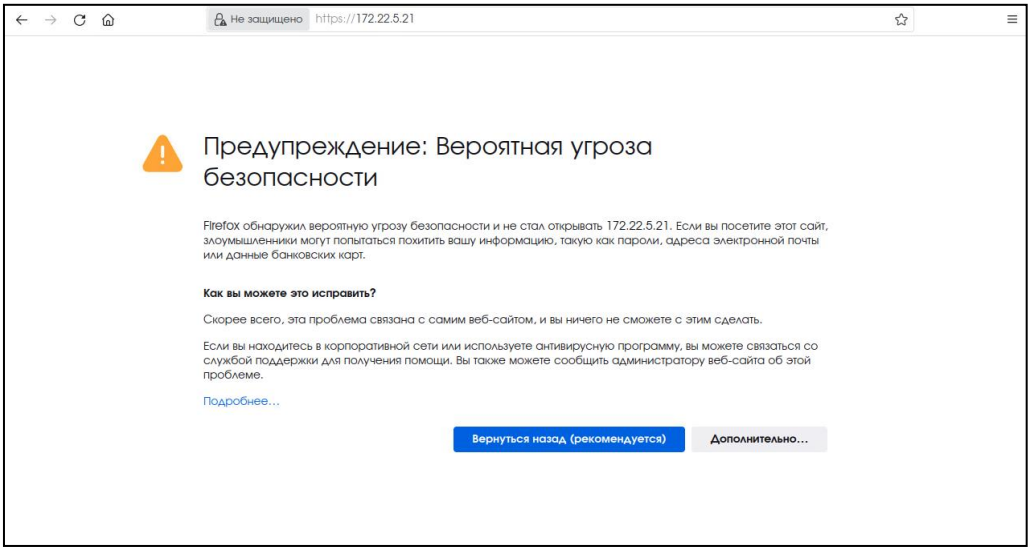


Рисунок 1 – Страница с предупреждением системы безопасности

[9] Учётные записи, находящиеся в домене, к которому подключён Центр регистрации Aladdin eCA.

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

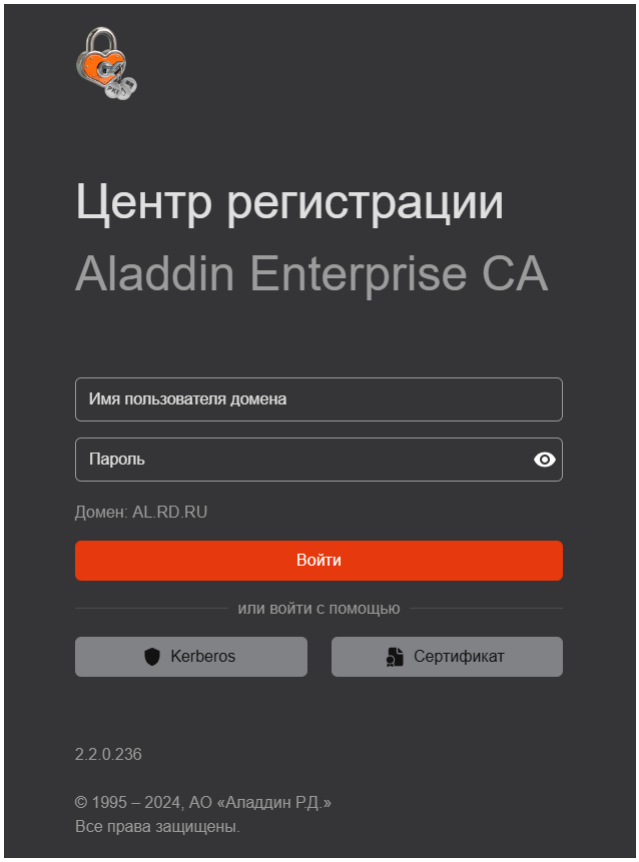


Рисунок 2 – Окно авторизации

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

.

Если у пользователя отсутствовала [10] учётная запись в Центре регистрации Aladdin eRA, то она будет автоматически создана с ролью «Получатель сертификатов».

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

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

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

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

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

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

Таблица 2 – Типовые ошибки при аутентификации по Kerberos-билету

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

3.2 Настройка Kerberos в веб-браузере

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

3.2.1 Настройка веб-браузера Mozilla Firefox

Далее в примере:

- `ra246.sambadc.host` – доменное имя Центра регистрации Aladdin eRA;
- `sambadc.host` – домен, (`SAMBADC.HOST` – realm в Kerberos);
- Версия браузера: 78.12.0esr (64-bit).

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

- Запустите веб-браузер Mozilla Firefox.
- В адресной строке введите `about:config` и нажмите Enter.
- Нажмите на кнопку **Принять риск и продолжить**.
- В поле «Поиск» (Filter) введите `negotiate`, чтобы ограничить список опций.
- Выполните двойное нажатие мышью на строке с параметром `network.negotiate-auth.trusted-uris`.
- В диалоговом окне введите:
  - Чтобы разрешить SPNEGO аутентификацию только по конкретной ссылке, введите полностью домен из ссылки (например, `ra246.sambadc.host`);
  - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена с точкой в начале (например, `.sambadc.host`);
  - Чтобы разрешить SPNEGO аутентификацию для нескольких доменов, введите их через запятую (например, `ra247.sambadc.host,ra246.sambadc.host`).
  - После запятой можно ставить пробел.

- Продублируйте введённое значение параметра `network.negotiate-auth.trusted-uris` в параметр `network.negotiate-auth.delegation-uris`.
- При необходимости удалите cookie, связанные с доменом Центра регистрации Aladdin eRA.

3.2.2 Настройка веб-браузера Chromium

Далее в примере:

- `ra246.sambadc.host` – доменное имя Центра регистрации Aladdin eRA;
- `sambadc.host` – домен, (`SAMBADC.HOST` – Realm в Kerberos);
- Версия браузера: Version 130.0.6723.69 (Official Build) (64-bit).

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

- Кликните правой кнопкой мыши на ярлыке "Chromium".
- Выберите "Свойства".
- В поле "Объект" к строке запуска браузера допишите
  - Чтобы разрешить SPNEGO аутентификацию только по конкретной ссылке, введите полностью домен из ссылки:
  - `--args --auth-server-whitelist="ra246.sambadc.host"`;
  - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена со звёздочкой и точкой в начале:
  - `--args --auth-server-whitelist="*.sambadc.host"`;
  - Чтобы разрешить SPNEGO аутентификацию для нескольких доменов, введите их через запятую:
  - `--args --auth-server-whitelist="ra246.sambadc.host,ra247.sambadc.host "`.
- При необходимости удалите cookie, связанные с доменом Центра регистрации Aladdin eRA.

Пример консольной команды: `chromium --args --auth-server-whitelist="ra246.sambadc.host"`

3.3 Описание элементов веб-интерфейса

Главный экран веб-интерфейса Центра регистрации Aladdin eRA для получателя сертификатов (субъекта РС) представлен на рисунке ниже (Рисунок 3).

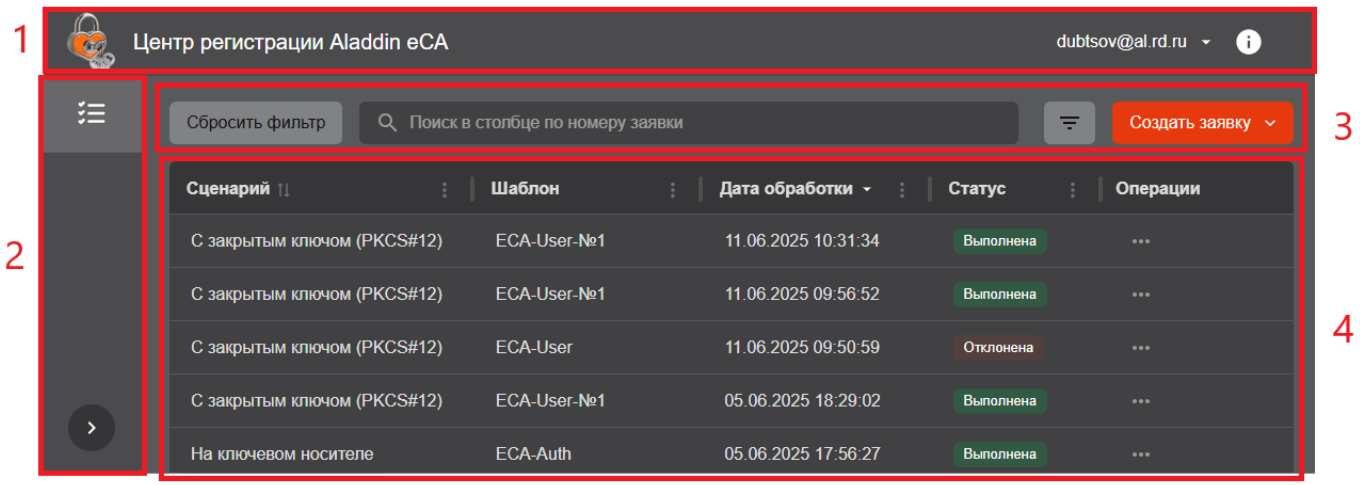


Рисунок 3 – Основные элементы веб-интерфейса

Цифрами на рисунке обозначены:

1 Верхняя панель (загогловок)

Заголовок отображается на всех страницах веб-интерфейса ViPNet TIAS и содержит следующие инструменты:

- Меню авторизованного получателя сертификатов (Рисунок 4).

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

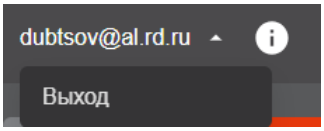


Рисунок 4 – Завершение рабочей сессии

-  - значок предназначен для предоставления сведении о текущей версии программы, контактной информация разработчика, правах на программное обеспечение (Рисунок 5).

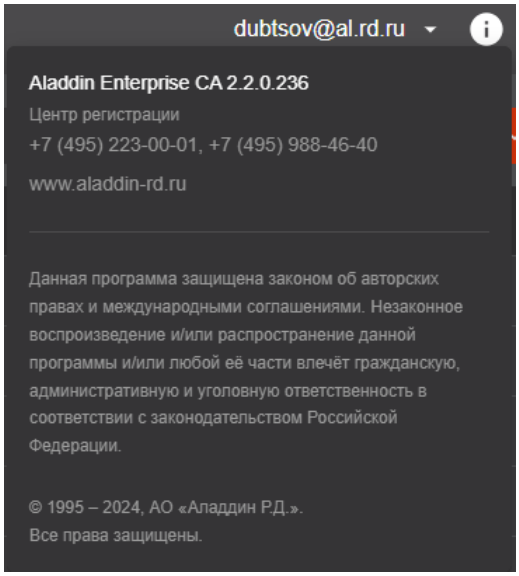


Рисунок 5 – Информация о программе

2 Боковая панель (панель навигации)

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

Полный вид боковой панели показан на рисунке ниже (Рисунок 6). Скрытый вид боковой панели показан на рисунке выше (Рисунок 3. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели.

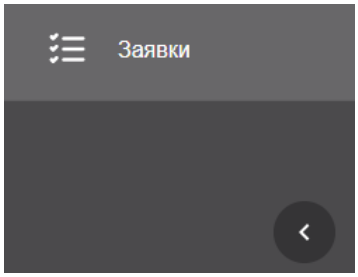


Рисунок 6 – Полный и скрытый виды боковой панели

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

- Просмотр списка заявок в табличном виде.
- Просмотр карточки заявки.
- Создание заявки на выпуск сертификата на основании запроса.
- Создание заявки на выпуск сертификата с закрытым ключом PKCS#12.
- Создание заявки на выпуск сертификата на ключевом носителе.
- Отмена заявки.
- Выгрузка сертификата.
- Импорт сертификата на ключевой носитель.
- Выгрузка цепочки сертификатов.
- Выгрузка контейнера закрытого ключа PKCS#12.
- Выгрузка CRL издателя.
- Выгрузка цепочки сертификатов издателя.
- Отзыв сертификата.

3 Панель инструментов

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

4 Панель просмотра

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

4 УПРАВЛЕНИЕ ЗАЯВКАМИ НА ВЫПУСК СЕРТИФИКАТОВ

4.1 Общие сведения о заявках

Процесс подачи заявки на выпуск сертификата включает:

- Выбор шаблона, по которому будет выпущен сертификат.

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

- Редактирование (при необходимости) атрибутов сертификата согласно выбранному шаблону (не выполняется при подаче заявки на основание запроса на сертификат PKCS#10 [11]).
- Указание пароля для защиты контейнера PKCS#12 (только при подаче заявки с закрытым ключом PKCS#12 [12]).
- Выбор алгоритма и длины ключа для генерации ключевой пары (не выполняется при подаче заявки на основание запроса на сертификат PKCS#10).

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

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

Заявка на выпуск сертификата имеет следующие атрибуты:

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

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

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

  - Ожидает подтверждения – заявка создана, получателю сертификатов (субъекту) назначены правила выпуска с автоматизированной (ручной) обработкой заявок уполномоченным пользователем Центра регистрации Aladdin eRA.
  - Выполнена – заявка обработана, в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта) успешно выпущен сертификат.
  - Отменена – заявка отменена получателем сертификатов (субъектом) или иным уполномоченным пользователем Центра регистрации Aladdin eRA.
  - Ожидает импорта на КН – заявка обработана, в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта) успешно выпущен сертификат, который ожидает импорта на ключевой носитель.
  - Новая – статус присваивается заявке при ее регистрации, сразу после этого происходит обработка заявки и её статус изменяется. Данный статус может быть отображен в веб-интерфейсе в случае ошибки при первичной обработке заявки.
- Общая информация о заявке:
  - Сценарий – наименование сценария, по которому была создана заявка на выпуск сертификата:
    - На основании запроса (PKCS#10).
    - С закрытым ключом (PKCS#12).
    - На ключевом носителе.
    - WSTEP [13].
  - Шаблон – шаблон, по которому будет и уже выпущен сертификат.
  - Центр сертификации - центр сертификации, в котором будет и уже выпущен сертификат по данной заявке, на основании используемого в сценарии создания заявки шаблона.
  - Внешний идентификатор – идентификатор из запроса на выпуск сертификата PKCS#10.
  - Дата создания – дата и время создания заявки.
  - Дата обработки – дата и время последней смены статуса (обработки) заявки (например, создание или отмена заявки).
  - Комментарий – комментарий, указанный уполномоченным пользователем Центра регистрации Aladdin eRA при обработке заявки.
- Информация об истории изменения заявки:
  - Дата – дата и время события, связанного с изменением заявки.
  - Имя учётной записи – отображаемое имя пользователя (получателя сертификатов), сделавшего изменение в заявке.
  - Событие – описание события, связанного с изменениями заявки (например, создание заявки).

4.2 Просмотр записей о заявках

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

Для просмотра информации о заявках на сертификаты подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки** (см. Рисунок 7).

[13] Заявки по сценарию «WSTEP» создаются в Центе регистрации Aladdin eRA автоматически в результате обработки запросов получателей сертификатов (субъекто РС) по протоколу MS-WSTEP (см. раздел 6).

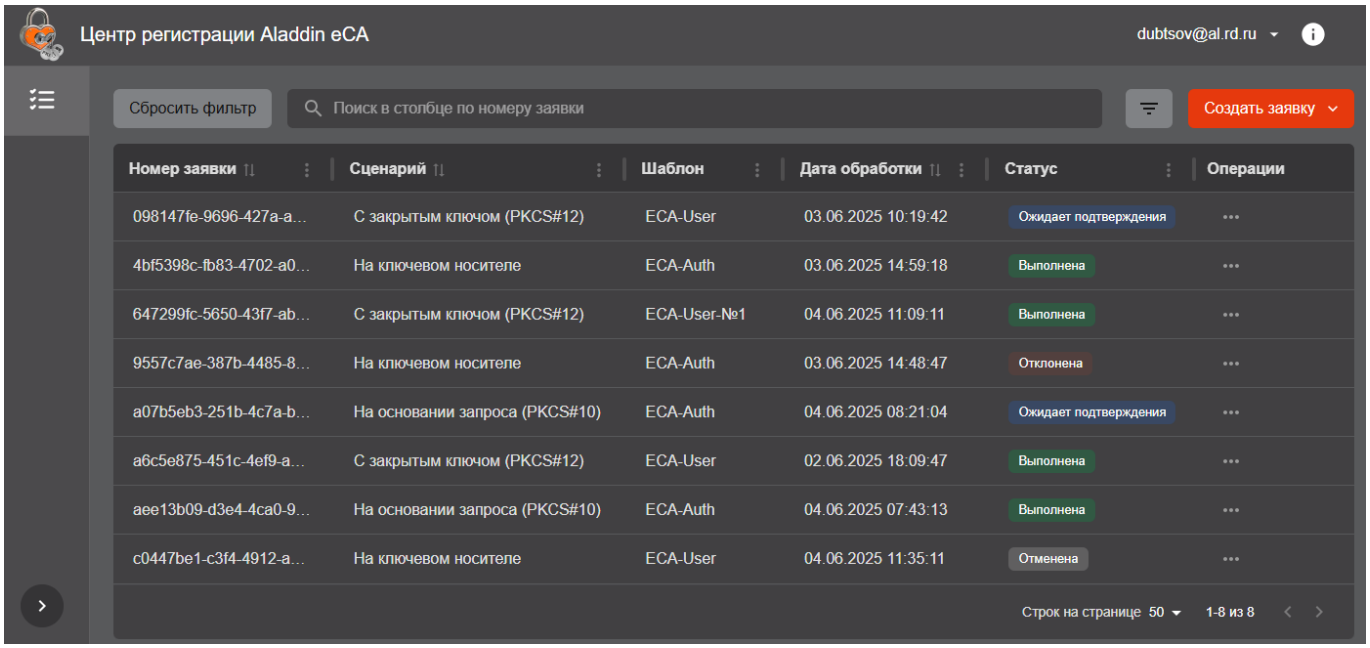


Рисунок 7 – Просмотр списка заведенных заявок получателя сертификатов (субъекта РС)

Информация о заявках отображается списком в табличном виде.

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

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

Записи о заявках выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 8).

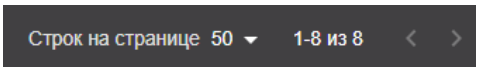


Рисунок 8 – Инструменты навигации списка заявок

Описание инструментов навигации:

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

Для удобства анализа информации о заявках в списке вы можете управлять видимостью колонок таблицы с заявками. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок **<Действие колонки>** и в открывшемя списке [14] выберите **<Скрыть [название колонки] колонку>** (см. Рисунок 9). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок **<Действие колонки>** и в открывшемя списке выберите **<Показать все колонки>** (см. Рисунок 9).

[14] Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

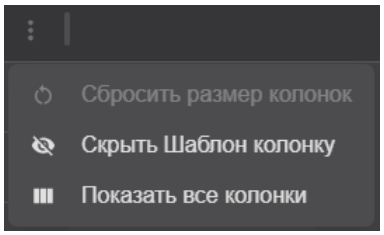


Рисунок 9 – Список действий с колонкой **[Шаблон]**

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

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

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

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

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

Чтобы выполнить сортировку записей о заявках по выбранному атрибуту, щелкните в заголовке сооответсвующей колонки значок **<Действие колонки>** и в открывшемя списке [15] (см. Рисунок 10) выберите:

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

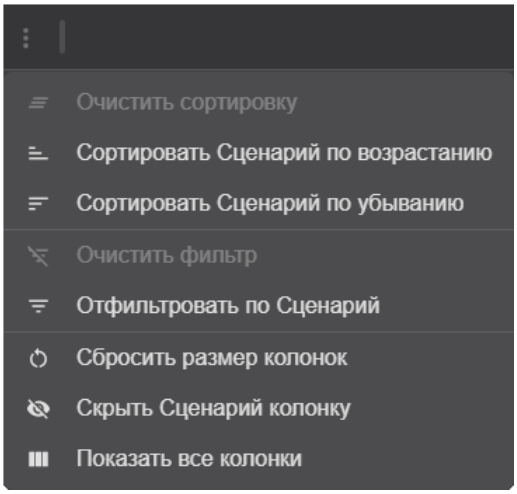


Рисунок 10 – Список действий с колонкой **[Сценарий]**

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками [16] (см. Рисунок 10):

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

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

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

Чтобы отменить сортировку записей о заявках по выбранному атрибуту, щелкните в заголовке сооответсвующей колонки значок **<Действие колонки>** и в открывшемя списке [17] (см. Рисунок 10) выберите **<Очистить сортировку>**.

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

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

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

По умолчанию фильтры скрыты. Чтобы использовать фильтры, нажмите на панели инструментов кнопку **<Фильтр>** или щелкните в заголовке колонок **[Сценарий]**, **[Дата обработки]** или **[Статус]** значок **<Действие колонки>** и в открывшемя списке (см. Рисунок 10) выберите **<Отфильтровать по [название колонки]>** (см. Рисунок 11).

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

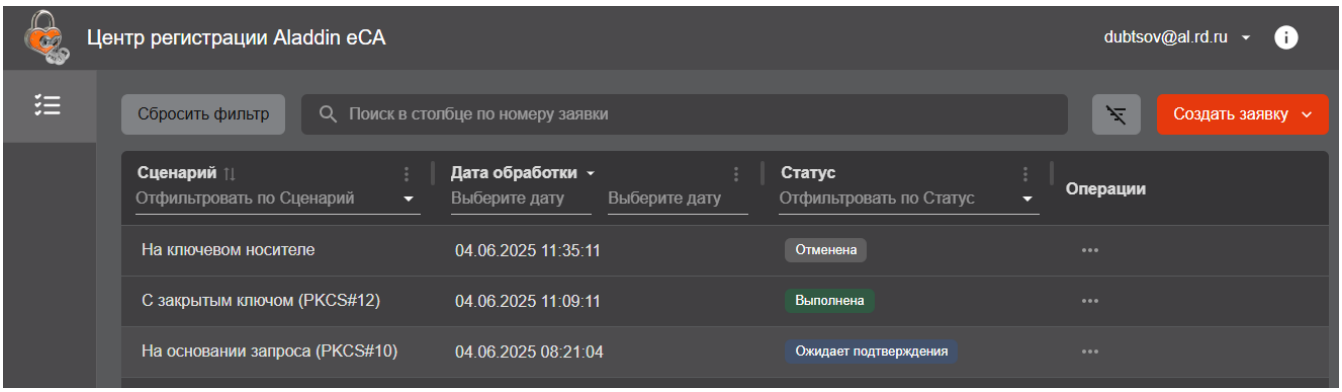


Рисунок 11 – Отображение фильтров в заголовках колонок включено

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

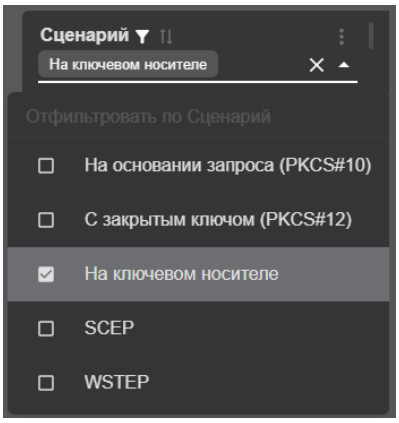
Фильтры по атрибутам заявок, представленным в колонках **[Сценарий]** (см. Рисунок 12а) и **[Статус]** (см. Рисунок 12б), обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов.

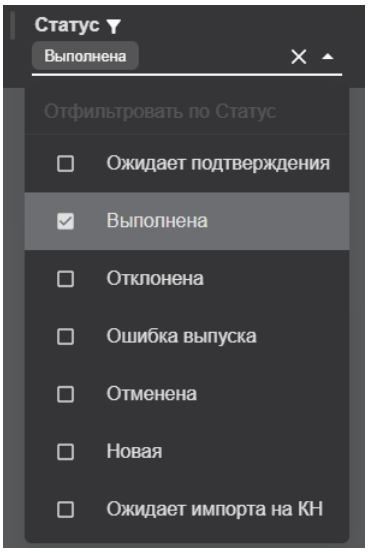
Фильтр по атрибуту заявок, представленном в колонке **[Дата обработки]** (см. Рисунок 12в), обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок (см. Рисунок 12).

Признаком применения фильтра является значок в заголовке соответствующей колонки (см. Рисунок 12).

[17] Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

а) 

б) 

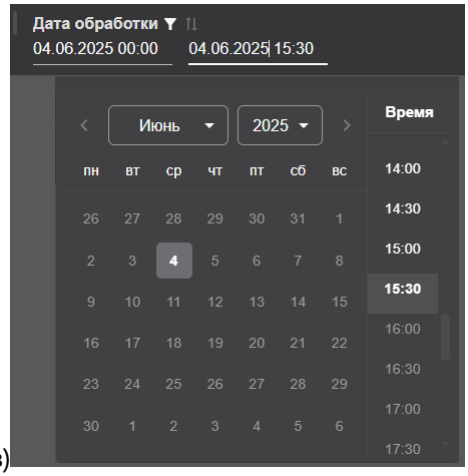
в) 

Рисунок 12 – Указание критериев выборки в фильтрах

Чтобы отменить действие определенного фильтра, щелкните в заголовке колонки значок **<Действие колонки>** и в открывшемся списке (см. Рисунок 10) выберите **<Очистить фильтр>** или щелкните в заголовке колонки значок (только для колонок **[Сценарий]** (см. Рисунок 12а) и **[Статус]** (см. Рисунок 12б)).

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

Чтобы выполнить выборку записей о заявках по их номерам, введите в поисковой строке, расположенной на панели инструментов, ключевое слово, содержащееся в номере заявки (см. Рисунок 13). Для отмены выборки заявок по их номерам щелкните в поисковой строке значок .

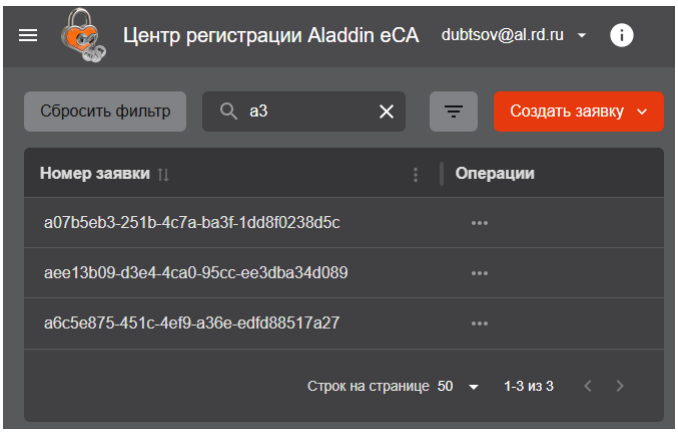


Рисунок 13 – Выборка заявок по их номерам с помощью поисковой строки

4.3 Просмотр карточки заявки на выпуск сертификата

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

Чтобы открыть карточку заявки:

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

В результате откроется карточка заявки.

Карточка заявки, по которой еще не выпущен сертификат, представлена на рисунке ниже (см. Рисунок 14). Описание атрибутов заявки приведено в разделе 4.1.

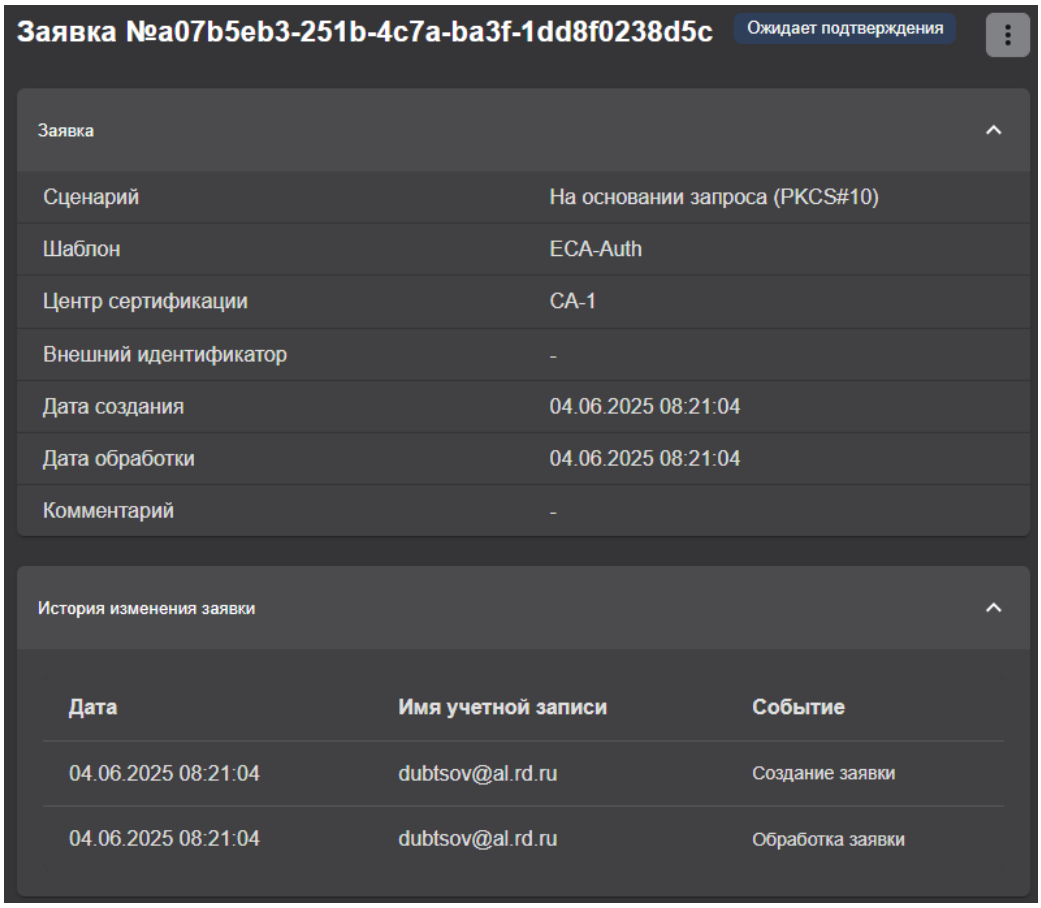


Рисунок 14 – Карточка заявки, по которой еще не выпущен сертификат

Карточка заявки, по которой уже выпущен сертификат, представлена на рисунке ниже (см. Рисунок 15). Описание атрибутов заявки (блоки «Заявка» и «История изменений заявки») приведено в разделе 4.1.

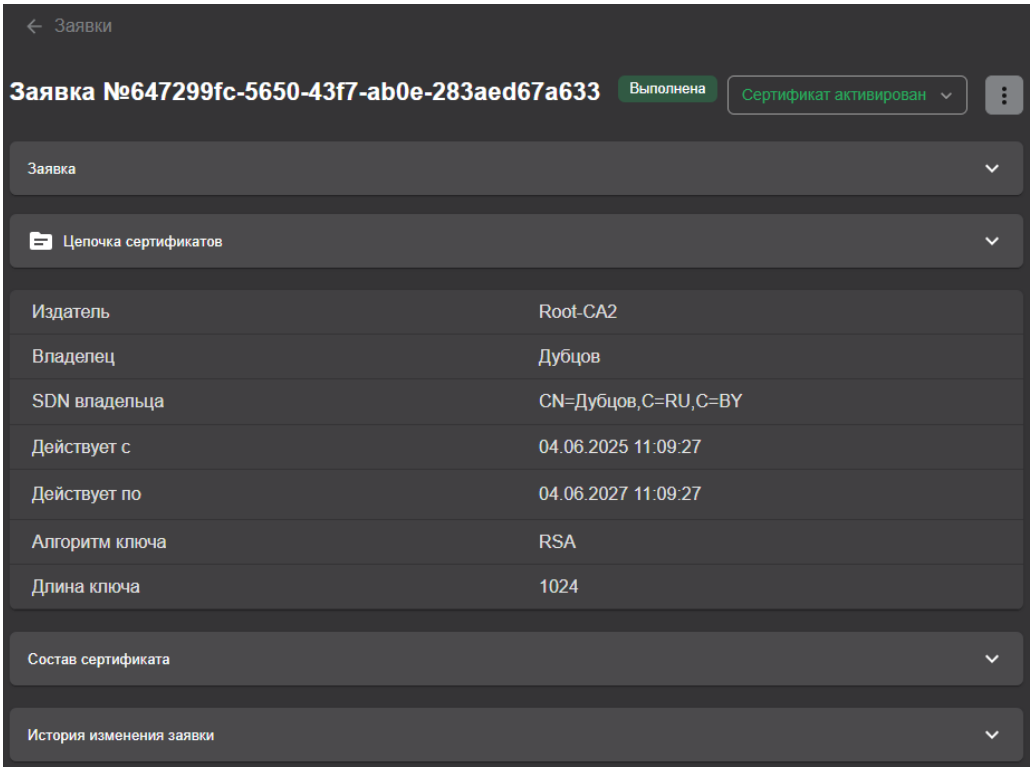


Рисунок 15 – Карточка заявки, по которой выпущен сертификат

Карточка заявки, по которой уже выпущен сертификат (см. Рисунок 15), содержит также информацию о выпущенном по ней сертификате (статус сертификата, блоки «Цепочка сертификатов», «Информация о сертификате» и «Состав сертификата»).

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

В блоке «Цепочка сертификатов» (см. Рисунок 16) представлена иерархическая коллекция сертификатов, которая ведёт от сертификата, выпущенного по данной заявке, к корню доверия (корневому центру сертификации).

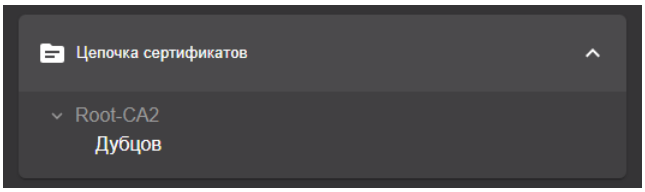


Рисунок 16 – Блок «Цепочка сертификатов»

В блоке «Информация о сертификате» (см. Рисунок 17) представлена следующая информацию о сертификате:

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

В блоке «Состав сертификата» (см. Рисунок 17) представлена следующая информацию о сертификате:

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

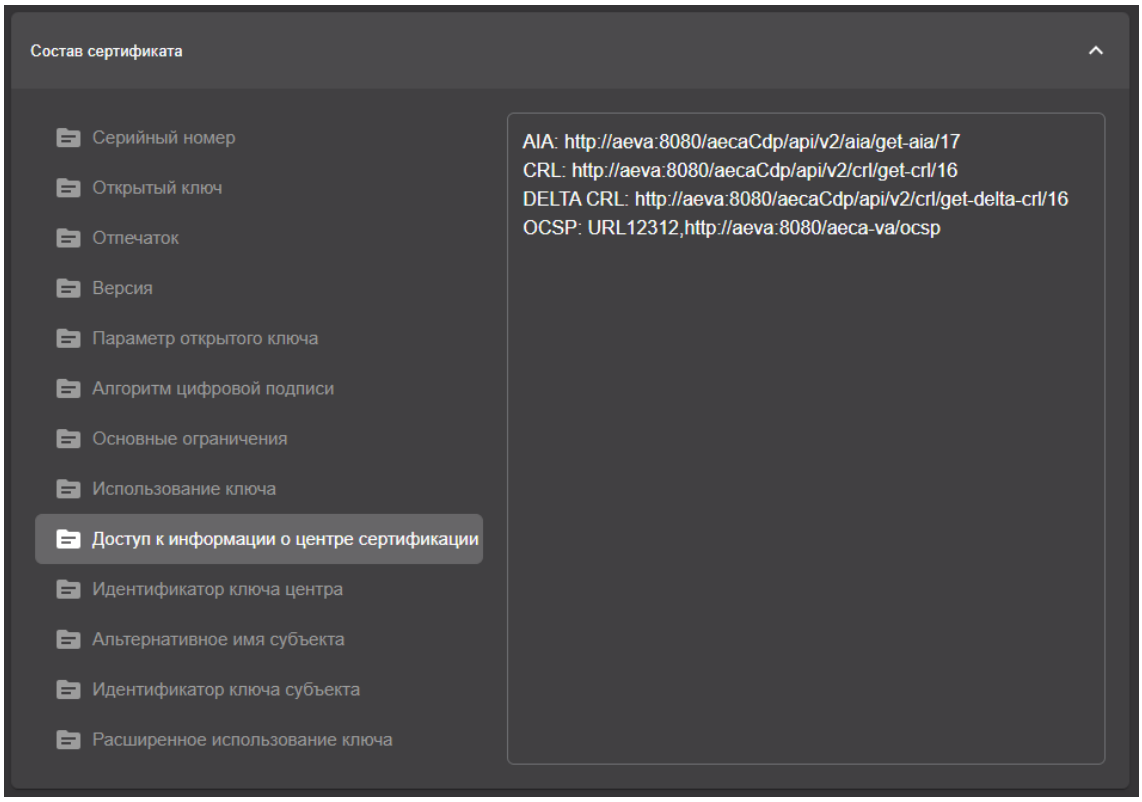


Рисунок 17 – Блок «Состав сертификата»

4.4 Создание заявок на выпуск сертификатов

4.4.1 Создание заявки на основании запроса PKCS#10

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

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

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

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку Создать заявку и выберите в открывшемся списке сценарий создания заявки **<На основании запроса>** (см. Рисунок 18).

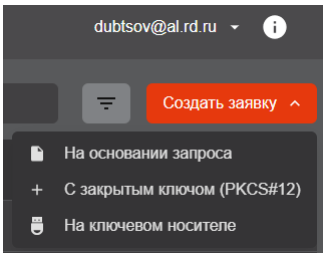


Рисунок 18 – Выбор сценария создания заявки

- В открывшемся окне «Создание заявки» (см. Рисунок 19):
  - Нажмите кнопку Выбрать файл и укажите путь к файлу с запросом на сертификат.
  - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат [18].
  - Нажмите кнопку Создать заявку.

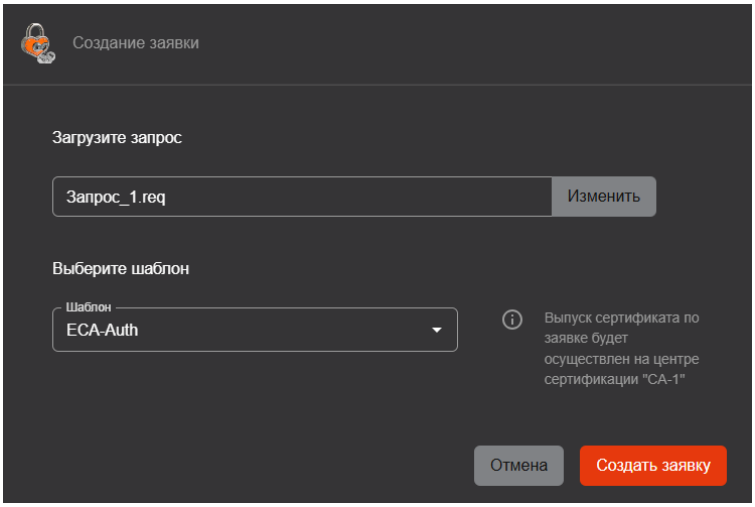


Рисунок 19 – Выбор файла с запросом и шаблона для выпуска сертификата

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

- Найдите заявку, из которой нужно выгрузить запрос, в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать запрос PKCS#10>** (см. Рисунок 20).

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

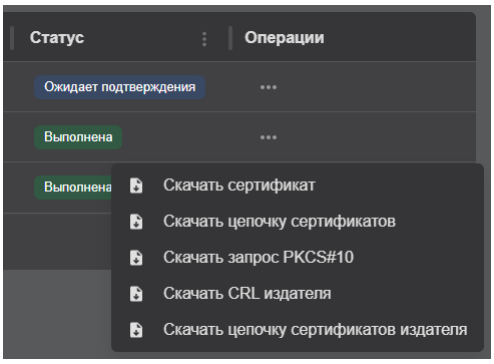


Рисунок 20 – Выгрузка запроса на выпуск сертификата

- Откройте карточку заявки, из которой нужно выгрузить запрос, (см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать запрос PKCS#10>** (см. Рисунок 21).

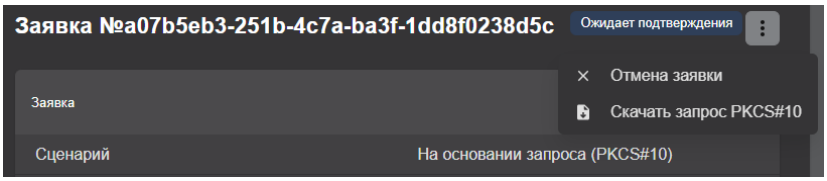


Рисунок 21 – Выгрузка запроса на выпуск сертификата

4.4.2 Создание заявки с закрытым ключом PKCS#12

Порядок создания заявки с закрытым ключом PKCS#12:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку Создать заявку и выберите в открывшемся списке сценарий создания заявки **<На основании запроса>** (см. Рисунок 18).
- В открывшемся окне «Создание заявки» (шаг 1 сценария) (см. Рисунок 22) в списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат [19], и нажмите кнопку Продолжить.

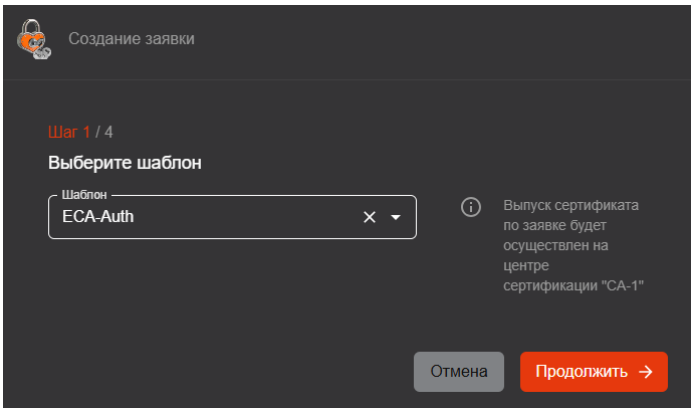


Рисунок 22 – Выбор шаблона для выпуска сертификата

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

- В открывшемся окне «Создание заявки» (шаг 2 сценария) (см. Рисунок 23) укажите атрибуты получателя сертификатов (субъекта РС):

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

– При необходимости выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений (см. Рисунок 23).

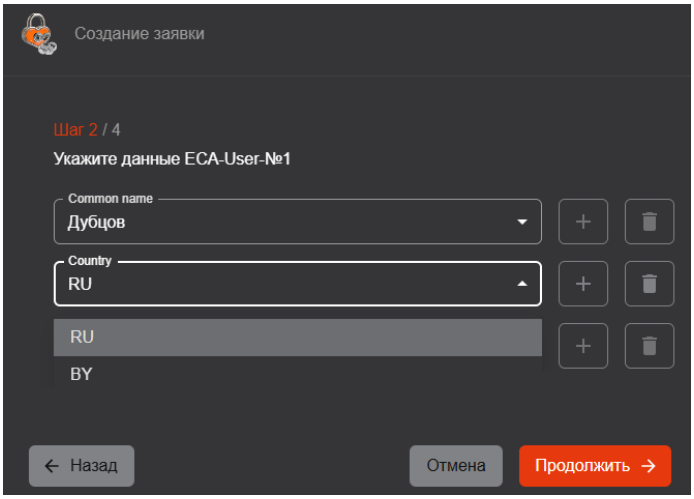


Рисунок 23 – Редактирование атрибутов получателя сертификатов (субъекта РС)

– При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку + и выберите в списках новых атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений) (см. Рисунок 24).

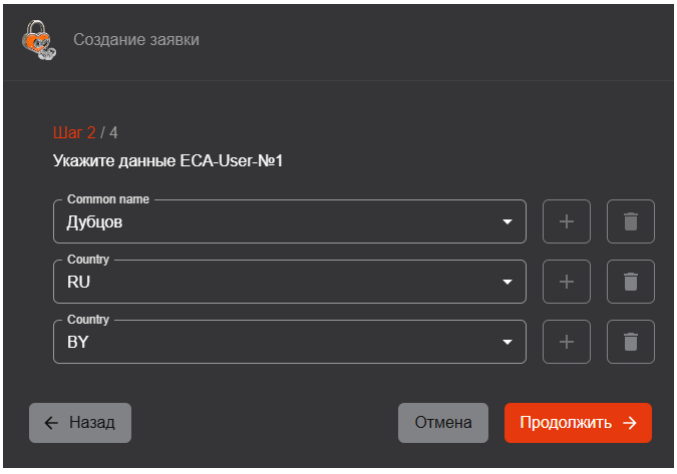


Рисунок 24 – Добавлен новый атрибут

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

В случае отсутствия у получателя сертификатов (субъекта РС) обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке (см. Рисунок 25). При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

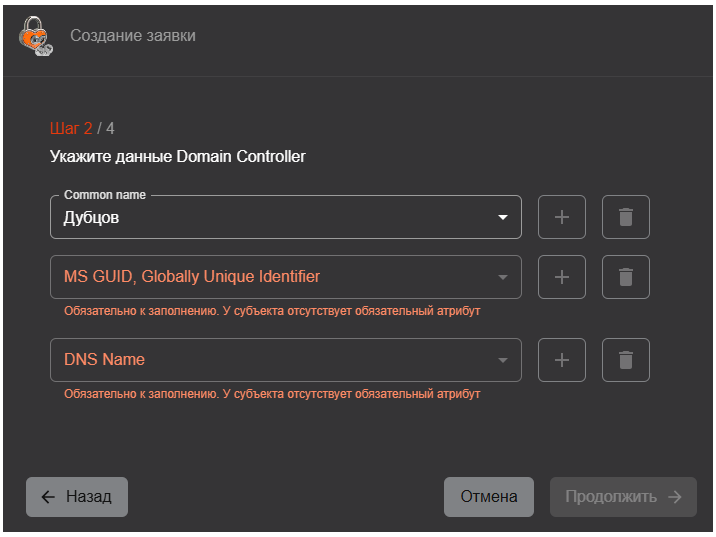


Рисунок 25 – У получателя сертификатов (субъекта РС) отсутствуют обязательные по шаблону атрибуты

Если у получателя сертификатов (субъекта РС) отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить (см. Рисунок 26).

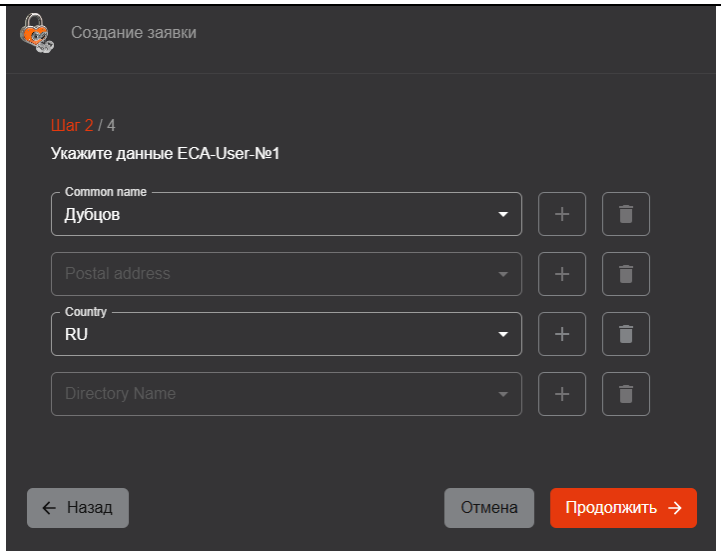


Рисунок 26 – У получателя сертификатов (субъекта РС) отсутствуют необязательные по шаблону атрибуты

- После редактирования атрибутов получателя сертификатов (субъекта РС) нажмите кнопку Продолжить.

- В открывшемся окне «Создание заявки» (шаг 3 сценария) (см. Рисунок 27) в соответствующих полях задайте и подтвердите пароль для контейнера PKCS#12 и нажмите кнопку Продолжить.

  Пароль должен удовлетворять следующим требованиям:

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

Для просмотра вводимых символов пароля щелкните в поле значок .

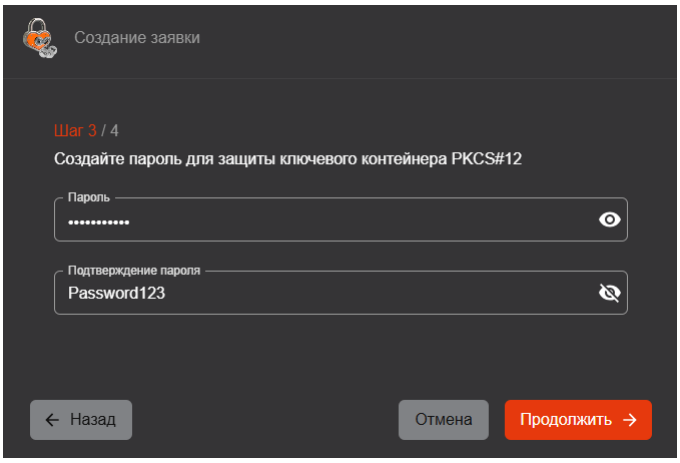


Рисунок 27 – Установка пароля для контейнера PKCS#12

- В открывшемся окне «Создание заявки» (шаг 4 сценария) (см. Рисунок 28):
  - В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
  - В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
  - Нажмите кнопку Создать заявку.

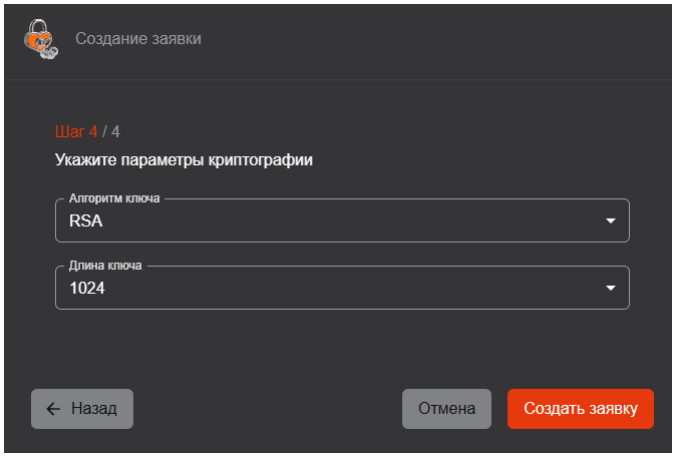


Рисунок 28 – Выбор алгоритма выработки ключевой пары и длины ключа

4.4.3 Создание заявки на ключевом носителе

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

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

Порядок создания заявки для импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку Создать заявку и выберите в открывшемся списке сценарий создания заявки **<На ключевом носителе>** (см. Рисунок 18).

Если приложение JC-WebClient не установлено (см. Рисунок 29) или к компьютеру не подключен ключевой носитель (см. Рисунок 30), создать заявку на ключевом носителе невозможно.

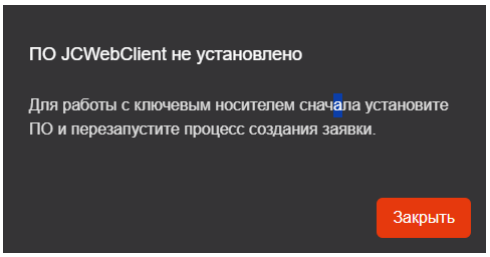


Рисунок 29 – Приложение JC-WebClient не установлено

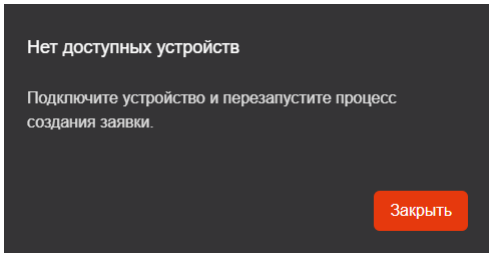


Рисунок 30 – Ключевой носитель не подключен к компьютеру

- В открывшемся окне «Создание заявки на сертификат» (шаг 1 сценария) (см. Рисунок 31):
  - В списке «Устройство» выберите подключенный ключевой носитель.
  - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
  - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат [20].
  - Нажмите кнопку Продолжить →.

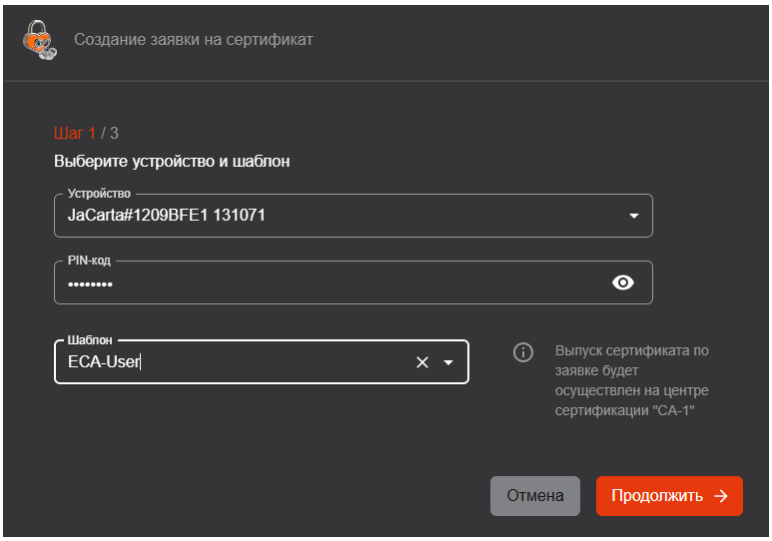


Рисунок 31 – Выбор ключевого носителя и шаблона для выпуска сертификата

- В отрывшемся окне «JC-WebClient. Подтверждение доверия к сайту» подтвердите доверие[21] к веб-интерфейсу Центра регистрации Aladdin eRA, нажав кнопку **<Доверяю>** (см. Рисунок 32).

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

[21] Приложение JC-WebClient запрашивает подтверждение доверия только один раз при первом взаимодействии.

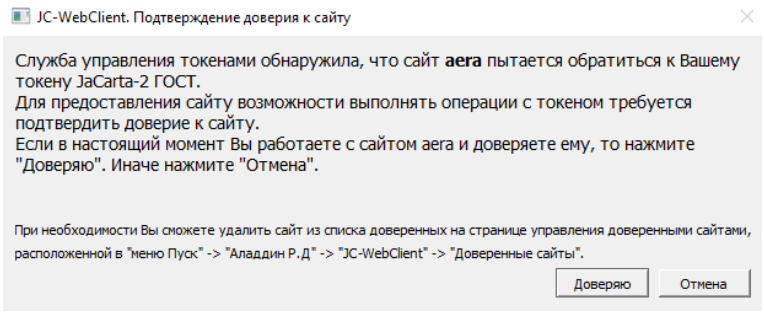


Рисунок 32 – Подтверждение доверия к Центру регистрации Aladdin eRA

- В открывшемся окне «Создание заявки на сертификат» (шаг 2 сценария) (см. Рисунок 33) укажите атрибуты получателя сертификатов (субъекта РС):

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

– При необходимости выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений (см. Рисунок 33).

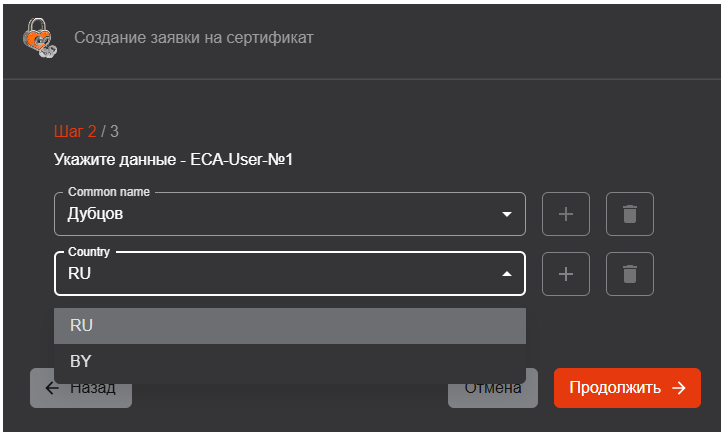


Рисунок 33 – Редактирование атрибутов получателя сертификатов (субъекта РС)

– При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку + и выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений) (см. Рисунок 34).

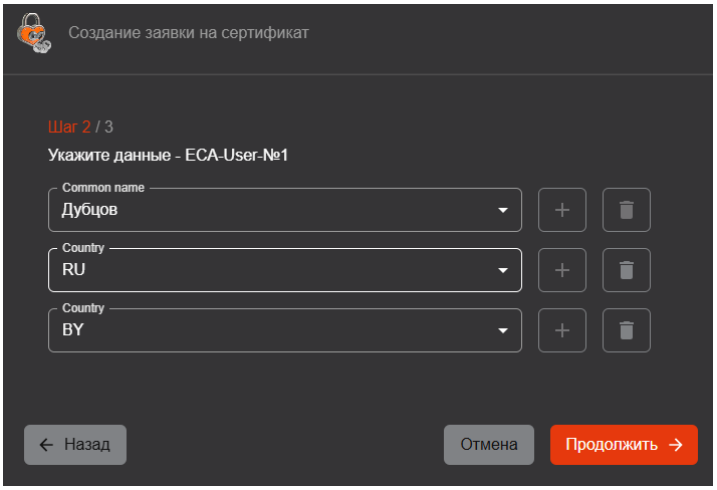


Рисунок 34 – Добавлен новый атрибут

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

В случае отсутствия у получателя сертификатов (субъекта РС) обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке (см. Рисунок 25). При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

Если у получателя сертификатов (субъекта РС) отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить (см. Рисунок 26).

- После редактирования атрибутов пользователя (субъекта) нажмите кнопку Продолжить →.

- В открывшемся окне «Создание заявки на сертификат» (шаг 3 сценария) (см. Рисунок 35):
  - В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
  - В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
  - Нажмите кнопку Создать заявку →.

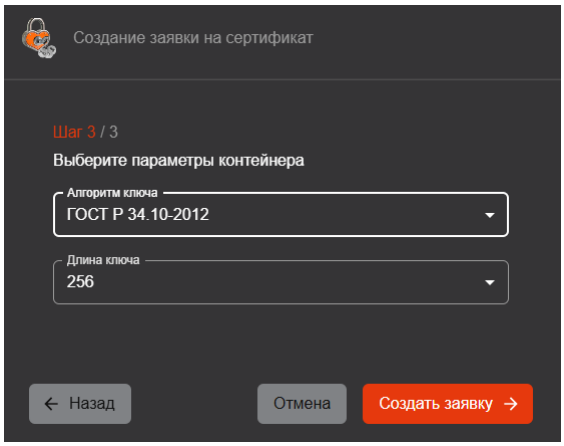


Рисунок 35 – Выбор алгоритма выработки ключевой пары и длины ключа

- В открывшемся окне «Создание заявки на сертификат» (процесс формирования заявки и его результат) (см. Рисунок 36) отображаются процессы:
  - Генерации ключевой пары.
  - Генерации запроса.
  - Создания заявки.

  Успешное завершения каждого процесса помечается значком .

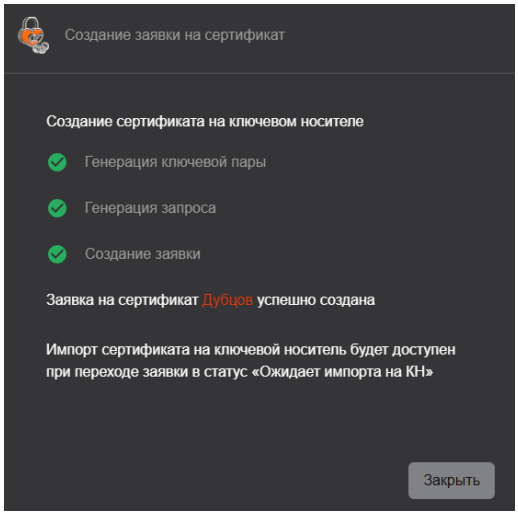


Рисунок 36 – Заявка на выпуск сертификата на ключевом носителе заведена успешно

В случае возникновения ошибок при формировании заявки процесс помечается значком .

Некоторые типы ключевых носителей поддерживают определенный набор алгоритмов выработки ключевых пар (например, в приведенном ниже примере при создании заявки на выпуск сертификата на электронном ключе JaCarta-2 ГОСТ был выбран неподдерживаемый алгоритм RSA) (см. Рисунок 37).

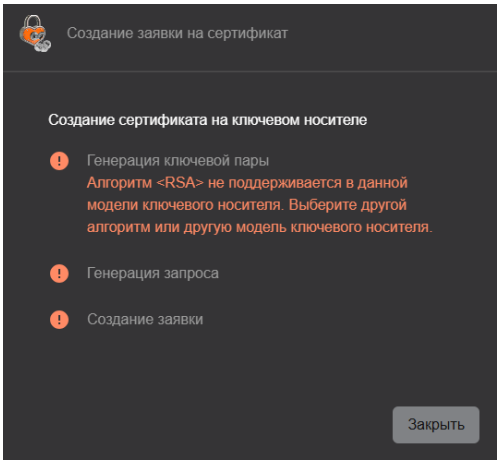


Рисунок 37 – Выбранный алгоритм не поддерживается в используемом ключевом носителе

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

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

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

4.5 Отмена заявки

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

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

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

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Инициируйте процесс отмены заявки одним из следующих способов:
  - Найдите заявку, которую необходимо отменить, в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Отмена заявки>** (см. Рисунок 38).

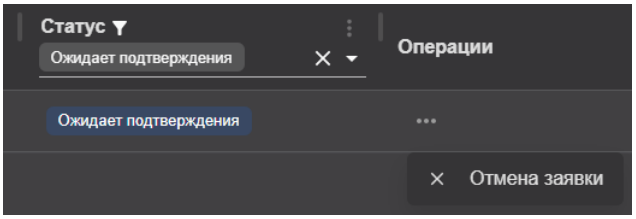


Рисунок 38 – Инициализация процесса отмены заявки на выпуск сертификата в спсике

– Откройте карточку заявки, которую необходимо отменить (см. раздел 4.3), на панели инструментов карточки заявки щелкните значок и выберите в открывшемся списке **<Отмена заявки>** (см. Рисунок 39).

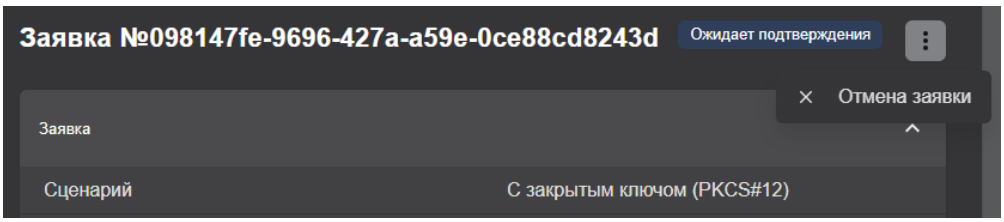


Рисунок 39 – Инициализация процесса отмены заявки на выпуск сертификата из ее карточки

- В открывшемся окне в поле «Комментарий» укажите причину отмены заявки и нажмите кнопку Отменить (см. Рисунок 40).

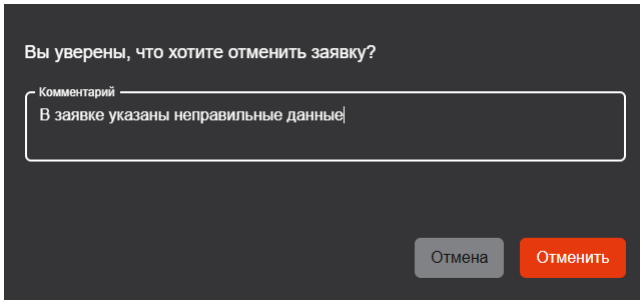


Рисунок 40 – Указание причин перед отменой заявки на выпуск сертификата

После отмены заявки указанный комментарий будет доступен для просмотра в карточке заявки (см. раздел 4.3) в атрибуте «Комментарий» блока «Заявка» (см. Рисунок 41).

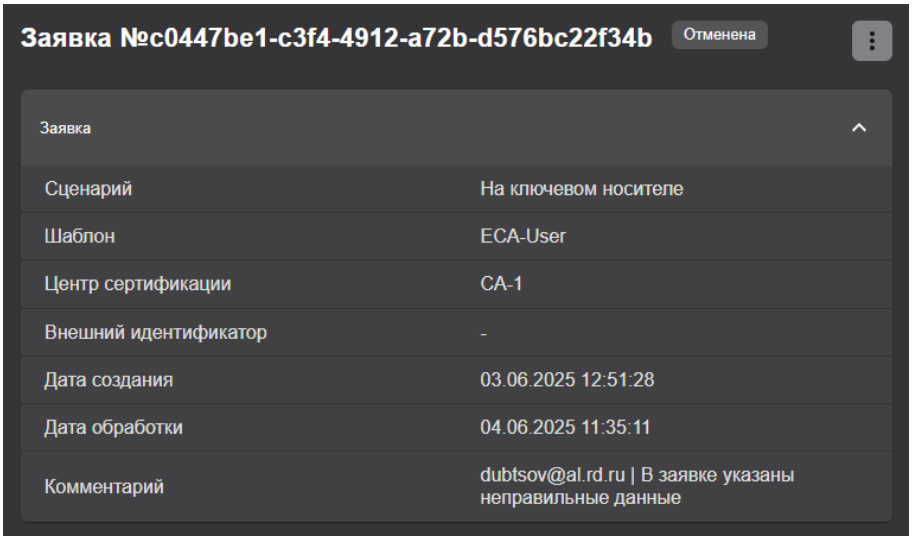


Рисунок 41 – Комментарий занесен в карточку отменной заявки

5 УПРАВЛЕНИЕ ВЫПУЩЕННЫМИ ПО ЗАЯВКАМ СЕРТИФИКАТАМИ

5.1 Общие сведения о работе с сертификатами

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

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

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

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

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

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

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

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

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

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

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

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

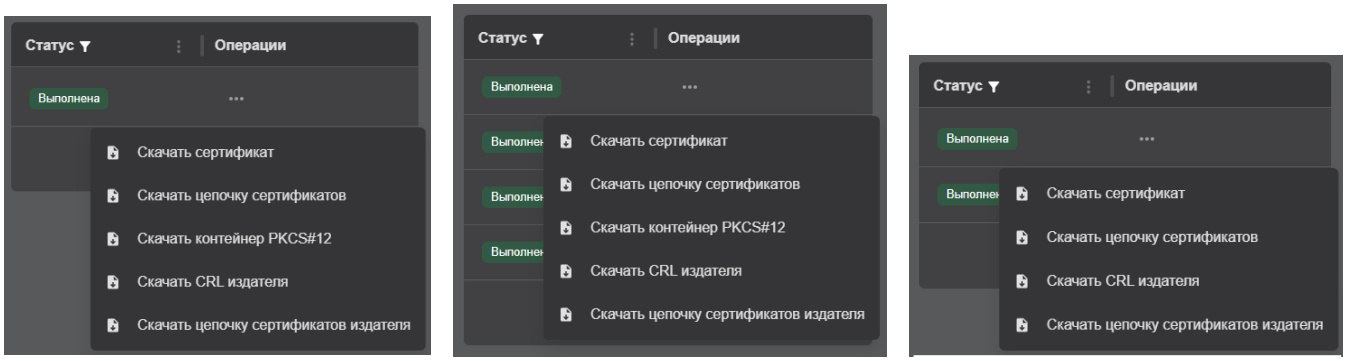
5.2 Выгрузка сертификата

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

Порядок выгрузки сертификата получателя сертификатов (субъекта РС):

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

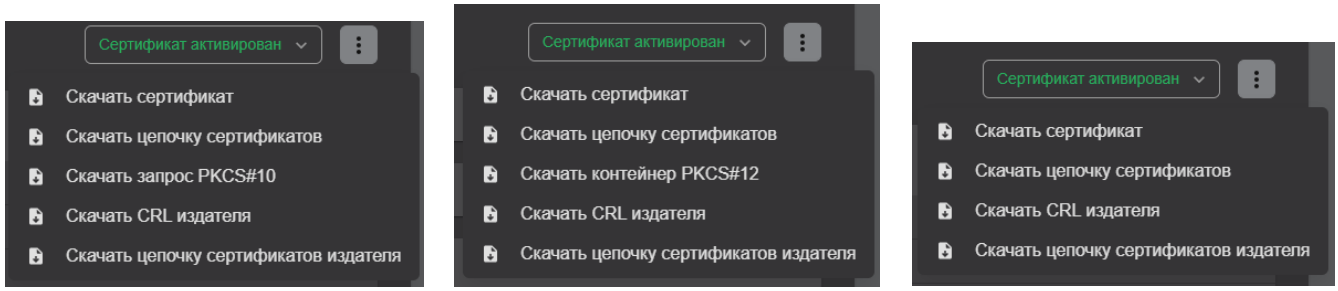
– Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать сертификат>** (см. Рисунок 42).



а) Заявка на основании запроса PKCS#10 **б) Заявка с закрытым ключом PRCS#12** **в) Заявка на ключевом носителе**[22]

Рисунок 42 – Выгрузка сертификата, выпущенного по заявкам с разными сценариями создания

– Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать сертификат>** (см. Рисунок 43).



а) Заявка на основании запроса PKCS#10 **б) Заявка с закрытым ключом PRCS#12** **в) Заявка на ключевом носителе**[23]

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

5.3 Выгрузка цепочки сертификатов

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

Порядок выгрузки цепочки сертификата получателя сертификатов (субъекта РС):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать цепочку сертификатов>** (см. Рисунок 42).
  - Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать цепочку сертификатов>** (см. Рисунок 43).

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

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

5.4 Выгрузка контейнера PCKS#12

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

Порядок выгрузки контейнера PCKS#12:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать контейнер PCKS#12>** (см. Рисунок 42).
  - Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать контейнер PCKS#12>** (см. Рисунок 43).

5.5 Выгрузка списка отозванных сертификатов (CRL)

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

Порядок выгрузки списка отозванных сертификатов (CRL):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать CRL издателя>** (см. Рисунок 42).
  - Откройте карточку заявки (см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать CRL издателя>** (см. Рисунок 43).

5.6 Выгрузка цепочки сертификатов издателя

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

Порядок выгрузки цепочки сертификатов издателя:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать цепочку сертификатов издателя>** (см. Рисунок 42).
  - Откройте карточку заявки см. раздел 4.3), на панели инструментов щелкните значок и выберите в открывшемся списке **< Скачать цепочку сертификатов издателя>** (см. Рисунок 43).

5.7 Отзыв сертификата

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

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

Порядок отзыва сертификата:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Откройте карточку заявки, по которой был выпущен сертификат, требующий отзыва (см. раздел 4.3).
- На панели инструментов карточки заявки нажмите кнопку Сертификат активирован и выберите в открывшемся списке **<Сертификат отозван>** (см. Рисунок 44).

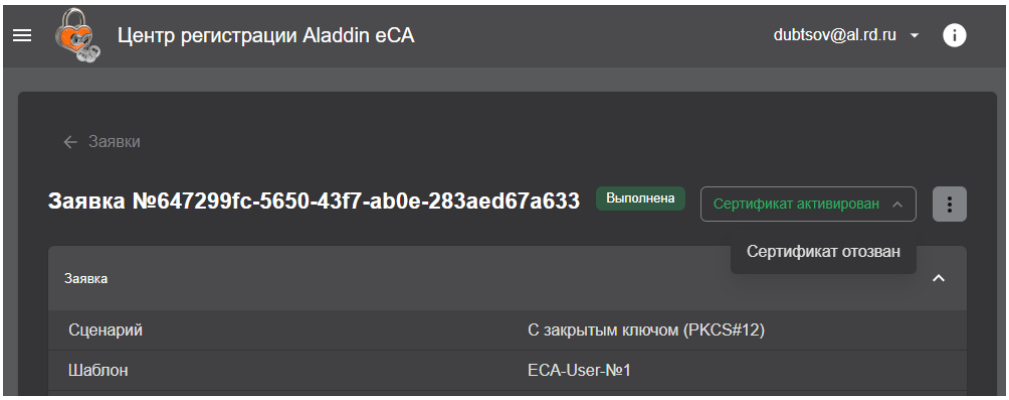


Рисунок 44 – Отзыв сертификата

- В открывшемся окне выберите в списке «Причина» причину отзыва сертификата, оставьте обязательный комментарий в поле «Комментарий» и нажмите кнопку Отозвать (см. Рисунок 45);

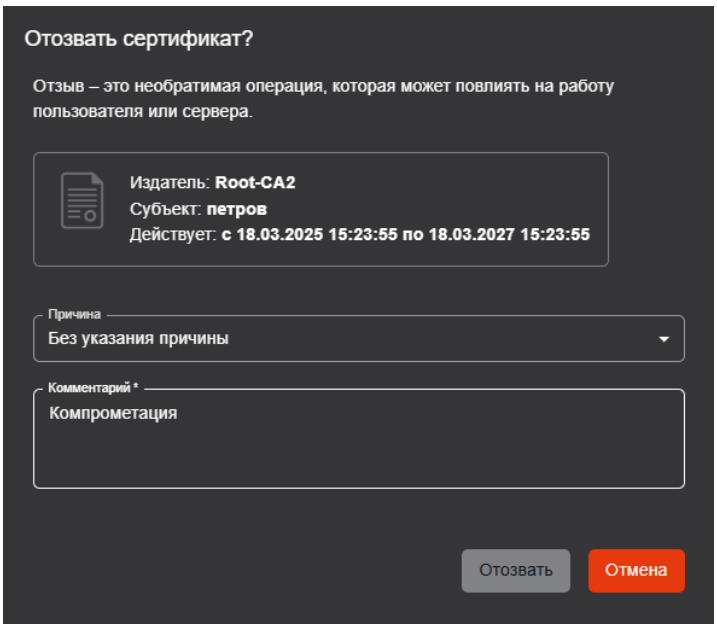


Рисунок 45 – Указание причины отзыва сертификата

В результате сертификат будет отозван (см. Рисунок 46).

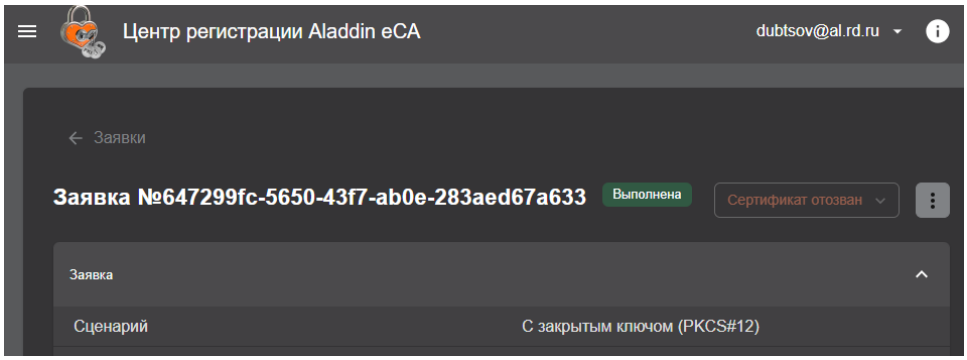


Рисунок 46 – Сертификат отозван

5.8 Импорт сертификата на ключевой носитель

Предварительные условия для импорта сертификата на ключевой носитель:

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

Порядок импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Инициируйте процесс отмены заявки одним из следующих способов:
  - Найдите заявку в списке (см. раздел 4.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Импортировать на КН>** (см. Рисунок 47).

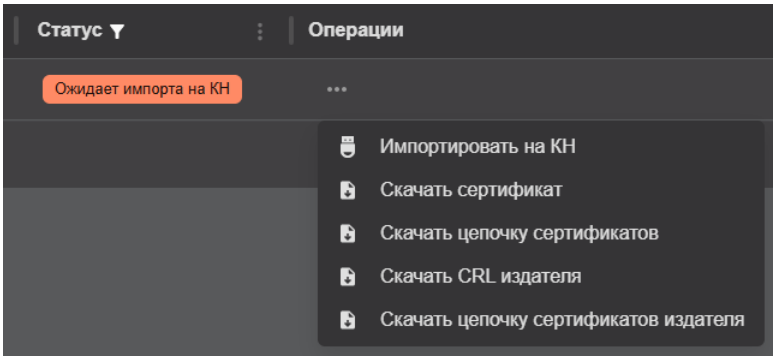


Рисунок 47 – Инициализация процесса импорта сертификата на ключевой носитель из списка

Если приложение JC-WebClient не установлено (см. Рисунок 29) или к компьютеру не подключен ключевой носитель (см. Рисунок 30), создать заявку на ключевом носителе невозможно.

  - Откройте карточку заявки, на панели инструментов карточки заявки щелкните значок и выберите в открывшемся списке **<Импортировать на КН>** (см. Рисунок 48).
- В открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 49):
  - В списке «Устройство» выберите подключенный ключевой носитель.
  - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
  - Нажмите кнопку Импортировать.

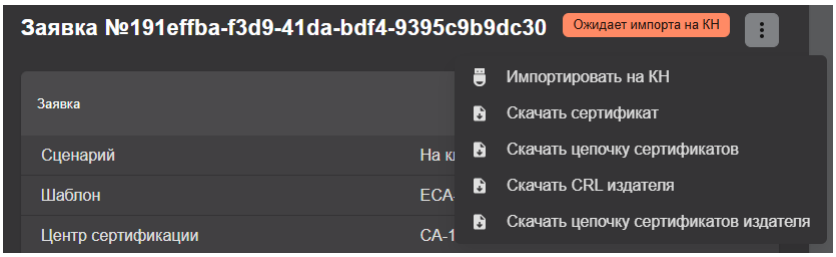


Рисунок 48 – Инициализация процесса импорта сертификата на ключевой носитель из карточки заявки

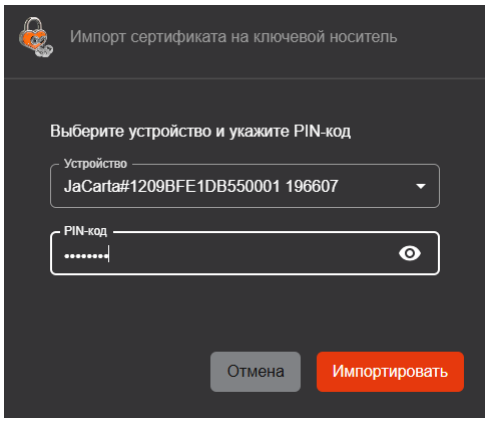


Рисунок 49 – Импорт сертификата на ключевой носитель

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

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

- В случае успешного импорта сертификата на ключевой носитель в открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 50) проверьте данные сертификата и нажмите кнопку Закрыть.

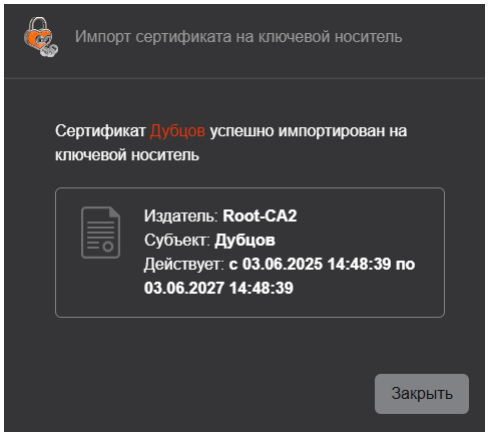


Рисунок 50 – Импорт сертификата на ключевой носитель успешно выполнен

6 ПОДДЕРЖКА ПРОТОКОЛОВ MS-XCEP И MS-WSTEP

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

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

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

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

Предварительные условия:

Корневой сертификат издающего Центра сертификации eCA, к которому подключена ресурсная система получателя сертификатов, должен быть установлен в хранилище «Доверенные корневые центры сертификации» (сертификат должен быть предоставлен пользователем с ролью «Администратор» Цента сертификации Aladdin eCA).

6.1 Обработка запроса на политики «GetPolices»

Центр регистрации Aladdin eRA при получении запроса «GetPolices» в случае успешной аутентификации получателя сертификат (субъекта РС), от имени которого был выполнен запрос, возвращает в ответе «GetPoliciesResponse» политику выпуска сертификатов.

Общие параметры возвращаемой политики соответствуют таблице ниже (Таблица 3).

Таблица 3 – Общие параметры возвращаемой политики

Параметр политики	Значение	Примечание
policyID	5817949c-a7cd-46ec-90ef-7782cd200b15	Уникальный идентификатор политики
policyFriendlyName	eCA enrollment policy	Отображаемое имя политики
nextUpdateHours	8	Время в часах, через которое клиент должен запросить обновление политики выпуска сертификатов с CEP-сервера. Значение «8» указано аналогично значению по умолчанию в Microsoft Certificate Service (MS CS).
policiesNotChanged	NULL	Параметр, используемый для указания факта изменения политики с момента последнего запроса клиентом. Значение «NULL» указано аналогично значению по умолчанию в MS CS.

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

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

Шаблоны, записываемые в поле «policies» ответа «GetPoliciesResponse», представляют собой шаблоны подключенного Центра сертификации Aladdin eCA, преобразованные в шаблоны по протоколу MS-XCEP (далее – шаблоны CEP).

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

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

В атрибуты возвращаемых шаблонов CEP записываются значения в соответствии с таблицей ниже (Таблица 4):

Таблица 4 – Значения атрибутов шаблонов в сообщении «GetPoliciesResponse»

Атрибут шаблона в сообщении «GetPoliciesResponse»	**Примечание**
commonName	Имя шаблона Центра сертификации Aladdin eCA
policySchema	3
validityPeriodSeconds	Период действия сертификата по шаблону Центра сертификации Aladdin eCA в секундах
renewalPeriodSeconds	10 % от периода действия сертификата по шаблону в секундах
enroll	true
autoEnroll	true[26]
minimalKeyLength	Минимальная длина ключа для алгоритма RSA по шаблону Центра сертификации Aladdin eCA
keySpec	1
keyUsageProperty	NULL
permissions	NULL
algorithmOIDReference	NULL
provider	Microsoft Base Cryptographic Provider v1.0
majorRevision	1
minorRevision	0
supersededPolicies	NULL
privateKeyFlags	0
subjectNameFlags	2181038080[27]
enrollmentFlags	0

[26] Указанное значение обозначает, что шаблон может использоваться при автоматическом выпуске сертификатов.

[27] Указанное значение обозначает, что от пользователя при создании запроса на сертификат не должно требоваться указание значений для SDN и SAN.

generalFlags	0 – для типа субъекта шаблона «Пользователь», 64 – для типа субъекта шаблона «Устройство», 128 - для типа субъекта шаблона «Корневой ЦС», 2048 – для типа субъекта шаблона «Подчиненный ЦС»
hashAlgorithmOIDReference	NULL
rARequirements	NULL
keyArchivalAttributes	NULL
extensions	Строка вида «Имя_шаблона@ID_шаблона»[28]

Параметры издателя сертификатов в возвращаемой политике (блок «cAs») соответствуют таблице ниже (Таблица 5).

Таблица 5 – Параметры издателя сертификатов в возвращаемой политике

Параметр издателя	Записываемое значение	Примечание
clientAuthentication	2	Данное значение указывается, если пользователь аутентифицируется на CEP-сервере по Kerberos-билету.
	4	Данное значение указывается, если пользователь аутентифицируется на CEP-сервере по имени пользователя и паролю
uri	Адрес CES-сервера	URI CES-сервера. На данный адрес будут направляться запросы пользователя на выпуск сертификата (запрос «RequestSecurityToken» по протоколу MS-WSTEP). Адреса CEP- и CES-серверов, реализуемых Центром регистрации Aladdin eRA, совпадают.
priority	1	Приоритет издателя. Прочие значения не применимы для политики, формируемой Центром регистрации Aladdin eRA.
renewalOnly	False	Значение указывает, что издатель может обрабатывать не только запросы на продление существующих сертификатов, но и запросы на выпуск новых сертификатов.
certificate	Сертификат активного центра сертификации Центра сертификации Aladdin eCA	Сертификат в Base64.
enrollPermission	True	Значение указывает, что пользователь может выполнять запросы к данному издателю.

6.2 Обработка запроса на выпуск сертификата «RequestSecurityToken»

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

- Создаёт от имени получателя сертификатов (субъекта РС) новую заявку на сертификат на основании запроса из поля «BinarySecurityToken» по шаблону, указанному в данном запросе на сертификат.

[28] Данное значение будет записываться в расширения создаваемого на клиенте запроса на сертификат и будет использоваться в рамках реализации функций CES-севера.

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

- В случае успешного выпуска сертификата по созданной заявке Центр регистрации Aladdin eRA генерирует и отправляет пользователю ответное сообщение «RequestSecurityTokenResponse», записывая в поле «RequestedSecurityToken» выпущенный по заявке сертификат, а также цепочку данного сертификата в поле «BinarySecurityToken».

  Если после создания заявки сертификат по ней не был успешно выпушен, Центр регистрации Aladdin eCA возвращает сообщение об ошибке с кодом «RequestFailed».

6.3 Создания политики регистрации сертификатов

Порядок создания политики регистрации сертификатов в ОС Windows:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог **Сертификаты – текущий пользователь > Личное > Сертификаты**.
- Вызовите контекстное меню и выберите **Все задачи > Дополнительные операции > Управление политиками регистрации сертификатов** (см. Рисунок 51).

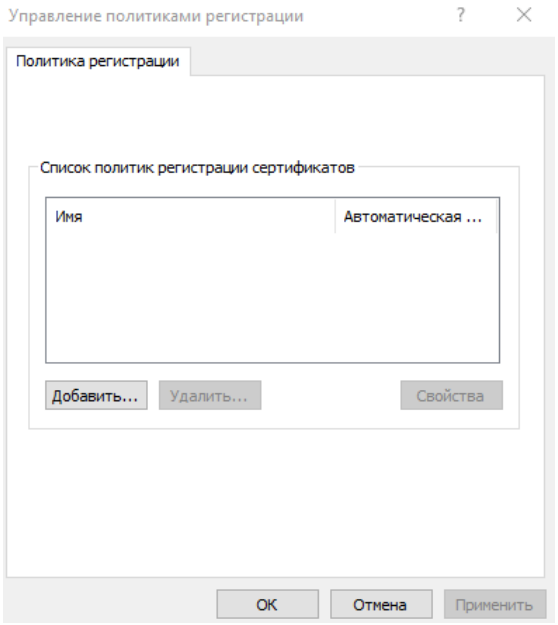


Рисунок 51 – Управление политиками регистрации сертификатов

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

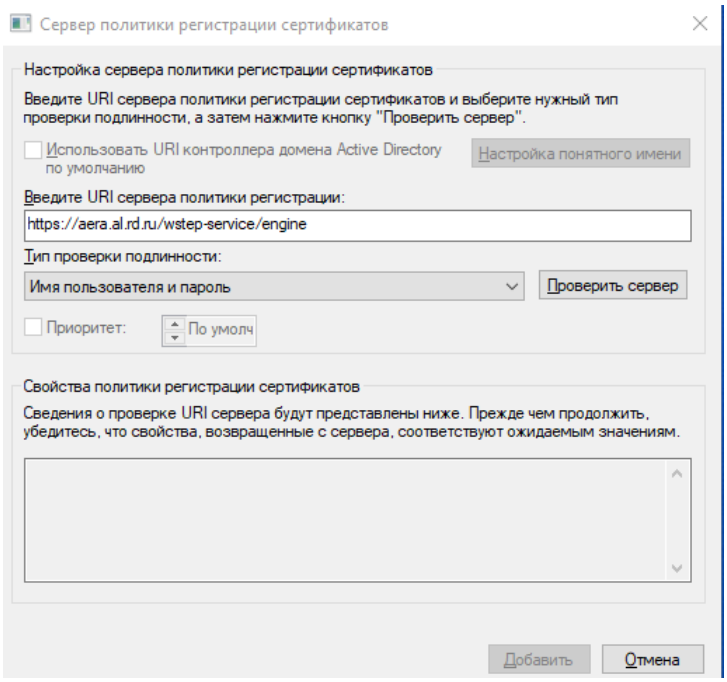


Рисунок 52 – Управление политиками регистрации сертификатов

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

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

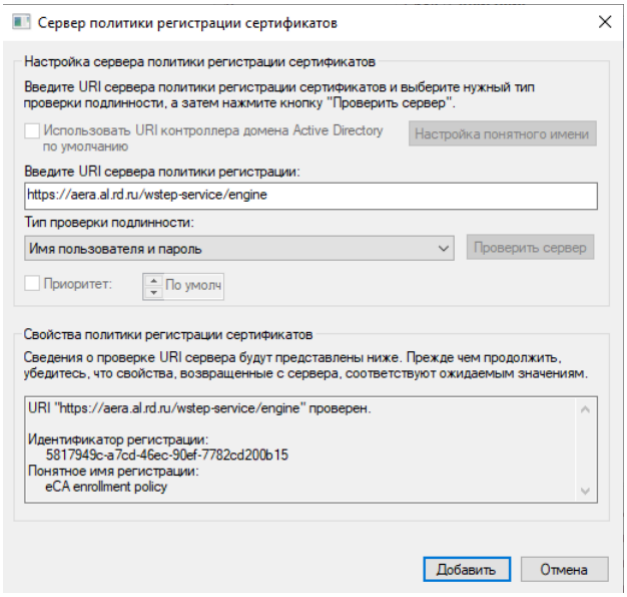


Рисунок 53 – Проверка сервера выполнена успешно

  - В случае успешной проверки сервера нажмите кнопку **<Добавить>**.
- В окне «Управление политикам и регистрации» нажмите кнопку **<Применить>**, а затем **<OK>**.

6.4 Запрос нового сертификата

Порядок запроса сертификата:

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

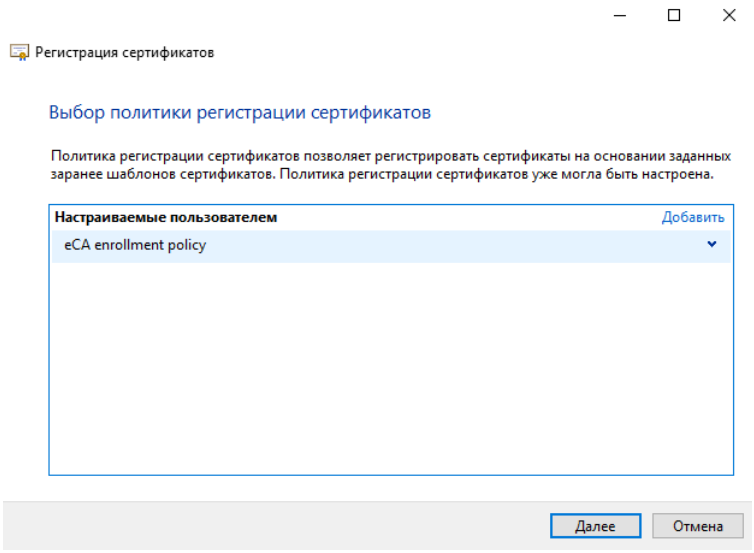


Рисунок 54 – Выбор политики регистрации сертификатов

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

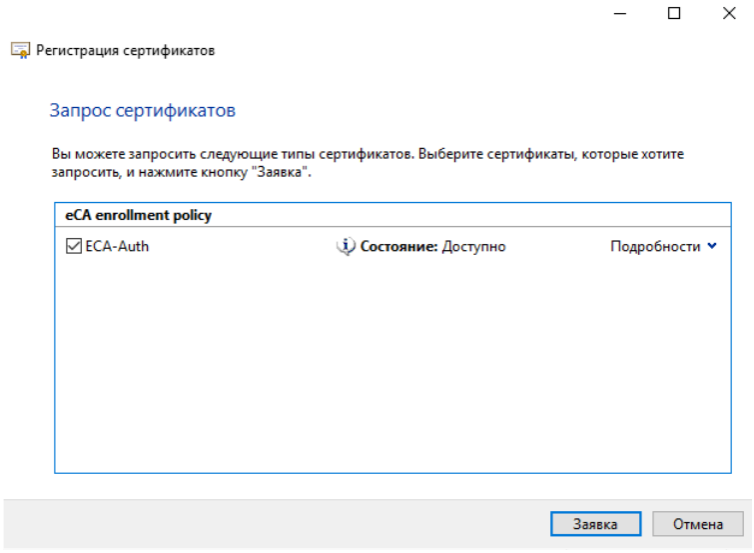


Рисунок 55 – Выбор шаблона для выпуска сертификата

- На 3 шаге мастера регистрации сертификатов выберите шаблоны, по которым необходимо выпустить сертификаты, и нажмите кнопку **<Заявка>**.
- На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 56).

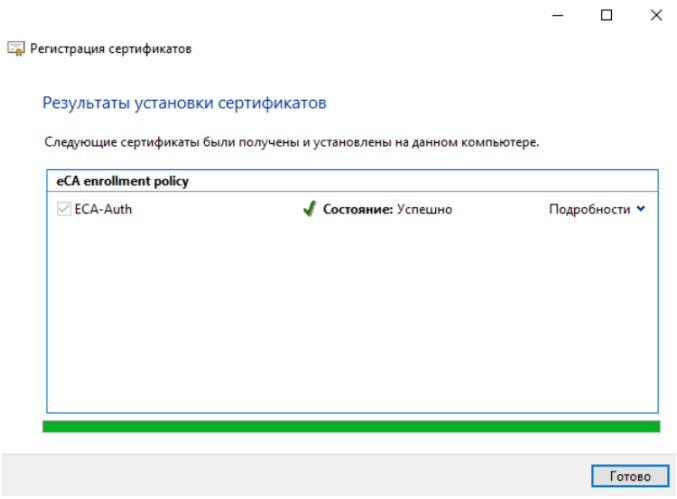


Рисунок 56 – Сертификат получен и успешно установлен в хранилище

6.5 Перевыпуск сертификатов

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

Порядок перевыпуска сертификата:

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

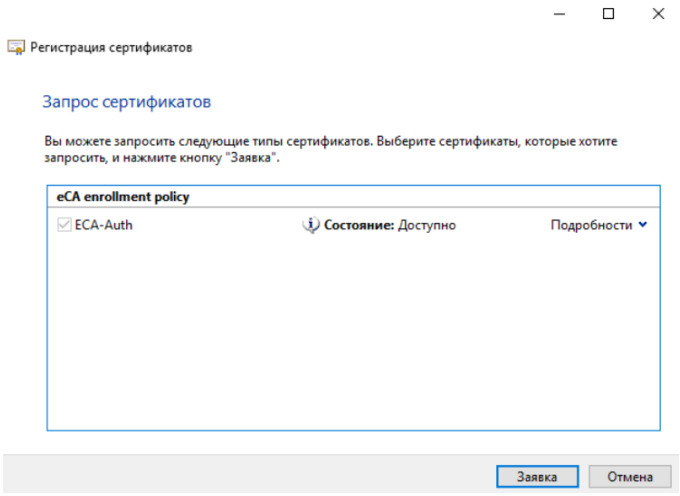


Рисунок 57 – Отправка заявки для выпуска сертификата

- На 2 шаге мастера регистрации сертификатов нажмите кнопку **<Заявка>**.
- На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 56).

ПРИЛОЖЕНИЕ 1. ОПИСАНИЕ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] ECA-Auth	8ecba810-7f48-4c4e-b803-99a97146e2ba	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р34.10-2012	Выключен										
[Deprecated] ECA-User	2d58b30c-3965-4555-9af4-fec4552af21e	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиент - Защита электронной почты	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
[Deprecated] ECA-WEB-Server	25bbd733-4d8c-43ce-ba5a-e9826eb7b16c	2y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей	+	- Аутентификация сервера	-	Common name	+	+	DNS name	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
[Deprecated] Domain Controller	bf2dac0a-f05f-49dd-95b4-e50691489b6a	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности	+	- Аутентификация клиента - Центр распространения ключей Kerberos	-	Common name[29]	+	+	DNS name[30]	+	+
					ECDSA	256								MS GUID[31]	+	+
					ГОСТ Р 34.10-2012	Выключен										

[29] Имя контроллера домена.

[30] FQDN – полное доменное имя вашего сервера.

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

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
							- Шифрование ключей		- SSH сервер							
[Deprecated] Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name[32]	+	+	MS UPN[33]	+	+
					ECDSA	256								RFC 822 Name[34]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name[35]	+	+	MS UPN[36]	+	+
					ECDSA	256								RFC 822 Name[37]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей	+	Аутентификация сервера	-	Common name[38]	+	+	DNS name[39]	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	-	-	RSA	1024	- Цифровая подпись	+	- Аутентификация клиента	-	Common name[40]	+	+	RFC 822 Name[41]	+	+
					ECDSA	256										

[32] Имя пользователя.

[33] Имя входа пользователя в формате e-mail адреса.

[34] Почтовый адрес пользователя, может совпадать с MS UPN.

[35] Имя веб-клиента.

[36] Имя входа пользователя в формате e-mail адреса.

[37] Почтовый адрес пользователя, может совпадать с MS UPN.

[38] Имя веб-сервера.

[39] FQDN – полное доменное имя вашего сервера.

[40] Имя пользователя.

[41] почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
					ГОСТ Р 34.10-2012	Выключен	- Подтверждение подлинности - Шифрование ключей - Шифрование данных		- Защита электронной почты - Вход с MS смарт-картой							
[Deprecated] ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffea	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name[42]	+	+	MS UPN[43]	+	+
					ECDSA	256					Organization[44]	-	+	Kerberos KPN[45]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] ALD PRO Smartcard Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name[46]	+	+	MS UPN[47]	+	+
					ECDSA	256					Organization[48]	-	+	RFC 822 Name[49]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab	2y	-	-	RSA	1024	Цифровая подпись	+	OCSP подписант	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										

[42] Имя контроллера домена ALD PRO.

[43] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[44] Организация.

[45] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[46] Имя пользователя ALD PRO.

[47] Имя входа пользователя в формате e-mail адреса.

[48] Организация.

[49] Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb	7d24y	-	-	RSA	1024	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
					ECDSA	256					Unique Identifier (UID)	-	+	DNS name	-	+
					ГОСТ Р 34.10-2012	256					Given name	-	+	MS UPN	-	+
											Initials	-	+	MS GUID	-	+
											Surname	-	+	IP address	-	+
											Organizational unit	-	+	Directory Name	-	+
											Locality	-	+	Uniform resource identifier	-	+
											State or province	-	+	Registered Identifier (OID)	-	+
											Domain component	-	+	Permanent identifier	-	+
											Country	-	+	Xmpp address	-	+
											Postal code	-	+	Service Name	-	+
											Business category	-	+	Subject Identification Method	-	+
											Telephone number	-	+	Kerberos KPN	-	+
											Pseudonym	-	+			
											Postal address	-	+			
											Street	-	+			
											Name	-	+			
											Title	-	+			
											Domain qualifier	-	+			
											Description	-	+			
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			

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

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			
											ИНН	-	+			
											ОГРН	-	+			
											ОГРНИП	-	+			
											СНИЛС	-	+			
											ИНН ЮЛ	-	+			
[Deprecated] SCEP Management	3e5df3d4-683c-4252-b862-467589c2225b	25y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей - Шифрование данных	+	-	-	Common name	+	-	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
User	f215f72f-9a9a-45c8-83e8-25879d52dcf6	1y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиент - Защита электронной почты	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
Domain Controller	eca2ad3d-944e-48ce-ba7b-114f16ad8fd4	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности	+	- Аутентификация клиента - Центр распространения ключей Kerberos	-	Common name[50]	+	+	DNS name[51]	+	+
					ECDSA	256								MS GUID[52]	+	+
					ГОСТ Р 34.10-2012	256										

[50] Имя контроллера домена.

[51] FQDN –полное доменное имя вашего сервера.

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

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
							- Шифрование ключей		- SSH сервер							
Smartcard Logon	682225f6-f189-412f-a456-c480d42efaa8	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name[53]	+	+	MS UPN[54]	+	+
					ECDSA	256								RFC 822 Name[55]	+	+
					ГОСТ Р 34.10-2012	256										
WEB-Client	18ecaacc-43d6-4aaa-afcc-1bc8e547e6f5	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name[56]	+	+	MS UPN[57]	+	+
					ECDSA	256								RFC 822 Name[58]	+	+
					ГОСТ Р 34.10-2012	256										
WEB-Server	61c901fa-c823-4899-87a0-df4035291fa0	1y	-	-	RSA	2048	- Цифровая подпись - Шифрование ключей	+	Аутентификация сервера	-	Common name[59]	+	+	DNS name[60]	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
S/MIME	0a7c4a9f-b260-46c5-94c5-58de5e977678	1y	-	-	RSA	2048	- Цифровая подпись	+	- Аутентификация клиента	-	Common name[61]	+	+	RFC 822 Name[62]	+	+
					ECDSA	256										

[53] Имя пользователя.

[54] Имя входа пользователя в формате e-mail адреса.

[55] Почтовый адрес пользователя, может совпадать с MS UPN.

[56] Имя веб-клиента.

[57] Имя входа пользователя в формате e-mail адреса.

[58] Почтовый адрес пользователя, может совпадать с MS UPN.

[59] Имя веб-сервера.

[60] FQDN – полное доменное имя вашего сервера.

[61] Имя пользователя.

[62] почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
					ГОСТ Р 34.10-2012	256	- Подтверждение подлинности - Шифрование ключей - Шифрование данных		- Защита электронной почты - Вход с MS смарт-картой							
ALD PRO Domain Controller	83afddde-5729-4562-a7ed-260f1c0f73d7	1y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name[63]	+	+	MS UPN[64]	+	+
					ECDSA	256					Organization[65]	-	+	Kerberos KPN[66]	+	+
					ГОСТ Р 34.10-2012	Выключен										
ALD PRO Smartcard Logon	85e99e47-479f-407e-98f8-ad13d51435a7	1y	-	-	RSA	2048	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name[67]	+	+	MS UPN[68]	+	+
					ECDSA	256					Organization[69]	-	+	RFC 822 Name[70]	+	+
					ГОСТ Р 34.10-2012	256										
OCSP Signer	eeb625cb-861e-458c-94ae-79b2e05090e5	1y	-	-	RSA	2048	Цифровая подпись	+	OCSP подписант	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										

[63] Имя контроллера домена ALD PRO.

[64] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[65] Организация.

[66] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[67] Имя пользователя ALD PRO.

[68] Имя входа пользователя в формате e-mail адреса.

[69] Организация.

[70] Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
Root CA	a1eb9d3a-b9b5-4e6d-8f2d-587ca9cc6554	15y	-	-	RSA	4096	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
					ECDSA	384					Unique Identifier (UID)	-	+	DNS name	-	+
					ГОСТ Р 34.10-2012	512					Given name	-	+	MS UPN	-	+
											Initials	-	+	MS GUID	-	+
											Surname	-	+	IP address	-	+
											Organizational unit	-	+	Directory Name	-	+
											Locality	-	+	Uniform resource identifier	-	+
											State or province	-	+	Registered Identifier (OID)	-	+
											Domain component	-	+	Permanent identifier	-	+
											Country	-	+	Xmpp address	-	+
											Postal code	-	+	Service Name	-	+
											Business category	-	+	Subject Identification Method	-	+
											Telephone number	-	+	Kerberos KPN	-	+
											Pseudonym	-	+			
											Postal address	-	+			
											Street	-	+			
											Name	-	+			
											Title	-	+			
											Domain qualifier	-	+			
											Description	-	+			
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											ИНН	-	+			
											ОГРН	-	+			
											ОГРНИП	-	+			
											СНИЛС	-	+			
											ИНН ЮЛ	-	+			
Sub CA	4f56589e-7e80-4fbe-b49f-662c9ba9a335	7y	--	-	RSA	3072	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
											Unique Identifier (UID)	-	+	DNS name	-	+
					ECDSA	256					Given name	-	+	MS UPN	-	+
					ГОСТ Р 34.10-2012	256					Initials	-	+	MS GUID	-	+
											Surname	-	+	IP address	-	+
											Organizational unit	-	+	Directory Name	-	+
											Locality	-	+	Uniform resource identifier	-	+
											State or province	-	+	Registered Identifier (OID)	-	+
											Domain component	-	+	Permanent identifier	-	+
											Country	-	+	Xmpp address	-	+
											Postal code	-	+	Service Name	-	+
											Business category	-	+	Subject Identification Method	-	+
											Telephone number	-	+	Kerberos KPN	-	+
											Pseudonym	-	+			
											Postal address	-	+			
											Street	-	+			
											Name	-	+			
											Title	-	+			
											Domain qualifier	-	+			
											Description	-	+			

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Unstructured address	-	+			
											Unstructured name	-	+			
											Email Address (E)	-	+			
											Serial number	-	+			
											Organization	-	+			
											ИНН	-	+			
											ОГРН	-	+			
											ОГРНИП	-	+			
											СНИЛС	-	+			
											ИНН ЮЛ	-	+			
SCEP Management	77004b9d-e195-40a3-aee0-dca5ad403f49	25y	-	-	RSA	2048	- Цифровая подпись - Шифрование ключей - Шифрование данных	+	-	-	Common name	+	-	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

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

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

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

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

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

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

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

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

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

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводи-тельного документа и дата	Подпись	Дата
	изме-ненных	заменен-ных	новых	аннулиро-ванных					