Проблемы построения PKI на Linux, обеспечения безопасности и доверия в корпоративной ИТ-инфраструктуре

Точки отказа и ключевые элементы

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

PKI-форум—2023, 13 сентября 2023 г.

Изменение и оценка киберугроз с началом СВО

- Посетил 7-8 конференций - что обсуждается?
  - Чем заместить прикладное ПО ушедших из РФ зарубежных вендоров
  - Беспрецедентный рост успешных атак из-за слабой или неправильной аутентификации пользователей
  - Массовые утечки баз данных и персональных данных
  - Блокирование поставок и производства для РФ микроэлектроники
  - Необходимость всеобщего перехода на Linux

✓ **Все просто фиксируют факты, приводят статистику, предлагают средства мониторинга вместо противодействия…**

✓ **Никто системно и всерьёз не предлагает переоценить риски - в первую очередь, связанные с работоспособностью всей нашей ИТ-инфраструктуры, найти и в первую очередь устранить ТОЧКИ ОТКАЗА**

✓ **Движемся по инерции, боремся с навязанными нам угрозами (плохие парни-хакеры - взломы ресурсов, эксплуатация уязвимостей, вирусы-шифровальщики…)**

Изменение и оценка киберугроз с началом СВО

“Мы порвём экономику России в клочья!”

- Барак Абама — помните?
- 2012 г. - PPD-20, CloudAct
  - Решение о закладке в объекты критической информационной инфраструктуры России **кибербомб**, которые можно привести в действие для **вывода из строя** системы командования и контроля вооруженных сил противника, **объектов его критически важной инфраструктуры**
  - Решение, обязывающее американских вендоров осуществлять сбор и передачу в АНБ, ЦРУ и ФБР т.н. "**телеметрии**"
  - **Запрет** американским вендорам **на передачу и/или раскрытие исходных кодов ПО и прошивок** "железа" другим государствам
  - Задание ЦРУ по разработке маскировочных программных средств проведения компьютерных атак, в том числе под "чужим флагом”

✓ **Это были не пустые слова**

- Национальная стратегия кибербезопасности США
  - Март 2023
    - “Мы задействуем все имеющиеся у нас возможности, весь заложенный арсенал средств для **блокирования и вывода из строя ИТ-инфраструктуры организаций КИИ противника** - и с помощью кибератак, и с проведением военных операций (силами зависимых партнёров)”

✓ **С нами пока только играют, основной арсенал средств ещё не задействован**

Насколько уязвимы наши ИТ-инфраструктуры и причём здесь PKI?

Ахиллесова пята всех наших ИТ-инфраструктур

Все помним Ахиллеса…

- Провожу аналогию
  - Тратим силы и бюджеты на внешний периметр, на борьбу с плохими парнями
  - А прилетит в другое место - куда не ждёшь
  - Мы не правильно оценивали политические риски, архитектурные уязвимости (критические зависимости) и продолжаем плыть по течению…
    - Недавно так было с производством российских процессоров - все яйца сложили в одну корзину - TSMC, с ИБ-сервисами (облачная аутентификация пользователей)
- ВОПРОСЫ
  - ✓ **Что является единой точкой отказа для всех наших ИТ-инфраструктур?**
  - ✓ **Приведёт ли такой отказ к недопустимому ущербу?**
  - ✓ **Удастся ли отсидеться, изолировав свою сеть от Интернета?**
  - ✓ **Верите ли, что Они этого не сделают?**
  - ✓ **Какой приоритет следует поставить решению этой задачи?**

Что является единой точкой отказа для всех наших ИТ-инфраструктур?

Корпоративный центр выпуска и обслуживания сертификатов - MS CA

- От него зависят
  - Доверенное взаимодействие всех объектов и компонентов ИТ-инфраструктуры
  - Аутентификация всех объектов системы - оборудования, пользователей, приложений (ПО)
  - Работоспособность доменов безопасности/службы каталога
  - Работа различных сервисов (удалённого доступа, VDI, VPN, RDP-шлюзы и др.)
- Никто не задумывается над вопросами
  - Что такое ДОВЕРИЕ, как оно обеспечивается, КОМУ мы доверяем?
  - Откуда берутся сертификаты доступа (машинные, пользовательские, ПО)?
  - Кто принимает решение "свой-чужой" (проверяет валидность сертификатов, пускает пользователей в систему)?

✓ **Как это будет работать при переходе на Linux? (ожидаем, что так же как в Windows?)**

✓ **Есть ли PKI под Linux?**

Можно ли построить безопасную доверенную ИТ-инфраструктуру крупной организации без PKI?

Что такое ДОВЕРИЕ и как оно обеспечивается

- 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
  - Система является **доверенной**, когда каждый её элемент надёжно (**гарантированно**) идентифицирован и аутентифицирован

✓ **Для ИБ важнее не доверие, а ГАРАНТИИ**

  - Гарантии даёт криптография (гарантированная стойкость), PKI (централизованная инфраструктура), безопасность закрытых ключей
  - Основа доверительных отношений - АУТЕНТИФИКАЦИЯ, для критических систем - **строгая (2ФА)**
  - Для СТРОГОЙ аутентификации между всеми компонентами ИТ-инфраструктуры необходимо разворачивание PKI (инфраструктуры открытых ключей)
  - Основа PKI - центр выпуска и обслуживания сертификатов (**корпоративный CA**)

✓ **Построить безопасную доверенную ИТ-инфраструктуру крупной организации без PKI нельзя**

Ключевые элементы и точки отказа в ИТ-инфраструктуре

Все смотрели фильм “Стиляги”?
Помните сцену - В Америке нет стиляг!

Для многих такое же откровение, что **в Linux нет полноценного PKI**...

Ключевой элемент и точка отказа всей ИТ-инфраструктуры

Проблема №1

- Ключевой и самый критичный элемент во всей ИТ-инфраструктуре - центр выпуска и обслуживания цифровых сертификатов (CA)
  - CA - основа доверенного взаимодействия всех объектов и компонентов в сети
- Практически все ИТ-инфраструктуры в России построены на базе MS CA (CS)
  - …и на 100% зависят от его работоспособности
  - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержки MS CA больше нет, купить его тоже нельзя
  - С 30 сентября 2023 г. Microsoft перестаёт продлевать подписки корпоративным клиентам из России
- Полноценных аналогов корпоративного MS CA в Open Source проектах нет
  - Коммерческие Enterprise-версии CA под Linux - стратегический товар - под строгим запретом, в Россию не поставляются

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

✓ **MS CA - ключевая точка отказа для всей ИТ-инфраструктуры**

✓ **Риски блокирования работы сервиса MS CA - очень большие (в т.ч. через закладки)**

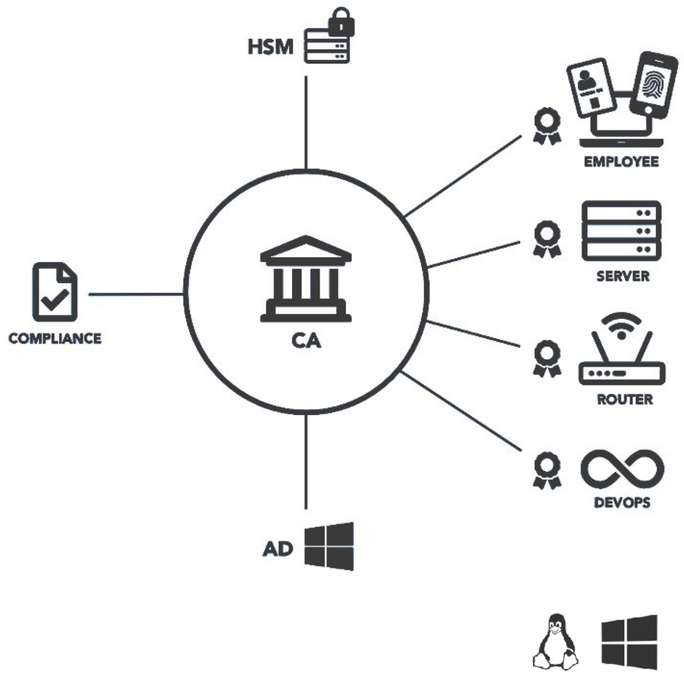
Проблемы построения PKI под Linux

Проблема №2

- 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/контроллерами доменов всех отечественных ОС (Linux)**

✓ **Простого аналога MS CA (CS) недостаточно - заткнём дыру, но задачи импортозамещения и санкционной независимости не решим**



Проблема №3

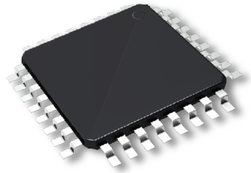
- В Linux нет полноценной поддержки PKI и 2ФА пользователей
  - В Windows аутентификацию пользователей (2ФА) реализуют **встроенные сервисы** (вкл. MS Smart Card Logon)
  - Полноценного аналога для Linux нет (клиента PKI и 2ФА)

✓ **Реализовать строгую аутентификацию пользователей для Linux можно (руками), но достаточно сложно**

Проблемы обеспечения строгой аутентификации в ИС

Проблема №4

- 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**

Что нужно сделать СРОЧНО,
чтобы не вырубили всю ИТ-инфраструктуру?

Что нужно сделать СРОЧНО

- Молиться, чтобы не заблокировали MS CA
- Параллельно MS CA поставить Aladdin Enterprise CA (на Linux)
- От корневого MS CA (пока работает) для него выпустить подчинённый сертификат
  - Невозможность выпуска сертификата для подчинённого CA от корневого CA полностью парализует работу всех сервисов и всей ИТ-инфраструктуры
- Для Aladdin Enterprise CA настроить автоматический выпуск новых сертификатов
  - Чтобы он постепенно перехватывал на себя выпуск/перевыпуск и обслуживание сертификатов
  - Это позволит произвести постепенный бесшовный переход на него (постепенное замещение MS CA - если Бог даст нам на это время…)

✓ **Делать это надо немедленно!**

✓ **С октября думаем запустить спец. программу**

Как и чем заменить MS CA

НОВИНКА!

Aladdin Enterprise CA

Корпоративный центр сертификации (CA) под Linux

- ключевой компонент

для обеспечения доверия в ИТ-инфраструктуре на базе PKI

Сертификация: по линии ФСТЭК России (до гостайны вкл.)

В Реестре отечественного ПО

Импортозамещение: Microsoft Certificate Services (MS CA)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

Aladdin Enterprise CA под Linux

- Обеспечивает
  - Создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)
  - Управление жизненным циклом цифровых сертификатов
  - Объединение всех компонентов ИТ-инфраструктуры в **единый домен безопасности,** их аутентификацию и безопасное взаимодействие
  - Обслуживание в **автоматическом** режиме всех объектов и компонентов корпоративной инфраструктуры ключами и цифровыми сертификатами
    - контроллеров доменов
    - серверов, Web-серверов, эл. почты
    - роутеров, маршрутизаторов, межсетевых экранов, VDI, VPN, RDP-шлюзов
    - компьютеров и др. устройств в доменах
    - M2M, IIoT-устройств
    - пользователей
  - Построение доверенной безопасной ИТ-инфраструктуры на базе PKI в сложных гетерогенных, облачных и мультиарендных инфраструктурах с разделением ролей и полномочий
  - Масштабирование, отказоустойчивость и разделение ролей
    - каждая функциональная роль центра сертификации (CA, RA, WebEnrol, CDP, DB и др.) может быть развёрнута на отдельном сервере в отказоустойчивой конфигурации

Aladdin Enterprise CA под Linux

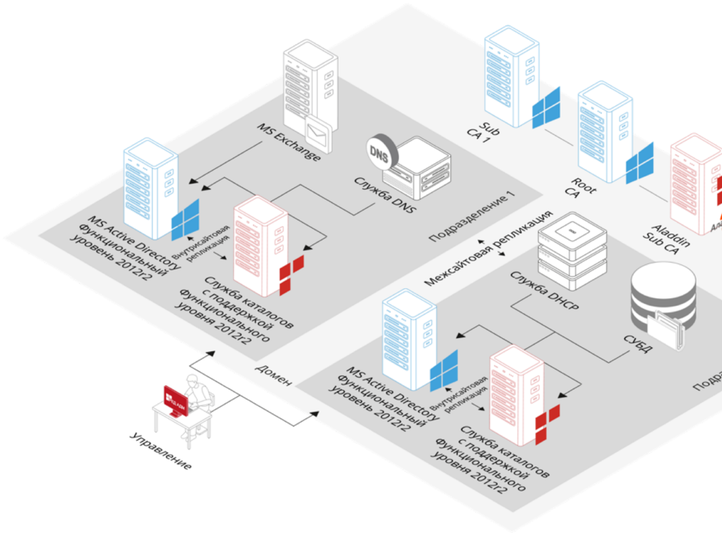
- Позволяет
  - Поставить Aladdin eCA параллельно с действующим MS CA
    - Выпустить на него подчинённый сертификат (от действующего корневого CA)
    - Настроить автоматический выпуск новых сертификатов
    - Импортировать и использовать действующие шаблоны сертификатов Microsoft CA, создавать новые
  - Одновременно работать с различными службами каталогов (**как Windows, так и Linux**)
    - MS Active Directory
    - Samba DC
    - FreeIPA
    - ALD Pro
    - **РЕД АДМ** (промышленная редакция) - **отработаны сценарии бесшовной миграции**
    - Альт Домен
  - Интегрироваться с различными внешними системами через REST API
    - IdM, IAM, IGA, SIEM, **JMS** и др.
  - Обеспечить строгую двухфакторную аутентификацию (в т.ч. под Linux)
  - Использовать различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды

Aladdin eCA в домене РЕД АДМ – сценарий миграции

- Процедура миграции PKI
  - Разработаны и протестированы подробные инструкции и методики по бесшовной миграции
    - Новая ветка ROOT
    - Действующий ROOT CA
  - Миграция шаблонов

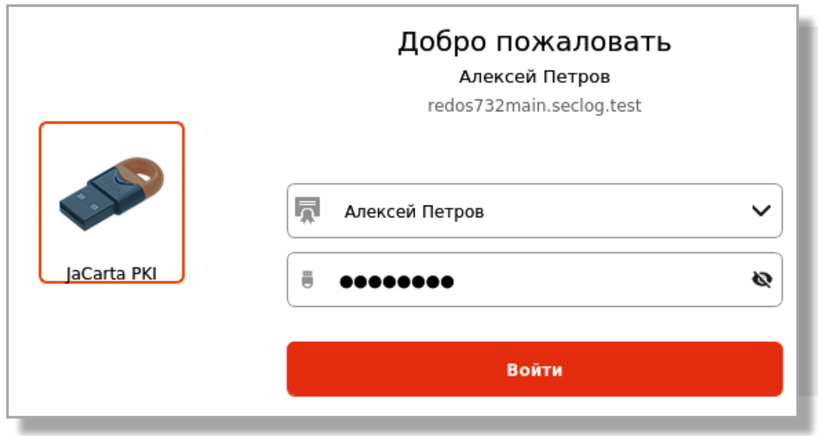
✓ **Сертификаты работают в Windows и Linux**

- Репликация с MS AD 2003, 2008_R2, 2012_R2, 2016 в домен РЕД АДМ:
  - Структуры домена
  - Пользователей
  - Двустороння репликация групповых политик
- В итоге получаем
  - Комплексную и бесшовную миграцию AD и CA
  - Плавный вывод продуктов Microsoft без остановки сервисов
  - Гарантию работоспособности инфраструктуры в случае отключения MS CA



Aladdin SecurLogon

НОВИНКА!



PKI-клиент и поддержка средств 2ФА в Linux

- замена MS Smart Card Logon

Проблемы:

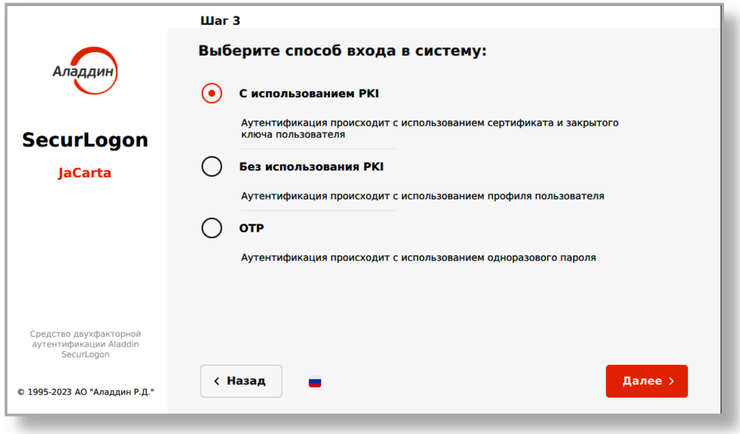
В MS Windows 2ФА пользователей реализует встроенная подсистема Windows Smart Card Logon

В российских ОС на базе Linux подобного механизма нет, всё надо делать руками (34 доп. пакета), но это будет только вход в Linux (замкнутая экосистема)

Aladdin SecurLogon

- Обеспечивает
  - **Полноценную поддержку PKI**, двух- и трёхфакторную **строгую** аутентификацию пользователей в смешанных гетерогенных средах, в ОС на базе Linux, Windows и macOS
  - Работу с доменами Microsoft AD, FreeIPA, Samba DC, ALD Pro
  - Усиленную аутентификацию пользователей с использованием автоматически сгенерированного сложного пароля длиной до 63 символов
    - Для инфраструктур, где **PKI ещё не развёрнута**
  - Применение политик входа на основе принадлежности пользователя к группе безопасности (только токен, токен или пароль, только пароль)
  - Групповое развёртывание и удалённую настройку с рабочего места администратора
  - Защиту удалённых соединений (RDP, SSH)
  - Дополнительные сервисные функции, позволяющие до входа в ОС разблокировать токен, сменить ПИН-код пользователя, кастомизировать окно приветствия и др.

✓ **Полноценная альтернатива Microsoft Smart Card Logon на отечественных ОС на базе Linux**



Работает с USB-токенами и смарт-картами JaCarta

Основа создания доверительных отношений

- СТРОГАЯ аутентификация пользователей

Строгая аутентификация для Linux

- Что значит СТРОГАЯ
  - Двухфакторная (2ФА), с использованием персонального специализированного защищённого устройства (требования новых ГОСТов)
    - с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом
    - с хранением сертификатов доступа с памяти устройства
    - с возможностью его использования только авторизованным пользователем
    - неклонируемого (Secure by design)
  - Взаимная (аутентификация обеих сторон)
  - С использованием защищённых протоколов
- Требуется
  - Во всех системах, обрабатывающих значимую информацию
    - гос. организации, КИИ, АСУ ТП и др.
  - Для администраторов, пользователей, удалённых пользователей
  - Развёрнутая инфраструктура открытых ключей (PKI)
  - Централизованное управление жизненным циклом сертификатов, средств 2ФА
  - Модуль поддержки средств 2ФА и PKI для Linux
    - **В Linux нет аналога MS Smart Card Logon**

Линейка USB-токенов и смарт-карт JaCarta
(вкл. российские чипы I и II категории)
с сертификацией по КС-3 (ФСБ) и УД-2 (ФСТЭК)

Средства для строгой двухфакторной аутентификации (2ФА) и ЭП

- безопасный доступ в Linux по сертификатам (PKI)

Проблемы:

В российских ОС на базе Linux нет поддержки средств 2ФА пользователей и PKI

Во многих ИТ-инфраструктурах в РФ до сих пор не используется 2ФА!

BIO-токен

2ФА на базе смарт-карт и USB-токенов уже недостаточно!

Нужна дополнительная надёжная биометрическая идентификация пользователей

ВАЖНО:

Для противодействия ВНУТРЕННЕМУ нарушителю

Чтобы ЭП стала действительно подписью, а не эл. печатью (физически не привязанной к своему владельцу)!

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*

Аладдин

Спасибо!

Сергей Груздев
ген. директор
АО "Аладдин"

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, IIoT-устройств, Web-порталов и эл. сервисов.