АКЦИОНЕРНОЕ ОБЩЕСТВО

«Аладдин Р.Д.»

РАЗВЁРТЫВАНИЕ PKI
В ИНФОРМАЦИОННОЙ СИСТЕМЕ

На базе решений компании АО «Аладдин Р.Д.»

Листов 45

2023

АННОТАЦИЯ

Инфраструктура открытых ключей (далее – PKI) является технологией безопасности, которая основывается на стандарте цифровых сертификатов X.509. Целью PKI является повышение безопасности IT-инфраструктуры предприятия за счёт предоставления механизмов доверия к результатам идентификации и строгой аутентификации, к результатам проверки электронной подписи. В основе этого механизма – доверие к корневому сертификату, обусловленное доверием выдавшему его корневому центру сертификации, и двумя основными криптографическими механизмами:

- шифрование – защищает данные от несанкционированного доступа третьих лиц путём шифрования данных криптографическими ключами. Только пользователи, имеющие необходимые ключи, могут получить доступ к данным. Шифрование обеспечивает секретность данных, но не защищает от их подмены;
- цифровая подпись – защищает данные от несанкционированного изменения или подделки путём применения к данным специальных алгоритмов, которые образуют цифровую подпись. Любые манипуляции по изменению данных будут немедленно обнаружены при проверке цифровой подписи. Цифровая подпись обеспечивает аутентичность и идентификацию документа.

Путём комбинирования шифрования и цифровой подписи можно организовать обеспечение конфиденциальности и защиты данных от несанкционированных изменений.

Цифровые сертификаты представляют собой эффективное средство определения подлинности, которое можно применять при аутентификации пользователей в процессе регистрации, для обеспечения безопасного обмена информацией.

Центр сертификации Aladdin Enterprise CA – это средство обеспечения строгой аутентификации для корпоративных и государственных информационных систем на базе отечественных операционных систем семейства Linux, обеспечивающее автоматизированное управление сертификатами доступа внутренних и дистанционных пользователей, а также технических средств информационной системы (выдача, распространение, отзыв).

Центр сертификации Aladdin eCA обеспечивает функционирование инфраструктуры открытых ключей и интеграцию с доменной инфраструктурой, с системами управления жизненным циклом смарт-карт и токенов, системами управления пользователями (IdM/IAM, IGA) и кадровыми системами.

В данном руководстве описано развертывание инфраструктуры открытых ключей на базе отечественных операционных систем семейства Linux (RED OS 7.3, Astra Linux 1.7 Смоленск).

Настоящий документ представляет собой руководство по развертыванию инфраструктуры открытого ключа в среде Linux и предназначен для системных инженеров и администраторов, ответственных за проектирование и реализацию решений по безопасности.

СОДЕРЖАНИЕ

1. ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

1.1 Принятые сокращения

ОС	Операционная система.
ПК	Персональный компьютер
ПО	Программное обеспечение.
СУБД	Система управления базами данных.
ЦС	Центр сертификатов.
AeCA, Aladdin eCA	Центр сертификатов доступа Aladdin Enterprise Certificate Authority
AeCA VA	Aladdin Enterprise Certificate Authority Validation Authority

1.2 Определения

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

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

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

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

Центр сертификации – комплекс средств, задача которых заключается в обеспечении жизненного цикла сертификатов доступа пользователей и устройств информационной системы, а также в создании инфраструктуры для обеспечения процессов идентификации и строгой аутентификации в информационной системе. Центр сертификации является частью Центра сертификатов доступа.

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

CRL (Certificate Revocation List) – список отзыва сертификатов. Подписанный электронный документ, публикуемый ЦС и содержащий список отозванных сертификатов, действие которых прекращено по внешним причинам, RFC 3280.

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

SSL (Secure Sockets Layer) или TLS (Transport Layer Security) — технология, обеспечивающая безопасность передачи данных между клиентом и сервером поверх открытых сетей.

PKI (Public Key Infrastructure) — инфраструктура открытого ключа, набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей.

1.3 Принятые обозначения

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

Таблица 1 — Элементы оформления

[Поле]	Ссылка на список литературы (приведен в конце документа)
<Кнопка>	Используется для выделения наименований кнопок
Меню:	Используется для выделения наименований пунктов меню
Ctrl+X	Используется для выделения сочетаний клавиш
file.exe	Используется для выделения имен файлов, каталогов, текстов программ
Термин	Используется для выделения первого и последующих вхождений определяемого в документе термина в тексте документа
Выделение	Используется для выделения отдельных значимых слов и фраз в тексте
Гиперссылка	Используется для выделения внешних ссылок
Ссылка [стр. **Ошибка! Закладка не определена.**]	Используется для выделения перекрестных ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
Рамка	Используется для выделения важной информации, вывод, резюме

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Компоненты домена безопасности информационной системы

Одним из вариантов построения единого пространства доверия в информационной системе является построение иерархической модели доверия[1]. Во главе всей структуры стоит один центр сертификации (ЦС), которому доверяют все субъекты информационной системы: пользователи, сервера, устройства и т.д. По сути, он является корневым ЦС. ЦС выпускает сертификаты для подчиненных центров, которые образовывают многоуровневую иерархию. Как правило, в корпоративных информационных системах развертывается двухуровневая иерархия: корневой и издающий ЦС. Трехуровневая иерархия: корневой, промежуточный и издающий используется реже и в рамках данного документа не рассматривается.

Второй компонент, не относящийся непосредственно к инфраструктуре открытых ключей, это контроллер домена в сочетании со службой каталогов пользователей и технических средств. Контроллер домена осуществляет аутентификацию в информационной системе (например, при помощи протокола Kerberos), а на основании учетных записей в каталоге осуществляется распределение полномочий в информационной системе.

За последние десятилетия на рынке сложилась ситуация, при которой в качестве ЦС, контроллера домена и службы каталогов использовались соответствующие службы в составе Microsoft Server: Certificate Services, Key Distribution Center и Active Directory. В данном документе мы рассмотрим вариант организации инфраструктуры открытых ключей на базе отечественных решений и, в частности, решений компании АО «Аладдин Р.Д.».

В качестве контроллера домена и службы каталогов будет рассмотрен ALD PRO. В качестве центра сертификации – Aladdin Enterprise CA. Отдельно стоит отметить, что в рамках переходного периода миграции информационной системы на отечественные решения возможна интеграция Aladdin Enterprise CA со службой Microsoft AD и KDC, и возможно использование Microsoft CS в качестве корневого центра сертификации.

Третий компонент домена безопасности – Центр валидации. В составе Aladdin Enterprise CA есть такой компонент. Он предоставляет следующие службы: точку распространения списков отзыва сертификатов (CRL DP), точку распространения сертификатов промежуточных ЦС (AIA) и онлайн-службу предоставления статусов сертификатов (OCSP). При планировании инфраструктуры необходимо учитывать возможность развертывания и регистрации нескольких Центров валидации на одном Центре сертификации с целью обеспечения резервирования: если один из источников информации о статусе сертификата становится недоступным, то используется резервный, и отказоустойчивости: равномерного распределения нагрузки между серверами.

В рамках данного документа мы рассмотрим возможность развертывания инфраструктуры открытых ключей в гетерогенной среде, где клиентские подключения могут осуществляться с операционных систем разного типа - семейства Microsoft Windows и семейства Linux. Для обеспечения аутентификации и предоставления доступа к работе с ОС семейства Linux необходимо использовать ПО Aladdin SecurLogon, для ОС семейства Windows аутентификация и доступ к ОС производится штатными средствами, входящими в состав ОС. Для хранения закрытых ключей и сертификатов пользователей для аутентификации рекомендуем использовать USB-токены или смарт-карты из линейки JaCarta PKI, JaCarta PRO или JaCarta 2 PKI/PRO.

Пользователи, сервера, сервисы, рабочие места и устройства являются участниками (субъектами) инфраструктуры открытых ключей. Они владеют закрытым ключом и сертификатом открытого ключа, который издается в одном из центров сертификации информационной системы.

---

[1] другие модели (кросс-сертифицированная, сетевая и т.д.) в рамках данного документа не рассматриваются

Все технические средства должны иметь доступ к центру валидации для обеспечения работы PKI-компонентов.

2.2 Планирование инфраструктуры

Любая организация, определяя цели развертывания PKI, должна руководствоваться своей политикой безопасности, учитывать специфику ведения бизнеса или характер деятельности, юридические и административные ограничения. Не менее важен при принятии решения о развертывании PKI и учет потребностей безопасности, например, необходимость повысить уровень защищенности корпоративной системы, связанной с Интернетом, или следовать требованиям безопасности, установленными государственными органами. Кроме того, условия импортозамещения программного обеспечения вынуждают многие компании использовать новые отечественные технологии и open source в условиях цифровой трансформации в соответствии с государственными задачами, чтобы соответствовать ожиданиям клиентов в отношении безопасности используемой ими системы. Выбирая ПО для импортозамещения, важно проверить его включение в российский реестр программного обеспечения, которое подтверждает, что оно действительно разработано и внедрено в России. Именно поэтому реализовать стратегию импортозамещения следует поручить надёжным партнёрам, каким и является АО «Аладдин Р.Д.».

В данном документе рассмотрено развёртывание инфраструктуры PKI с помощью «Центра сертификатов доступа Aladdin Enterprise Certificate Authority», включённого в реестр программного обеспечения, о чём свидетельствует запись в реестре №14433 https://reestr.digital.gov.ru/reestr/901298/.

Развёртывание инфраструктуры PKI на базе «Центра сертификатов доступа Aladdin Enterprise Certificate Authority» возможно в уже существующем домене под управлением MS AD, ALD PRO, Samba DC, FreeIPA или после развертывания новой доменной структуры.

Поскольку сценарии использования ПО «Центра сертификатов доступа Aladdin Enterprise Certificate Authority» продолжают расширяться и усложняться, проиллюстрируем наиболее распространённые (см. Рисунок 1).

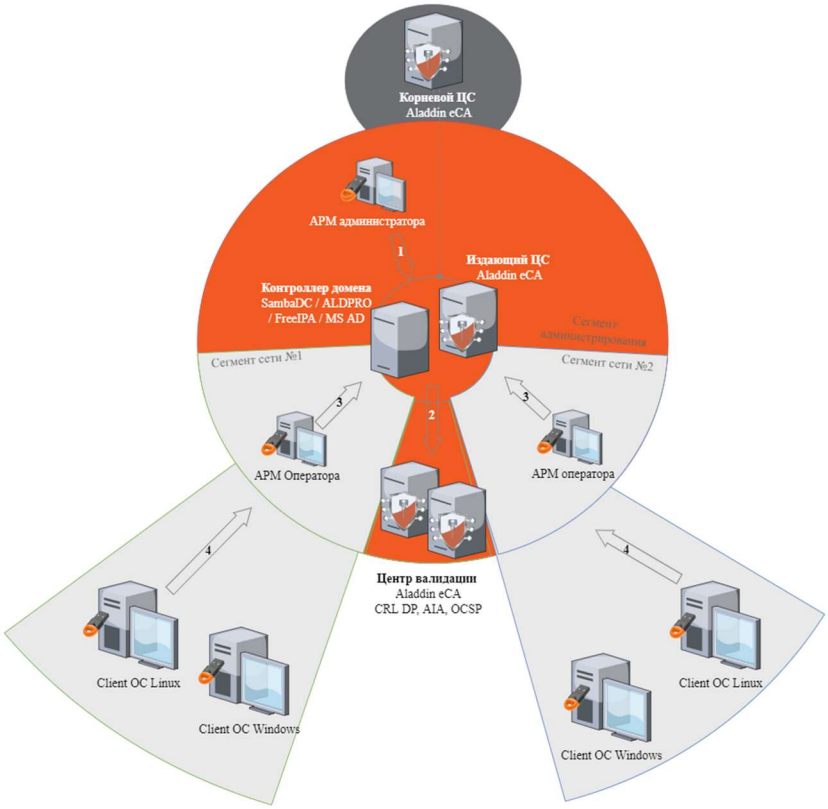


Рисунок 1 – Развёртывание инфраструктуры PKI на базе ПО АЕСА

В данной инфраструктуре возможно выполнение следующих сценариев:

1. Администрирование доменов. Инфраструктура открытого ключа позволяет распределить права на централизованное создание, распространение и аннулирование ключей для выбранных групп безопасности или членов этих групп – доменных пользователей и субъектов, между назначенными операторами. Оператор принимает решение о выдаче сертификатов, об отказе в его выдаче или о переводе сертификата в статус «Приостановлен» или «Отозван». Реализуются правила политики, в соответствии с выставленными администратором установками, путём выдачи сертификатов, предназначенных для Web-аутентификации операторов, и запуска «Центра сертификации» с ограниченным интерфейсом и в соответствии с назначенными политиками.
2. Публикация данных. Настройка осуществляется с помощью оснастки ПО «Центр сертификации» посредством регистрации Центров валидации для автоматического определения узлов CDP (CRL Distribution Point) и узлов AIA (Authority Information Access), создания OCSP-сервиса, а также производится настройка параметров публикации для полных списков CRL и списков изменений CRL. Центр сертификации в необходимом количестве публикует полные списки аннулированных сертификатов CRL (Certificate Revocation Lists) и списки изменений CRL (Delta CRL), цепочку сертификатов, а также регистрирует в соответствующей базе данных все транзакции по сертификатам и CRL.
3. Управление жизненным циклом сертификатов. В данном сценарии выполняется ряд базовых операций, возникающих в течение жизненного цикла сертификата:
   - при выпуске сертификатов для субъектов доменной структуры ПО «Центр сертификации» поддерживается автоматическое заполнение определённых полей шаблона сертификата данными, полученными из ресурсной системы, источниками которой являются контроллеры домена инфраструктуры;
   - при выпуске сертификата есть возможность установить его на электронный носитель;
   - отзыв сертификата;
   - приостановление действия сертификата, выпущенного для пользователя;
   - возобновление сертификата пользователя после выхода на работу из отпуска;
   - поиск всех сертификатов пользователя;
   - контроль сроков действия сертификатов путём автоматического оповещение пользователей по истечению срока действия сертификата, с возможностью настройки шаблона рассылки оповещений.
4. Аутентификация и проверка статуса сертификатов. Клиентские компьютеры с установленными операционными системами необходимо ввести в домен. Каждый сертификат содержит конкретную идентификационную информацию о пользователе, в том числе его имя, открытый ключ и уникальную цифровую подпись, которая закрепляет сертификат за пользователем. В качестве основного механизма проверки статуса сертификатов используется протокол OCSP, обеспечивающий простоту развёртывания, администрирования и наименьшее время выдачи ответа.

При создании собственного центра сертификации в первую очередь следует определить требуемый тип иерархии что, в свою очередь, определяет необходимое количество серверов. При выборе количества уровней следует учитывать:

- количество сотрудников предприятия. Жестких критериев не существует. Как правило, многоуровневая структура включает от 2 до 4 уровней;
- количество удаленных филиалов или отделений. При небольшой численности сотрудников, но наличии большого количества филиалов, удаленных друг от друга, можно порекомендовать создание нескольких ЦС;
- структуру управления предприятием. Отдельный ЦС может понадобиться для каждого филиала, если филиалы имеют собственные органы управления;

- выделенный бюджет. Многоуровневая структура подразумевает большое количество оборудования и лицензий для операционных систем.

2.3 Иерархии PKI

Поскольку ЦС выстраиваются в древовидную иерархию, возможно организовать иерархию, где на каждом уровне ЦС будет выполнять как роль издающего ЦС, так и дополнительные функции. В самом простом случае один ЦС может совмещать все роли, т.е. быть корневым, обеспечивать какие-то политики выдачи (разделение ЦС по ролям) и выдавать сертификаты конечным потребителям. Например, в головном офисе держат корневой ЦС, выдающий сертификаты только другим ЦС, которые уже на себе накладывают политики выдачи. Они могут не обслуживать напрямую конечных потребителей, а выдавать сертификаты другим подчинённым ЦС, которые, в свою очередь, и будут обслуживать конечных потребителей.

Помимо задач по выпуску сертификатов, каждый ЦС периодически выпускает списки отзыва (Certificate Revocation List, CRL). Как и сертификаты, целостность списков отзыва обеспечивается цифровой подписью. CRL содержит серийные номера сертификатов, действие которых прекращено по какой-либо причине до официального истечения срока действия сертификата. Таким образом ЦС обеспечивает своевременное изъятие недействительного сертификата из оборота.

Проверка статуса отзыва сертификатов может выполняться несколькими способами – онлайн и оффлайн. В онлайн-протоколе OCSP – запрос на сервер позволяет проверяющей стороне узнать текущее состояние сертификата. Сервер возвращает окончательный ответ с цифровой подписью, указывающий статус сертификата. В оффлайновом режиме респондент получает свои данные из опубликованных списков отозванных сертификатов CRL и, следовательно, зависят от частоты публикации ЦС. Базовый список CRL включает полный список отзыва, в связи с чем трафик списков отзыва будет существенным по размеру. Для уменьшения трафика предусматривается возможность публикации дифференциального списка отзывов DeltaCRL. Это позволяет публиковать базовый CRL реже и на более длительный срок, а для ускорения времени реакции пользователей на отозванные сертификаты в промежутке выпускать несколько дифференциальных CRL.

Каждый клиент после установки доверия сертификата через цепочку должен убедиться, что ни один сертификат в цепочке не был отозван своим издателем. Для этого клиент перебирает каждый сертификат в цепочке, выбирает CRL/DeltaCRL, предоставленный издателем, и проверяет наличие/отсутствие текущего сертификата в списке CRL. Если текущий сертификат находится в CRL/DeltaCRL, то доверие к сертификату (и всем ветвям дерева под ним) автоматически обрывается.

Здесь следует отметить один крайне важный и принципиальный момент: невозможно отозвать корневой (самоподписанный) сертификат. Т.е. если по какой-то причине он был скомпрометирован, его можно отозвать только принудительным удалением сертификата из хранилища сертификатов каждого клиента.

2.3.1 Одноуровневая иерархия PKI

В одноуровневой иерархии PKI центр сертификации обеспечивает весь требуемый функционал. Данный вариант приемлем для небольших компаний. При необходимости может быть совмещен с сервером центра сертификации.

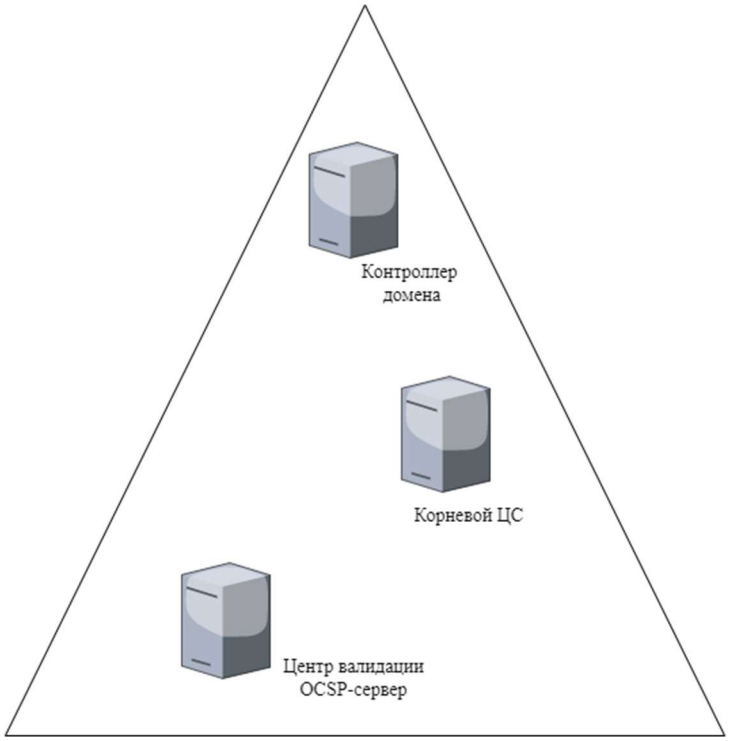


Рисунок 2 – Одноуровневая иерархия PKI

2.3.2 Двухуровневая иерархия PKI

Рекомендуемая конфигурация. Корневой сервер используется только для выдачи сертификатов одному или нескольким промежуточным центрам сертификации. Корневой центр сертификации находится в режиме offline и может не входить в Active Directory. При необходимости центр валидации может быть совмещен с сервером промежуточного центра сертификации.

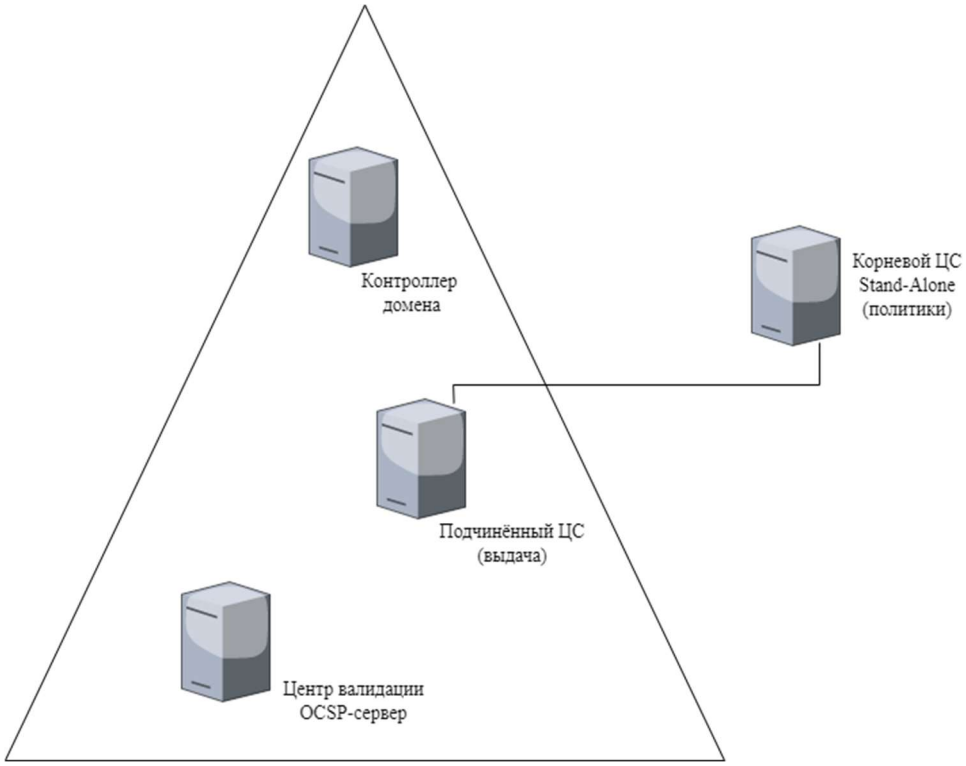


Рисунок 3 - Двухуровневая иерархия PKI

3 ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

3.1 Общие сведения

Предлагаемые решения компании Аладдин Р.Д. по организации инфраструктуры открытых ключей рассчитаны на отечественную среду функционирования (Red OS, Astra Linux и т.д.) с возможностью миграции с западных решений компании Microsoft.

Аппаратные и программные требования к серверам Центра сертификации и Центра валидации приведены в пункте 2.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-1.

4 ОБЩЕЕ ОПИСАНИЕ ПРОЦЕССА РАЗВЕРТЫВАНИЯ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Рассмотрим развертывание инфраструктуры открытых ключей на примере двухуровневой иерархии, состоящей из корневого отключенного от сети центра сертификации (Stand-Alone Root CA) и подчиненного издающего корпоративного центра сертификации (Subordinate CA).

Таким образом, типовая структурная схема может выглядеть так, как это показано на рисунке 3, где:

Корневой ЦС (Root CA) — выдаёт сертификат только подчинённому ЦС;

Подчинённый издающий ЦС (Subordinate CA) — выдаёт сертификаты конечным потребителям и публикует свой сертификат и списки отзыва на Центре валидации (Validation Authority);

Центр валидации (Validation Authority) — является хранилищем сертификатов ЦС и их списков отзыва, которые может скачать любой клиент;

Клиентские подключения — получают свои сертификаты у подчинённого ЦС и скачивают списки отзыва с сервера отзыва.

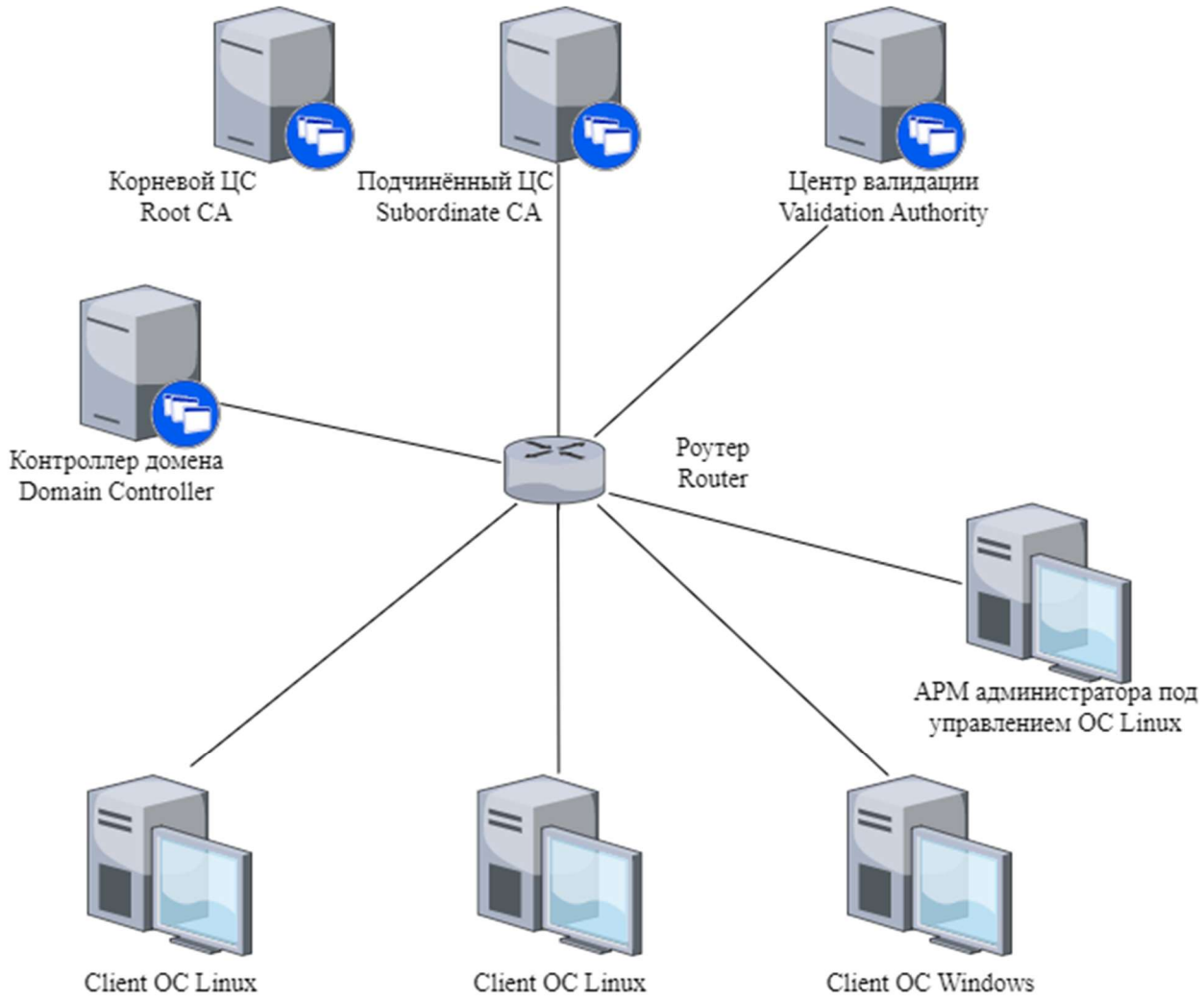


Рисунок 4 – Структурная схема PKI системы

4.1 Состав стенда

В данном примере структура PKI развертывается на нескольких компьютерах и включает в себя следующие компоненты:

- Root CA (корневой ЦС) – ПК с предустановленным ПО AeCA CA в соответствии с требованиями, указанными в пункте 2.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-1. В переходный период на длительном этапе миграции в качестве корневого центра сертификации может использоваться Microsoft Certificate Services.
- Subordinate CA (издающий ЦС) – ПК с предустановленным ПО AeCA CA в соответствии с требованиями, указанными в пункте 2.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-1.
- Domain Controller (контроллер домена) на базе проекта ALD PRO.
- Центр валидации – ПК с предустановленным ПО AeCA VA в соответствии с требованиями, указанными в пункте 2.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-1.
- АРМ Администратора – ПК с предустановленным ПО JC-WebClient 4.3.3 (для 64-битных систем) и поддерживаемым браузером согласно пункту 2.5.1 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-1 и Мастером групповой настройки.
- Client 01 – ПК на базе ОС семейства Linux, далее с помощью Мастера Групповой настройки будет установлено ПО Aladdin SecurLogon.
- Client 02 – ПК на базе ОС семейства Linux, далее с помощью Мастера Групповой настройки будет установлено ПО Aladdin SecurLogon.
- Client 03 – ПК на базе ОС семейства Windows.

4.2 Ввод в эксплуатацию корневого центра сертификации

Корневой ЦС (Root CA) позволяет выпускать сертификаты для пользователей, серверов или отдельных программ и служб в инфраструктуре.

К созданию центра сертификации необходимо отнестись с большой ответственностью, т. к. пересоздание корневого сертификата может повлечь за собой отзыв старых и выдачу новых сертификатов клиентам, или необходимость поддерживать несколько сертификатов доверенных центров в системах, что вызывает дополнительную нагрузку на администрирующий персонал. Желательно, как можно полнее отразить процессы жизненного цикла сертификатов в формальных документах.

Следует внимательно отнестись к физической охране сервера сертификации и обеспечить доступ к нему только узкому кругу ответственных лиц. Для улучшения защиты можно использовать шифрование файловой системы, где развернуты файлы центра.

Для установки корневого ЦС:

- На сервере корневого Центра сертификации установите вспомогательное ПО в соответствии с процедурами, приведёнными в разделе 3 RU.АЛДЕ.03.01.020-01 32 01-1 Центр сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора;
- Произведите подготовку предустановочных конфигурационных файлов и выполните установку компонента «Центр сертификации Aladdin eCA» в соответствии с разделом 4 «Центра сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора» RU.АЛДЕ.03.01.020-01 32 01-1.

После завершения установки в терминале будут выведены учётные данные администратора инициализации, от имени которого необходимо будет выполнять дальнейшие действия по инициализации. Их следует сохранить в надёжном месте. Также сертификат данного пользователя можно получить в каталоге /opt/aeca/p12/superadmin.p12.

- Выполните настройку АРМ администратора Центра сертификации в соответствии с процедурами, описанными в разделе 2 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководство администратора RU.АЛДЕ.03.01.020-01 32 01-2, для этого:
  - импортируйте сертификат администратора инициализации superadmin.p12 в браузер;
  - подключитесь по IP-адресу УЦ, например, `https://<ip-адрес>:8888/aecaCa/`.

Все дальнейшие действия по работе с УЦ осуществляются через веб-браузер.

- Зайдите на сервер ЦС как Администратор.
- Выполните начальную инициализацию ЦС в соответствии с разделом 3 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2, для этого:
  - Загрузите лицензию для корневого ЦС.
  - Имя ЦС будет задано автоматически, в зависимости от данных загруженной лицензии.
  - Задайте опциональный суффикс в формате X.500. При задании суффикса следует руководствоваться несколькими рекомендациями:
    - суффикс должен отражать название отдела или подразделения, которое отвечает за его управление в атрибуте OU (Organizational Unit);
    - дублировать полное название организации (атрибут O, Organization);
    - отражать юридическое место дислокации ЦС. Для этого достаточно использовать атрибуты L (Locality) и C (Country). Как правило, это название города и страны, где юридически зарегистрирована организация. Если необходимо, можно указать штат/область посредством атрибута S (State).
  - Установите срок действия сертификата. Обычно задают срок минимум в 2 – 5 раз больше, чем планируемый срок действия выданных сертификатов подчинённых ЦС. Максимальный срок жизни сертификата равен 25 лет, вы можете изменить его в соответствии с вашей политикой. Сертификаты уровня CA имеют более длительный срок действия, поскольку истечение срока действия сертификата CA автоматически означает прекращение действия всех выданных им сертификатов. Как ориентировочные значения можно принять 20-летний жизненный цикл для корневого сертификата.
  - Определите параметры шифрования, выбрав алгоритм ключа, длину ключа и алгоритм хэш-суммы.
  - Создается корневой сертификат в виде файла формата ***.pem.
    ***.pem — файл публичного сертификата ЦС. Серверы и клиенты будут использовать этот сертификат для подтверждения единой сети доверия. Копия этого файла должна иметься у всех серверов, использующих ваш ЦС. Все стороны будут использовать публичный сертификат для подтверждения подлинности системы.

4.3 Ввод в эксплуатацию подчиненного центра сертификации

После установки корневого центра сертификации необходимо установить подчиненный центр сертификации для реализации ограничений политики инфраструктуры открытого ключа и для выдачи сертификатов конечным клиентам. Использование хотя бы одного подчиненного центра

сертификации способствует защите корневого центра сертификации от необязательного воздействия извне.

Управление подчиненным ЦС дает возможность подписывать сертификаты пользователей для строгой аутентификации в домене, для корпоративной электронной подписи и для серверной инфраструктуры.

Если подчиненный центр сертификации будет использоваться для выдачи сертификатов пользователям или компьютерам с учетными записями, содержащимися в домене, установка подчиненного центра сертификации в качестве центра сертификации предприятия позволит использовать существующие данные учетной записи клиента в доменных службах для выдачи сертификатов и управления ими, а также для публикации сертификатов в доменных службах.

Для установки подчиненного ЦС:

- На сервере подчинённого Центра сертификации установите вспомогательное ПО в соответствии с процедурами, приведёнными в разделе 3 RU.АЛДЕ.03.01.020-01 32 01-1 Центр сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора;
- Произведите подготовку предустановочных конфигурационных файлов и выполните установку компонента «Центр сертификации Aladdin eCA» в соответствии с разделом 4 «Центра сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора» RU.АЛДЕ.03.01.020-01 32 01-1.

После завершения установки в терминале будут выведены учётные данные администратора инициализации, от имени которого необходимо будет выполнять дальнейшие действия по инициализации. Их следует сохранить в надёжном месте. Также сертификат данного пользователя можно получить в каталоге /opt/aeca/p12/superadmin.p12.

- Выполните настройку АРМ администратора Центра сертификации в соответствии с процедурами, описанными в разделе 2 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководство администратора RU.АЛДЕ.03.01.020-01 32 01-2, для этого:
  - импортируйте сертификат администратора инициализации superadmin.p12 в браузер;
  - подключитесь по IP-адресу УЦ, например, `https://<ip-адрес>:8888/aecaCa/`.

Все дальнейшие действия по работе с УЦ осуществляются через веб-браузер.

- Зайдите на сервер ЦС как Администратор.
- Выполните начальную инициализацию ЦС в соответствии с разделом 3 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2, для этого:
  - Загрузите лицензию для подчинённого ЦС.
  - Имя ЦС будет задано автоматически, в зависимости от данных загруженной лицензии.
  - Задайте опциональный суффикс в формате X.500. При задании суффикса следует руководствоваться несколькими рекомендациями:
    - суффикс должен отражать название отдела или подразделения, которое отвечает за его управление в атрибуте OU (Organizational Unit);
    - дублировать полное название организации (атрибут O, Organization);
    - отражать юридическое место дислокации ЦС. Для этого достаточно использовать атрибуты L (Locality) и C (Country). Как правило, это название города и страны, где юридически зарегистрирована организация. Если необходимо, можно указать штат/область посредством атрибута S (State).
  - Определите параметры шифрования, выбрав алгоритм ключа, длину ключа и алгоритм хэш-суммы.

- Создается подчиненный центр сертификации в состоянии «Запрос».
- Скачайте файл запроса .csv созданного подчиненного ЦС.
- Перенесите файл запроса .csv созданного подчиненного ЦС на АРМ корневого ЦС любым удобным способом.
- Загрузите файл-запрос с носителя в приложение AECA CA, установленное на корневом УЦ.
- Выполните процедуру подписания запроса на сертификат подчиненного ЦС в соответствии с пунктом 4.3.2.2 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2

  Сертификаты подчиненного ЦС подписывается корневым ЦС, который надежно хранится в автономном режиме и используется для подписи сертификатов конечных объектов. Корневой ЦС подтверждает достоверность промежуточных CA, которые, в свою очередь, подтверждают полномочия ЦС самого нижнего уровня. Выдающие сертификаты ЦС подтверждают достоверность сертификатов индивидуальных пользователей, которым были выданы сертификаты. На каждом уровне выдается сертификат для нижестоящего уровня и определяются политики и правила, управляющие использованием и временем жизни сертификатов. Иерархическая система взаимосвязей сертификатов формирует цепочку сертификации.

Скачайте цепочку сертификатов корневого ЦС в формате *.pem на последнем этапе подписания запроса на сертификат ЦС

- , и перенесите её любым удобным способом на АРМ подчиненного ЦС.
- Импортируйте цепочку сертификатов в подчиненный ЦС в состоянии «Запрос» в соответствии с пунктом 4.3.1.3 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2.
- Подчиненный ЦС из состояния «Запрос» переходит в состоянии «Активирован».

4.4 Ввод в эксплуатацию центра валидации

4.4.1 Развёртывание центра валидации

Для обеспечения проверки статуса сертификатов в рамках инфраструктуры открытых ключей предприятия и частичного снятия нагрузки с издающего Центра сертификации необходимо развернуть Центр валидации для дальнейшей его настройки через Центр сертификации.

Центр валидации поддерживает взаимодействие с администратором, работающим на удалённом сервере, только по протоколу HTTPS с аутентификацией удалённого администратора по клиентскому сертификату, и администратором, работающим локально на сервере Центра валидации по протоколам HTTP/HTTPS без дополнительной аутентификации.

- На сервере Центра валидации установите вспомогательное ПО (СУБД, Open JDK) в соответствии с процедурами, приведёнными в разделе 3 RU.АЛДЕ.03.01.020-01 32 01-1 Центр сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора;
- Произведите подготовку предустановочных конфигурационных файлов и выполните установку компонента «Центр валидации Aladdin eCA» в соответствии с разделом 5 «Центра сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора» RU.АЛДЕ.03.01.020-01 32 01-1.

После завершения установки в терминале будут выведены учётные данные администратора инициализации, от имени которого необходимо будет выполнять дальнейшие действия по инициализации. Их следует сохранить в надёжном месте. Также сертификат данного пользователя можно получить в каталоге /opt/aeca/p12/superadmin.p12.

- Выполните настройку АРМ администратора Центра валидации в соответствии с процедурами, описанными в разделе 2 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководство администратора RU.АЛДЕ.03.01.020-01 32 01-2, для этого:
  - импортируйте сертификат администратора инициализации superadmin.p12 в браузер;
  - подключитесь по IP-адресу УЦ, например, `https://<ip-адрес>:8888/aecaVa/`.
- Все дальнейшие действия по работе с Центром валидации осуществляются через сервер Подчинённого Центра сертификации.

4.4.2 Регистрация центра валидации для подчиненного ЦС

После того, как корневой ЦС установлен и сконфигурирован, необходимо приступать к регистрации Центра валидации на подчинённом Центре сертификации для:

1) создания и настройки сервиса распространения списков отзыва CRL DP. Каждый издающий (подчиненный) ЦС будет публиковать свой список отзыва, используя HTTP-протокол и web-сервер Центра валидации.

- Для настройки этого сервиса необходимо задать:
  - период обновления списка отозванных сертификатов CRL. Обновление CRL происходит автоматически через заданный период времени, который возможно изменять кратно одному часу, дню, месяцу, году. Рекомендации по сроку обновления CRL:
    - все ЦС, которые выдают сертификаты только другим ЦС (не конечным потребителям), должны публиковать CRL сроком действия от 3-х до 12 месяцев с запасом в один месяц;
    - все ЦС, которые выдают сертификаты конечным потребителям (пользователям и устройствам), должны публиковать базовые CRL не реже одного раза в неделю.
  - период обновления DeltaCRL – время между публикациями Delta CRL;
  - срок действия перекрытия – задается период действия текущего списка CRL до публикации нового списка CRL, согласно настроенному периоду.

После изменения значений «Автообновления CRL» необходимо сохранить изменения и опубликовать CRL.

- Точка распространения списков отзыва, которая будет регистрироваться в издаваемых сертификатах с указанием пути, по которому клиенты могут скачать список отзыва. Этот путь публикуется в сервисе CRL для каждого ЦС.

2) создания и настройки сервиса AIA для определения места хранения актуальных сертификатов издающих ЦС. Сертификаты подчиненных (издающих) ЦС из этого хранилища можно использовать для создания цепочки сертификатов, которую можно проследить до корневого сертификата.

- Для доступа к хранилищу сертификатов используются те же точки распространения развернутого web-сервера, что для распространения CRL.
- Обе эти точки содержатся во всех выданных удостоверяющим центром сертификатах и, соответственно, должны быть доступны всем потребителям. Клиенты должны обладать возможностью проверять цепочку сертификатов и список отзыва, обращаясь по тем данным, которые указаны в сертификате, то есть определены в AIA и CRL при настройке.

3) развертывания OCSP-сервера, работающего по протоколу HTTP. OCSP-сервер обрабатывает запросы на проверку сертификатов субъектов, так что здесь следует применять аппаратное обеспечение сервера с возможностью масштабирования, соответствующей прогнозируемой потребности в подключениях;

4) внесения сведений об OCSP-сервере (url-адрес OCSP) в удостоверяющий центр для добавления местонахождения сервера OCSP в подписываемые им сертификаты. Когда удостоверяющий центр подписывает сертификат, обычно он добавляет в сертификат адрес сервера OCSP. Например, когда пользователь встречает сертификат сервера, он отправляет запрос серверу OCSP, указанному в сертификате. На этом адресе OCSP-ответчик ожидает запросы и сообщает о статусе сертификата - отозван он или нет. Ответчику OCSP необходима криптографическая пара для подписания ответа, который он отправляет запрашивающей стороне. Криптографическая пара OCSP должна быть подписана тем же удостоверяющим центром, которым подписан проверяемый сертификат.

- Перед регистрацией Центра валидации необходимо выполнить настройку автообновления периода обновления CRL, при необходимости, настроить публикацию DeltaCrl, и выпустить первый CRL согласно пунктам 4.8.1 и 4.8.2 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2.
- Регистрация Центра валидации выполняется в соответствии с пунктом 4.8.3 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2. Основные этапы регистрации Центра валидации:
  - скопируйте и перенесите на текущий подчинённый ЦС сертификат суперадмина web-сервера «Центра валидации» `/opt/aeca/p12/superadmin.p12` и пароль из файла `generated_passwords.txt`, данные строки `superadmin_password` , полученный после установки ПО AeCA VA;
  - запустите Мастер регистрации центра валидации, нажав кнопку <Зарегистрировать +> на вкладке «Центры валидации» сервера Подчинённого Центра сертификации;
  - в открывшемся окне Мастера регистрации укажите ip-адрес или имя хост-сервера с указанием доменной зоны, на котором развёрнут компонент «Центр валидации» Aladdin eCA;
  - загрузите предварительно скачанный сертификат `superadmin.p12` сервера Центр валидации;
  - далее выполните подписание запроса OCSP нажав одноимённую кнопку в окне Мастера регистрации центра валидации.
- В результате:
  - активированы службы AIA и CRL DP;
  - активирована служба OCSP.
- Компьютер с именем SubCA установлен, обновлён и сконфигурированы параметры безопасности. Данный компьютер будет выполнять роль издающего центра сертификации.

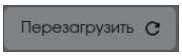
4.5 Подключение ресурсной системы

Для загрузки субъектов доменной структуры и дальнейшего выпуска для них сертификатов необходимо выполнить подключение к ресурсной системе контроллера домена на сервере подчинённого Центра сертификации.

- Aladdin Enterprise CA поддерживает следующие типы ресурсных систем:
  - Samba DC;
  - ALD PRO;
  - MS AD;
  - FreeIPA.
- При необходимости подключения к ресурсной системе контроллера домена по протоколу TLS выполните настройку согласно Приложению А. Таблица 1 настоящего документа.

- Выполните подключение контроллера домена к ресурсной системе подчиненного ЦС для загрузки всех субъектов доменной сети в Центр Сертификации в соответствии с пунктом 4.7.1 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2.

4.6 Настройка АРМ администратора

- АРМ Администратора предназначен для выполнения организационно-технических мероприятий, связанных с формированием служебных ключей и сертификатов пользователей, управления Центром сертификации, автоматизированной настройки рабочих мест пользователей. АРМ администратора функционирует в ОС Astra Linux 1.7 Смоленск в конфигурации «Минимальный сервер» с опцией SSH-сервер и уровнем безопасности «Базовая защита» или RED OS 7.3. АРМ администратора взаимодействует с Центром сертификации по HTTPS протоколу.
- К основным функция АРМ администратора относятся:
  - обеспечение взаимодействия с Центром сертификации;
  - шифрование информации передаваемой ЦС с использованием протокола HTTPS с двусторонней аутентификацией;
  - организация просмотра информации из БД ЦС, относящейся к пользователю;
  - подписание запросов на формирование сертификатов;
  - обеспечение возможности получения пользователем нескольких сертификатов;
  - запись электронного сертификата открытого ключа пользователя на электронный ключ;
  - отзыв сертификатов;
  - просмотр журнала событий ЦС;
  - публикация списков отозванных сертификатов открытых ключей пользователей;
  - скачивание списка отозванных сертификатов в виде файла;
  - сохранение сертификата (цепочки сертификатов) Центра;
  - создание учётной записи оператора.
- Перед началом работы с Центром сертификации на АРМ администратора необходимо произвести двустороннюю HTTPS-аутентификацию администратора для входа в учётную запись, когда веб-клиент проверяет сертификат веб-сервера и веб-сервер проверяет сертификат веб-клиента.
- Предварительно на Подчинённом удостоверяющем центре:
  - создайте учётную запись АРМ администратора в соответствии с пунктом 4.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2;
  - выпустите сертификат для учетной записи администратора АРМ на вкладке «Учётные записи», выделив созданную учётную запись администратора АРМ и нажав кнопку <Выпустить сертификат>, в соответствии с пунктом 4.5.4 или 4.5.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2. Запишите или запомните пароль для выпущенного сертификата;
  - на вкладке «Настройки» в поле «Разрешенные издатели» выберите издателя – Подчинённый удостоверяющий центр, от имени которого был выпущен сертификат учетной записи, и активируйте проверку издателя, передвинув ползунок вправо;
  - на вкладке «Настройки» нажмите кнопку 

для применения настроек веб-сервера.

- Для настройки аутентификации произведите следующие действия на АРМе администратора:
  - скопируйте и перенесите созданный сертификат администратора на АРМ администратора;
  - откройте браузер. Для браузера Firefox в меню выберите Настройки – Приватность и Защита – Сертификаты. Нажмите кнопку <Просмотр сертификатов>;
  - выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку <Импортировать>;
  - выберите файл перенесённого сертификата учетной записи на локальном диске. Нажмите кнопку <Открыть>;
  - введите пароль, указанный при создании сертификата учетной записи администратора в открывшемся окне, и нажмите кнопку <Ок>;
  - для входа в Центр сертификации по учетной записи введите в адресную строку: `<адрес_хоста_развертывания_продукта>:<порт>/<aecaCa>/`;
  - в появившемся окне «Запрос идентификации пользователя» выберите установленный сертификат учетной записи;
  - в случае успешной установки сертификата откроется страница с предупреждением системы безопасности. Нажмите кнопку <Advanced>;
  - по нажатию кнопки <Advanced> на странице предупреждения системы безопасности осуществляется переход на страницу ошибки распознавания сертификата. Нужно принять риски, нажав кнопку <Accept the Risk and Continue> на текущей странице;
  - аутентификация выполнена успешно, в случае перехода в Центр сертификации с указанием отображаемого имени на верхней панели соответствующей учетной записи.

4.7 Настройка рассылки уведомлений об истечении срока действия сертификата

- Для мониторинга сроков окончания действия сертификатов пользователей удобно использовать инструментарий AeCA CA для настройки уведомлений об истечении срока действий сертификата. Сервис автоматически определит окончания сроков действия сертификатов и оповестит вовремя всех пользователей по электронной почте.
- Для получения списка пользователей, для которых выпущены сертификаты с помощью AeCA CA, сервис использует данные базы данных aecatest и подключенных ресурсных систем.
- Далее, должен быть отредактирован конфигурационный файл email.env, в котором редактируется список элементов данных, содержащих информацию для мониторинга, а также список соответствующих триггеров.
- По умолчанию владелец сертификата будет уведомлён за 30, 7, 1 день до окончания срока действия сертификата.
- Для выполнения сценария должна быть указана электронная почта в учётных доменных записях пользователей.
- Уведомления об окончании срока действия сертификатов будут приходить при каждом выполнении сценария.
- Продление срока действия сертификата возможно через выпуск нового сертификата в центре сертификации. Если данные владельца не изменяются, то изменениям подвергается только криптографическая составляющая электронного сертификата.

- Подробное описание процедуры настройки уведомлений об истечении срока действия сертификатов пользователей приведено в пункте 4.10 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2.

4.8 Обеспечение возможности строгой аутентификации пользователей в домене

- Строгая аутентификация пользователей в домене производится по протоколу PKINIT (RFC 4556), механизму предварительной проверки подлинности для Kerberos, используя сертификаты X.509 для проверки подлинности KDC.
- Для настройки аутентификации пользователя в системе по сертификату вначале необходимо выполнить выпуск сертификата контроллера домена и его установку с целью подтверждения его подлинности в доменной структуре.

4.8.1 Выдача сертификата контроллера домена

- После загрузки субъектов доменной сети необходимо выпустить сертификат доступа контроллеру домена, используя автоматически подставленные данные контроллера домена, выбрав шаблон сертификата, соответствующий типу контроллера «ALD PRO Domain Controller». Процедура выпуска сертификата контроллера домена ALD PRO описана в подразделе 4.4.7.1 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2.
Процедура для выпуска сертификата контроллера домена, как для нового субъекта, приведена в Приложении А, Таблица 3.
- Сформированный и подписанный сертификат контроллера домена обязательно скачайте на последнем шаге работы «Мастера создания сертификата» в формате .p12. Далее скачать сертификат DC в контейнере PKCS#12 невозможно!

4.8.2 Установка сертификата контроллера домена ALD PRO

Произведите установку сертификата контроллера домена ALD PRO в соответствии с процедурой, описанной в Приложении А, Таблица 2:

- Скачайте цепочку сертификатов ЦС, от имени которого был выпущен сертификат контроллера домена.
- Скопируйте и перенесите сертификат контроллера домена в контейнере PKCS#12 и цепочку сертификатов ЦС на АРМ с установленным контроллером домена.
- Если ранее на контроллер домена устанавливались цепочки сертификатов ЦС, удалите ранее установленную цепочку сертификатов.
- Установите цепочку сертификатов выпускающего ЦС.
- Обновите списки сертификатов.
- Установите выпущенный контейнер PKCS#12 для контроллера домена
- Перезапустите сервис ipa.

4.8.3 Подготовка АРМ пользователей

- Запустите АРМ администратора.
- Установите «Мастер групповой настройки» согласно процедуре, приведенной в Приложении Б, Таблица 5.
- Произведите подготовку АРМ пользователей для дальнейшей двукратной аутентификации в домене с использованием сертификата на электронном ключе, установив необходимое программное обеспечение методом групповой настройки в соответствии с процедурой, описанной в Приложении Б, Таблица 6:

- в окне настройки параметров сканирования сети введите ip-адрес контроллера домена и порт (выставляются автоматически по умолчанию), логин и пароль учетной записи администратора с правами root и начните процесс сканирования сети;
- после завершения сканирования сети посмотрите статус доступности репозитория по протоколу ssh для узлов, на которых будет производится настройка двухфакторной аутентификации;
- в случае статуса узла «Ошибка доступа по ssh» произведите проверку подключения к целевой машине и в случае необходимости, произведите настройку доступа ssh на настраиваемых узлах;
- после настройки доступа по ssh на целевых машинах необходимо произвести повторное сканирование сети;
- после успешного сканирования необходимо выбрать узлы для дальнейшей настройки, выбрать действие «Установить SL»;
- укажите путь к устанавливаемым пакетам SecurLogon и Единому клиенту JaCarta, выберите файл лицензии или введите ключ активации, добавьте цепочку сертификатов выпускающего сертификаты пользователей ЦС для установки в локальное хранилище сертификатов с целью верификации пользовательских сертификатов при аутентификации на целевых машинах;
- запустите процесс настройки;
- после окончания настройки на выбранных АРМ настроена сетевая двухфакторная аутентификация по сертификату пользователя на электронном ключе.

4.8.4 Выдача сертификата пользователю на электронном носителе

После настройки двухфакторной аутентификации при входе пользователя на АРМ необходимо выпустить сертификат на электронном носителе для учетной записи пользователя в домене. Учетная запись пользователя однозначно идентифицирует пользователя, который использует компьютерную систему. Учетная запись сообщает системе, что необходимо применить соответствующую авторизацию, чтобы разрешить или запретить доступ пользователей к ресурсам.

- Выпуск сертификата произведите на подчиненном издающем ЦС, для этого выполните действия согласно процедуре, описанной в пункте 4.6.6 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2:
- Откройте Центр сертификации – вкладку «Субъекты доступа»;
- Выберите контроллер домена и разверните группы безопасности;
- В выпадающем меню выберите группу безопасности, для пользователя которой необходимо выпустить сертификат;
- Выберите учетную запись пользователя, для которого нужно выпустить сертификат;
- Нажмите на меню, расположенное справа в строке <Выпустить сертификат>;
- В открывшемся подменю выберите <На ключевом носителе>;
- Последовательно выполните шаги Мастера создания сертификата, выбрав шаблон сертификата «ALD PRO Smartcard Logon» при аутентификации в домене под управлением ALD PRO, FreeIPA;
- Важно! При выпуске сертификата необходимо установить флажок в чек-боксе «Публиковать сертификат в ресурсную систему» для дальнейшей успешной аутентификации пользователя в домене;
- После генерации и записи сертификата на ключевом носителе извлеките электронный ключ из USB-разъема.

4.8.5 Аутентификация пользователя

Для доступа пользователя в систему:

- Включите ПК пользователя.
- Вставьте электронный ключ с выпущенным сертификатом в USB-разъем АРМ пользователя.
- В графическом окне аутентификации пользователя в домене с использованием средств двухфакторной аутентификации JaCarta на центральной панели выберите электронный ключ с сертификатом пользователя.
- В поле «Логин» выберите пользователя из выпадающего списка – имя пользователя считывается из поля «CN» выбранного сертификата с указанием домена текущего ПК при сетевой аутентификации.
- В поле «PIN-код» введите PIN-код электронного ключа, в соответствии с назначенной политикой входа, для выбранного пользователя. Максимальное количество неверных последовательных попыток ввода PIN-кода пользователя, после которого возможность использования PIN-кода пользователя будет заблокирована, определяется при настройке параметров токена в ПО «Единый Клиент JaCarta».
- Сразу после введения учетных данных начинается процедура аутентификации, которая заключается в проверке подлинности данных пользователя сервером.
- Процедура аутентификации прошла успешно, если пользователь вошел в систему.

4.9 Итог

PKI установлена успешно, если вся итоговая конфигурация соответствует ожидаемым значениям и оснастка Aladdin Enterprise CA не показывает ошибок.

5 ОБЩЕЕ ОПИСАНИЕ ПРОЦЕССА РАЗВЕРТЫВАНИЯ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ НА БАЗЕ ALADDIN ENTERPRISE CERTIFICATION CENTER И СУЩЕСТВУЮЩЕГО ЦЕНТРА СЕРТИФИКАЦИИ MICROSOFT CERTIFICATE SERVICES

- Для успешного решения задачи миграции на отечественное ПО, глубоко проанализировав ситуацию, компания Аладдин Р.Д., имеющая большой опыт реализации работ по миграции на отечественное программное обеспечение в сфере управления цифровыми сертификатами и ключевыми носителями, предлагает предприятиям решение для максимально самостоятельного осуществления процесса поэтапного перехода от действующего Центра сертификации Microsoft к Центру сертификации АеСА, соответствующего требованиям ФСБ и ФСТЭК России, с минимальным привлечением специалистов со стороны. Этот принцип можно назвать достаточным при наличии у специалистов заказчика практических реальных навыков администрирования отечественных ОС.
- Продукты компании Аладдин Р.Д. поддерживают взаимодействие с сервисами Microsoft Active Directory и Certificate Services, что обеспечивает плавное выполнение миграции на платформу Центра сертификации АеСА.
- На первоначальном этапе предусматривается совместное использование решений по управлению цифровыми сертификатами Microsoft Certificate Services и Aladdin Enterprise Certificate Authority для чего необходимо произвести добавление подчинённого издающего Центра сертификации Aladdin eCA, функционирующего на сервере под управлением ОС семейства Linux (см. п. 2.5 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-1) в развёрнутую инфраструктуру PKI на платформе Windows. Как правило, на этом этапе не возникает проблем в использовании издаваемых сертификатов на разных операционных системах и иных устройствах: стандарты сертификатов и PKI являются кроссплатформенными. Криптографические алгоритмы шифрования и электронной подписи, используемые при выпуске сертификатов Центром сертификации АеСА, соответствуют международным стандартам RFC, описанные документами из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети.

5.1 Подготовка инфраструктуры

Перед установкой подчинённого Центра сертификации АеСА следует провести подготовку инфраструктуры (см. Рисунок 5) в следующем объеме:

- проверить наличие и работоспособность центра сертификации MS CS (установка в формате Standalone),
- скопировать «имя издателя», используемое корневым Microsoft Certificate Services (обычно совпадает с hostname), для дальнейшего выпуска лицензии подчинённому ЦС Aladdin Enterprise Certificate Authority;
- получить лицензию для установки подчинённого ЦС Aladdin Enterprise Certificate Authority, где в качестве корневого центра будет указано “имя издателя” MS CS;
- на выделенную вычислительную машину:

- установить вспомогательное ПО в соответствии с процедурами, приведёнными в разделе 3 RU.АЛДЕ.03.01.020-01 32 01-1 Центр сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора;
- произведите подготовку предустановочных конфигурационных файлов и выполните установку компонента «Центр сертификации Aladdin eCA» в соответствии с разделом 4 «Центра сертификатов Aladdin Enterprise Certificate Authority. Руководства администратора» RU.АЛДЕ.03.01.020-01 32 01-1;
- выполните настройку АРМ администратора Центра сертификации в соответствии с процедурами, описанными в разделе 2 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководство администратора RU.АЛДЕ.03.01.020-01 32 01-2
- выполнить ввод в эксплуатации с использованием полученной лицензии
- выполните начальную инициализацию ЦС в соответствии с разделом 3 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2, используя полученную лицензию;
- скачайте файл запроса .csv созданного подчиненного ЦС.

Примечание. Для выполнения преобразований используются средства certreq (программа встроена в ОС Windows) и openssl (программа входит в базовые средства ОС Linux). На схеме (см. Рисунок 5) они условно показаны на целевых вычислительных машинах, но использовать эти средства можно на любом рабочем месте.

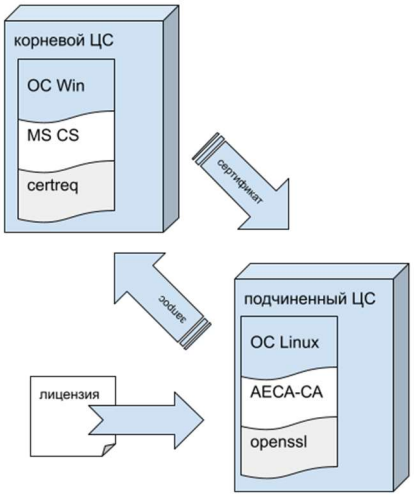


Рисунок 5 – Совместное использование ЦС AeCA и MS CS

5.2 Получение сертификата подчинённого ЦС AeCA

- Для получения сертификата следует выполнить следующие действия:
  - скопировать файл запроса на вычислительную машину, где развёрнут MS CS;
  - подписать запрос на сертификат подчинённого ЦС AeCA средствами MS CS;
  - скачать полученный сертификат в контейнере p7b;
  - выделить цепочку сертификатов корневого ЦС MS CS;
  - импортировать выделенную цепочку сертификатов в подчинённый ЦС AeCA.

5.2.1 Конвертация запроса на сертификат подчинённого ЦС AeCA

- Перенесите полученный файла запроса на сертификат подчинённого ЦС AeCA на машину, где развёрнут корневой Центр сертификации MS CS для подписания запроса, например, в файл c:\subca.csr;
- создайте текстовый файл c:\subca.inf следующего содержания:

```
[BasicConstraintsExtension]

Critical=Yes
```

- запустить терминал командной строки Power Shell и выполнить изменение запроса, выполнив команду:

```
certreq -policy C:\subca.csr  C:\subca.inf  C:\subca_ms.csr
```

где:

`C:\subca.csr` – ранее созданный файл запроса;

`C:\subca.inf` – ранее созданный файл дополнения;

`C:\subca_ms.csr` – результирующий файл запроса, который можно подписать в MS CS.

5.2.2 Подписание запроса на сертификат на корневом ЦС MS CS

Для подписания запроса на сертификат подчинённого ЦС AeCA используйте панель управления MSCS.

Выпуск сертификата по запросу производится следующим образом (далее рисунки приведены для версии ОС «server 2019»):

- Откройте web-браузер и перейдите по адресу localhost/certsrv (см. Рисунок 6).
- На открывшейся странице перейдите по ссылке «Запрос сертификата».

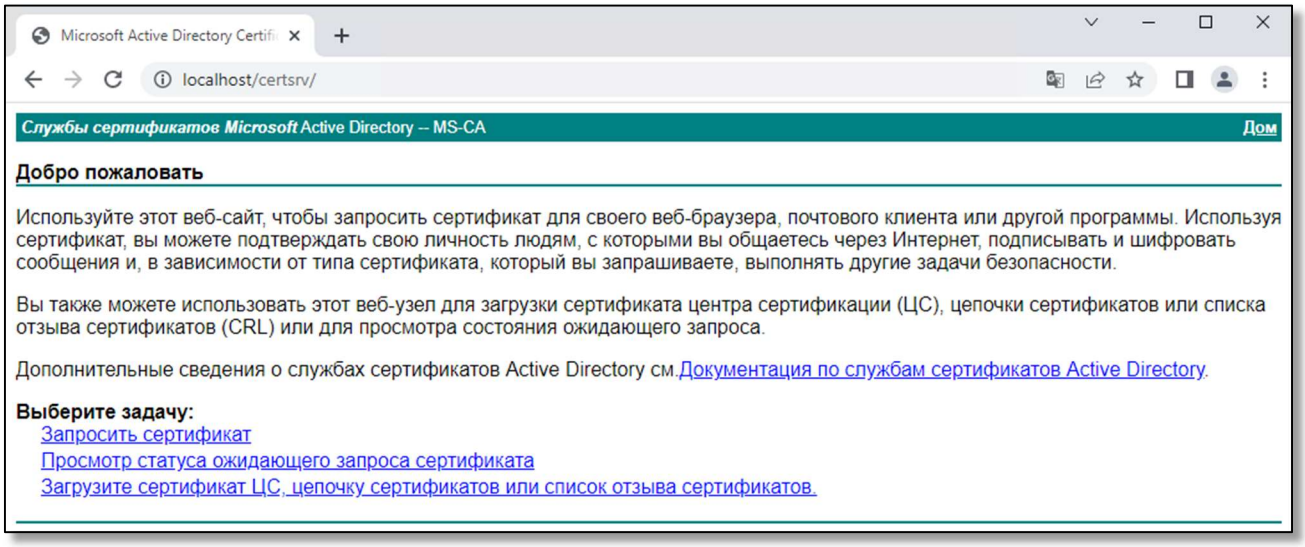


Рисунок 6 – Приветственное окно службы сертификации MS CS

- Далее нажмите на ссылку «Расширенный запрос сертификата» (см. Рисунок 7).

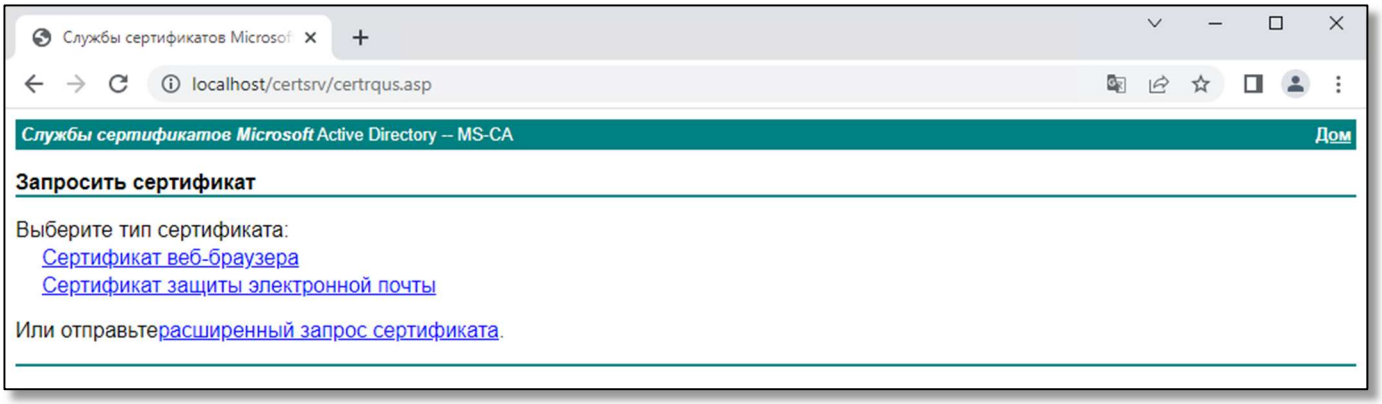


Рисунок 7 – Окно запроса сертификата службы сертификации MS CS

- В появившееся окно (см. Рисунок 8) в поле «Сохраненный запрос» (Saved Request) скопируйте содержимое преобразованного файла subca_ms.csr, полученного на шаге 5.2.1 и нажмите кнопку <Выдать> (Submit);

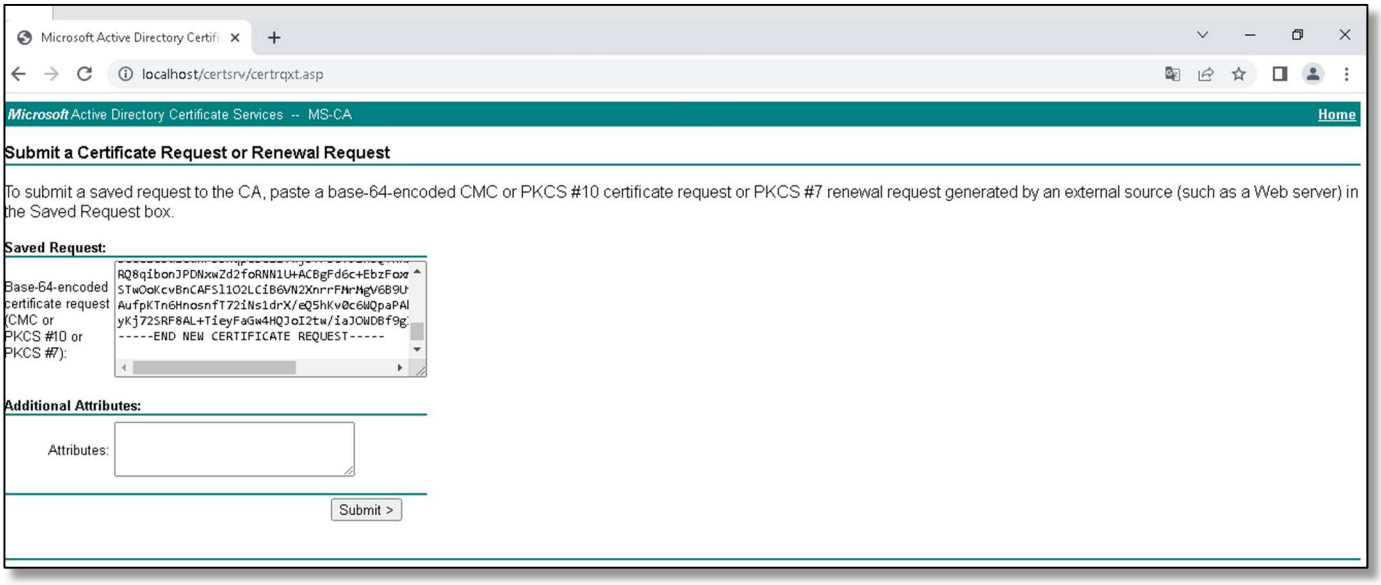


Рисунок 8 – Окно вставки содержимого запроса сертификата службы сертификации MS CS

- Откройте Server Manager и в меню Tools кликните на Certification Authority (Центр сертификации). Находясь внутри, вы можете раскрыть название своего Центра сертификации и увидеть ряд папок, включая одну внизу с названием «Pending Requests» (Запросы в ожидании) (см. Рисунок 9).

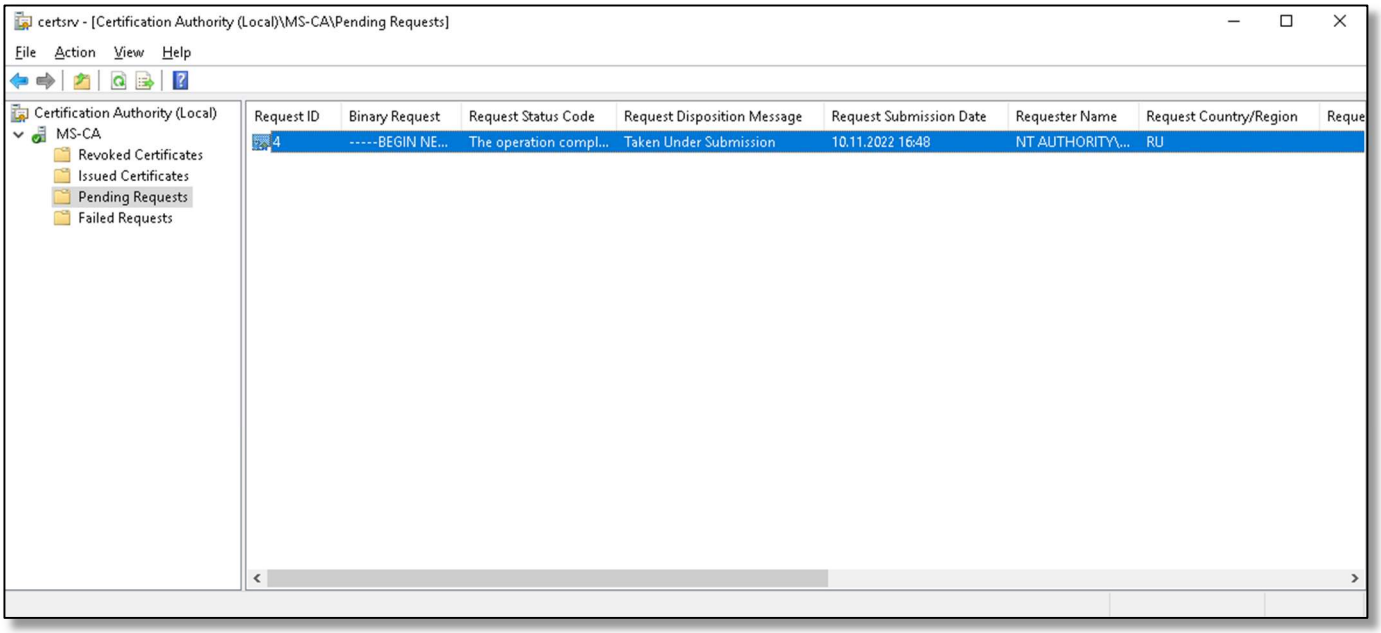


Рисунок 9 – Окно Центра сертификации

- в раздел «Pending Requests» (Запросы в ожидании) нажмите правой клавишей мыши на созданном запросе и выберите «All Tasks -> Issue» (Все задачи -> Выдать) (см. Рисунок 10).

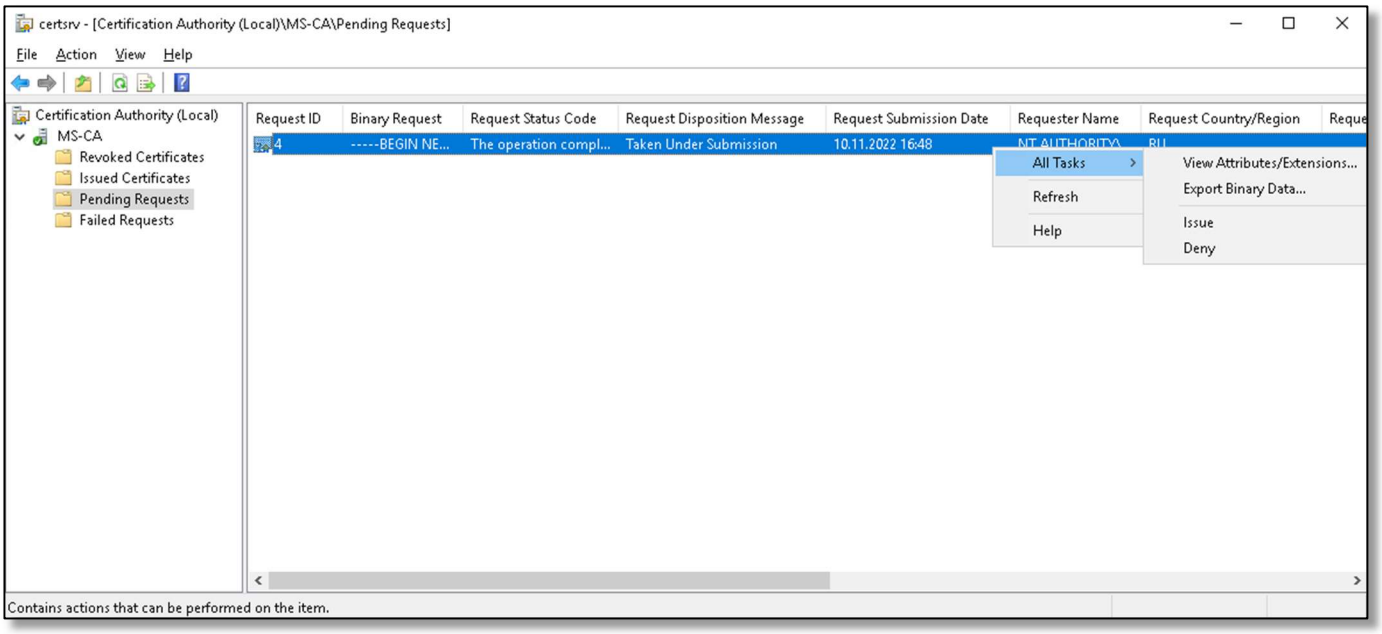


Рисунок 10 – Окно запросов в ожидании Центра сертификации

- Перейдите в раздел «Issued Certificates» (Выданные сертификаты), выберите полученный сертификат, двойным нажатием левой кнопки мышки на выбранном сертификате откройте окно со свойствами сертификата, выберите вкладку «Details» (Состав) нажмите кнопку <Copy to File> (Копировать в файл) (см. Рисунок 11).

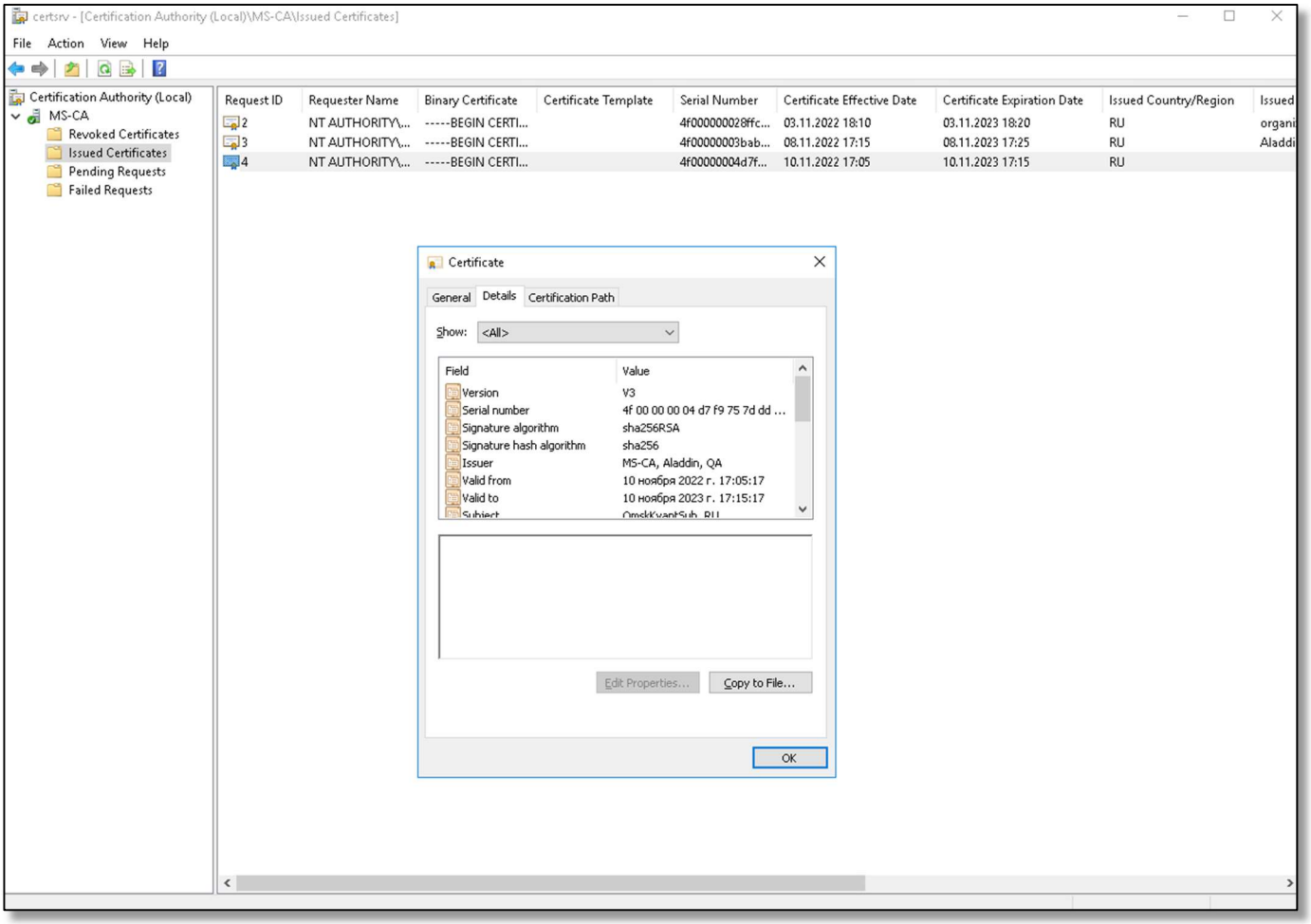


Рисунок 11 – Окно свойств сертификата

- При копировании выбрать формат .p7b и поставить флаг «Включить все сертификаты в путь», нажмите кнопку <Next> (Далее) и укажите место сохранения сертификата.

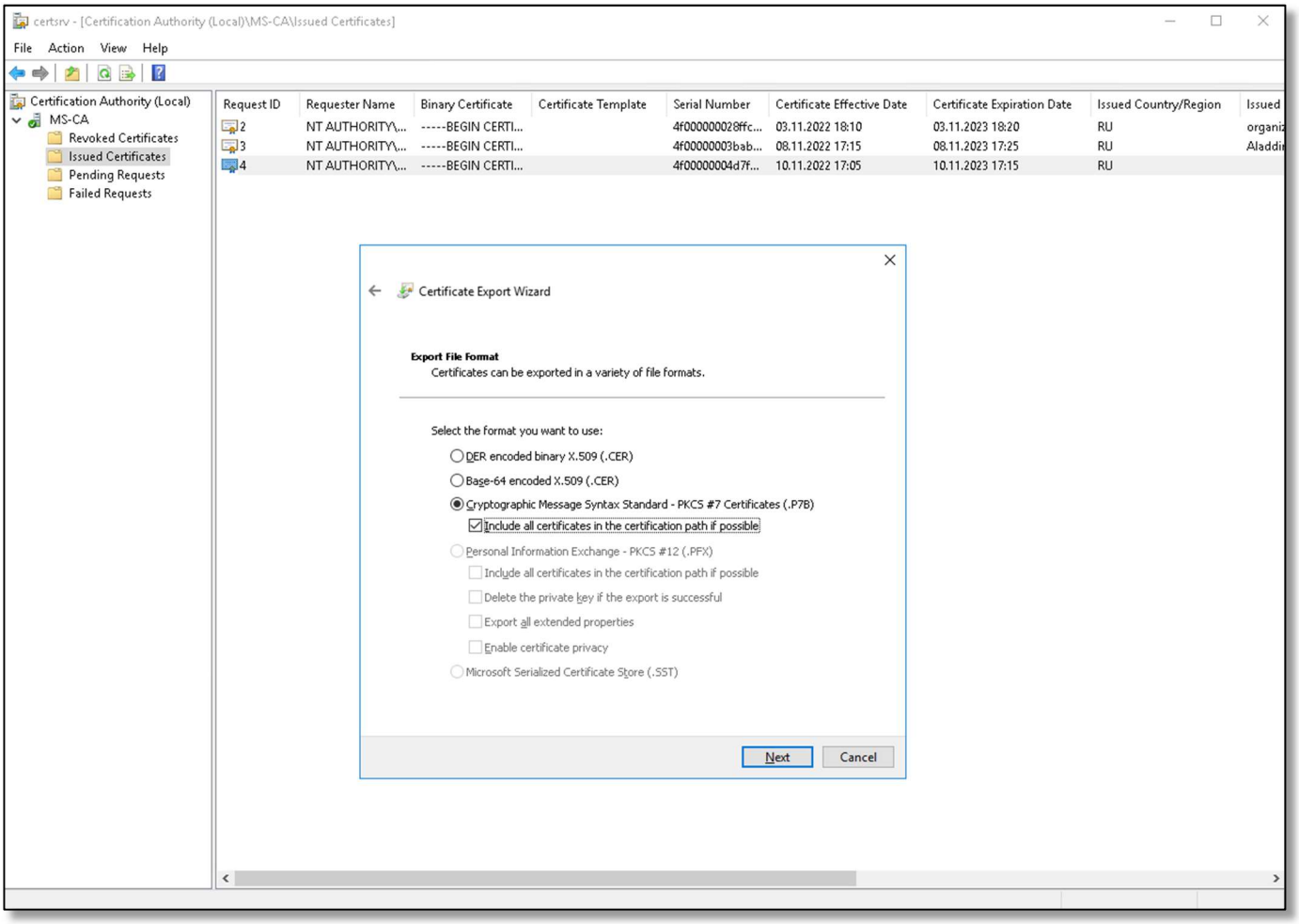


Рисунок 12 – Окно экспорта цепочки сертификатов

- Дождитесь появления сообщения об успешном завершении экспорта сертификата. В результате будет получен p7b-контейнер.
- Далее, нужно выделить цепочку сертификатов из p7b-контейнера, используя средство openssl в любой доступной среде. Получение цепочки выполняется командой:

```
openssl pkcs7 -print_certs -inform DER -in certificate.p7b -out subca_chain.pem
```

где:
`certificate.p7b` – контейнер p7b, полученный из MS CS;
`subca_chain.pem` – результирующая цепочка сертификатов, используемая для активации подчинённого ЦС AeCA.

5.2.3 Активация подчинённого ЦС AeCA

- Для активации подчинённого Центра сертификации в состоянии «Запрос» импортируйте выделенную цепочку сертификатов корневого ЦС MS CS в соответствии с пунктом 4.3.1.3 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2.
- Подчиненный ЦС из состояния «Запрос» переходит в состоянии «Активирован», считается доверенным центром сертификации и готов для дальнейшей работы.

6 КОНТАКТЫ

6.1 Офис (общие вопросы)

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

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

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

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

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

6.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт: www.aladdin-rd.ru/support/index.php.

Коротко о компании

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

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

Основные направления

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

Лицензии

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

СПИСОК ЛИТЕРАТУРЫ

1. RU.АЛДЕ.03.01.020-01 32 Центр сертификатов доступа Aladdin Enterprise CA. Руководство администратора «Аладдин Р.Д.»
2. RU.АЛДЕ.03.01.020-01 30 Центр сертификатов доступа Aladdin Enterprise CA. Формуляр – «Аладдин Р.Д.»
3. Единый Клиент JaCarta. Руководство администратора для операционных систем семейства Linux «Аладдин Р.Д.»
4. RU.АЛДЕ.02.07.002 32 Средство двухфакторной аутентификации Aladdin SecurLogo. Руководство администратора «Аладдин Р.Д.»

ПРИЛОЖЕНИЕ А. НАСТРОЙКА КОНТРОЛЛЕРА ДОМЕНА

А.1 Настройка контроллера домена ALD PRO для подключения в качестве источника ресурсной системы AeCA по протоколу TLS

Выполните процедуру подключения к ALD PRO по протоколу TLS в соответствии с таблицей 2 от имени пользователя с правами root.

Таблица 2 – Процедура подключения к ALD PRO по протоколу TLS

№	Описание шага	Команда	Примечание (при необходимости)
1	Скопировать текущий сертификат контроллера домена	На хосте, где развёрнут контроллер домена, к которому будет происходить подключение по протоколу TLS, скопируйте сертификат контроллера домена `/etc/ipa/ca.crt`	Указано стандартное расположение сертификата контроллера домена
2	Перенесите скопированный сертификат на сервер AECA CA, с которого необходимо произвести подключение	Поместите скопированный сертификат контроллера домена, к которому выполняется tls подключение, в домашний каталог пользователя, который будет выполнять команды в терминале	
3	Конвертируйте сертификат контроллера домена для tls соединения	Выполните команду, находясь в папке с сертификатом контроллера домена: `openssl x509 -outform der -in ca.crt -out aldpro.der`	

4	Получите путь к каталогу с установленным java одним из способов для переменной среды JAVA_HOME	способ 1:
		`dirname $(dirname $(readlink -f $(which javac)))`
		способ 2:
		`update-alternatives --config javac`	

5	Импортируйте полученный сертификат контроллера домена в хранилище keystore java	`sudo keytool -import -alias ald-cert -keystore 'поставьте полученное значение JAVA_HOME'/lib/security/cacerts -file ~/aldpro.der` где: `JAVA_HOME` - переменная среды, указывающая на каталог с установленным; `JAVA` (например, `JAVA_HOME="/usr/lib/jvm/java-11-openjdk-amd64/"`); `alias ald-cert` - псевдоним сертификата в хранилище ключей (присвоить имя в зависимости от ресурсной системы); `keystore cacerts` - имя файла хранилища для хранения сгенерированной пары ключей; `file ~/ca.der` – путь к импортируемому сертификату	
6	Перезапустите службу AeCA CA	`sudo systemctl restart aecaca`	

А.2 Поиск глобального идентификатора контроллера домена ALD PRO

В случае, если выпуск сертификата контроллера домена ALD PRO, происходит для нового субъекта и ресурсная система, содержащая субъект, для которого должен быть выпущен сертификат, не зарегистрирована в Центре сертификатов доступа, то для нахождения требуемого значения поля «objectGUID» шаблона выполните процедуру в соответствии с Таблица 3 от имени пользователя с правами root.

Таблица 3 – Поиск глобального идентификатора контроллера домена

№	Описание шага	Команда	Примечание (при необходимости)
1	Выполните команду для определения значения глобального идентификатора контроллера домена	`ipa host-show <hostname> --all | grep ipauniqueid`	где `[hostname]` – короткое имя контроллера домена.

А.2 Установка сертификата контроллера домена ALD PRO

Выполните процедуру интеграции сертификата контроллера домена ALD PRO в соответствии с таблицей 3 от имени пользователя с правами root.

Таблица 4 – Процедура установки сертификата контроллера домена ALD PRO

№	Описание шага	Команда	Примечание (при необходимости)
1	Скачайте цепочку сертификатов ЦС и выпущенный контейнер PKCS#12 для контроллера домена на АРМ	Любым удобным способом переместите контейнер PKCS#12 и цепочку сертификатов ЦС на АРМ с установленным контроллером домена	Выпуск сертификата контроллера ALD PRO произвести в соответствии с пунктом 4.4.7.1 «Центр сертификатов Aladdin Enterprise Certificate Authority» Руководства администратора RU.АЛДЕ.03.01.020-01 32 01-2
2	Просмотр установленной цепочки сертификатов	`ipa-cacert-manage list`	

3	В случае, если ранее на контроллер домена устанавливались цепочки сертификатов ЦС, удалите ранее установленную цепочку сертификатов	`ipa-cacert-manage delete псевдоним сертификата подчинённого ЦС`
		`ipa-cacert-manage delete псевдоним сертификата корневого ЦС`
		где псевдоним сертификата ранее получен на шаге 2, при помощи команды `list`	

4	Установите цепочку сертификатов выпускающего ЦС	`ipa-cacert-manage install «имя цепочки сертификатов».chain.pem`	
5	Убедитесь, что цепочка сертификатов установлена	`ipa-cacert-manage list`	

№	Описание шага	Команда	Примечание (при необходимости)
6	Обновите списки сертификатов	`ipa-certupdate`	
7	Установите выпущенный контейнер PKCS#12 для контроллера домена	`ipa-server-certinstall -k «имя контейнера».p12`	Команду необходимо выполнить под учётной записью администратора домена
8	Перезапустите сервис	`systemctl restart ipa`	
9	Обновите службы сертификации на клиентских ПК	`sudo su ipa-certupdate`	

ПРИЛОЖЕНИЕ Б. АРМ АДМИНИСТРАТОРА RED OS

Б.1 Установка «Мастера групповой настройки»

Выполните процедуру установки «Мастера групповой настройки» в соответствии с Таблица 5 от имени пользователя с правами root.

Таблица 5 – Процедуры установки «Мастера групповой настройки»»

№	Описание шага	Команда	Примечание (при необходимости)
1	Распакуйте архив, находясь в папке, где расположен пакет	`tar -xvf {имя файла} -C <путь распаковки архива>`	Инсталляционный rpm-пакет будет автоматически распакован по указанному пути
2	Установите МГН	`sudo ./install.sh`	Требуется доступ к репозиторию или диск с дистрибутивом ОС

Б.2 Групповая настройка сетевой двухфакторной аутентификации на АРМ доменных пользователей

Выполните процедуру групповой настройки сетевой двухфакторной аутентификации с помощью «Мастера групповой настройки» в соответствии с Таблица 6 от имени пользователя с правами root.

Таблица 6 – Процедуры групповой настройки двухфакторной аутентификации

№	Описание шага	Команда	Примечание (при необходимости)
1	Запустите ПО «Мастер групповой настройки» в графическом интерфейсе ОС, открыв главное меню	В открывшемся меню выберите язык интерфейса Мастера групповой настройки	
2	Введите настройки параметров сканирования сети	Введите ip-адрес домена, порт, логин и пароль учетной записи администратора с правами root, нажмите кнопку <Сканировать сеть>	Предварительно должен быть настроен доступ по ssh учетной записи с правами root к настраиваемому узлу
3	Проверьте статус найденных при сканировании узлов	В случае ошибки доступа к репозиторию проверьте доступ по ssh: ssh {логин администратора @доменное имя компьютера, к которому происходит подключение}	
4	При необходимости настройте доступ к репозиторию на узлах	На настраиваемом узле в консоли выполните команду: `nano /etc/ssh/sshd_config` В файле найдите и приведите строку к виду: `PermitRootLogin yes`	Рекомендуем выставлять данную настройку только на время пуско-наладочных работ. После окончания работ, рекомендуем вернуть 2х ступенчатую авторизацию в целях безопасности.
5	В мастере групповой настройки выберите узлы, для которых необходимо настроить	отметьте галочкой соответствующие узлы, выберите «Действие» - установить SL, нажмите кнопку <Продолжить>	

№	Описание шага	Команда	Примечание (при необходимости)
	двухфакторную аутентификацию		
6	Загрузите дистрибутивы и цепочку сертификатов подчиненного ЦС	В соответствующих полях укажите: путь к дистрибутивам SecurLogon, Единому клиенту JaCarta, введите ключ активации или выберите из .txt файла, добавьте цепочку сертификатов издающего центра сертификации и запустите установку	
7	Дождитесь окончания процесса настройки	В случае успешной установки – на выбранных узлах будет настроена сетевая двухфакторная аутентификация по сертификату на электронном ключе, выпущенному ЦС, цепочку сертификатов которого мы загрузили.	
8	Обновите службы сертификации для клиентской машины в домене ALD PRO	`ipa-certupdate`	
9	Перезагрузите АРМ		

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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