



## Корпоративный центр сертификации

### Aladdin Enterprise CA 2.0

- Отечественная замена Microsoft CA
- PKI уровня Enterprise на базе отечественных ОС
- Бесшовная миграция на Linux без перерыва в производстве
- Сертификация ФСТЭК
- Техническая поддержка при внедрении и эксплуатации

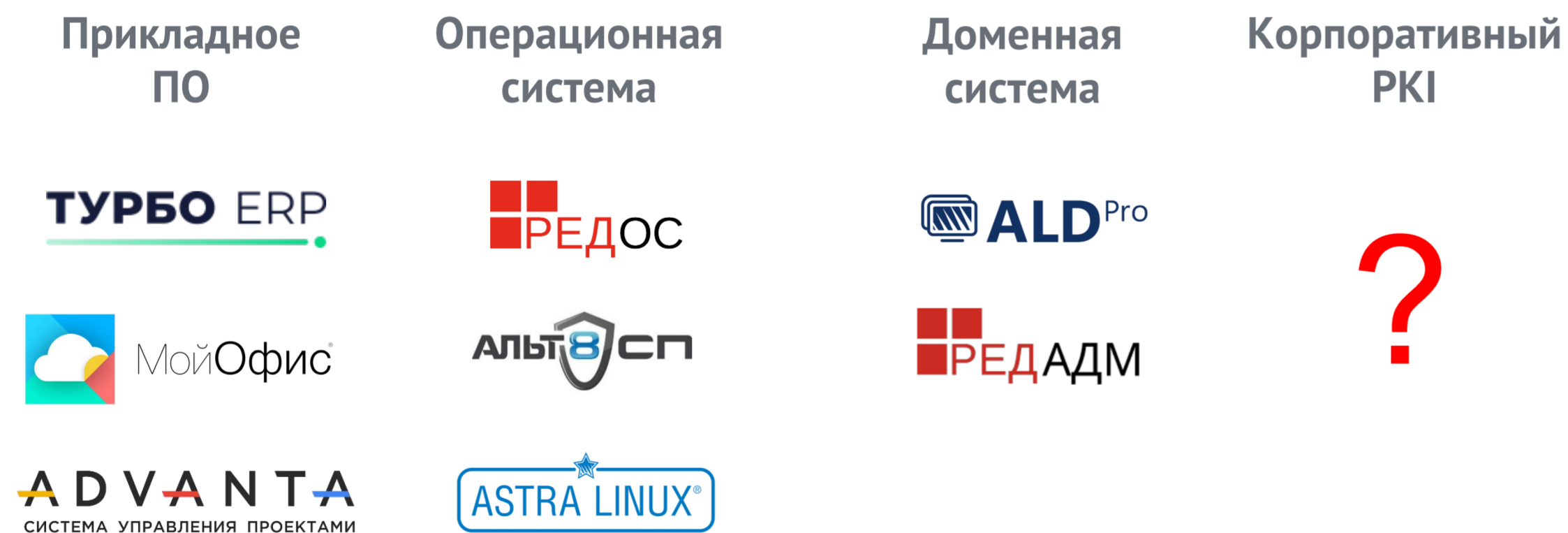
Денис Полушин  
менеджер продукта АО "Аладдин Р.Д."

# Импортозамещение: что важно?

Многие организации при импортозамещении ограничиваются заменой клиентских операционных систем, прикладного и офисного ПО на отечественные.

Недостаточно заместить только операционные системы и прикладное ПО. Нельзя игнорировать компоненты домена безопасности. В который в частности входит средство для организации PKI: "Корпоративный Центр сертификации".

Это сердце IT-инфраструктуры предприятия.



## Что значит Корпоративный центр сертификации

- Возможность параллельной работы в **гетерогенной среде** – как с наследием Microsoft, так и с отечественными решениями
- Реализация **строгой аутентификации** пользователей Linux – аналог встроенных сервисов Windows, включая MS Smart Card Logon
- Наличие необходимых сертификатов от отечественных **регуляторов**
- **Технологическая совместимость** с отечественными ОС и доменами
- Наличие квалифицированной технической **поддержки** и обновлений

# Корпоративный PKI - это ...

On-prem Центр Сертификации + вспомогательные службы

Это сертификаты для



веб-серверов, внутрикорпоративных порталов



сотрудников (аутентификация, удалёнка, внутренний ЭДО, почта)



АРМ, ноутбуков, компьютеров (подключение по 802.1x)



мобильных устройств

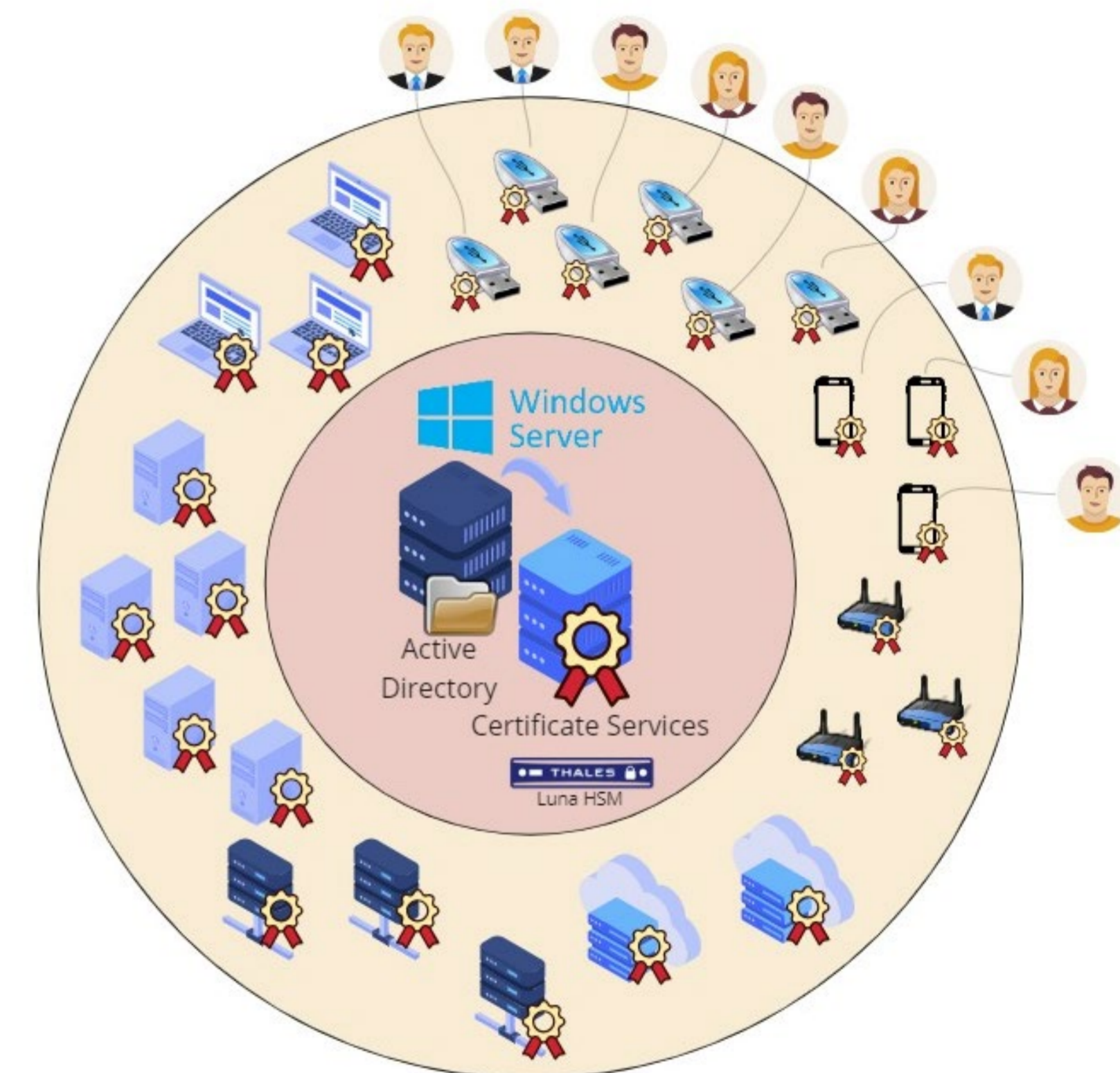
**До недавнего времени типовое решение для корпоративного PKI**



**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



# Чем рискуем сейчас?

## Риски использования PKI на основе Microsoft

**Более 90%** информационных систем в России построены на Microsoft Active Directory и используют Microsoft Certificate Services в качестве сервиса генерации и управления цифровыми сертификатами (сертификаты доступа, PKI инфраструктура).

- × Microsoft ушел с рынка РФ, приобрести его невозможно
- × Возможность полного отключения сервисов
- × Отсутствие поддержки и обновлений
- × Не соответствует требованиям регулятора

## Риски IT-инфраструктуры без PKI

PKI создает доверенную среду для безопасного взаимодействия пользователей и систем в сети. Это внутренний периметр безопасности, гарантирующий защиту от умышленных или непредумышленных действий внутренних нарушителей.

- × Аутентификацию на основе паролей легко взломать
- × Внутренняя сеть не защищена от подключения «неизвестных» устройств
- × Уязвимость к фишингу (не защищена почта)
- × Сложно обеспечить безопасное подключение удаленных пользователей и устройств

## А может сделать PKI на базе open-source?

Для такого уровня это слишком рискованно и слишком сложно.

- × Отсутствие поддержки
- × Доступные компоненты не уровня Enterprise
- × Недостаток экспертизы

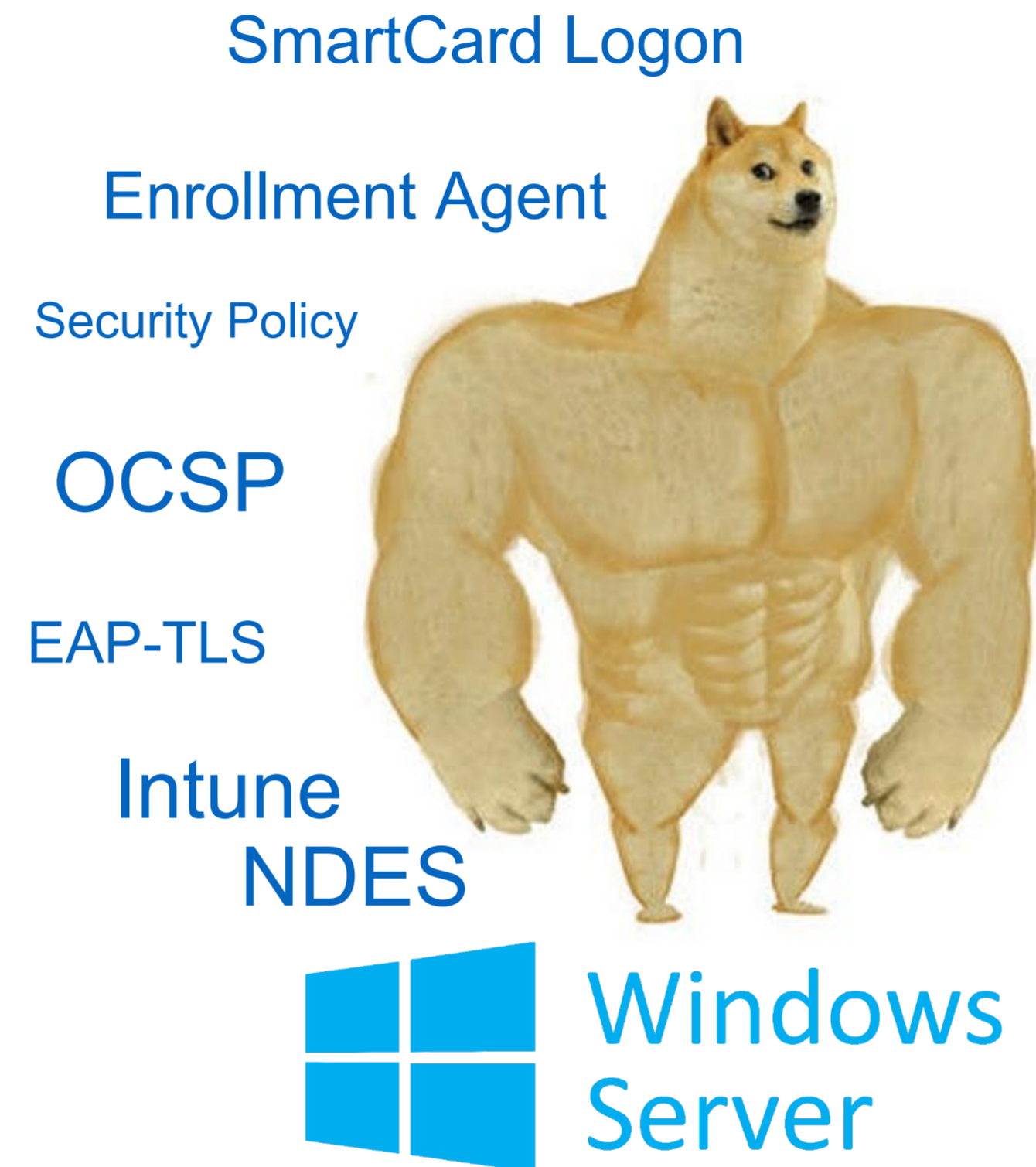
# Корпоративный PKI у всех разный

Сейчас компании в России делятся на тех, кто использует PKI на базе Microsoft и тех не использует всех возможностей PKI.

И то и другое – это риск для безопасности информационной системы.

**Задачи разные – решение одно.**

Построить корпоративную PKI-инфраструктуру на базе отечественных решений.



Наш админ может сам сделать SSL-сертификат

# Aladdin Enterprise CA: основа отечественной PKI



## Aladdin Enterprise CA

В Реестре отечественного ПО запись от 08.08.2022 (№14433)

Сертификация ФСТЭК России УД-4 (до гостайны вкл.)

Поддержка отечественных ОС и доменной инфраструктуры



РЕД АДМ

### Базовая функциональность PKI

- Иерархии ЦС
- Управление ЖЦ сертификатов
- Шаблоны
- RSA/ECDSA, CRL DP, AIA, OCSP

### Распределение ключевого функционала

- Центр сертификации
- Центр Валидации
- Центр Регистрации

### Ролевая модель, делегирование полномочий

- Роль администратора
- Роль оператора

### Задачи обслуживания

- Резервное копирование
- Мониторинг
- Журнал событий

### Бесшовная миграция с Microsoft CA

- Импорт шаблонов
- Интеграция с AD
- bypass с действующим MSCA

### Другие возможности

- REST API

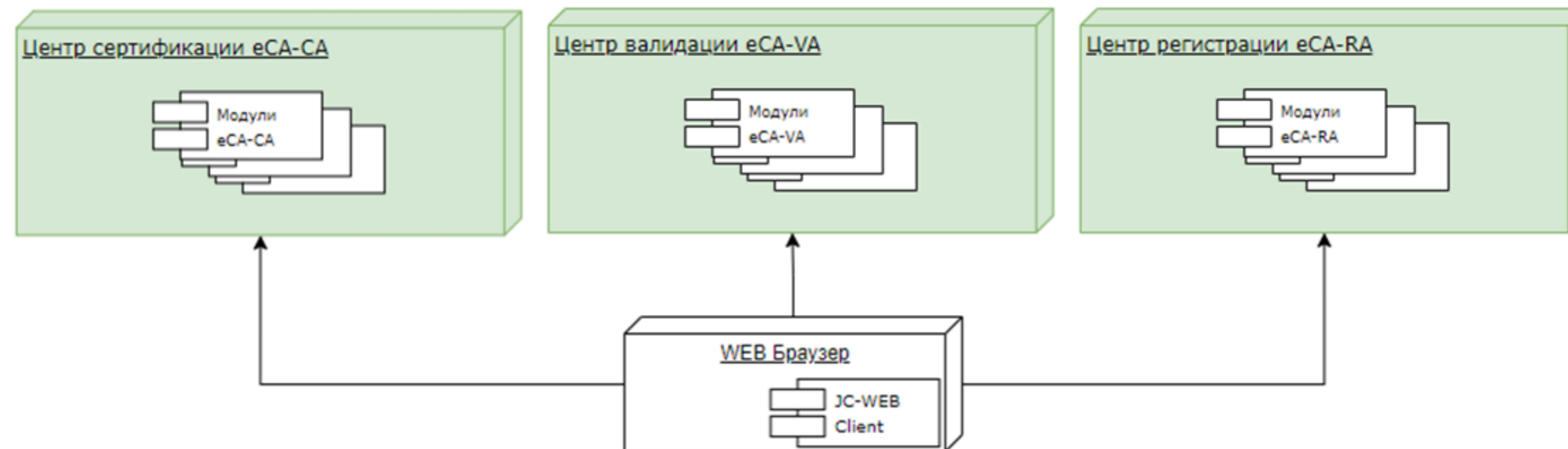
# Aladdin Enterprise CA: архитектура



## Aladdin Enterprise CA

### Центр сертификации уровня Enterprise

Для среднего и крупного бизнеса



### Центр сертификации

Ядро продукта, обеспечивает выпуск сертификатов, управление их статусами, подключение к каталогу пользователей и т.д.

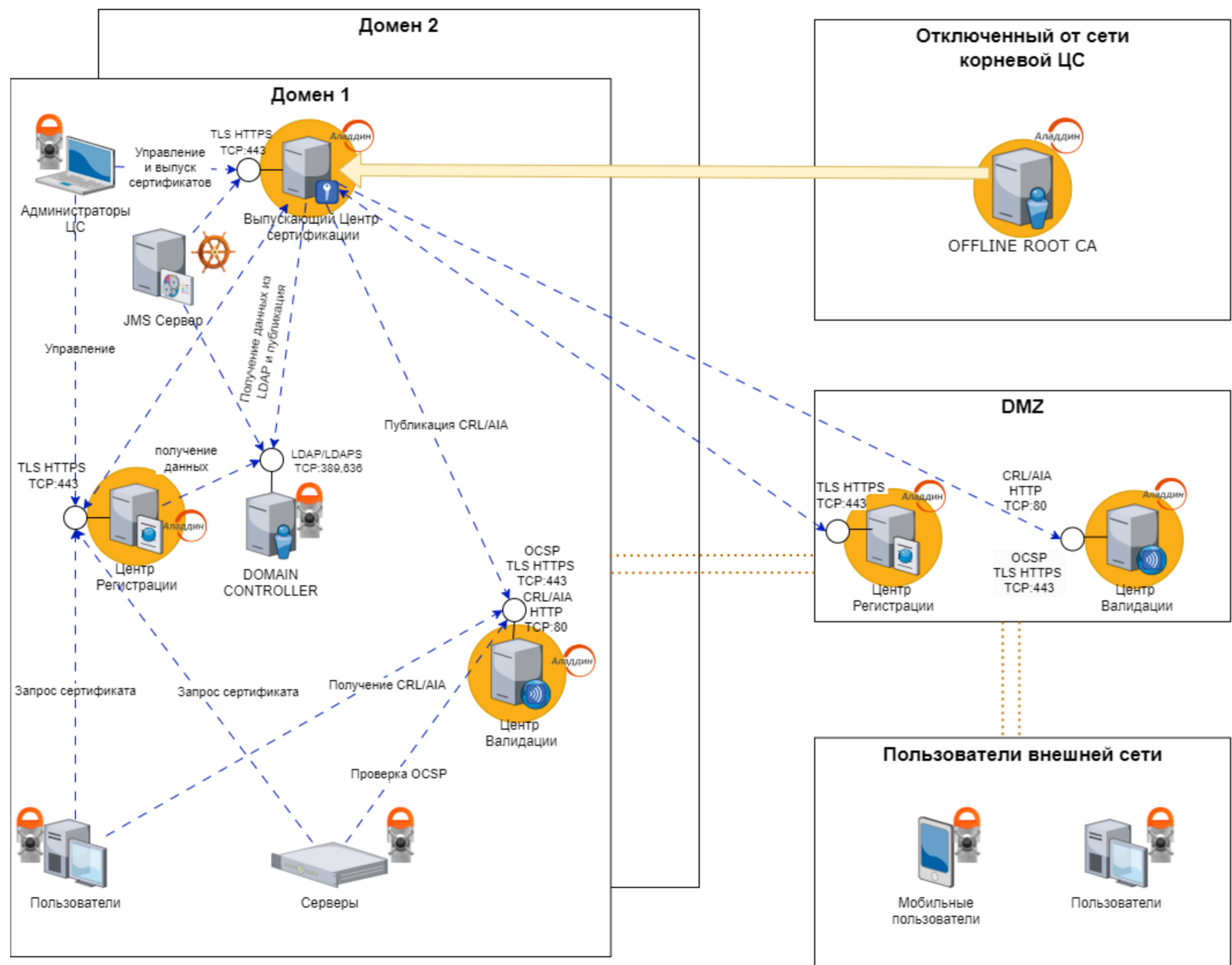
### Центр валидации

Предоставляет сведения об издателе и об отозванных сертификатах. Предоставляет точку скачивания CRL: CRL Distribution Point и службу OCSP для онлайн-проверки статусов сертификатов.

### Центр регистрации

Компонент, предоставляющий возможность самим пользователям или техническим устройствам подключаться (аутентифицироваться) и оформлять заявку на получение сертификата. Заявка может быть обработана автоматически, с автоматической выдачей сертификата.

# Aladdin Enterprise CA: схема развёртывания



## Компонент Центр Сертификации

- Корневой ЦС разворачивается в максимально изолированном сегменте локальной сети. Владеет самоподписанным сертификатом организации;
- Выпускающий ЦС разворачивается во внутрикорпоративном сегменте сети. Владеет сертификатом организации, используемым для обслуживания сертификатов пользователей, серверов;
- Выпускающий ЦС может обслуживать несколько отдельных доменов;
- К выпускающему ЦС может быть подключено другое приложение, например JMS4LX, или АИС предприятия для выдачи и обслуживания сертификатов;

## Компонент Центр Валидации

- Может быть развернут как во внутрикорпоративном сегменте для обслуживания внутренней инфраструктуры и сотрудников предприятия, так и в DMZ для обслуживания внешних пользователей, дистанционных пользователей или контрагентов;

## Компонент Центр Регистрации

- (доступен в 2024)
- Разворачивается для пользователей или устройств для которых требуется автоматическая выдача сертификатов;
  - Обслуживает только один домен;



# Aladdin Enterprise CA: схема лицензирования

Две схемы лицензирования – подписочная на 1 год и неограниченная по времени, с возможностью продления технической поддержки.

Базовая лицензия:



= N ×

**Клиентская лицензия**  
Владелец сертификата

+

**Серверная лицензия**  
Базовый набор PKI

**Количество субъектов** =  
Владельцев сертификатов

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

**На один субъект:**

- + 3 действующих сертификата
- + 3 DNS-имени

**Дополнение к клиентской лицензии:**

1. Возможность увеличения количества действующих сертификатов
2. Возможность увеличения количества DNS-имен

**Включает в себя:**

- + 1 Центр сертификации  
+ Failover (доступен в 2024)
- + 2 Коннектора к ресурсным системам
- + 2 Центра валидации  
+ Служба OCSP
- + 1 Центр регистрации (доступен в 2024)

**Дополнение к серверной лицензии:**

1. Подключение к ресурсной системе
2. Возможность задания Wildcard-имен
3. Дополнительный Центр валидации
4. Служба OCSP на Центре валидации
5. Дополнительный Центр регистрации

# Три подхода к миграции и схемы применения

## 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)

# Где рекомендуется использовать PKI?

## 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.



# Конкуренты? Средства УЦ классов КС...КВ?

## Aladdin Enterprise CA

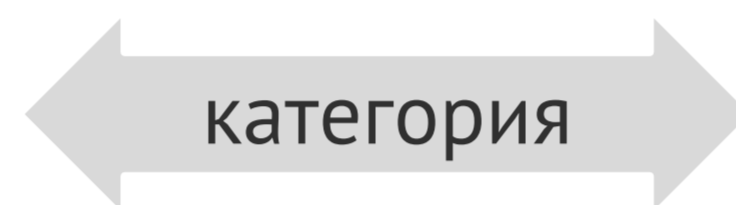
Средства защиты ИТ-инфраструктуры

Обеспечение доверия к каждому элементу инфраструктуры заказчика

ФСТЭК России, приказы 17, 21, 239, 31

Тесная интеграция в инфраструктуру, автоматизация

Департамент ИТ



## Отечественные Средства УЦ

Средства ИБ КЭП, НКЭП

Юридическая значимость

ФСБ России, приказы 795, 796

Изоляция в контролируемой зоне

Департамент ИБ

# Конкуренты? Решения open source?

## Нет доступных решений уровня Enterprise

EJBCA Community Edition vs Enterprise Edition

## Требует глубоких знаний Linux и PKI

Например, как обеспечить аутентификацию в домене по сертификатам?

## Дорогой! Сопоставимо с разработкой продукта

Разработка интеграции, доработка, внедрение

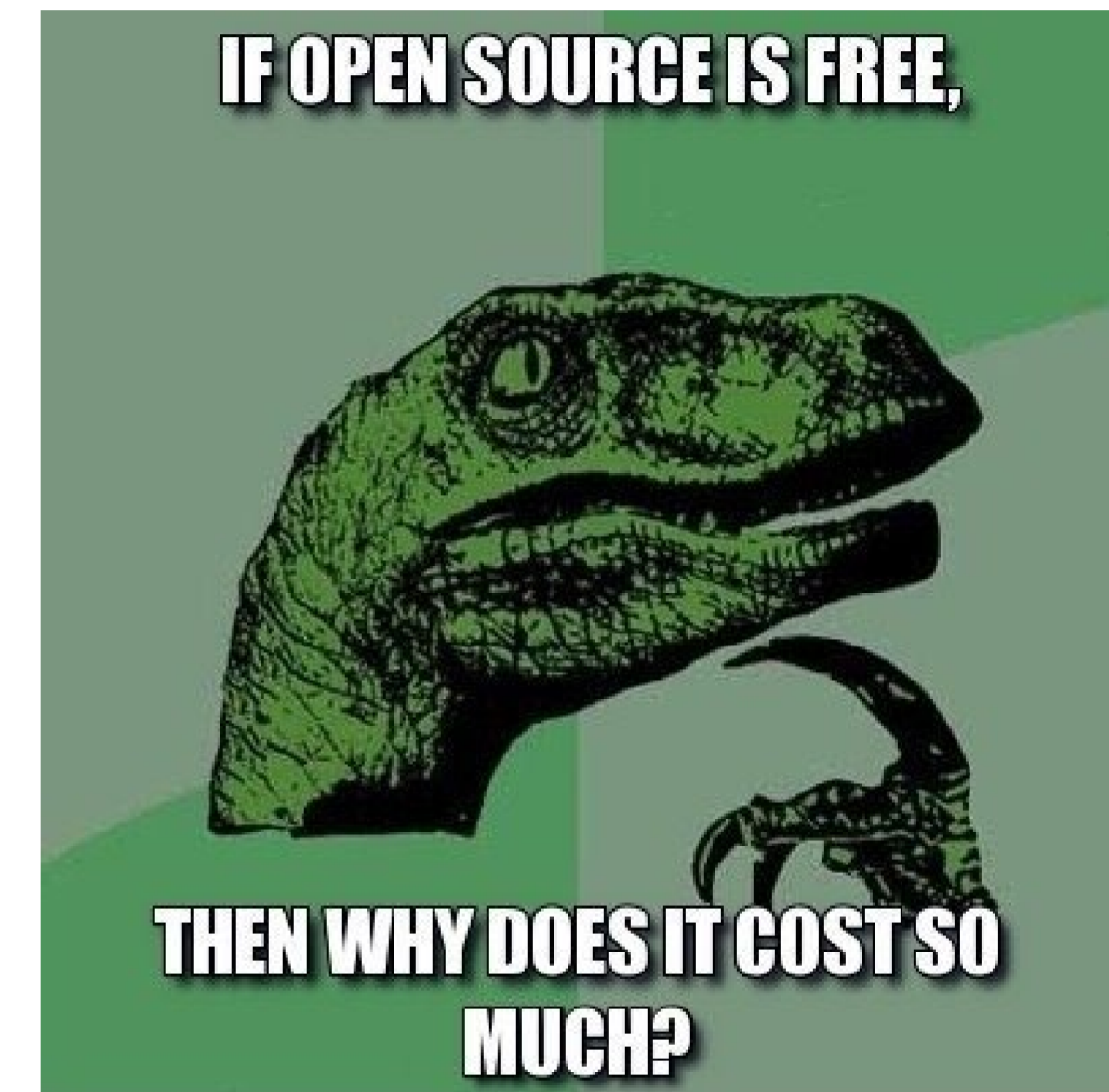
Техническая поддержка и исправление ошибок

Отслеживание и устранение уязвимостей

## Минимум документации и она на английском

## Отсутствие сертификатов регуляторов

Отсутствие такой возможности (пример с EJBCA)



EJBCA OpenXPKI DogTag  
OpenCA Boulder CFSSL XCA

# 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

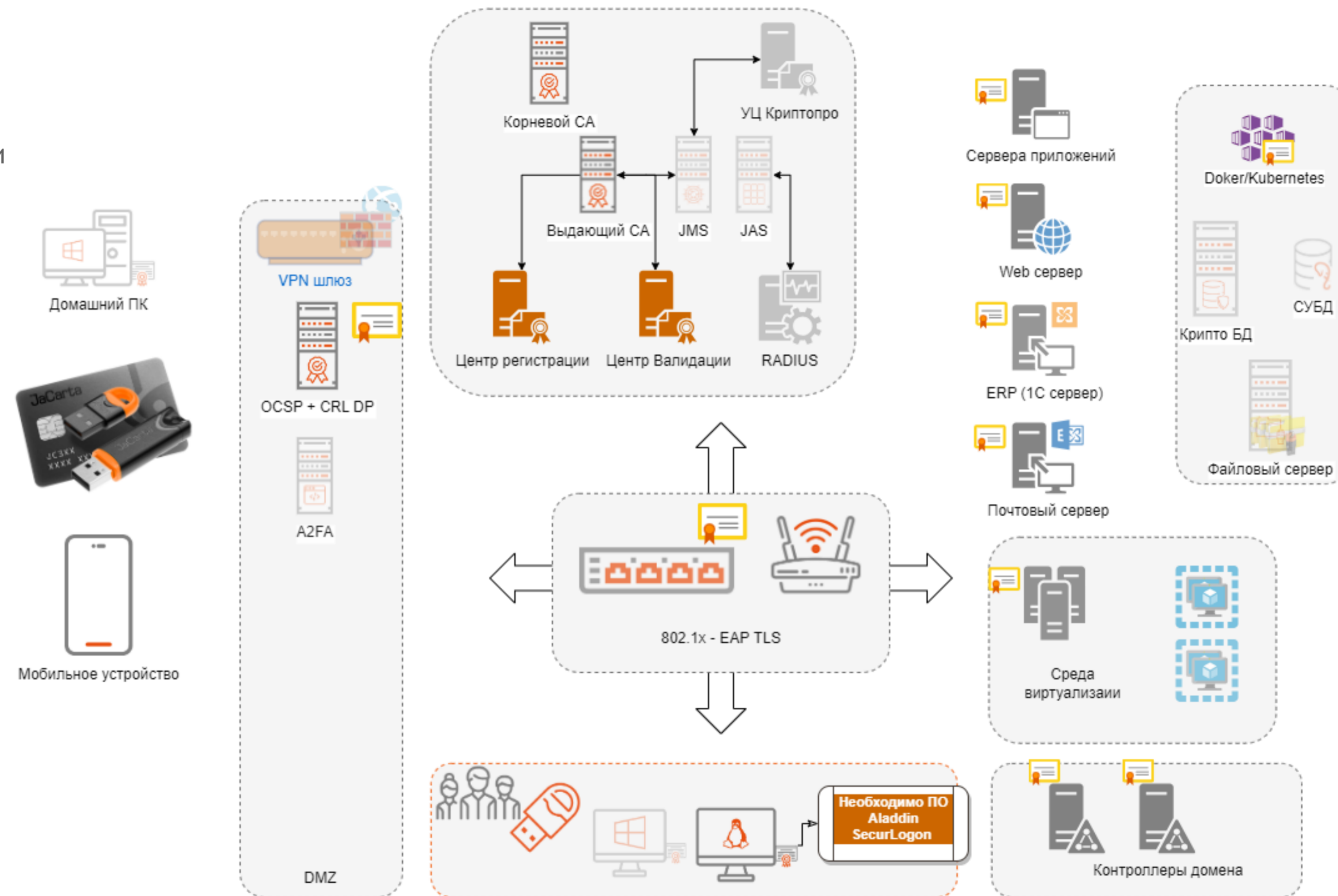
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- Aladdin SecurLogon
- Аутентификация по OTP / PUSH / SMS

## 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

## 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



# План действий

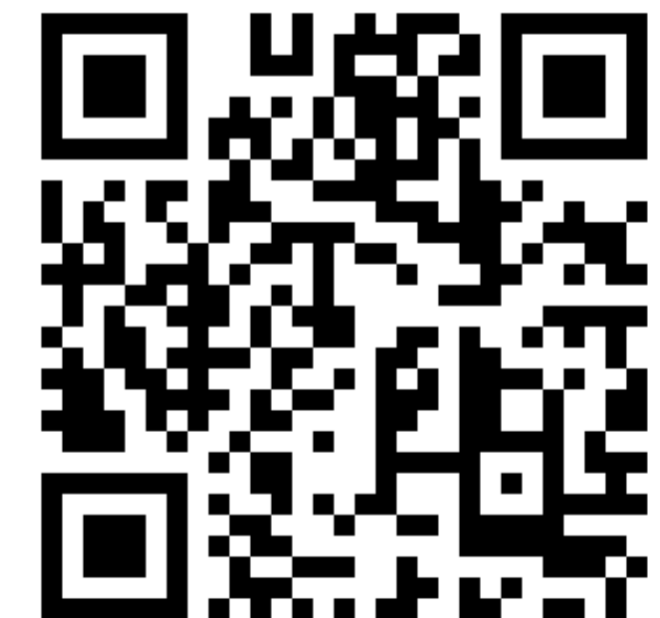


## Aladdin Enterprise CA (Aladdin eCA)

Центр сертификации под Linux  
для организации инфраструктуры  
открытых ключей в ИС

- 1 Узнать стоимость и необходимые контакты  
<http://promo.aladdin.ru/eca>
- 2 Получить демо и провести пилот
- 3 Узнать о специальных условиях

Программа по **импортозамещению** Аладдин





*Аладдин - будь собой в электронном мире!*



Спасибо!

Денис Полушин  
Менеджер продукта аЕСА  
АО "Аладдин"

[www.aladdin.ru](http://www.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, IoT-устройств, Web-порталов и эл. сервисов.