Что вместо Microsoft CA?

Повышаем уровень доверия в банковской инфраструктуре

Денис Полушин
Руководитель направления PKI

Василий Перфильев
Ведущий инженер

Виды аутентификации и доверие субъектов ИС

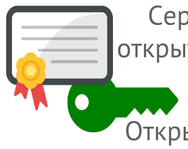
- Основа доверия в ИС – АУТЕНТИФИКАЦИЯ
  - Это процедура "установление подлинности" (докажи то, что ты - это ты)
  - ИАФ – определенная ФСТЭК мера защиты, используемая при аттестации ИС
- Как обеспечивается аутентификация (доверие)
  - **Простая** (для предоставления доступа, однофакторная, односторонняя)
    - 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

Проект приказа ФСТЭК России

ГОСТ Р 58833-2020
Защита информации
ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Строгая аутентификация = Public Key Infrastructure (де-факто)

Корень доверия



Сертификат открытого ключа

Открытый ключ

Центры сертификатов доступа

Субъекты аутентификации (строгой)

Закрытый ключ

Корневой Центр сертификации

В сейфе отключен от сети

Издающий ЦС

Сервер в контролируемой зоне

HSM

Требования безопасности информации (ИАФ, УПД, РСБ ОЦЛ. ...)

Отказоустойчивость, высоконагруженность

Интеграция с доменом, IDM, прикладными системами

Удобство обслуживания сотен тысяч субъектов

Аутентификатор

Аутентификатор

Аутентификатор

Аутентификатор

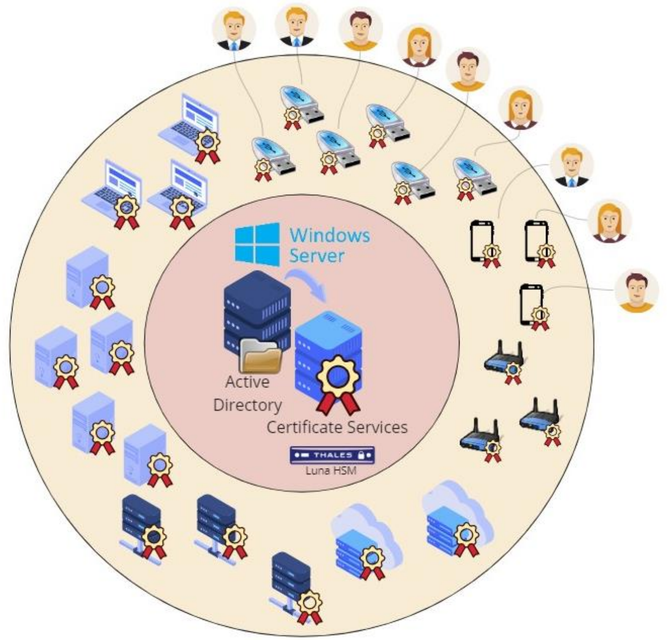
Ключевой носитель
Нельзя извлечь!

Защищенное хранилище ОС

На чем построена Корпоративная PKI в банковских ИС?

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
- С 1 января 2025 года все СЗКО должны перейти на отечественные решения.
- П. 6 Указа Президента РФ №250 от 01.05.2022 г. о запрете использования СЗИ из недружественных стран.
- Повышенные требования по обеспечению безопасности обрабатываемой информации в финансовом секторе (683-П, 684-П Банка России, стандарт ГОСТ 57580, приказ №321 Минкомсвязи

Aladdin Enterprise CA: основа отечественной PKI

Aladdin Enterprise CA

В Реестре отечественного ПО №14433

Сертификат ФСТЭК России, УД-4

№ 4835

Поддержка отечественных ОС и доменной инфраструктуры

РЕДОС · ASTRALINUX special edition · alt linux · ALD Pro · РЕД АДМ

Базовая функциональность PKI

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

Идентификация и аутентификация

- Строгая для администраторов и операторов
- Kerberos – для пользователей

Ролевая модель, делегирование полномочий

- Роль администратора, оператора
- Полномочия на домен, группы, подразделения
- Полномочия на шаблоны

Задачи обслуживания

- Резервное копирование
- Мониторинг
- Журнал событий безопасности
- Интеграция с SIEM и syslog
- Кластер отказоустойчивости
- Балансировка CRL DP, OCSP

Бесшовная миграция с Microsoft CA

- Импорт шаблонов
- Интеграция с Active Directory
- bypass с действующим MSCA

Другие возможности

- REST API
- Меры защиты
- Тесты на 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.

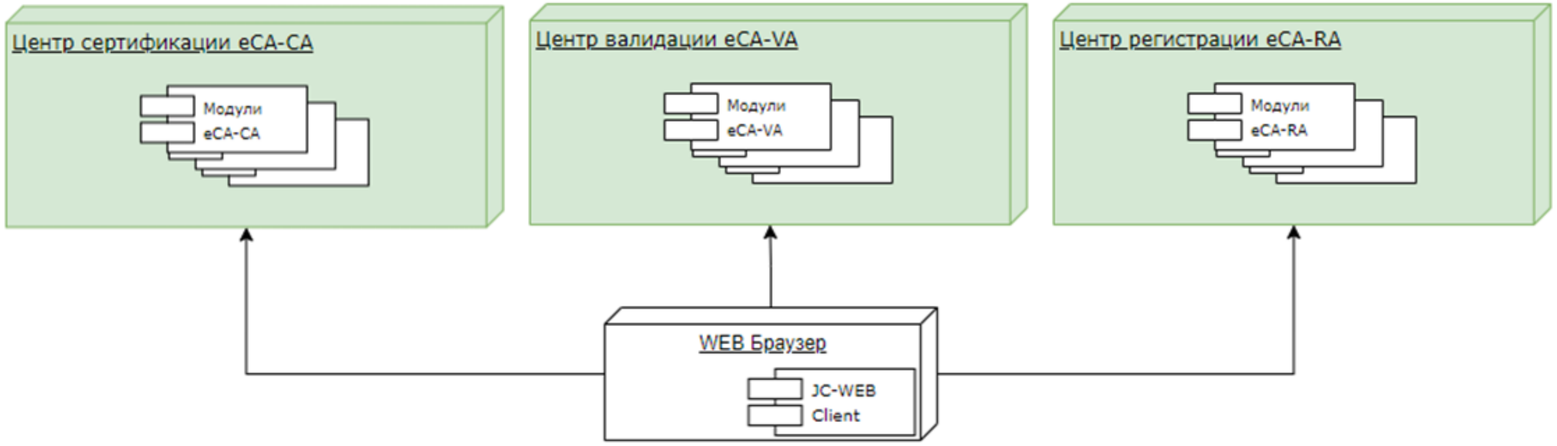
Компании, предоставляющие облачные услуги, могут повысить безопасность своих платформ, внедрив PKI для защиты данных клиентов, аутентификации пользователей и защиты каналов связи.

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;

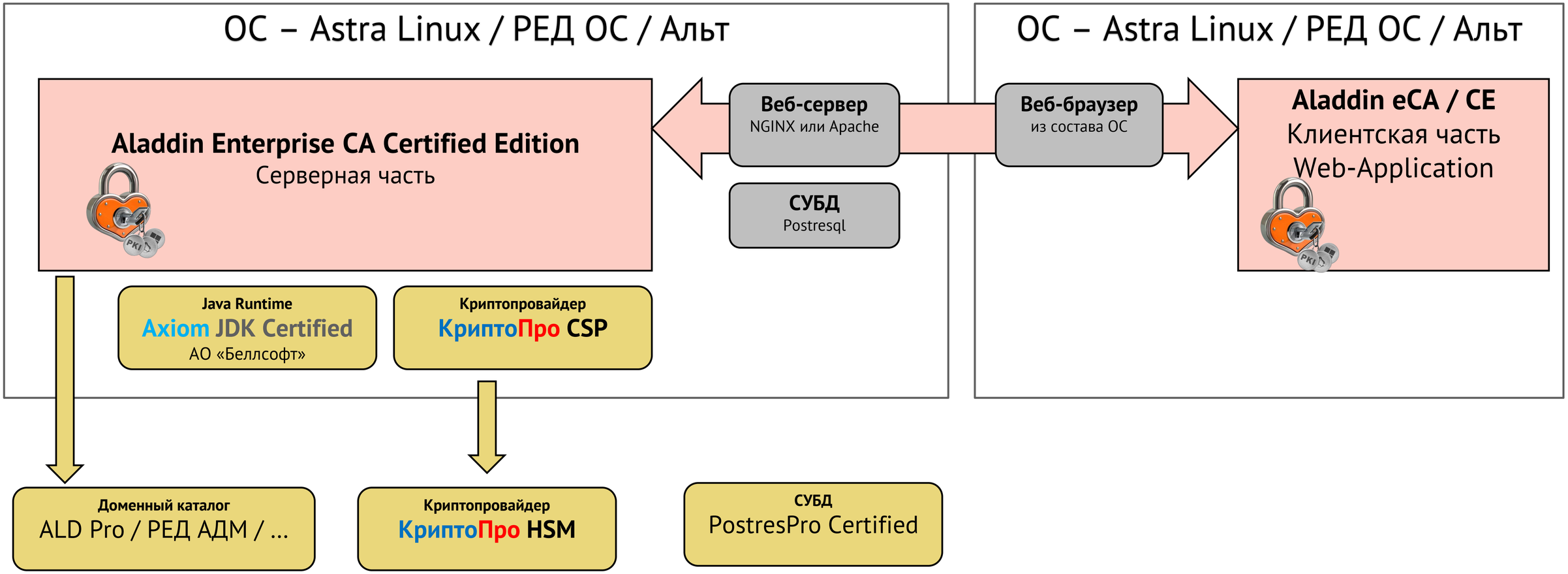
Центр валидации

- 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: три варианта миграции

Вариант 1 Заказчик не планирует пока уходить с AD, но планомерно уводит сервисы на отечественные ОС

Сохраняется действующая ветка PKI с корневым CA на базе серверной роли Microsoft MS CS

- Aladdin eCA разворачивается еще одним подчиненным в параллель к действующему CA
- Импортируются действующие шаблоны из Microsoft CS
- Срок действия сертификатов заканчивается и новые сертификаты выпускаются уже на Aladdin eCA

Разворачивается новая ветка PKI параллельно с Microsoft MS CS

- Разворачивается еще один корневой CA и группа выдающих на базе Aladdin eCA
- Параллельно работает две ветки PKI от отдельных корневых CA
- Импортируются действующие шаблоны из Microsoft CS
- Новые сертификаты выпускаются уже на Aladdin eCA

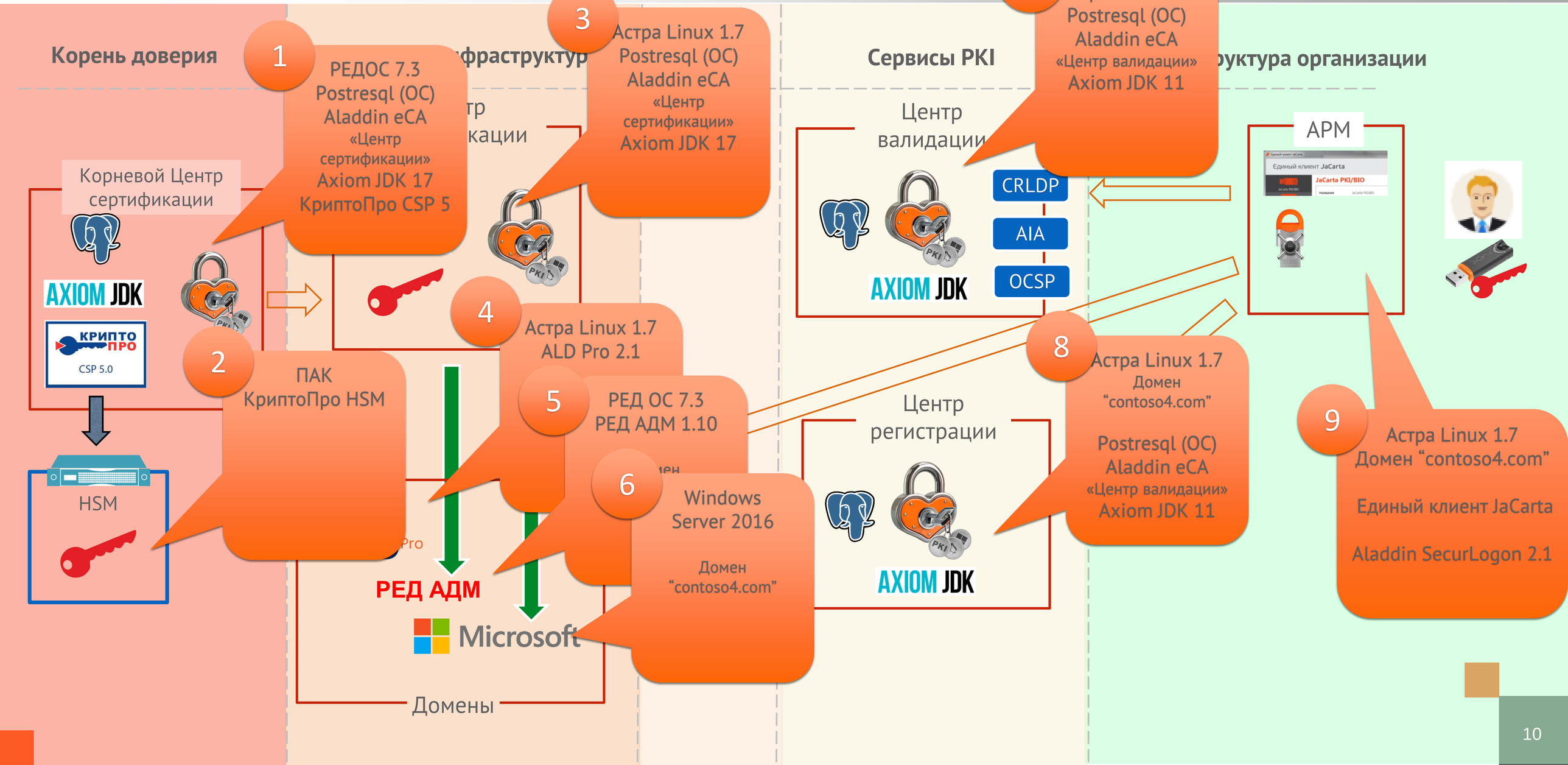
Вариант 2 Новый домен с доверительными отношениями со старым

- Aladdin eCA разворачивается в новом домене и работает параллельно с Microsoft CA
- Пользователи и сервисы домена постепенно и вручную переносятся в новый домен

Вариант 3 Бесшовная миграция

- Отечественное средство управления каталогом пользователей включается в существующий домен как дополнительный контроллер
- Aladdin eCA разворачивается совместно с новым средством
- Пользователи и сервисы постепенно и вручную мигрируют на отечественные решения (сохраняя свое присутствие в домене)

Схема и сценарий демонстрации



Aladdin Enterprise CA : текущее состояние и развитие

RTM eCA 1.2
- Базовый PKI
- Домены
- Полномочия
- …
- Опытные пилоты и внедрения

RTM eCA 2.0
- Подача на сертификацию
- Улучшение скоростных характеристик
- Кластер отказоустойчивости
- Багфикс и улучшения

RTM eCA 2.1
- ГОСТ и HSM
- Кластер отказоустойчивости
- Балансировки
- Полномочия на шаблоны
- …

Сертификат ФСТЭК

RC eCA 2.2
- Центр регистрации
- Работа с заявками
- Autoenrollment
- Единая ролевая модель

SCEP / ACME

Интеграция с политиками доменов

Развитие ролевой модели

. . .

Приоритеты могут определяться конкретными проектами и обязательствами

2022…2023 | 2024H1 | H2 | 2025

Aladdin Enterprise CA: схема лицензирования

		Состав исполнений		
		Базовое	Стандартное	Корпоративное
1	Компонент Центр сертификации	+	+	+
2	Отказоустойчивый кластер	-	-	+
3	Подключение доменов	1	2	unlim
4	Подключение Центров валидации	1	2	unlim
5	Служба OCSP	-	-	+
6	Подключение Центров регистрации	1	2	unlim
7	Подключение HSM	-	-	+
8	Количество субъектов	100	0	0
9	Сертификатов на 1 субъект	3	3	unlim
10	DNS-имен на 1 субъект	3	3	unlim

Типы лицензий:

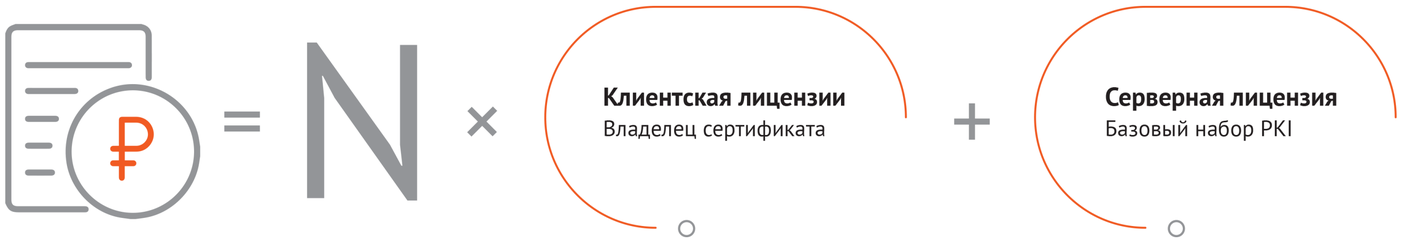
Подписка годовая
Безлимитная лицензия

Уровни Технической поддержки:

1. Базовая
2. Расширенная

Субъект = Владелец сертификата

+ Пользователи с сертификатами
+ Серверы с SSL-сертификатами
+ АРМ защищенных сертификатами
+ Иные технические устройства



Комплексный подход Аладдин

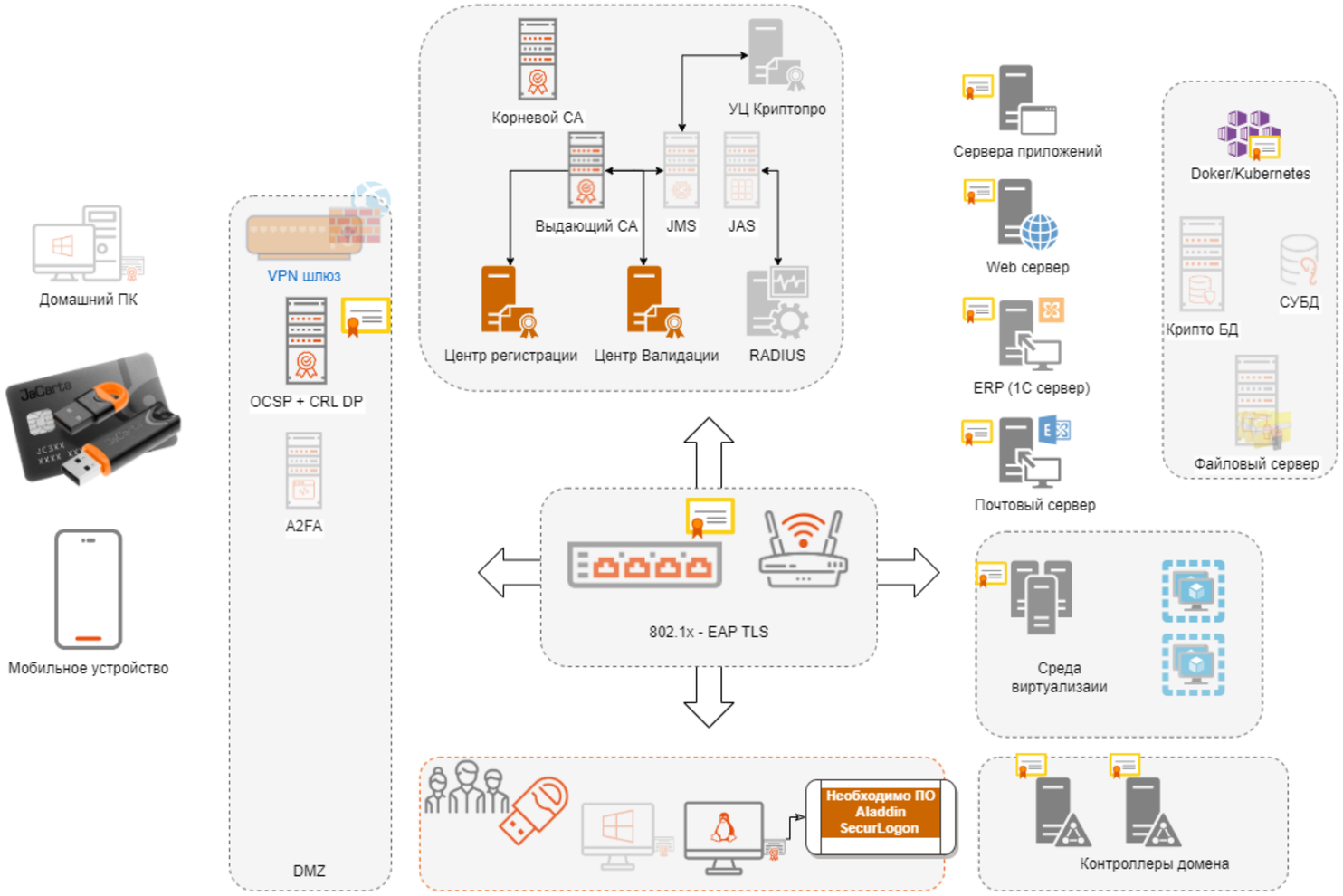
PKI корпоративного уровня
- Строгая аутентификация пользователей
- Доверие к инфраструктуре, сертификаты серверов и компьютеров

Управление ЖЦ средств 2ФА
- JaCarta Management System 4 Linux
- Учет ключевых носителей
- Учет СКЗИ

Усиленная аутентификация
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- Aladdin SecurLogon
- Аутентификация по OTP / PUSH / SMS

Дистанционная работа ("удаленка")
- Aladdin LiveOffice

Защита данных при хранении и обработке
- КриптоБД
- SecretDisk Linux
- Защита данных от утечек
- Централизованное управление (скоро)



Центр компетенций Аладдин

Разработаем план импортозамещения

и поможем его реализовать

РЕДОС

АЛЬТ 8 СП

ASTRA LINUX®

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

Microsoft

Помощь в миграции инфраструктуры с Windows на Linux

+ Разработка плана миграции на базе готовых отработанных методик

Проектная команда

Ситников Алексей

Руководитель направления по финансовому сектору
(коммерческий департамент)

+7 910 406 5410
A.Sitnikov@aladdin.ru

Шалимов Сергей

Руководитель центра развития
(коммерческий департамент)

+7 977 280 8412
S.Shalimov@aladdin.ru

Полушин Денис

Руководитель направления PKI
(продуктовая дирекция)

+7 916 010 0618
D.Polushin@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.