
# Проблемы применения сертификатов доступа

## при осуществлении идентификации и аутентификации субъектов доступа в ИС

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

www.aladdin.ru

# Начну с матчасти…

## Аутентификация - основа создания доверительных отношений

- Что такое ДОВЕРИЕ и почему это так важно?
  - *Доверие - это открытые взаимоотношения между людьми (субъектами), содержащие уверенность в порядочности другого, в возможности поделиться с ним личной или сокровенной информацией, в его ответственности не воспользоваться этой информацией вам во вред…*
  - Применительно к ИТ-инфраструктуре - это определение тоже работает
    - Если мы строим доверенную ИТ-инфраструктуру гос. организации, КИИ и т.д., то **каждый её элемент должен быть доверенным** - значит надёжно идентифицированным и аутентифицированным
  - Этого достаточно? Нет!

"В деле, которым я занимаюсь, нужно оперировать другими категориями - здесь вопрос не в доверии, а в **гарантиях**"

*В.В. Путин*

# Матчасть: нац. стандарты по идентификации и аутентификации

- Действующие стандарты
  - ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения
  - ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. **Уровни доверия идентификации**
  - ГОСТ Р 59381-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции
  - ГОСТ ISO/IEC 24760-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования.
  - ГОСТ Р 59382-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы
  - ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом
  - ГОСТ Р 59515-2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности
- Проекты стандартов (в работе)
  - Защита информации. Идентификация и аутентификация. **Уровни доверия аутентификации**
  - Защита информации. Идентификация и аутентификация. Управления идентификацией и аутентификацией
  - Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости идентификации и аутентификации
  - Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией

# Требования к аутентификации

- Что обеспечивает ДОВЕРИЕ и даёт гарантии?
  - Какой тип аутентификации нужен для критически важных систем?
  - Как его реализовать?

Вероятность и размер возможного ущерба

Уровень значимости информации в ИС

| Тип аутентификации | Низкая | **Средняя** | **Высокая** |
|---|---|---|---|
| **Высокая** | Усиленная | **Строгая** | **Строгая** |
| Средняя | Простая | Усиленная | **Строгая** |
| Низкая | Простая | Простая | Усиленная |

Кому:
- Гос. организации
- Федеральные структуры
- **Организации КИИ**
- Крупный и ср. бизнес
- **Производители СЗИ**

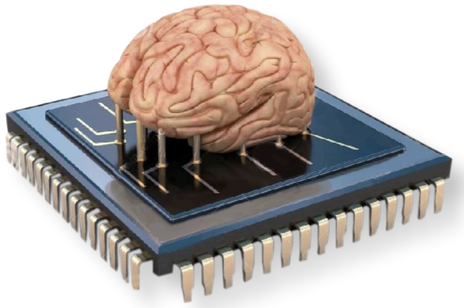
Для кого:
- **Для всех пользователей ИС**
- Для администраторов
- **Для удалённых пользователей**

*Сейчас они есть у всех!*
*Но и этого недостаточно*

*С началом СВО на первое место выходит внутренний нарушитель (был сильно недооценён)*

# Что нужно для реализации СТРОГОЙ аутентификации

- В ИС с высокой важностью информации и высоким размером возможного ущерба
  - Должна применяться **строгая** взаимная двухфакторная аутентификация пользователей (2ФА)
- Строгая аутентификация обеспечивается использованием
  - Инфраструктуры открытых ключей (PKI) - **сертификатов доступа**
  - Специализированных защищённых и сертифицированных аппаратных средств аутентификации (**второго фактора**):
    - Хранение цифрового **сертификата** пользователя
    - Выполнение **криптографических** операций с использованием **неизвлекаемых** закрытых ключей пользователя (требуются для поддержки защищённых протоколов аутентификации)
    - Возможность использования только **аутентифицированным** пользователем



✓ **Программные токены, смартфоны, генераторы одноразовых паролей (OTP) не обеспечивают СТРОГУЮ 2ФА**

  - Централизованным управлением и поддержкой жизненного цикла сертификатов, средств 2ФА
  - Сервисом аутентификации (локальным или доменным)
    - Он должен быть своим, доверенным, а не как в Windows - чужим

# Проблемы обеспечения строгой аутентификации в ИС

## Проблема №1

- Ключевой и самый критичный элемент во всей ИТ-инфраструктуре - **центр выпуска и обслуживания цифровых сертификатов** (CA)

  CA обслуживает:

  - домены безопасности/службы каталога
  - сервисы для удалённого доступа - VDI, VPN, RDP-шлюзы
  - различные сервисы, включая аутентификацию устройств, пользователей, приложений

  **CA - основа доверенного взаимодействия всех объектов и компонентов**

- Практически все ИТ-инфраструктуры в России построены на базе MS CA
  - …и на 100% зависят от его работоспособности
  - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержка MS CA больше не осуществляется, купить его тоже нельзя
  - Аналоги под Linux не делали - кто купит, если MS CA был бесплатен?

✓ **Не путать с УЦ для ЭП (63-ФЗ) — разные задачи и разные требования!**

# Проблемы обеспечения строгой аутентификации в ИС

## Проблема №2

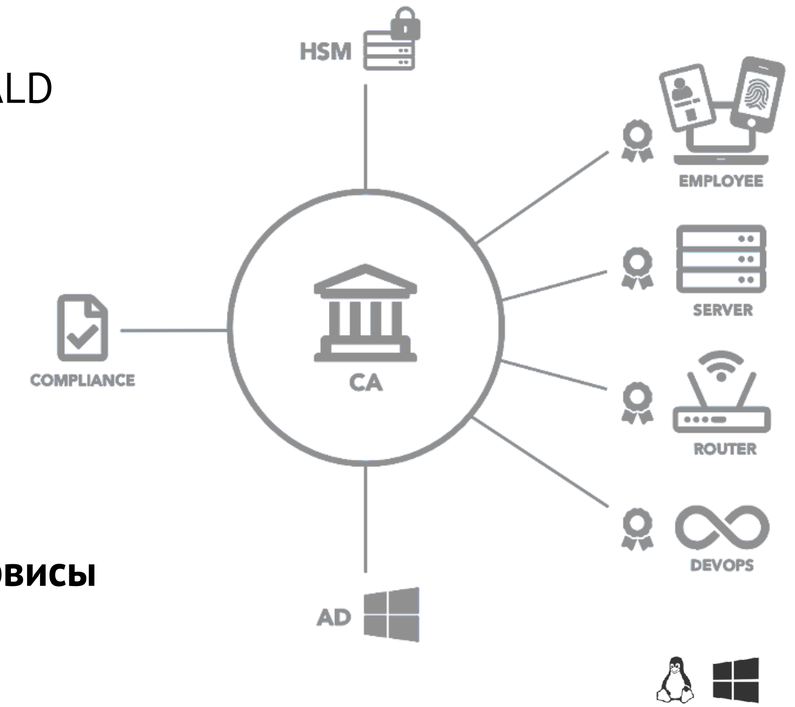
- Как заменить корневой CA?
  - Замена корневого CA полностью парализует работу всех сервисов
  - Сертификаты для подчинённых CA выпускаются на 5-10 лет
  - ✓ **Нужен CA, умеющий работать параллельно (bypass) с подчинённым MS CA, который будет постепенно перехватывать на себя выпуск и обслуживание сертификатов**
  - ✓ **Делать это надо немедленно!**

# Проблемы обеспечения строгой аутентификации в ИС

## Проблема №3

- Импортозамещаемся, переходим на отечественные ОС (Linux)
  - Одномоментно перейти на Linux и отказаться от Windows никто не сможет
  - В Linux свои службы каталогов и домены безопасности (FreeIPA, Samba DC, ALD Pro)

✓ **Корпоративный CA должен уметь одновременно работать и с MS AD, и со службами каталогов Linux**




## Проблема №4

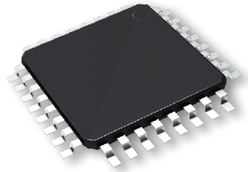
- В Linux нет полноценной поддержки PKI и 2ФА пользователей
  - В Windows аутентификацию пользователей (2ФА) реализуют **встроенные сервисы** (вкл. MS Smart Card Logon)
  - Полноценного аналога для Linux нет (клиента PKI и 2ФА)

✓ **Реализовать строгую аутентификацию пользователей для Linux можно (руками), но достаточно сложно** (в разных дистрибутивах всё делается по-разному)

# Проблемы обеспечения строгой аутентификации в ИС

## Проблема №5

- M2M, IIoT и пр. оборудование которое работает "в полях", на новых территориях… (с большими рисками компрометации)
  - Необходима строгая аутентификация подключаемых устройств
    - Мы должны быть точно уверены, что это именно то устройство, что его не подменили, не перепрошили
  - Должно быть доверенное взаимодействие
    - Мы должны доверять данным, получаемым из этого источника
    - Для "слабых" устройств нужны "лёгкие" защищённые протоколы (DTLS,…) и машинные сертификаты
    - Мы должны иметь доверенный защищённый канал управления, передачи данных, **обновления**
    - Большой парк устройств невозможно обслуживать без системы централизованного управления
  - Мы замещаем особо критичные импортные M2M-устройства в режиме "ошпаренной кошки" чтобы успеть к 1.01.2025 г. (Указ Президента)
    - Как будем исправлять ошибки, устранять обнаруженные уязвимости, обновлять ПО и прошивки?



✓ **В каждом устройстве, работающем в КИИ, должен быть аппаратный модуль безопасности (Secure Element) и машинный сертификат**


# Наш опыт проработки вопроса с заменой MS CA

# Роль и значение корпоративного CA

- Важность CA
  - CA - ключевой и самый критичный элемент всей ИТ-инфраструктуры
  - На CA завязано абсолютно всё
    - Работа серверов, коммуникационного оборудования, доступ в систему, управление правами
  - Блокирование работы CA остановит работу всей ИТ-инфраструктуры
- Риски
  - Безальтернативный монополист на рынке - Microsoft Certificate Services (MS CA)
  - CA - только под Windows
  - Microsoft ушёл из России, MS CS больше не продаётся и не поддерживается
  - Риски блокирования работы сервиса CA - большие
- Осознание проблемы
  - Сервера MS выносят в Киргизию, Грузию, Китай чтобы их не заблокировали, чтобы получать обновления,.. подключаются по VPN

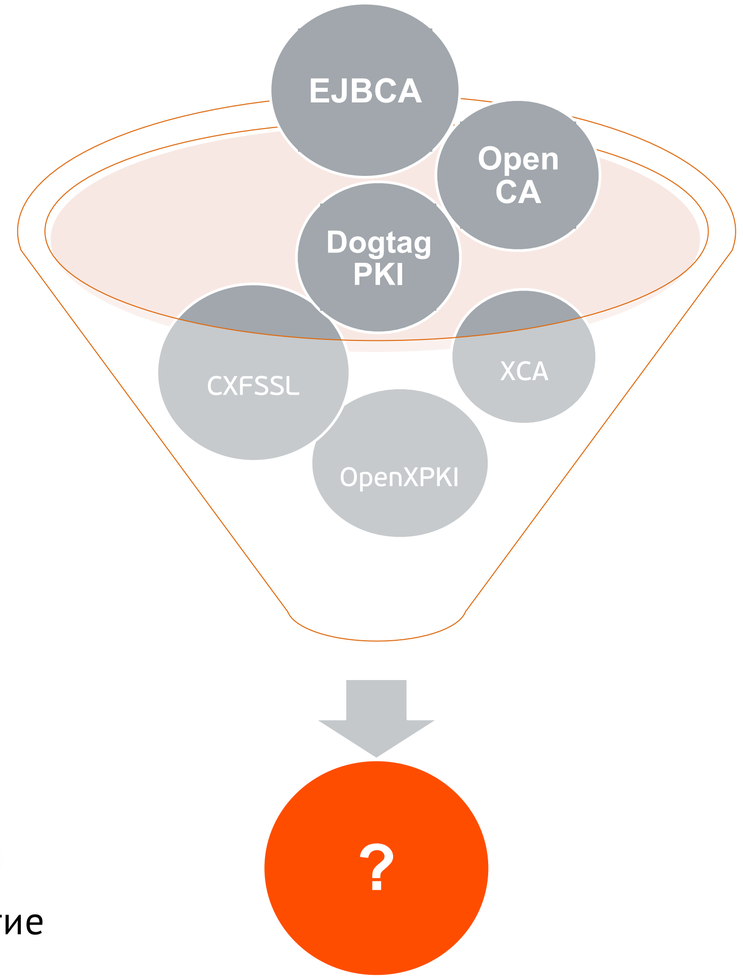
✓ **Корень доверия в другой стране???**

  - В 2020 г. ряд крупных компаний, проводя инвентаризацию своих ИТ-инфраструктур, выявил и осознал уровень проблемы и рисков
    - Поручили нам проработать возможные варианты замещения MS CA

# Результаты поисков и исследований

## Open Source

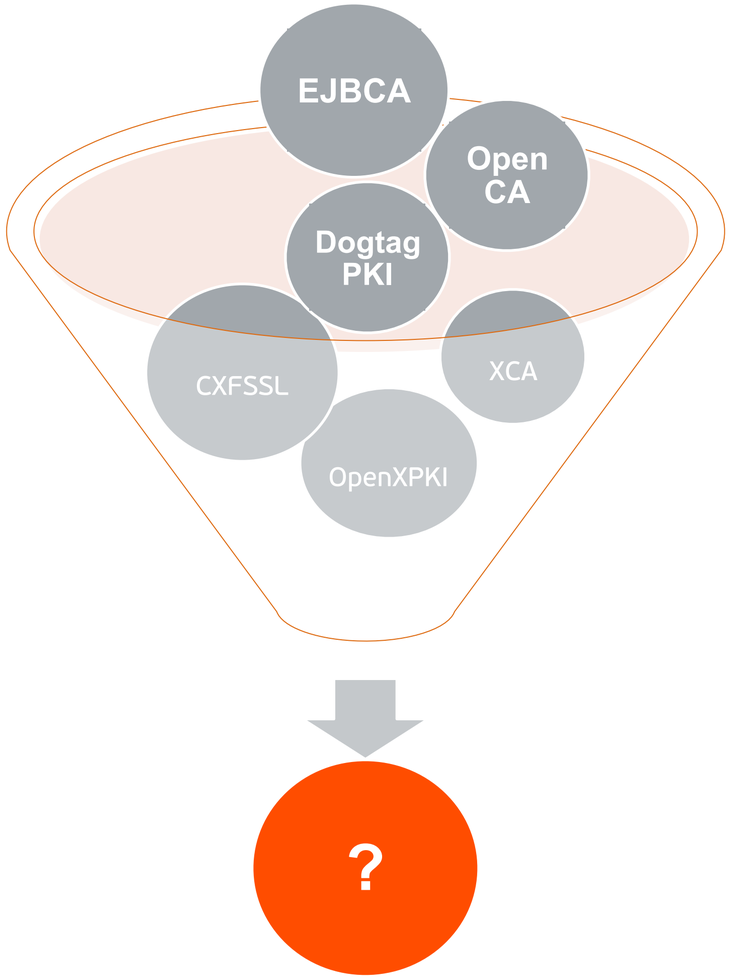
- Опубликовано достаточно много проектов CA
  - Критерии отбора
    - Необходимая и достаточная функциональность
    - Иерархия CA (2-3 уровня)
    - Совместимость с доменами (MS CA, Samba DC, FreeIPA)
    - Работа в гетерогенных сетях
    - Ролевая модель и делегирование полномочий
    - Выпуск и обслуживание машинных сертификатов в автоматическом и полуавтоматическом режимах (для серверов, роутеров, маршрутизаторов, исполнительного оборудования "в полях" - M2M, IIoT и др.)
    - Возможность масштабирования
    - Используемый стек технологий, SDK, документация (возможность сертификации)
    - Зрелость, распространённость, наличие успешных внедрений, поддержка, развитие
  - Из всех проектов, которые **могли бы претендовать** на необходимый нам уровень Enterprise, мы отобрали 7



# Результаты поисков и исследований

## Open Source

- Результаты исследований (почти год)
  - Из 7-ми отобранных проектов по нашим критериям прошли только 3
  - Смогли поставить, запустить и настроить - 1
  - Сделаны под базовые ОС из СПО, под российские ОС надо переделывать
  - Решения на базе Open Sourse
    - Требует очень глубоких знаний Linux и PKI
    - Представляют собой поделки, сделанные "на коленке"
    - Большинство решений для Enterprise не подходят
    - Сильно обрезанные и очень старые коммерческие версии, выложены в Open Source "для затравки - "попробуйте, а потом приходите к нам за нормальной платной коммерческой версией"
    - Включают порядка 40% бинарного кода (без исходников и документации)
  - Попробовали договориться о покупке коммерческой версии (еще в 2020 г.)
    - Цена одной инсталляции (не передачи прав!) - от 250,000 евро
    - Продукт стратегический, двойного назначения (!!!), в Россию ни под каким предлогом не поставляется (находится под полным запретом)
    - О передаче исходников (для сертификации) и речи быть не может

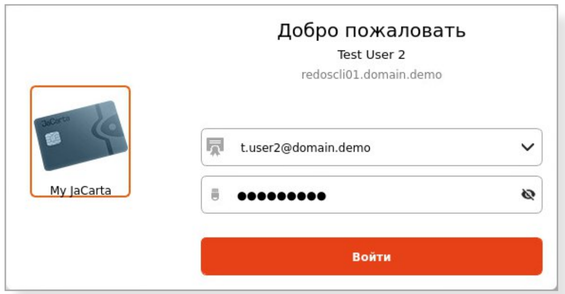


# Что сделано

- Для крупного якорного заказчика с огромной ИТ-инфраструктурой
  - Проработали отказоустойчивую масштабируемую многоуровневую архитектуру корпоративного CA
  - На базе одного из проектов собрали и запустили MVP
    - Решили проблемы несовместимости с отечественными ОС, VDI и пр.
    - Сделали поддержку 2ФА и PKI в Linux

✓ **SecurLogon - полнофункциональный аналог Windows Smart Card Logon**

  - В инфраструктуре заказчика в процессе тестирования продукта выявили проблемные зоны, которые надо будет расшивать
  - Написали недостающие сервисы
  - Проработали вопрос и получили Решение ФСТЭК России о сертификации (сначала на УД-4, потом, после ряда доработок "движка" - на УД-2)




✓ **Выпустили версию 1.1- Aladdin Enterprise CA**

  - Провели комплексное тестирование, по результатам получили Заключение заказчика и рекомендацию на внедрение у себя и во всех дочках
  - Задачи I этапа выполнены
    - Встать с MS CA параллельно, перехватить выпуск и обслуживание машинных и пользовательских сертификатов
    - Выдать на подчинённые CA новые сертификаты от корневого CA (MS CA) - пока он ещё работает
    - Выпустить сертификаты на все сервера
    - Обеспечить интеграцию с LDAP-каталогами

# Что дальше?

- Задачи MVP и v1, которые решали на I этапе
  - Собрать функционально полный CA, который может стать альтернативой MS CA и, при необходимости, быстро заместить его

  ✓ **Сделано**
- Задачи v2
  - Переписать "движок" и подготовить продукт к сертификации
    - В составе кода - 92 бинарника
    - В "движке" и в разных сервисах используются разные стеки технологий (устаревшие)
    - Устранение уязвимостей
    - Проработка API и SDK для дополнительных сервисов (для др. разработчиков)
  - Разработать новые сервисы для автоматизации
    - Автоматический выпуск сертификатов для АРМов, серверов и др. оборудования
  - Поддержка HSM
  - Обеспечение отказоустойчивости, масштабирования, восстановления и др.

  ✓ **В работе (2023 г.)**
- Пилоты
  - Пока работаем только с теми, кто осознал критическую зависимость своей ИТ-инфраструктуры от MS CA и недопустимые риски в случае блокирования его работы
  - Работаем вместе, как партнёры

# Давайте делать всё правильно и безопасно!

- Нам дали уникальную возможность сделать всё правильно
  - Не пытаться точечно заместить один продукт другим, а начать с проектирования правильной и безопасной ИТ-инфраструктуры
- На банковском рынке это удалось сделать
  - Россия совершила "квантовый скачок" - перепрыгнула целую эпоху платёжных карт с магнитной полосой, сразу на смарт-карты - и стала одним из лидеров
- У нас есть исторический шанс
  - Спроектировать наши ИТ-инфраструктуры изначально правильно и безопасно, без наследования "родимых пятен"
  - Давайте стараться делать всё правильно и безопасно! …и немного на вырост
    - *PKI, сертификаты доступа, строгая аутентификация каждого субъекта инфраструктуры*


# Aladdin Enterprise CA

подробнее здесь:

**Стенд С-50**

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

# О компании

АЛАДДИН – ведущий российский разработчик-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.