



Ключевые компоненты для построения безопасной доверенной ИТ-инфраструктуры

Сергей Груздев

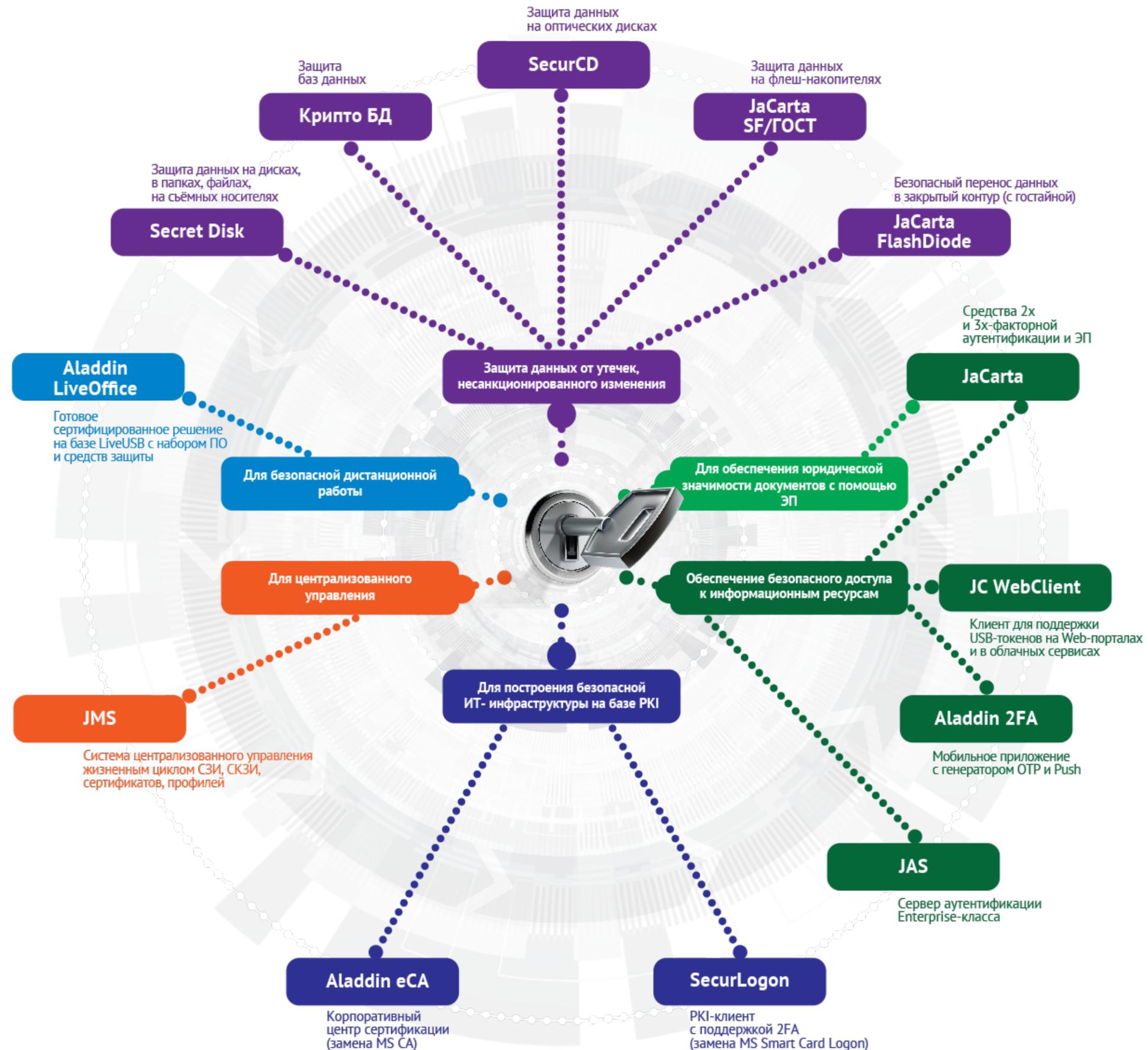
ген. директор АО "Аладдин Р.Д."



Линейка продуктов

HASP - eToken - JaCarta - ...

Линейка продуктов сильно выросла и изменилась:
- ключевые решения для построения безопасной доверенной ИТ-инфраструктуры



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 **ответственности**, что другой не воспользуется 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
- ◆ Одной уверенности мало, нужны меры (уровни) доверия и гарантии...



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

В.В. Путин

Гарантии дают **криптография** (гарантированная стойкость) и **PKI**

Аутентификация

- основа создания доверительных отношений

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

Тип аутентификации	Вероятность и размер возможного ущерба		
	Низкая	Средняя	Высокая
Высокая	Усиленная	Строгая	Строгая
Средняя	Простая	Усиленная	Строгая
Низкая	Простая	Простая	Усиленная

Уровень значимости информации в ИС

Кому:

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

Для кого:

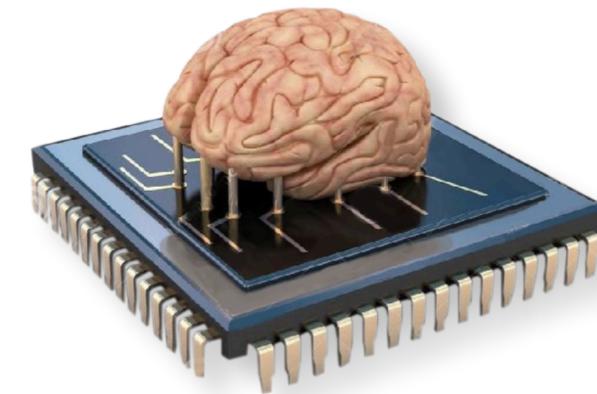
- **Для всех пользователей ИС**
- Для администраторов
- **Для удалённых пользователей**

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

Сейчас они есть у всех!
Но и этого недостаточно

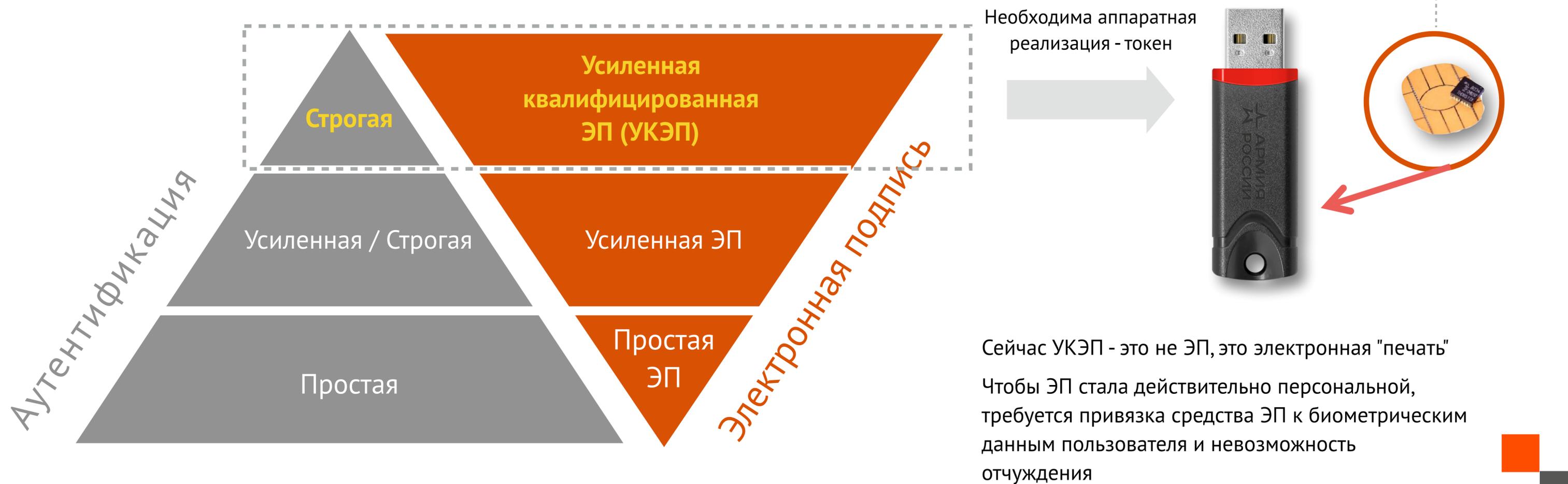
Что нужно для реализации СТРОГОЙ аутентификации

- ◆ 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 (ОТР) 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!



Тип аутентификации определяет тип ЭП в ИС

- ◆ Надёжность системы определяется по её самому слабому звену
 - Если в ИС необходимо обеспечить **юридически значимую ЭП**, приравненную к собственноручной, то для получения усиленной квалифицированной ЭП (УКЭП) должна быть обеспечена **СТРОГАЯ** аутентификация пользователей
 - Строгая аутентификация предполагает **ДВУХФАКТОРНУЮ** (с использованием защищённого неклонировемого аппаратного устройства с поддержкой криптографии "на борту" с неизвлекаемым закрытым ключом ЭП)



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

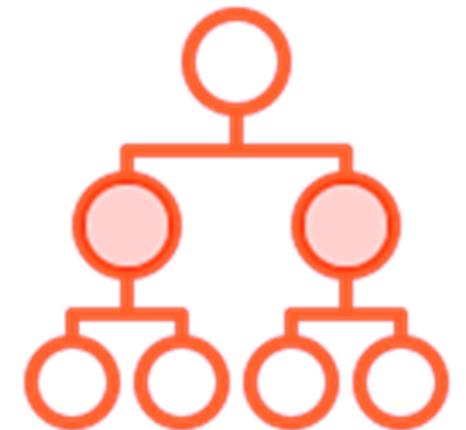
- ◆ Практически все ИТ-инфраструктуры в России построены на базе MS CA
 - ...и на 100% зависят от его работоспособности
 - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержка MS CA больше не осуществляется, купить его тоже нельзя
 - Аналогов под Linux нет - кто купит, если MS CA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



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

Проблема №2

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

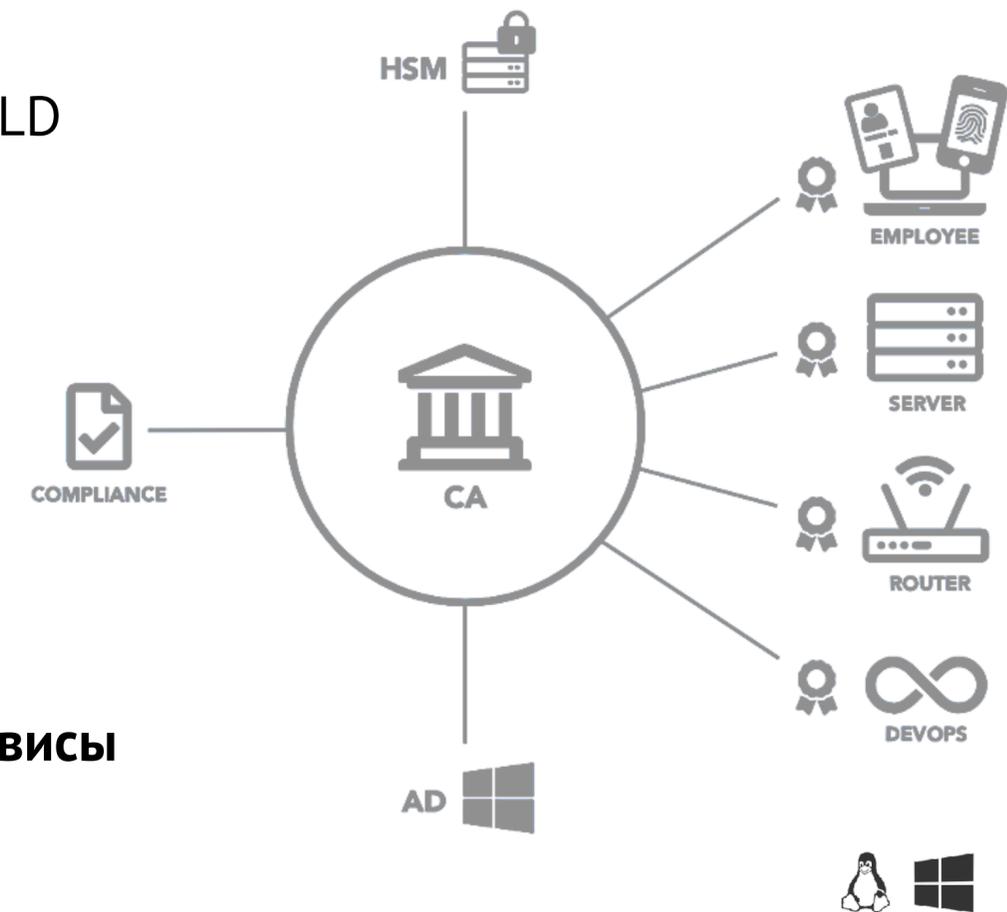


Проблема №3

- ◆ 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**

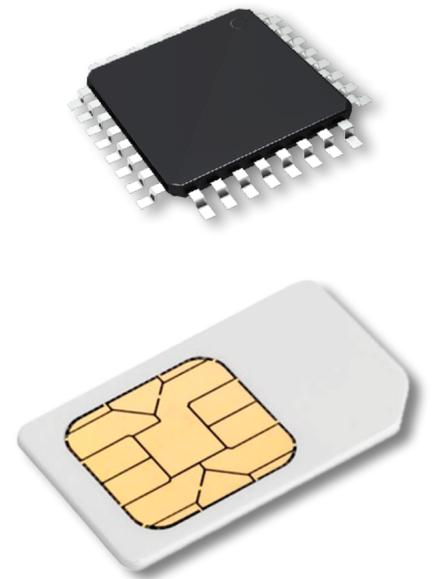
Проблема №4

- ◆ 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)



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**





Корпоративный центр сертификации (CA)

- **ключевой компонент**

для построения безопасной доверенной
ИТ-инфраструктуры на базе PKI на Linux

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

В Реестре отечественного ПО

Импортозамещение: Microsoft Certificate Services (MS CA)



Актуальность и важность замещения MS CA

- ◆ Корпоративный центр выпуска и обслуживания сертификатов (CA)
 - Основа (сердце) всей ИТ-инфраструктуры современной организации
 - работоспособности доменов безопасности/службы каталога
 - различных сервисов
 - аутентификации устройств, пользователей, приложений
 - доверенного взаимодействия всех объектов и компонентов
 - ◆ Риски
 - 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
 - Полноценных аналогов MS CA в Open Source проектах нет
 - Коммерческие Enterprise-версии CA под Linux в Россию не поставляются (под строгим запретом)
- ✓ **Риски блокирования работы сервиса MS CA - очень большие**



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, IoT-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
 - Работать параллельно с действующим Microsoft CA
 - 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
 - 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
- ✓ **Замена для Microsoft Certificate Services (MS CA)**





Средства для строгой двухфакторной аутентификации (2ФА) и ЭП
- безопасный доступ в Linux по сертификатам (PKI)



Строгая аутентификация для Linux

◆ Что значит СТРОГАЯ

- Двухфакторная (2ФА), с использованием персонального специализированного защищённого устройства
 - с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом
 - с хранением сертификатов доступа с памяти устройства
 - с возможностью его использования только авторизованным пользователем
 - неклонировемого (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)

Добро пожаловать

Алексей Петров
redos732main.seclog.test



Алексей Петров

••••••••

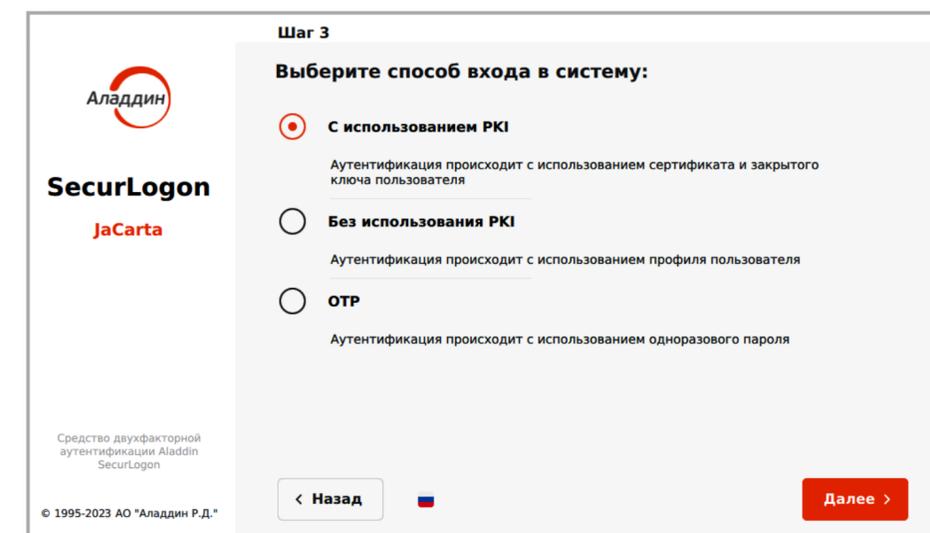
Войти

PKI-клиент и поддержка средств 2ФА в Linux - замена MS Smart Card Logon

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

◆ 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**





Готовое сертифицированное средство
для организации безопасной дистанционной работы
с возможностью подключения к ГИС, обработки информации
ограниченного распространения

Использует ViPNet Client

- можно лицензировать отдельно и дополнительно зарабатывать на услугах!

◆ Позволяет

- Использовать специализированное защищённое USB-устройство Aladdin LiveOffice вместо служебного ноутбука
 - как удалённое рабочее место (терминал) с набором предустановленного и преднастроенного ПО
 - работать в замкнутой доверенной программно-аппаратной среде
- Автоматически выполнить все требования и политики безопасности
- Полностью соответствовать требованиям ФСТЭК и ФСБ России по организации безопасной дистанционной работы
- Обеспечить централизованное управление (с использованием JMS)
- Решается проблема контролируемой зоны, не требуется аттестация рабочего места сотрудника
- В 5-7 раз экономить бюджет при организации дистанционной работы сотрудников и контрагентов



◆ Примеры кейсов

- Работа с внешними контрагентами (не сотрудниками организации)
 - Заказчик ведёт базу эл. полисов, оформляют полисы - контрагенты (не сотрудники)
 - Выдать всем им служебные защищённые ноутбуки - дорого, а заставить всех их выполнять требования безопасности - невозможно
 - Риски утечки информации, компрометации учётных данных, атак на ИС, внесение несанкционированных изменений в базу - огромны
 - Решение - подключать к работе с ИС только тех, кто самостоятельно приобрел правильное сертифицированное средство, обеспечивающее безопасную дистанционную работу
- Онлайн-работа и дистанционное обслуживание 1С-бухгалтерии, ERP, фреш
 - Практически все организации КИИ, гос., ФОИВы работают на 1С - установлено **в закрытом контуре, информация критически важная**
 - Администрирование, обслуживание, поддержку осуществляют 1С-франчайзи, используя **удалённое подключение**
 - Требуется выдача служебного компьютера (являющегося частью ГИС), аттестация рабочего места, организация контролируемой зоны - очень сложно и дорого





◆ Обеспечивает

- Полноценную дистанционную работу с любого недоверенного компьютера, например, с личного
 - в ГИС, КИИ, АСУ ТП, МИС и др. до 1-го класса защищённости
 - в ИСПДн до 1-й уровня защищённости персональных данных
- Возможность обработки персональных данных
- Возможность обработки коммерческой, служебной тайны
 - налоговой, врачебной, банковской, нотариальной, аудиторской, в области обороны и др.
- Защиту от внутреннего нарушителя - **пользователь не сможет:**
 - скопировать, распечатать, переслать служебный документ
 - передать посторонним и скомпрометировать свой аккаунт, пароль, параметры подключения
 - загрузить в информационную систему троян или вирус

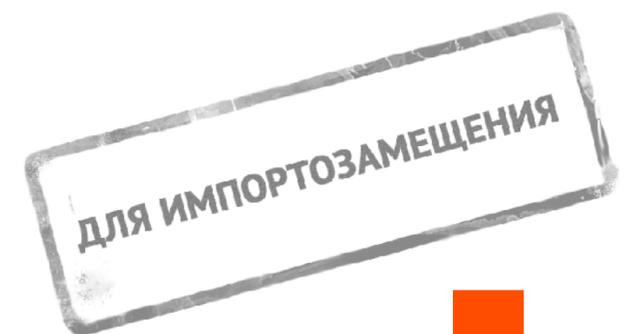
✓ **Является альтернативой служебному ноутбуку с набором установленных приложений и сертифицированных средств защиты**

- ◆ Сертификаты: ФСТЭК России, ФСБ России (на компоненты, содержащие криптографию)



Защита данных на дисках - замена MS BitLocker

Вся служебная информация, выносимая за пределы организации, должна быть зашифрована
В условиях санкций, атак на КИИ, "окирпичивания" многих зарубежных продуктов продолжать использовать встроенный в MS Windows BitLocker - лучший способ похоронить свои данные



- ◆ Обеспечивает
 - Предотвращение утечки и несанкционированного доступа к ценной информации при утере, краже, изъятии, ремонте, неправильной утилизации компьютеров, серверов, носителей информации
 - Прозрачное шифрование данных
 - на ноутбуках, ПК, планшетах сотрудников
 - на файл-серверах и серверах приложений (в т.ч. баз данных)
 - на съёмных носителях
 - Соккрытие наличия ценной информации на защищённом компьютере, сервере или носителе
 - Гарантированное необратимое удаление данных
 - Экстренное блокирование доступа к защищённым разделам на серверах (базы данных, корпоративная почта и др.) по сигналу "тревога"
 - Безопасную передачу конфиденциальной информации по незащищённым каналам связи
 - Фиксацию фактов доступа к защищённой информации
 - Защиту от действий привилегированных пользователей (системных администраторов)
 - Централизованное управление, интеграцию с системой управления JMS (для Enterprise-версии)



- Персональная версия
- Для серверов (приложений, файловых)
- С централизованным управлением (Enterprise)
- Версия под Linux - имеет сертификат МО для работы с ГТ ("СС")



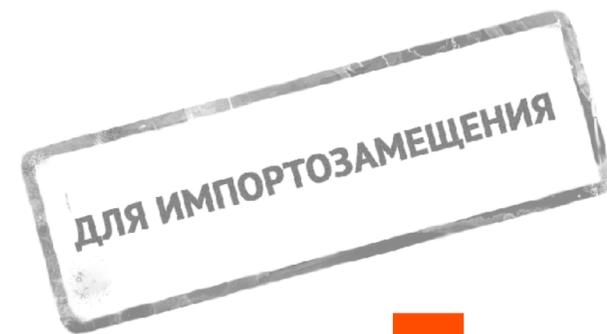
Защита баз данных

- импортозамещение встроенных в зарубежные СУБД средств защиты на отечественные, сертифицированные

Не всегда можно отказаться от использования Oracle и др. зарубежных СУБД

- огромные базы, которые российские аналоги не потянут
- огромное количество работающих приложений, для переноса которых могут потребоваться десятилетия

Технология "оправославливания" зарубежных СУБД позволяет существенно снизить риски и продолжить их использование



◆ Обеспечивает

- Защиту главных информационных активов организации (ERP, CRM, ИБС, ИСПДн и др.)
 - от утечек и кражи
 - от внесения несанкционированных изменений и искажения чувствительной информации
 - от несанкционированного доступа к критически важным данным администраторов СУБД (внутренних нарушителей)
- Обезличивание персональные данные
- Прозрачное селективное (выборочное) шифрование критически важных данных в СУБД с использование российских алгоритмов
- Двухфакторную аутентификацию пользователей при доступе к данным в СУБД
- Централизованное управления ключами шифрования, исключающее возможные несанкционированные действия администраторов БД
- Реализацию требований регуляторов
 - по обеспечению конфиденциальности и целостности информации в СУБД
 - по защите персональных данных, PCI DSS, ИС организаций КИИ
 - по моделям разделения доступа - дискретной и мандатной
- Получение некорректируемой юридически значимой доказательной базы для проведения расследований инцидентов информационной безопасности

◆ Сертификаты ФСБ России до класса КС-3



Для СУБД Oracle,
MS SQL, Tibero, PostgreSQL,
Postgres Pro, Jatoba

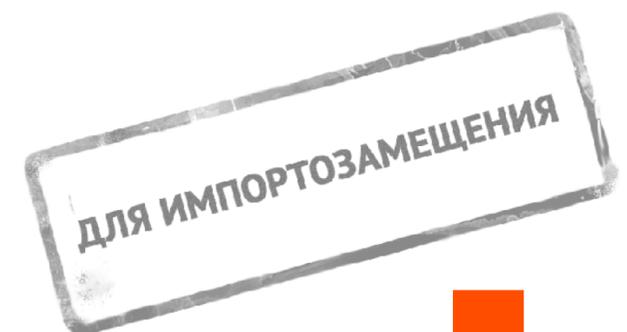


Система централизованного управления жизненным циклом сертификатов, токенов, СЗИ, СКЗИ

Включает высокопроизводительный сервер аутентификации
Enterprise-класса - JAS

Импортозамещение: любого импортного аналога

Версии: Linux, Windows



JMS - система централизованного управления Enterprise-класса

◆ Обеспечивает

- Учёт и управление жизненным циклом
 - токенов, смарт-карт, "облачных", программных токенов, OTP/PUSH/SMS аутентификаторов, U2F-токенов
 - защищённых съёмных носителей
 - смарт-карт ридеров
 - средств безопасной дистанционной работы
 - СЗИ, СКЗИ, сертификатов, объектов РКІ, профилей
- Автоматизацию большинства рутинных операций и применения политик безопасности (например, требований к ПИН-кодам)
- Быструю подготовку типовых профилей, конфигураций для разных групп пользователей, ввод в эксплуатацию новых средств, "взятие под управление" выпущенных до внедрения JMS
- Удобный сервис самообслуживания пользователей (Web-портал)



JMS - система централизованного управления Enterprise-класса

◆ Позволяет

- Интегрироваться с внешними ресурсными системами - источниками информации о пользователях и рабочих станциях, с сервисом "облачной" подписи КриптоПро DSS и др.
- Связывать учётные записи пользователей из различных ресурсных систем
- Обслуживать сертификаты для аутентификации и ЭП, выданных различными удостоверяющими центрами
- Вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
- Автоматически рассылать уведомления
- Дистанционно и безопасно обновлять "прошивки" устройств (firmware), образы встроенных ОС и приложений (только для своих продуктов!)
- Добавлять необходимую функциональность за счёт разработки и подключения дополнительных модулей и коннекторов
- Использовать версию для Linux или для Windows

◆ Сертификаты

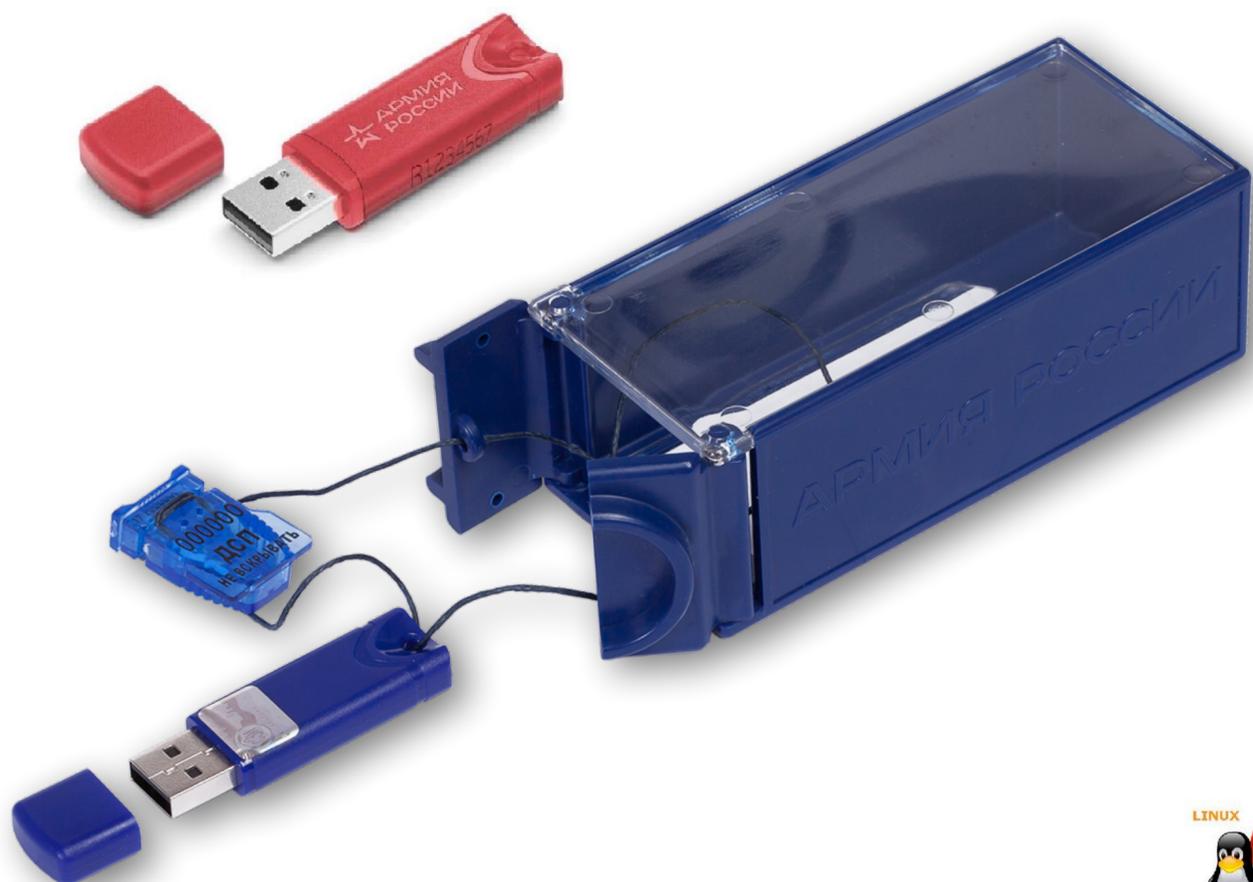
- ФСТЭК России
- Минобороны России (для работы с гостайной со степенью секретности "Совершенно секретно")



Что массово поставляем в силовые ведомства

ЗМНИ JaCarta SF/ГОСТ

Защищённый служебный USB-накопитель для безопасного хранения, переноса информации с контролем её отчуждения (разрешением копирования на данный компьютер или с него)



НОВИНКА!

JaCarta FlashDiode

Персональный специализированный однонаправленный USB-флеш-накопитель для безопасного переноса информации из открытого контура в закрытый (с ГТ)

- Для замены одноразовых (неперезаписываемых) оптических дисков CD-ROM и дорогих однонаправленных USB-шлюзов
- Для ускорения и удешевления процесса



НОВИНКА!

SecurCD

Защита данных от утечек при их передаче на CD-ROM



Давайте делать всё правильно и безопасно!

- ◆ Нам дали уникальную возможность сделать всё правильно
 - Не пытаться точно 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*
- ◆ Сможем заработать на этом!





Инфраструктурные продукты Аладдин для построения PKI на Linux

Сергей Груздев
ген. директор АО "Аладдин Р.Д."



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.