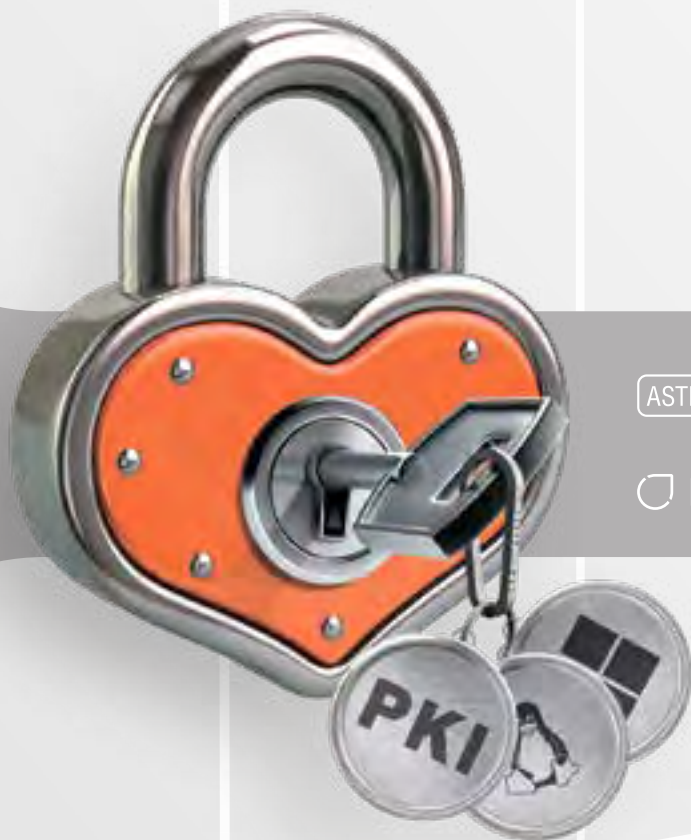


Корпоративный центр сертификации



ASTRA LINUX

РЕДОС

АЛЫН СП

РОСА

SberLinux OS

Aladdin Enterprise CA

- ▶ Построение доверенной PKI-инфраструктуры в гетерогенных средах
- ▶ Полнофункциональная замена Microsoft CA с бесшовной миграцией без остановки сервисов
- ▶ Автоматизация выпуска, распространения и гарантированная доставка сертификатов
- ▶ Поддержка российских криптоалгоритмов ГОСТ, международных стандартов RSA/ECDSA и др.
- ▶ Обеспечение соответствия требованиям регуляторов: приказы ФСТЭК России №117, 21, 31, 239

Сертифицирован ФСТЭК России (УД-4, №4835), на сертификации под гостайну
Положительное заключение ФСБ России (№ 149/3/4/79)
Включён в Единый реестр российского ПО (№14433, №25921)



Электронная
версия буклета

КОРПОРАТИВНЫЙ ЦЕНТР СЕРТИФИКАЦИИ

Что важно знать

Корпоративный центр сертификации (Certificate Authority, CA) – критический компонент ИТ-инфраструктуры любой современной организации. Он обеспечивает выпуск и управление цифровыми сертификатами, которые лежат в основе доверенного взаимодействия всех элементов инфраструктуры, а также:

- ▶ **Строгой аутентификации** пользователей и устройств (сертификаты SmartCard Logon).
- ▶ **Защиты подключений во внутренней** инфраструктуре (802.1x, RADIUS, mTLS).
- ▶ **Защищённого удалённого доступа** (ГОСТ-VPN).
- ▶ **Безопасности веб-сайтов** и корпоративных порталов.
- ▶ **Электронной подписи** документов и защищённой электронной почты (S/MIME).
- ▶ **Доверенной загрузки** и защиты конечных устройств.

Многие годы корпоративные сети при построении полноценной инфраструктуры открытых ключей (PKI) полагались на Microsoft CA – сервис, встроенный в Windows, который за более чем два десятилетия фактически стал отраслевым стандартом. Однако изменения технологического ландшафта и усиливающиеся требования регуляторов заставляют компании искать отечественные альтернативы.

Ключевая проблема: при миграции на российские операционные системы (Linux) организации сталкиваются с необходимостью замещения Microsoft CA, который является фундаментом безопасности в ИТ-инфраструктуре Microsoft.

... Без полноценной замены центра сертификации невозможно обеспечить единый высокий уровень доверия в информационной системе.

Что такое PKI и зачем нужен центр сертификации?

PKI (Public Key Infrastructure) – инфраструктура открытых ключей – это совокупность программных, аппаратных и организационных средств, обеспечивающих управление цифровыми сертификатами и криптографическими ключами.



Центр сертификации (CA) – центральный элемент PKI, который:

- ▶ Выпускает цифровые сертификаты для пользователей, устройств и ПО.
- ▶ Подтверждает подлинность сертификатов.
- ▶ Управляет их жизненным циклом (выдача, продление, отзыв, проверка статуса).

Без центра сертификации невозможно:

- ▶ Обеспечить строгую аутентификацию на основе криптографии.
- ▶ Создать единую доверенную среду, где каждый компонент проходит проверку перед получением доступа.
- ▶ Подтвердить подлинность пользователей, ПО и оборудования в информационной системе.

Основные риски при использовании Microsoft CA

Риск	Описание
Регуляторные ограничения	Указ Президента РФ №250 запрещает использование иностранных средств защиты информации в госорганах и ОКИИ
Фрагментация инфраструктуры	Отсутствие единого PKI в гетерогенной среде создаёт разрывы в безопасности
Невозможность аттестации	Информационные системы не могут быть аттестованы без сертифицированных средств криптографической защиты

Сравнение подходов к организации корпоративной PKI

Проблема импортозамещения центра сертификации заключается в том, что простое "выключение" Microsoft CA и попытка использовать альтернативные решения "вручную" приводит к потере управляемости, нарушению бизнес-процессов и рискам безопасности.

В таблице ниже показано, как различные подходы справляются с ключевыми задачами.

Критерий	Microsoft CA (иностранное ПО)	Самостоятельная сборка (OpenSSL, ручное администрирование)	Aladdin Enterprise CA
Автоматизация выпуска сертификатов	Да	Нет (ручные процессы)	Autoenrollment, SCEP, WSTEP, ACME
Бесшовная миграция с Microsoft CA	—	Нет	Без остановки сервисов
Включение в реестр ПО	Нет	Нет	№14433, №25921
Интеграция с доменными службами	Active Directory	Нет	Active Directory, РЕД АДМ, ALD Pro, Альт Домен, POCA Dynamic Directory
Поддержка ГОСТ-алгоритмов	Частично	Частично	Полная
Работа на российских ОС (Linux)	Нет	Требуется глубокой доработки	Полная поддержка
Сертификация ФСТЭК России	Нет	Нет	№4835 (УД-4)
Управление жизненным циклом сертификатов	Да	Частично	Полное
Централизованное управление	Да	Нет	Единая ролевая модель
Устранение уязвимостей	Нет	Нет (ручные процессы)	Да
Техническая поддержка	Нет	Нет	Поддержка от вендора согласно SLA

Aladdin Enterprise CA обеспечивает полноценную замену Microsoft CA с сохранением всех ключевых функций и автоматизации, сохраняет доменную автоматизацию выпуска и позволяет переводить инфраструктуру на российские ОС поэтапно, без остановки сервисов и снижения уровня безопасности.

► Aladdin Enterprise CA

Aladdin Enterprise CA (Aladdin eCA) — это сертифицированный корпоративный центр сертификации для Linux, полнофункциональная отечественная альтернатива Microsoft CA.

Aladdin Enterprise CA обеспечивает:

- Объединение отечественных компонентов ИТ-инфраструктуры в единый домен безопасности.
- Строгую аутентификацию пользователей, ПО и устройств в информационной системе.
- Защиту подключений к сетевым устройствам и маршрутизаторам (RADIUS, 802.1x).
- Электронную подпись документов и защищённую электронную почту (S/MIME).
- Безопасную работу ГОСТ-VPN с аутентификацией по сертификату.
- Защиту инфраструктур VDI и Kubernetes.
- Работу дочерних организационных структур (multitenancy) с изоляцией цепочек доверия.

Ключевые возможности

1. Бесшовная миграция с Microsoft CA

- Импорт ключа Центра Сертификации и шаблонов из Microsoft CA.
- Поддержка MS Active Directory и параллельная работа с действующим Microsoft CA.
- Возможность безопасного извлечения закрытых ключей.

2. Полноценная PKI-функциональность

- Автоматический выпуск, распространение и гарантированная доставка сертификатов (Autoenrollment).
- Поддержка протоколов SCEP, MS-WSTEP и ACME для распространения сертификатов на устройства.
- Публикация CRL/deltaCRL в LDAP-каталоги, OSCP-сервис проверки статуса.
- Выпуск одноразовых сертификатов для VDI и Kubernetes: ограниченный срок жизни, быстрый выпуск, исключение из CRL.
- Портал самообслуживания для пользователей.

3. Поддержка российской и зарубежной криптографии

- Российские: ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.
- Международные: RSA, ECDSA и др.

4. Гибкая архитектура

- Три ключевых компонента: Центр сертификации, Центр регистрации, Центр валидации.
- Поддержка нескольких издателей и иерархии.
- Геораспределённое развёртывание, резервирование компонентов.
- Распределение ролей и назначение полномочий.

5. Интеграция в гетерогенных средах

- Полная поддержка любых типов доменов: отечественных, open source и Microsoft.
- Поддержка российских ОС и виртуальных сред, развёртывание в Docker / Kubernetes.
- Интеграция с КриптоПро HSM.
- Поддержка средств многофакторной аутентификации JaCarta и Рутокен.
- Удобный API для интеграции с внешними приложениями.

Безопасность решения

Продукт спроектирован как защищённый сервис — это необходимо для компонента, который сам является источником доверия:

► Защита ключа Центра сертификации

Закрытый ключ может храниться в защищённом контейнере на диске или в аппаратном модуле (HSM).

► Разделение полномочий

Роли: Администратор ЦС, Оператор центра регистрации, Администратор аудита, Пользователь.

► Аудит

Операции событий жизненного цикла компонентов решения журналируются.

Поддерживается выгрузка событий в SIEM (syslog).

► Защита управления

Поддержка различных типов аутентификации на портале самообслуживания (сертификат, логин/пароль, Kerberos).

► Безопасность протоколов выпуска

SCEP применяется с защищёнными одноразовыми challenge-паролями и ограничением допустимых шаблонов. Реализованы протоколы WSTEP, ACME.

► Управление данными

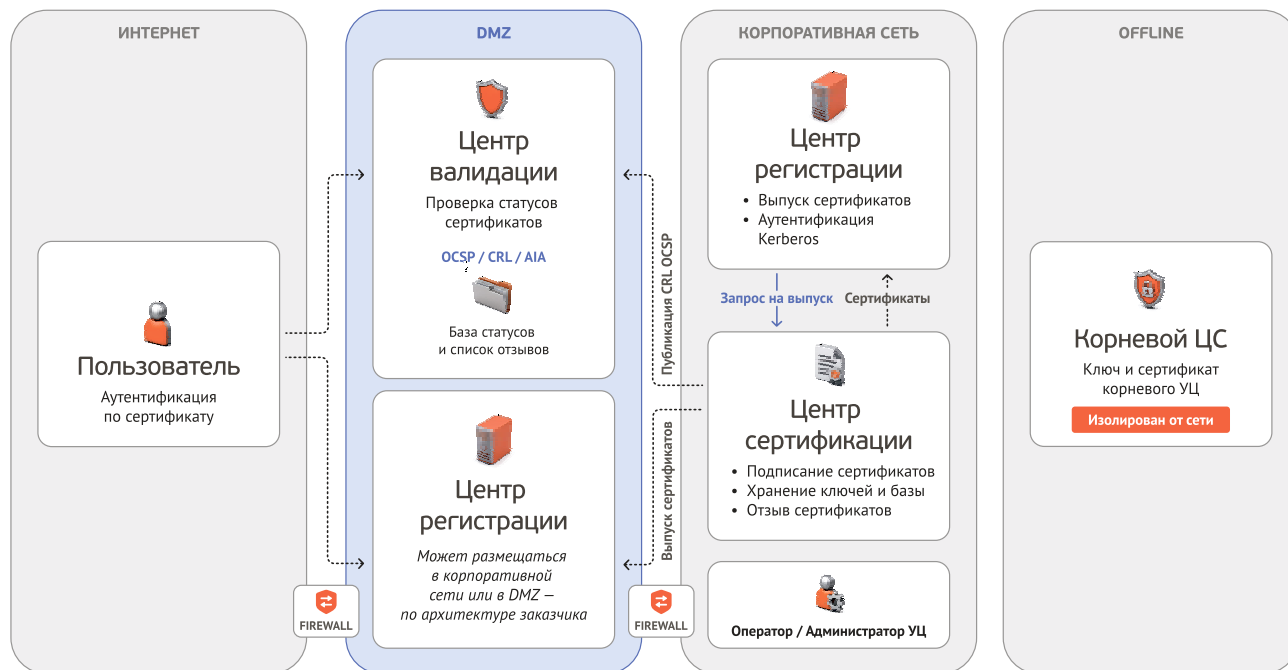
Получение данных из LDAP настраивается выборочно (состав атрибутов и соответствие полей субъектов).

Архитектура и отказоустойчивость

Архитектура решения

Aladdin Enterprise CA построен как набор трёх взаимодействующих комплексов — Центра сертификации, Центра регистрации и Центра валидации. Каждый комплекс включает серверную часть и веб-интерфейс и разворачивается на отдельном сервере: выпуск сертификатов, регистрация субъектов и проверка статусов разделены между независимыми узлами. Продукт одновременно подключается к нескольким доменным службам каталогов — от Microsoft AD до отечественных доменов, — объединяя гетерогенную инфраструктуру в единое пространство доверия.

Состав решения и связи его компонентов показаны на схеме ниже.



Отказоустойчивость на всех уровнях:

- HA Proxy распределяет нагрузку между узлами ЦВ и исключает единые точки отказа на веб-уровне.
- Кластер PostgreSQL с репликацией и арбитром сохраняет данные при отказе любого узла БД.

Компоненты

Центр регистрации — приём и проверка заявок, идентификация субъектов, взаимодействие со службами каталогов и протоколами, автоматический перевыпуск и распространение (autoenrollment). Резервируется по схеме балансировки и кластеризации.

Центр сертификации — выпуск сертификатов и CRL; ключ ЦС — в HSM.

Центр валидации — проверка статуса сертификатов (OCSP) и валидация цепочек для зависимых сервисов. Резервируется по схеме балансировки и кластеризации.

Балансировка и кластеризация

Каждый из компонентов eCA может объединяться в кластер с внешним балансировщиком нагрузки. Поддерживаются холодное резервирование (active-passive) и горячее (active-active); новые узлы добавляются клонированием виртуальной машины и переносом контейнера закрытого ключа, а при размещении ключей ЦС во внешних HSM все узлы кластера подключаются к одному аппаратному модулю. Общее состояние хранится во внешней СУБД (PostgreSQL, Postgres Pro или Jatoba), которая сама допускает кластерную конфигурацию, — отказ любого отдельного узла не останавливает выпуск и проверку сертификатов.

Высокая доступность и отказоустойчивость конфигурации реализована при помощи:

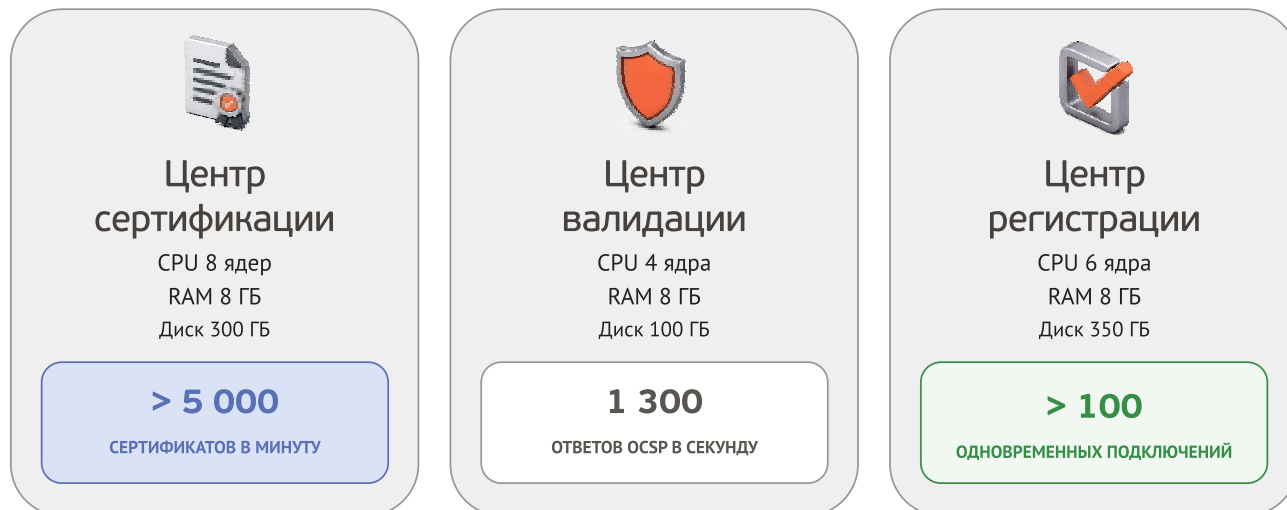
- резервирования всех компонентов приложений на площадках,
- геораспределённого развёртывания с несколькими точками публикации CRL/AIA,
- поддержки кластерной конфигурации баз данных,
- резервного копирования конфигурации и баз данных,
- мониторинга: health-check компонентов, метрики для систем мониторинга (Zabbix/Prometheus).

Производительность и масштабируемость:

Потребность в ресурсах определяется двумя параметрами — количеством выпускаемых сертификатов и числом одновременных подключений. Дальнейший рост нагрузки закрывается горизонтально — добавлением узлов в кластер, а экспорт метрик в Prometheus позволяет заранее видеть запас мощности и планировать расширение.

Типовые профили и требования к ресурсам показаны на схеме ниже.

Потребляемые ресурсы и производительность одного узла:



Горизонтальное масштабирование

Производительность растёт линейно — добавьте узлы в кластер для увеличения ёмкости отказоустойчивости. Каждый компонент поддерживает отказоустойчивую кластерную конфигурацию. Указанные характеристики — максимальная производительность одного узла, реальная ёмкость зависит от профиля нагрузки.

Производительность ЦС при выпуске большого количества сертификатов:

• Скорость выпуска сертификатов

PKCS#10, RSA-2048, ключ ЦС RSA-4096	78 rps
Throwaway RSA-2048	121 rps
PKCS#12 RSA-2048	41 rps
PKCS#12 ECDSA-256	54 rps

• Скорость отклика в UI-операциях при 1 млн сертификатах в БД

Отображение списка сертификатов	0,9 с
Поиск сертификата	0,8 с
Отзыв и генерация	0,9 с

• Рост объема БД на объем выпущенных сертификатов

500K		7 Гб БД
1 млн		14 Гб БД
3 млн		40 Гб БД

Соответствие нормативным требованиям

Aladdin Enterprise CA применяется для выполнения требований:

Нормативный акт	Область регулирования
Приказ ФСТЭК России №117	Защита информации в ГИС
Приказ ФСТЭК России №21	Защита персональных данных в ИСПДн
Приказ ФСТЭК России №31	Защита информации в АСУ ТП
Приказ ФСТЭК России №239	Защита информации в ОКИИ
Приказ ФСБ России №378	О требованиях к использованию СКЗИ для защиты ПДн
Указ Президента РФ №250	Запрет использования иностранных СЗИ
ФЗ-152	О персональных данных
ФЗ-187	О безопасности КИИ
Постановление Правительства РФ №1236	О запрете иностранного ПО в госорганах

Технические характеристики

Параметр	Значение
Сертификация	ФСТЭК России УД-4 №4835
Реестры ПО	Единый реестр российского ПО: №14433 (08.08.2022) и №25921 (28.12.2024)
Поддерживаемые ОС	Российские ОС на базе Linux: Astra Linux, РЕД ОС, Альт, SberLinux OS, РОСА
Поддерживаемые домены	РЕД АДМ, ALD Pro, Альт Домен, Dynamic Directory, SambaDC, FreeIPA, Microsoft AD (для миграции и обратной совместимости)
Среда развёртывания	Физические и виртуальные серверы, Docker, Kubernetes, российские среды контейнеризации
Поддерживаемые криптопровайдеры	Встроенные в ОС, КриптоПРО CSP (заключение о корректности встраивания СКЗИ № 149/3/4/79)
Криптоалгоритмы	ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, RSA (2048/4096), ECDSA (256, 384, 521)
Протоколы	SCEP, MS-WSTEP, REST API, LDAP, OCSP, CRL, ACME
Интеграции	HSM КриптоПро, средства 2ФА/3ФА и ЭП – JaCarta, Рутокен

Управление жизненным циклом средств аутентификации и ЭП, учёт СКЗИ, SSO осуществляется с помощью Aladdin JMS/JIP.

О компании

"Аладдин" – ведущий российский разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов.

Компания работает на рынке с апреля 1995 г. (31 год).

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, во многих крупных организациях и Федеральных структурах – стандартом де-факто.

Компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Минобороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной, производство, поставку и поддержку продукции в рамках гособоронзаказа.

Большинство продуктов компании имеют сертификаты соответствия ФСТЭК, ФСБ, Минобороны России и могут использоваться при работе с гостайной со степенью секретности до "Совершенно Секретно".

С 2012 г. в компании внедрена система менеджмента качества продукции (СМК), ежегодно проводится внешний аудит, имеются соответствующие сертификаты ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и ГОСТ РВ 0015.002-2020 на соответствие требованиям российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Ключевые компетенции:

- ▶ Аутентификация:
 - Подготовлено 14 национальных стандартов по идентификации и аутентификации;
 - Выпущено учебное пособие "Аутентификация – теория и практика";
 - Защищена докторская диссертация.
- ▶ Доверенная загрузка и "стерилизация" импортных ARM-процессоров с TrustZone.
- ▶ Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, JavaCard.
- ▶ Биометрическая идентификация и аутентификация по отпечаткам пальцев (Match On Card/Device).
- ▶ PKI для Linux и российских ОС.
- ▶ Прозрачное шифрование на дисках, флеш-накопителях.
- ▶ Защита баз данных.
- ▶ Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и электронных сервисов.

