Aladdin Enterprise CA

Что нового в импортозамещении Microsoft CA

Денис Полушин

Руководитель направления PKI

Павел Данилов

Ведущий аналитик

Виды аутентификации и доверие субъектов ИС

- Основа доверия в ИС – АУТЕНТИФИКАЦИЯ
  - Это процедура "установление подлинности” (докажи то, что ты - это ты)
  - ИАФ – определенная ФСТЭК мера защиты, используемая при аттестации ИС
- Как обеспечивается аутентификация (доверие)
  - **Простая** (для предоставления доступа, однофакторная, односторонняя)
    - Логин / Пароль
  - **Усиленная** (для предоставления доступа, двухфакторная, одно- или двухсторонняя)
    - OTP (с хранением секретного ключа на токене или смартфоне)
    - U2F (стандарт FIDO Alliance - "Мир без паролей")
  - **Строгая** (для установления доверительных отношений в ИС и предоставления доступа, двухсторонняя, с использованием криптографии, PKI и сертификатов)
    - Машинные сертификаты (протокол 802.1x)
    - Программные сертификаты (для использования только доверенного ПО)
    - Пользовательские сертификаты (для 2ФА пользователей в ИС)
      - а) сертификат на КН (JaCarta PKI) с неизвлекаемым закрытым ключом;
      - б) сертификат на компьютере в личном хранилище пользователя

ГОСТ Р 58833-2020
Защита информации
ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

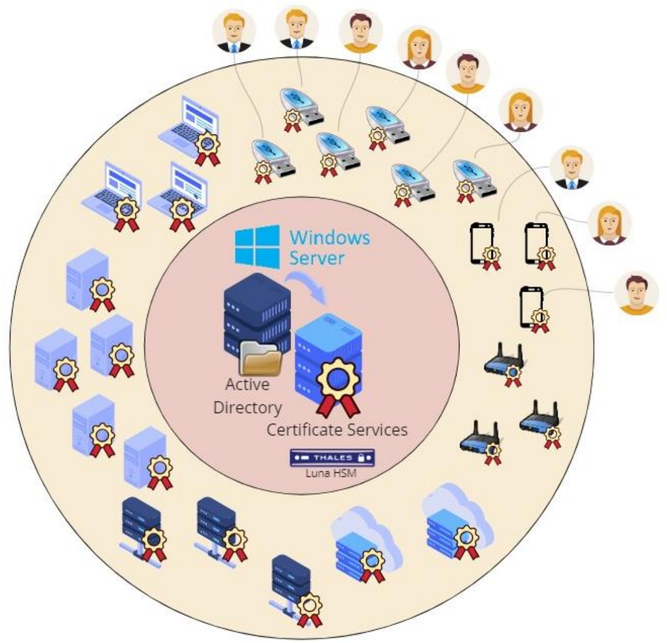
Проект приказа ФСТЭК России

regulation.gov.ru
ID проекта: 153633

Корпоративная PKI – система строгой аутентификации

До недавнего времени типовое решение для корпоративного PKI

Windows Server **Microsoft CA = Microsoft Certificate Services**



За 20+ лет

- тесная интеграция с каталогом пользователей
- сценарии автоматизации (Enrollment Agent, NDES, InTune)
- интеграция с HSM Thales
- развитое комьюнити, учебные центры
- must-have знания и навыки у любого сисадмина

Настоящее время:

Microsoft остановил деятельность в РФ, прекратил продлевать лицензии

Указ Президента РФ №250 от 01.05.2022 г. о запрете использования СЗИ из недружественных стран.

Отраслевые требования, приказы, постановления и стандарты по обеспечению безопасности обрабатываемой информации.

Aladdin Enterprise CA: основа отечественной PKI

Aladdin Enterprise CA

В Реестре отечественного ПО 14433, 25921

Сертификат ФСТЭК России, УД-4

№ 4835

Поддержка отечественных ОС и доменной инфраструктуры

РЕДОС **РЕД АДМ**

alt linux

ALD Pro ASTRALINUX special edition

Бандл «Домен безопасности» AXOFT

Базовая функциональность PKI

- Построение иерархии PKI
- Управление ЖЦ сертификатов
- Шаблоны сертификатов
- RSA / ECDSA / **ГОСТ**
- CRL DP, AIA, OCSP
- Защита ключа ЦС **при помощи HSM**
- **SCEP** для распространения сертификатов

Идентификация и аутентификация

- Строгая для администраторов и операторов
- **Kerberos**

Ролевая модель, полномочия

- Физическое разделение компонентов (ЦС, ЦР, ЦВ)
- Роль администратора, оператора, пользователя
- Полномочия на домен, группы, подразделения
- Полномочия на шаблоны
- **Автоматическое и ручное подтверждение заявок**

Задачи обслуживания

- Резервное копирование
- Мониторинг
- Журнал событий безопасности
- Интеграция с SIEM и syslog
- Кластер отказоустойчивости и балансировки

Бесшовная миграция с Microsoft CA

- **Импорт ключа ЦС из MS**
- Импорт шаблонов MS
- Интеграция с Active Directory
- Публикация сертификатов и CRL
- bypass с действующим MSCA
- **WSTEP для автоматического распространения**

Другие преимущества

- REST API для интеграции с внешними системами
- Меры защиты
- Отсутствие ВУ и НДВ

Aladdin Enterprise CA: где рекомендуется использовать

Крупные предприятия со сложной ИТ-инфраструктурой и большой базой пользователей.

Им PKI поможет не только усилить безопасность за счет строгой аутентификации, но и облегчить управление ею.

Отрасли с высоким уровнем регулирования, объекты КИИ.

Финансы, здравоохранение, энергетика, государственное управление и оборона – там, где работают с конфиденциальными данными и предъявляют строгие требования к соблюдению нормативных требований.

Электронная коммерция и онлайн-услуги.

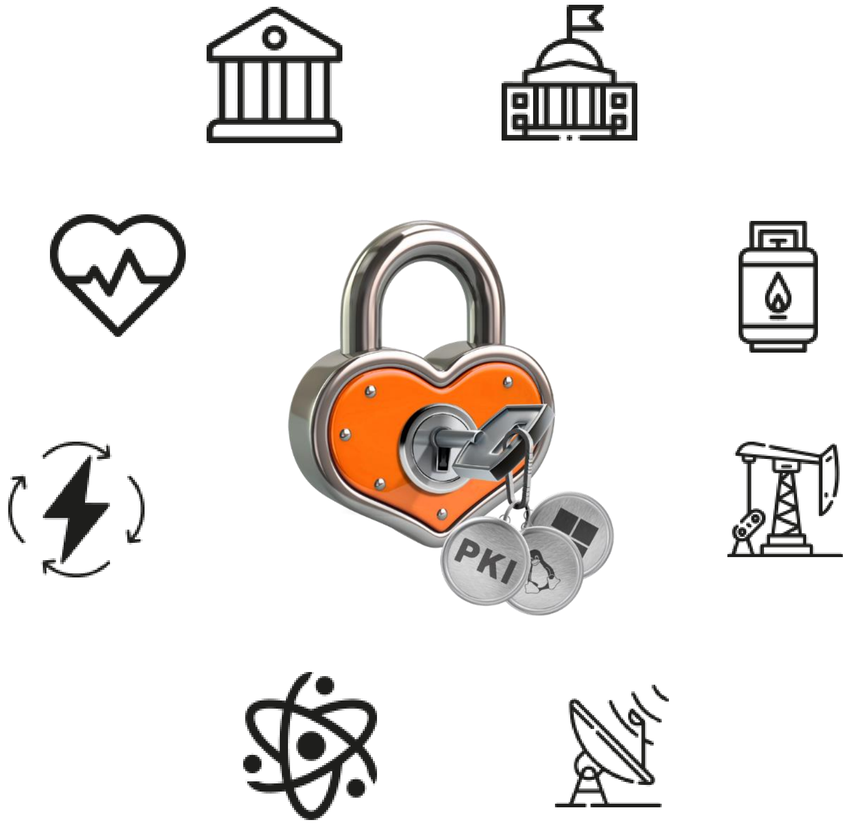
Компаниям, занимающимся онлайн-транзакциями, платформами электронной коммерции и цифровыми услугами, следует использовать PKI для обеспечения безопасности данных клиентов, защиты онлайн-транзакций и установления доверия со своими пользователями.

Транснациональные компании.

Компании, работающие в разных странах и нуждающиеся в безопасной связи и обмена данными между своими филиалами или с партнерами, как правило, используют PKI.

Поставщики облачных услуг.

Компании, предоставляющие облачные услуги, могут повысить безопасность своих платформ, внедрив PKI для защиты данных клиентов, аутентификации пользователей и защиты каналов связи.

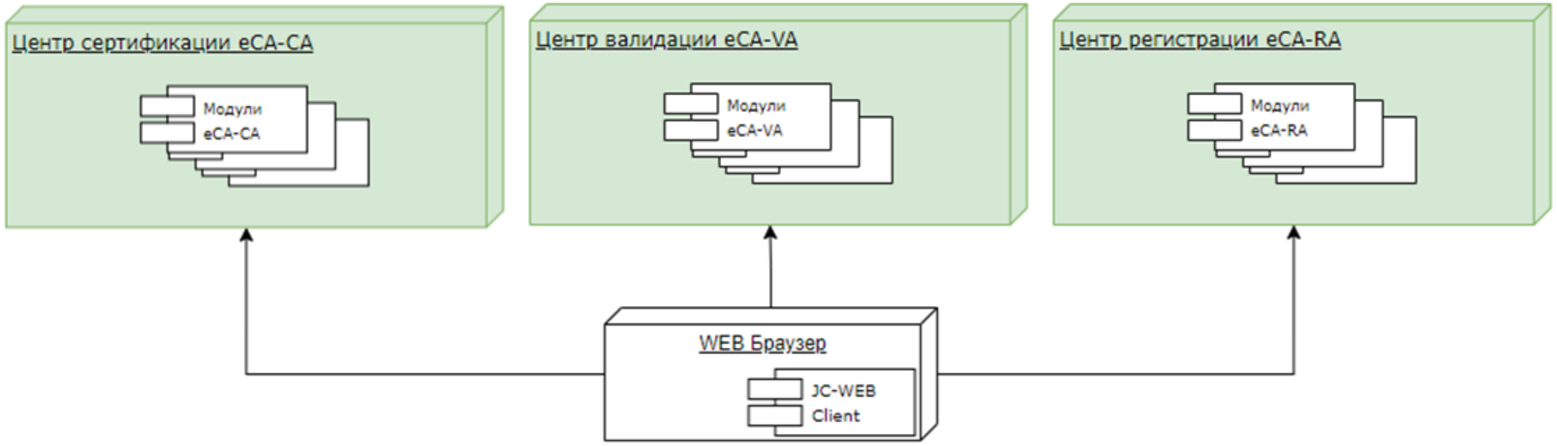


Aladdin Enterprise CA: архитектура решения

Aladdin Enterprise CA

Центр сертификации уровня Enterprise

Для среднего и крупного бизнеса



Центр сертификации

- Ядро продукта;
- Управление ЖЦ сертификатов;
- Шаблоны;
- Интеграция с доменом;
- HSM;

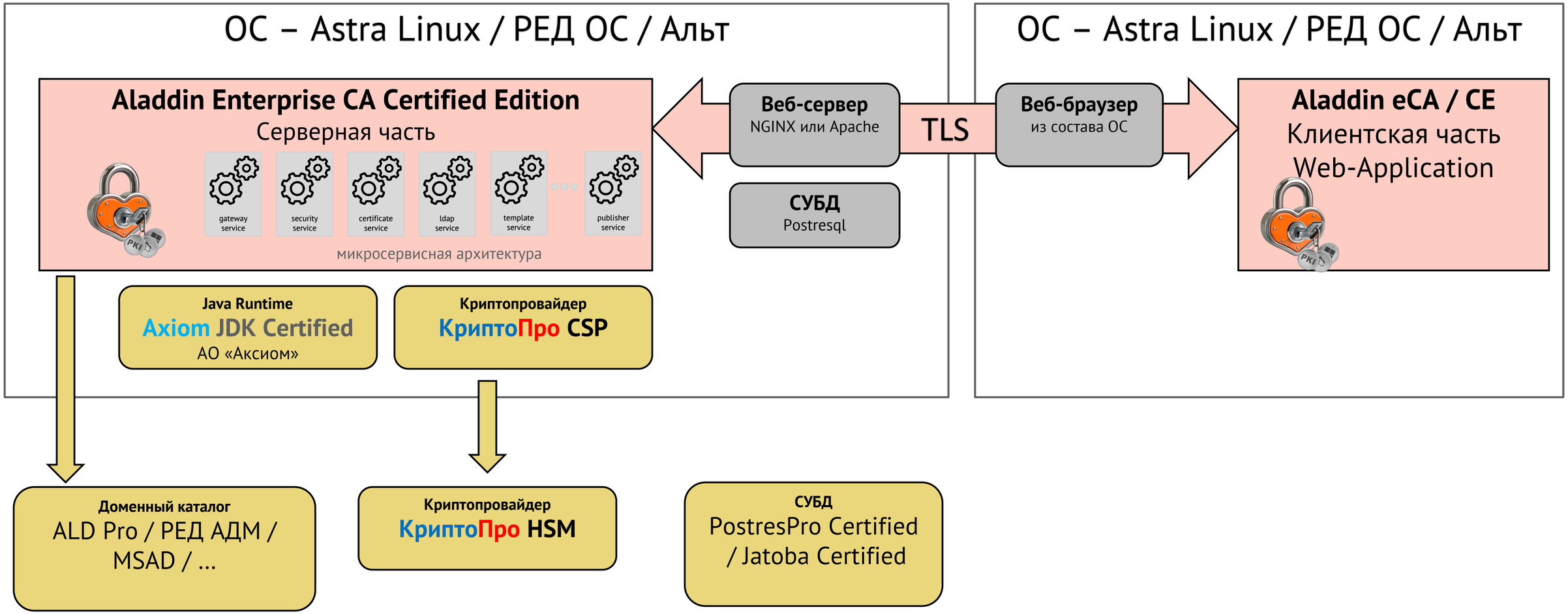
Центр валидации

- CRL DP;
- OCSP;
- AIA;
- Реестр сертификатов.

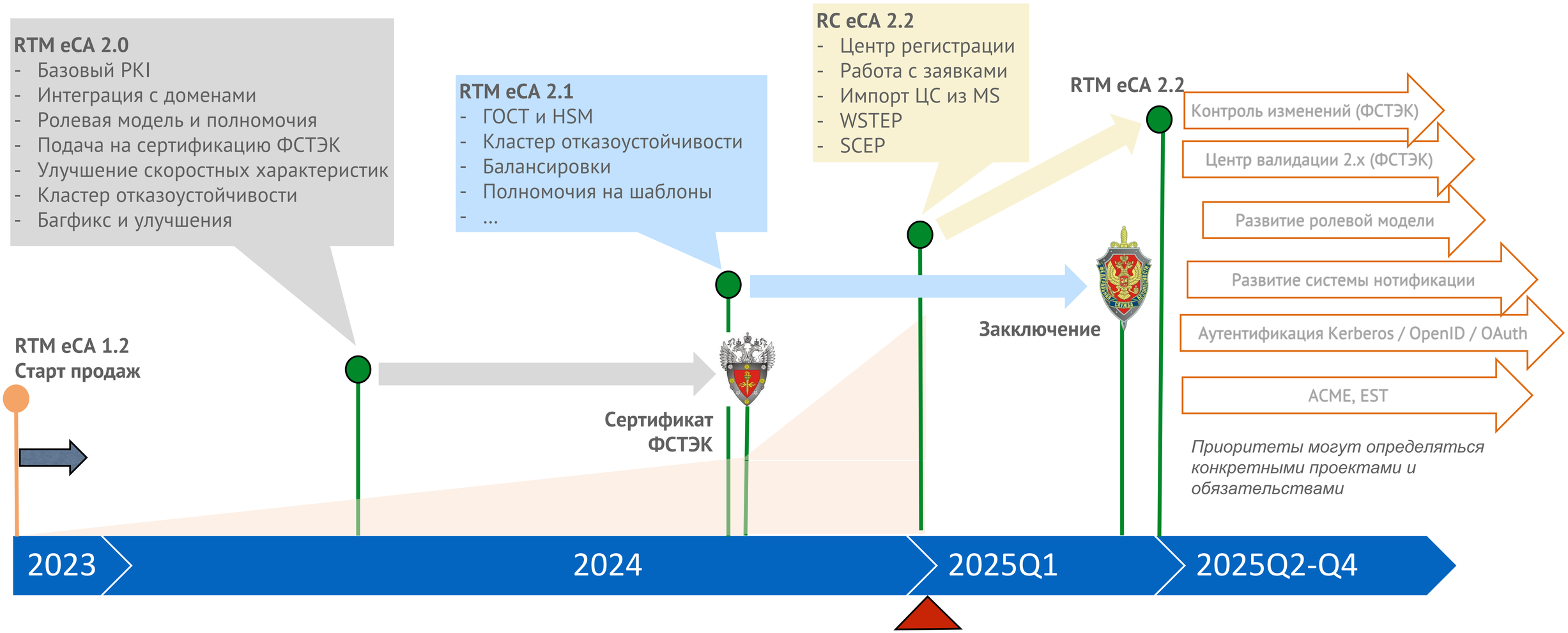
Центр регистрации

- Подключение пользователей;
- Заявки на сертификат
- Подтверждение заявок;
- Автоматизация;
- SCEP, ACME, MS-WSTEP;
- Единая ролевая модель;

Aladdin Enterprise CA: среда функционирования



Aladdin Enterprise CA : текущее состояние и развитие



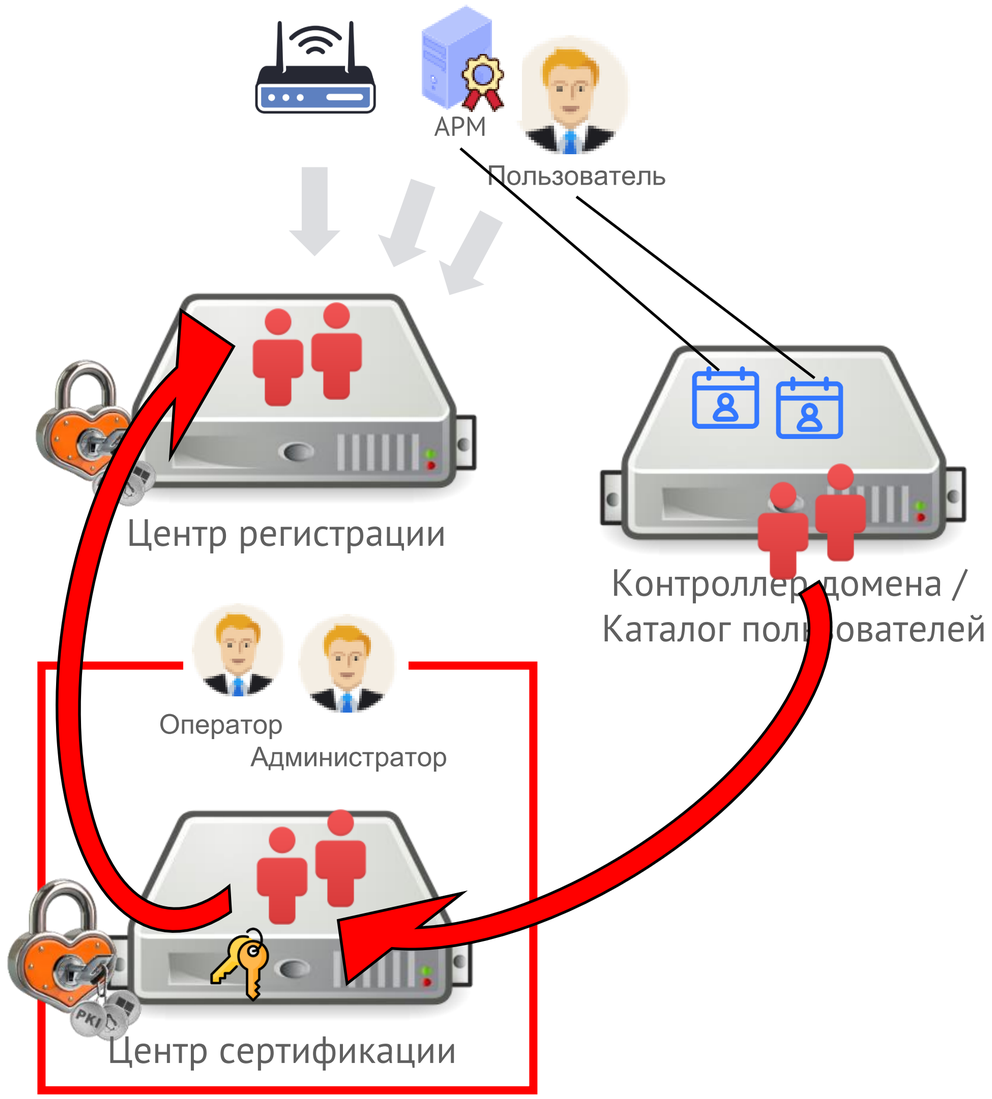
Сценарии демонстрации Aladdin Enterprise CA

1. Инициализация ЦС: алгоритмы ГОСТ, место хранения – HSM
2. Инициализация ЦС: корневой и подчиненный на одном сервере
3. Инициализация ЦС: импорт ключа из MS CA, и сразу на HSM
4. Компоненты, ролевая модель и полномочия на субъекты, группы и шаблоны
5. Обзор компонента «Центр регистрации», заявки, правила выпуска
6. Заявка на пользовательский сертификат от владельца, подтверждение от оператора
7. Заявка на серверный сертификат от сисадмина, подтверждение от администратора ИБ
8. Автоматическое распространение сертификатов через политики MS AD (протокол WSTEP)
9. Автоматическая доставка сертификата на устройство (протокол SCEP)

Сценарий 1 - 3. Варианты инициализации Центра сертификации

	Ключ	Алгоритм	Хранилище ключа	Описание
1	Новый	RSA / ECDSA	Локальное	Обычный сценарий
2	Новый	ГОСТ	Локальное	Использование алгоритмов ГОСТ
DEMO 3	Новый	ГОСТ	HSM	**Алгоритмы ГОСТ на HSM**
DEMO 4	Новый	RSA / ECDSA	Изъят в надежное хранилище	**Корневой и подчиненный на одном сервере**
5	Новый	RSA	HSM	Корпоративный PKI RSA на HSM
6	Из MS CA	RSA	Локальное	Миграция с MS CA
7	Из MS CA	RSA	Изъят в надежное хранилище	Миграция MS Standalone Root CA и MS Enterprise CA на один сервер
DEMO 8	Из MS CA	RSA	Импорт в HSM	**Миграция с MS CA с импортом на HSM**
9	Существующий	RSA / ECDSA	Импорт в HSM	Обновление с 2.0 Или дозакупка HSM

Сценарий 4. Центр регистрации и единая ролевая модель



Управление учетными записями и их полномочиями осуществляется в Центре сертификации

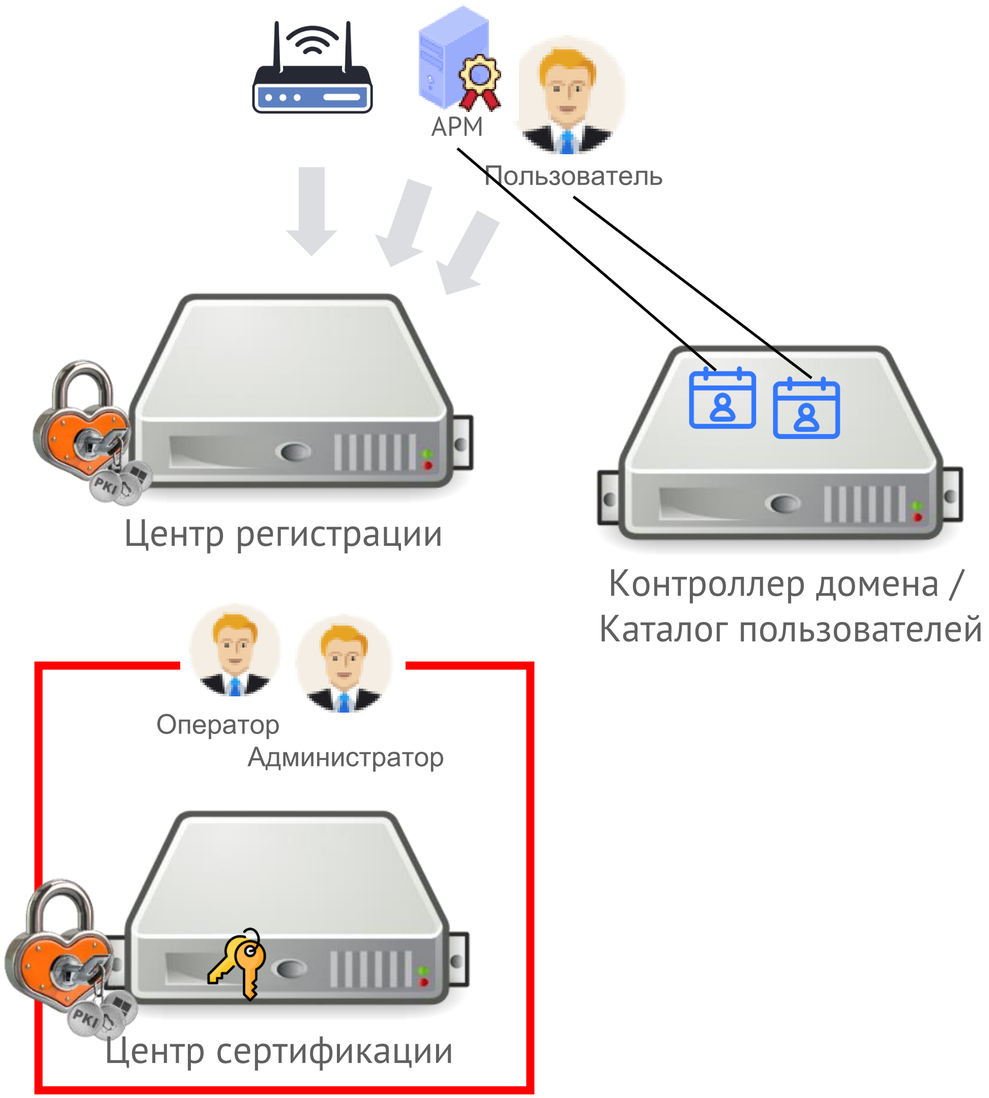
Привилегированный пользователь домена – он же Оператор всего eCA с определенными полномочия на группы, на пользователей и на шаблоны

Распространяются на подключенные Центры регистрации

Сценарий демонстрации:

1. В Центре сертификации создать оператора
2. Задать полномочия на субъекты и шаблоны
3. Убедиться, что созданная учетная запись появилась в Центре регистрации

Сценарий 5. Обзор компонента «Центр регистрации»



Компонент для обеспечения сертификатами непосредственно субъектов информационной системы.

Обеспечивает физическую изоляцию ключевого компонента «Центр сертификации»

Выполняет аутентификацию субъектов (пользователей, устройств)

Выдает сертификаты на основании политик или через подтверждение

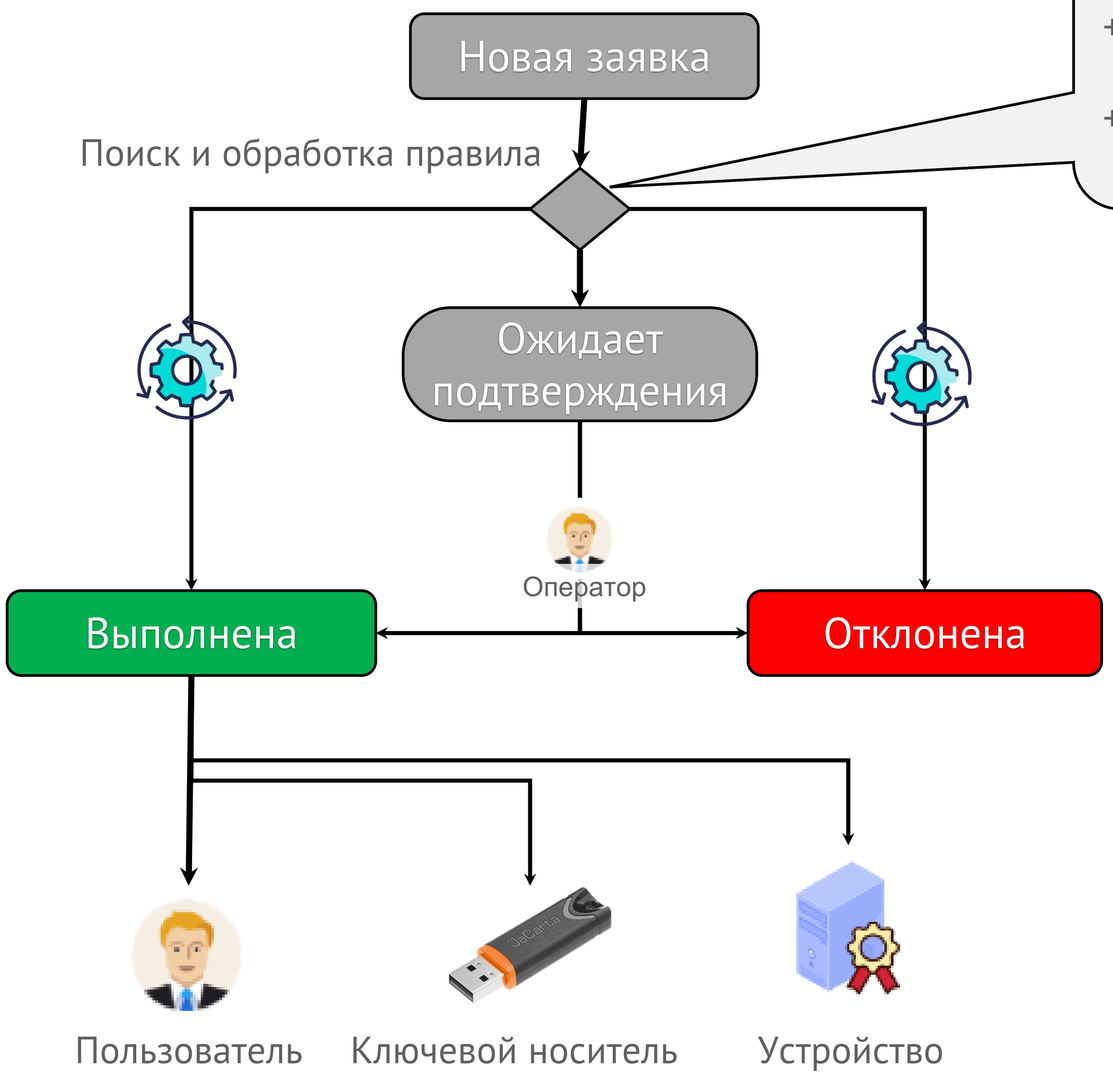
Лицензируется число подключений к Центру сертификации:

- Базовое исполнение – одно
- Стандартное исполнение – два
- Корпоративное исполнение - неограниченно

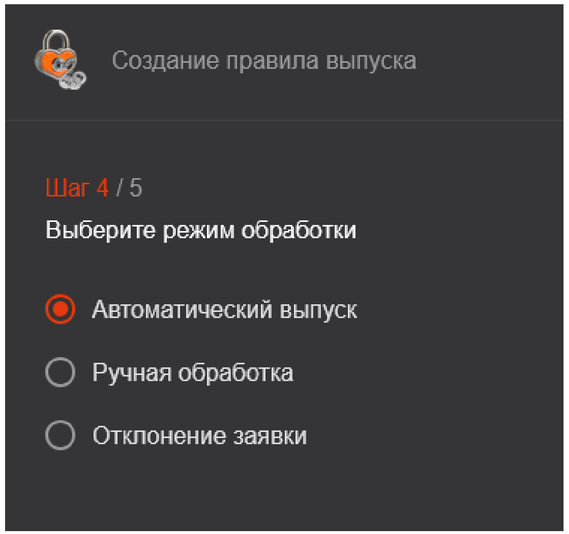
Сценарий демонстрации:

- Обзор веб-интерфейса администратора

Сценарий 6. Заявка на пользовательский сертификат от владельца, подтверждение от оператора

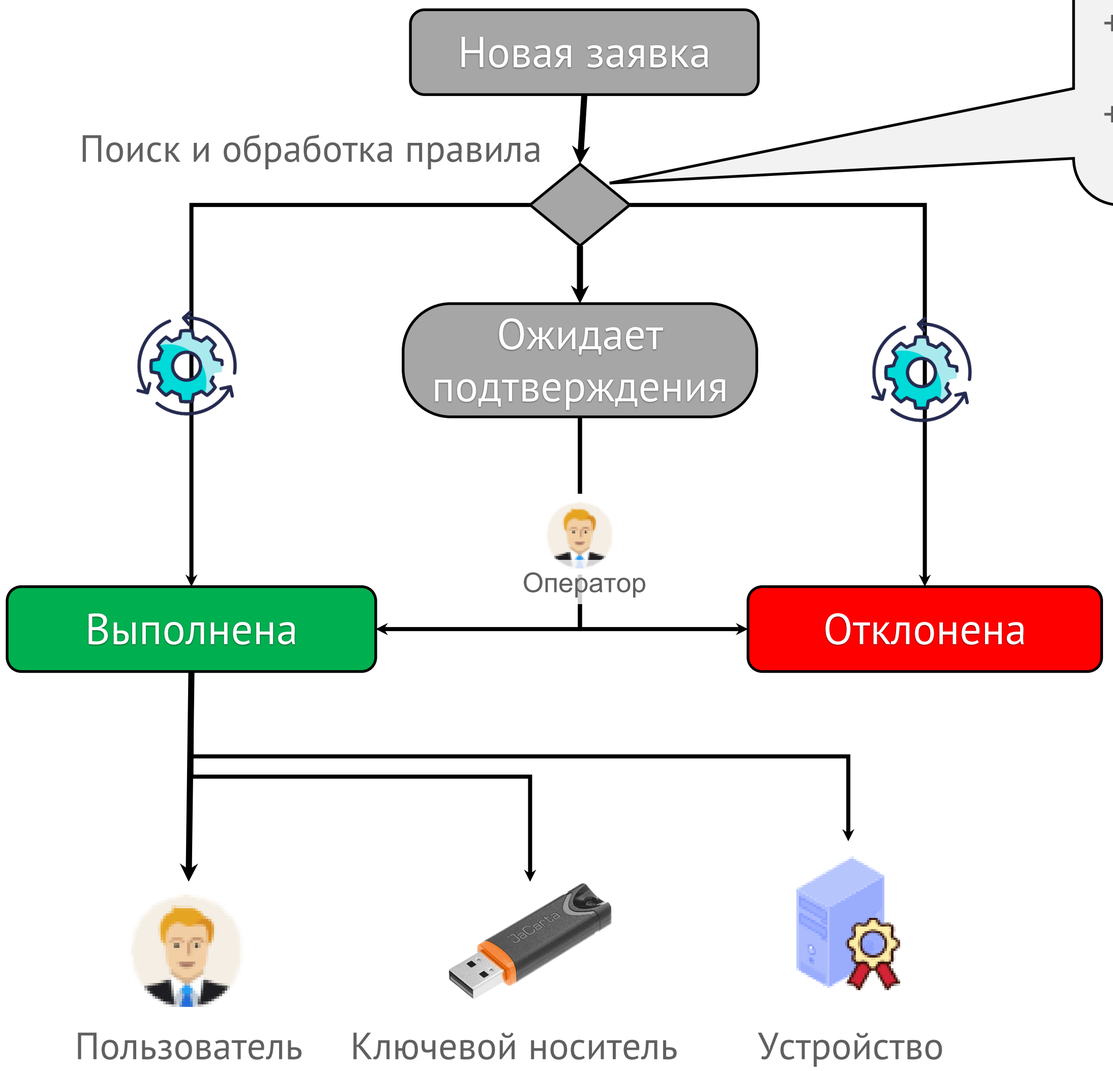


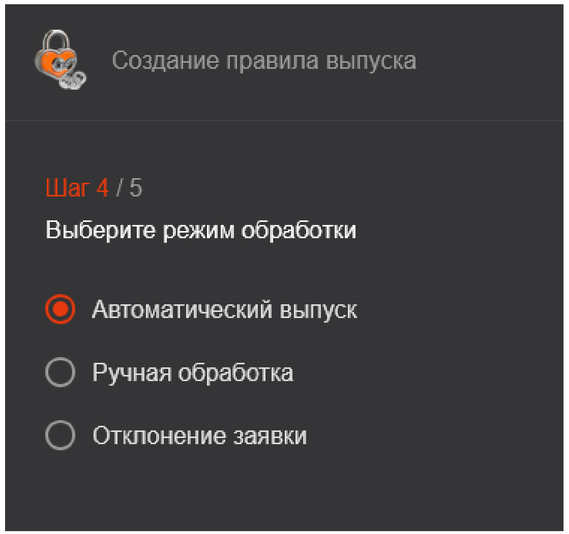
Условия срабатывания правила:
+ Инициатор заявки входит в список
  ИЛИ входит в группу из списка
+ Шаблон в заявке входит в список



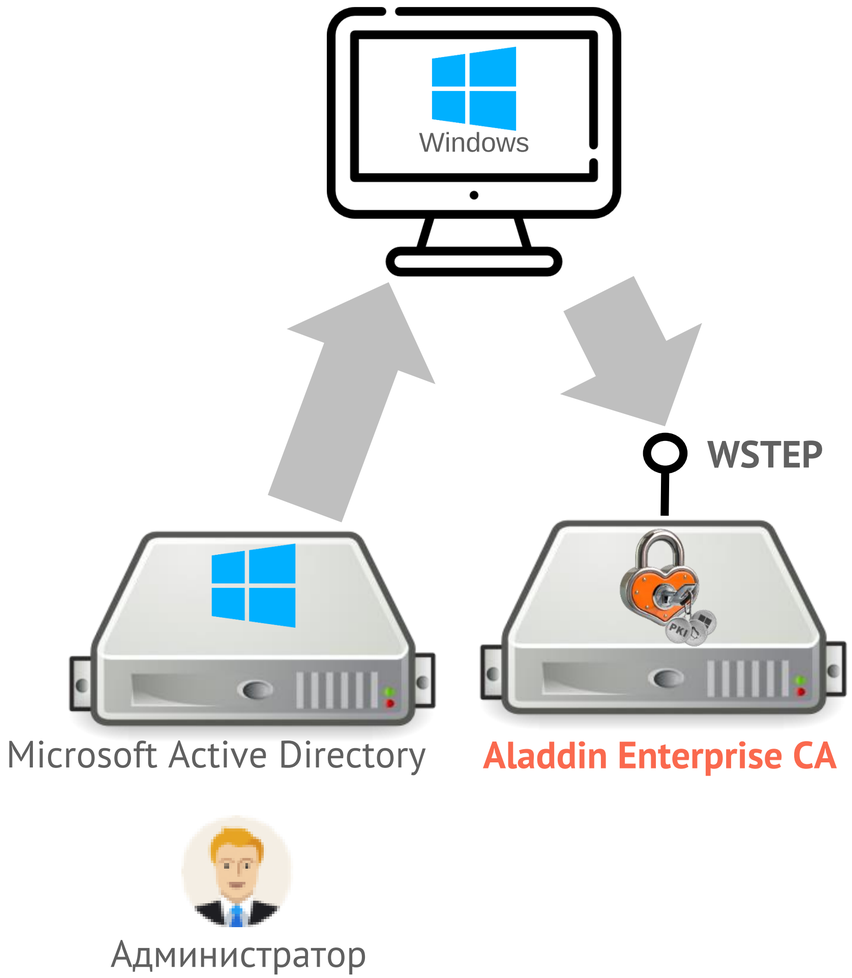
Сценарий 7. Заявка на серверный сертификат от сисадмина, подтверждение от администратора ИБ

Условия срабатывания правила:
+ Инициатор заявки входит в список
  ИЛИ входит в группу из списка
+ Шаблон в заявке входит в список





Сценарий 8. Автоматическое распространение сертификатов через политики MS AD при помощи протокола WSTEP



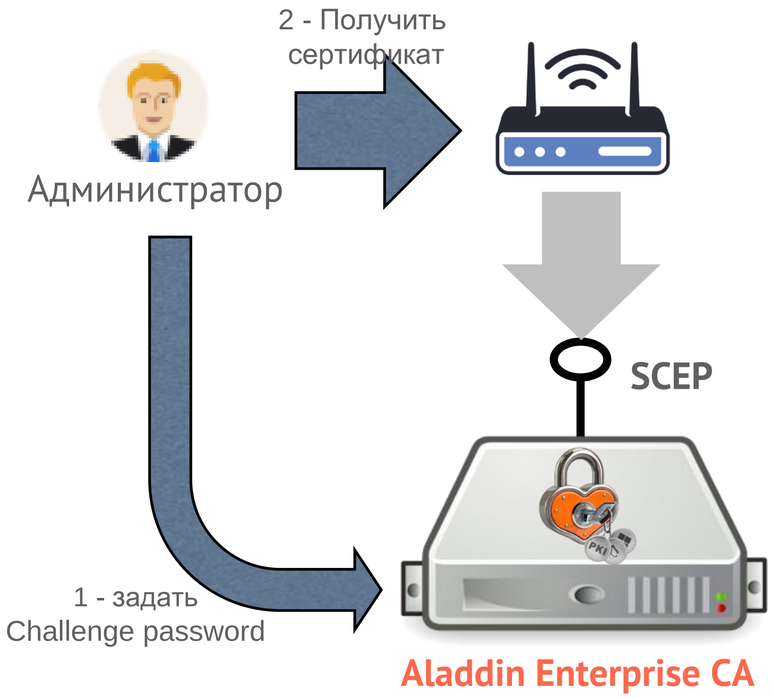
WSTEP – проприетарный протокол, разработанный Microsoft, описан в документации MSDN

Предназначен для формирования сертификатов на основании политик Microsoft AD

Сценарий демонстрации:

1. Администратор в MS AD создает политику распространения сертификатов
2. Пользователь первый раз входит в ОС на клиентской машине
3. АРМ пользователя автоматически получает сертификат в реестр.

Сценарий 9. Автоматическая доставка сертификата на устройство (протокол SCEP)



SCEP – стандартный протокол (RFC 8894), изначально разработанный CISCO для доставки сертификатов на устройства.

В составе Microsoft CA реализован в виде отдельного сервиса NDES (Network Device Enrollment Service).

Преимущественно полуавтоматический

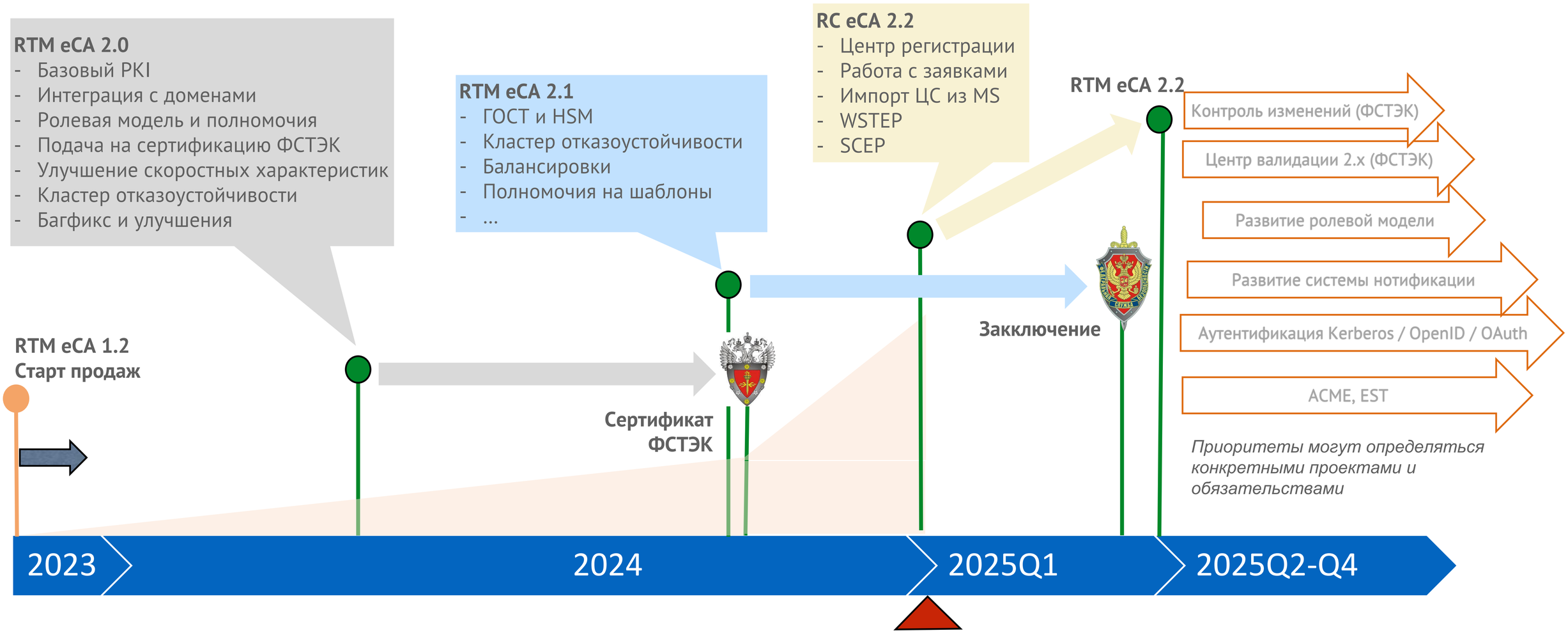
Сценарий демонстрации:

1. Администратор в Центре регистрации настраивает правило выпуска для всех субъектов
2. Администратор в Центре регистрации создает профиль для обработки SCEP-пакетов
3. Администратор в Центре регистрации задает challenge password для выпуска сертификатов по SCEP-протоколу
4. Администратор инициирует сценарий получения сертификата на устройстве

Сценарии демонстрации Aladdin Enterprise CA

1. Инициализация ЦС: алгоритмы ГОСТ, место хранения – HSM
2. Инициализация ЦС: корневой и подчиненный на одном сервере
3. Инициализация ЦС: импорт ключа из MS CA, и сразу на HSM
4. Компоненты, ролевая модель и полномочия на субъекты, группы и шаблоны
5. Обзор компонента «Центр регистрации», заявки, правила выпуска
6. Заявка на пользовательский сертификат от владельца, подтверждение от оператора
7. Заявка на серверный сертификат от сисадмина, подтверждение от администратора ИБ
8. Автоматическое распространение сертификатов через политики MS AD (протокол WSTEP)
9. Автоматическая доставка сертификата на устройство (протокол SCEP)

Aladdin Enterprise CA : текущее состояние и развитие



Спасибо за внимание ☺ Вопросы?

Центр компетенций Аладдин

Разработаем план импортозамещения

и поможем его реализовать

Помощь в построении системы 2ФА на базе отечественных ОС

+ Инфраструктура открытых ключей (PKI)
+ Удалённое подключение сотрудников
+ Централизованное управление защищёнными носителями информации

Интеграция системы 2ФА в ИТ-инфраструктуру заказчика

+ Обеспечение связи с доменами на базе РЕД АДМ, ALD Pro и др.
+ Обеспечение связи с системами IdM

Помощь в миграции инфраструктуры с Windows на Linux

+ Разработка плана миграции на базе готовых отработанных методик

Страница продукта
https://aladdin-rd.ru/catalog/aladdin-eca/

Партнерский отдел
partners@aladdin.ru

Денис Полушин
d.polushin@aladdin.ru

Павел Данилов
p.danilov@aladdin.ru

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.

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

Компания имеет все необходимые лицензии ФСТЭК, ФСБ 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 требованиями российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Ключевые компетенции

- Аутентификация
  - Подготовлено 7 национальных стандартов по идентификации и аутентификации (ГОСТ 58833-2020, ГОСТ Р 70262-2022)
  - Выпущено учебное пособие "Аутентификация – теория и практика"
  - Защищена докторская диссертация
- Доверенная загрузка и технология "стерилизации" импортных ARM-процессоров с TrustZone
- Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, смарт-карт, 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 и технология "опровославливания" зарубежных СУБД
- Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и эл. сервисов.