Ключевые компоненты для построения безопасной доверенной ИТ-инфраструктуры.

Дмитрий Шуралев

АО "Аладдин Р.Д."

Комплексный подход в построении защищенной ИС

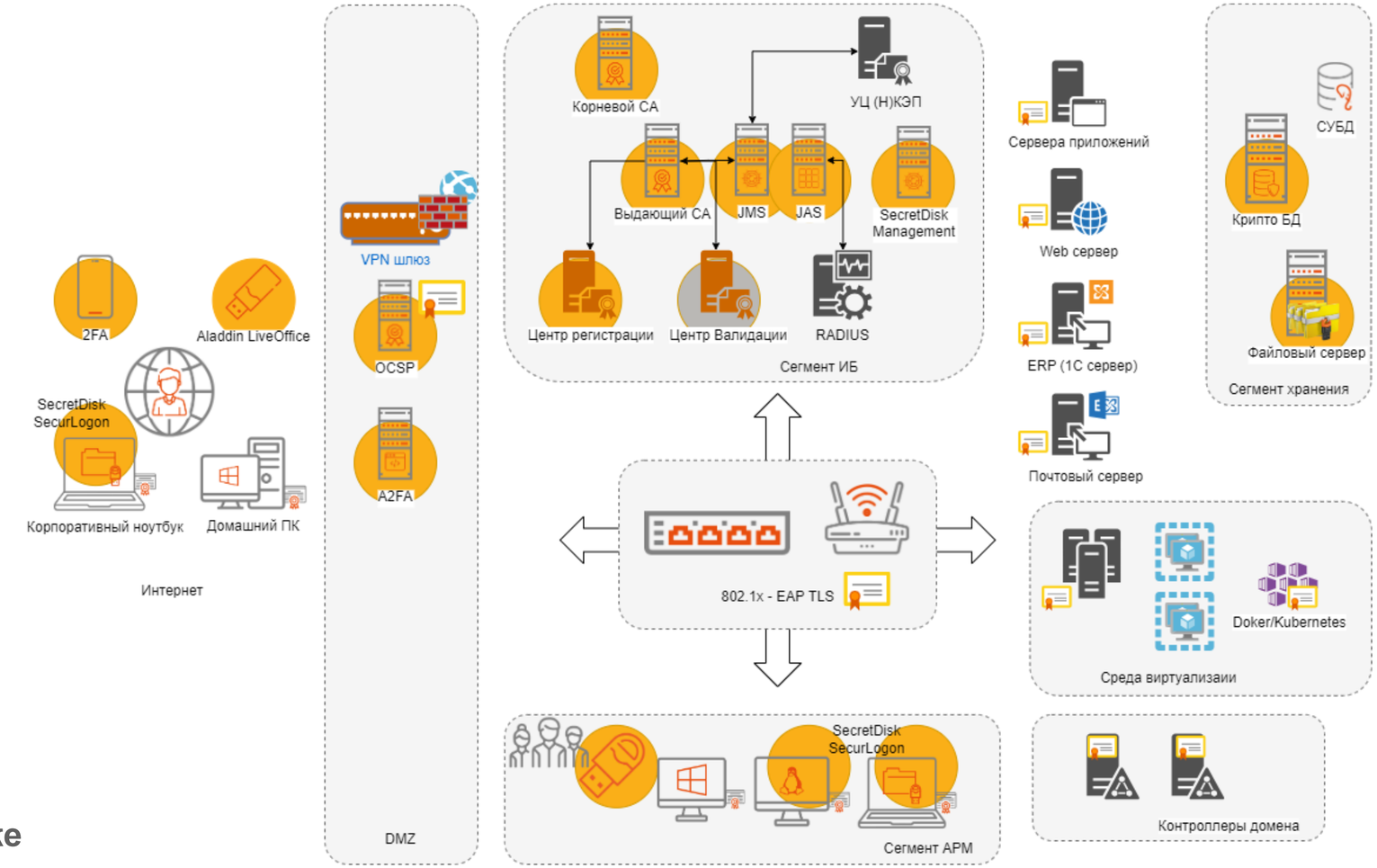
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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

Усиленная аутентификация
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- 2FA
- 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 (v2.0 ноябрь)

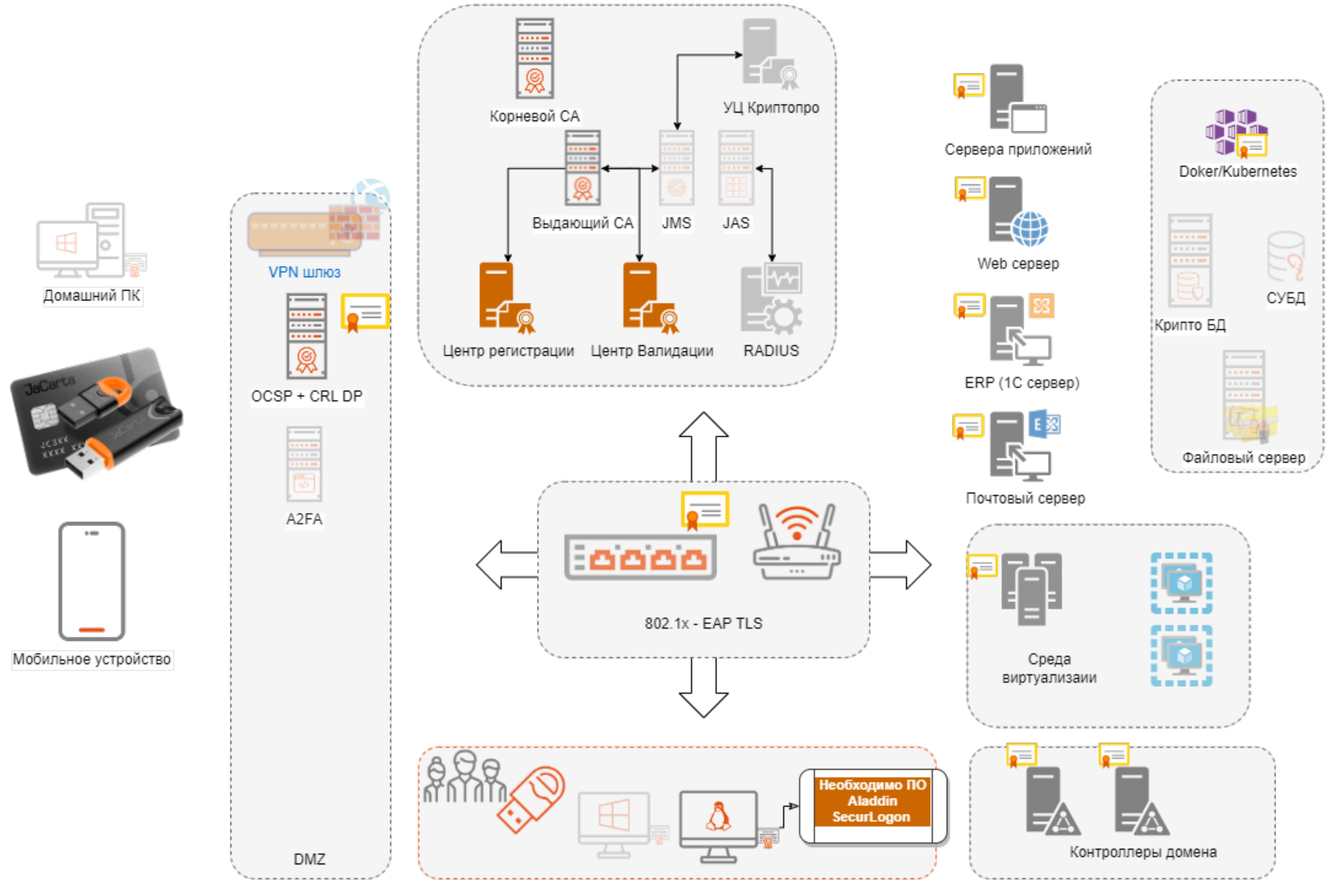


Aladdin Enterprise CA – замена Microsoft Certificate Services (MS CA)

Назначение - создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)

Цель - объединение всех компонентов ИТ-инфраструктуры в единый домен безопасности, их аутентификацию и безопасное взаимодействие

- **В Реестре отечественного ПО**
  №2021663130
- **На сертификации ФСТЭК России УД4**
  Срок получения сертификата конец Q2 2024

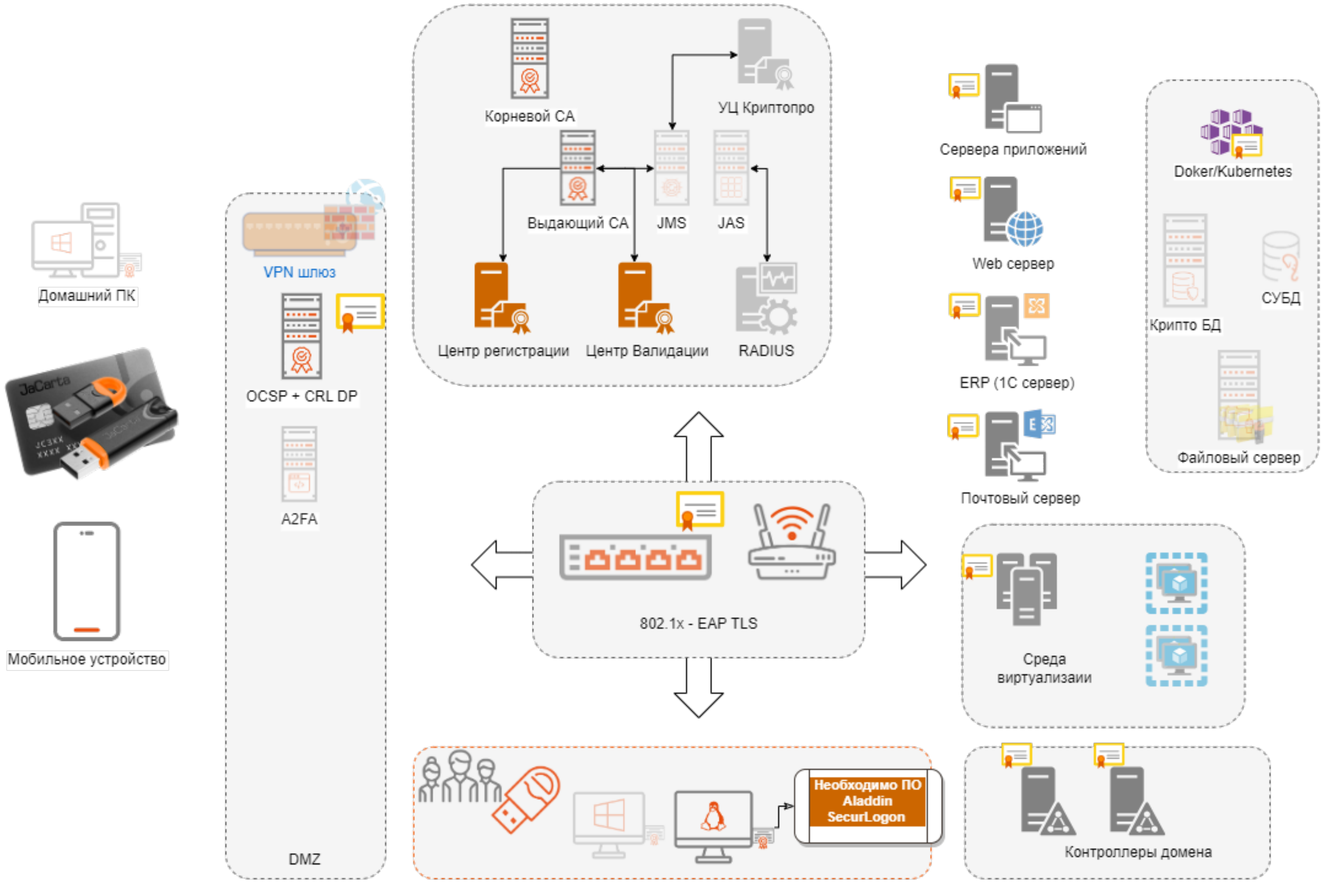


Aladdin Enterprise CA – замена Microsoft Certificate Services (MS CA)

- **Построение иерархии центров сертификации (корневой, подчиненный)**
  - Центр сертификации - выпуск сертификатов, управление сертификатами, управление шаблонами, управление ролевой моделью и правами операторов и администраторов CA.
  - Центр валидации – точка распространения CRL, поддержка протокола OCSP
  - Центр регистрации – выпуск сертификатов по запросам, API, портал самообслуживания, на мобильные

- **Интеграция с доменами**
  - MS Active Directory
  - РЕД АДМ (промышленная редакция)
  - Альт Домен
  - ALD Pro
  - Samba DC
  - FreeIPA

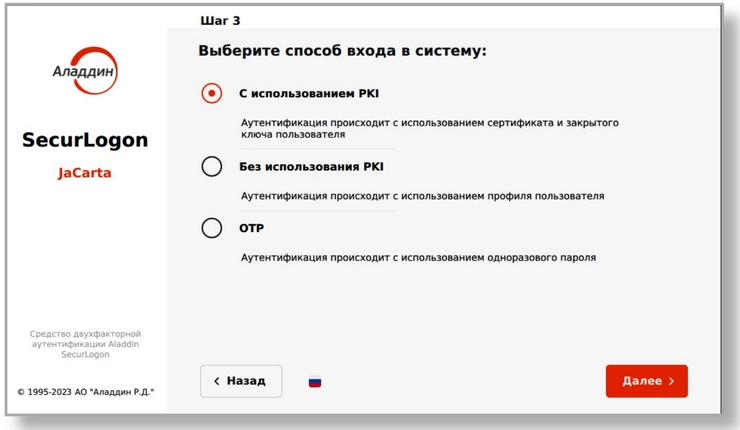
- **Поддержка PKI на клиенских АРМ с использованием ПО Aladdin SecurLogon**
  - Обязательный компонент на отечественных ОС
  - Не требуется на ОС Windows



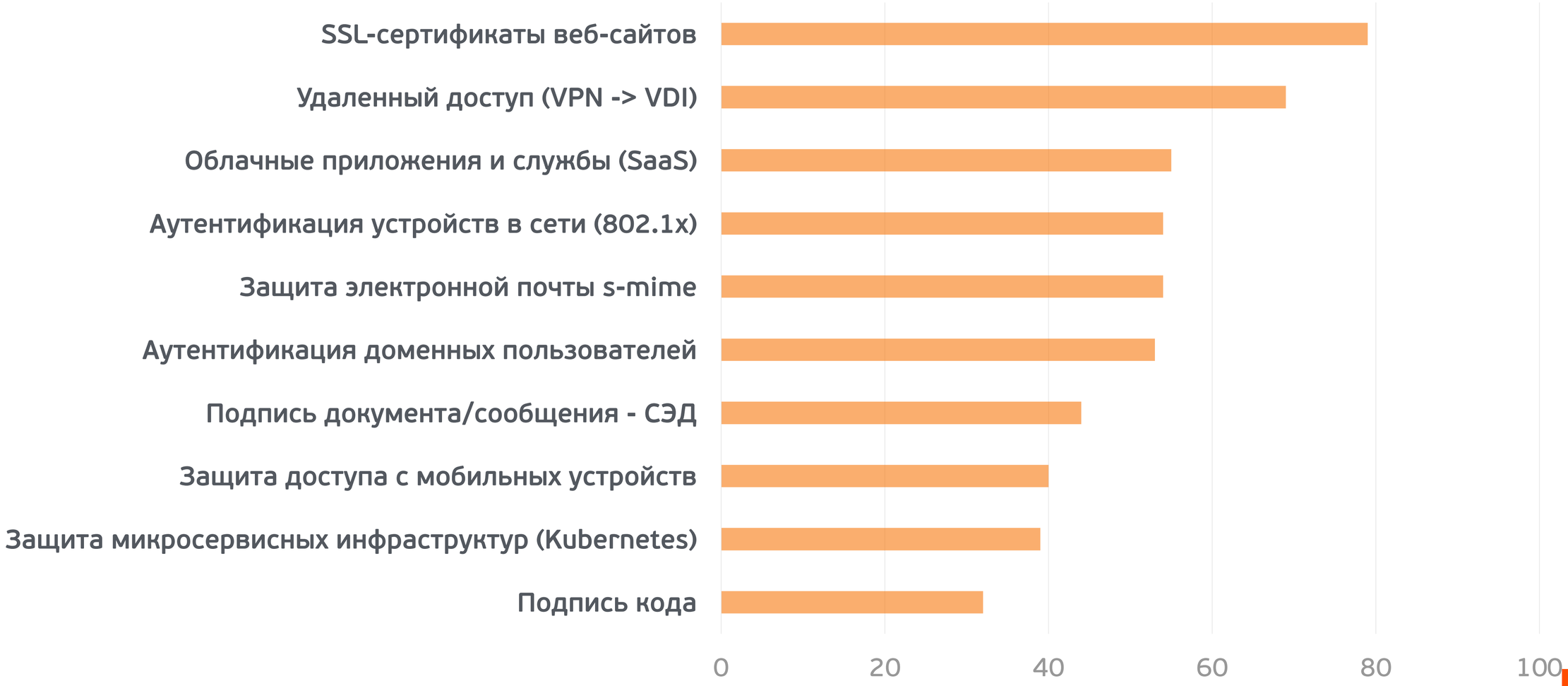
Aladdin SecurLogon

- 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**



Типовые сценарии применения цифровых сертификатов



Aladdin Enterprise CA под Linux

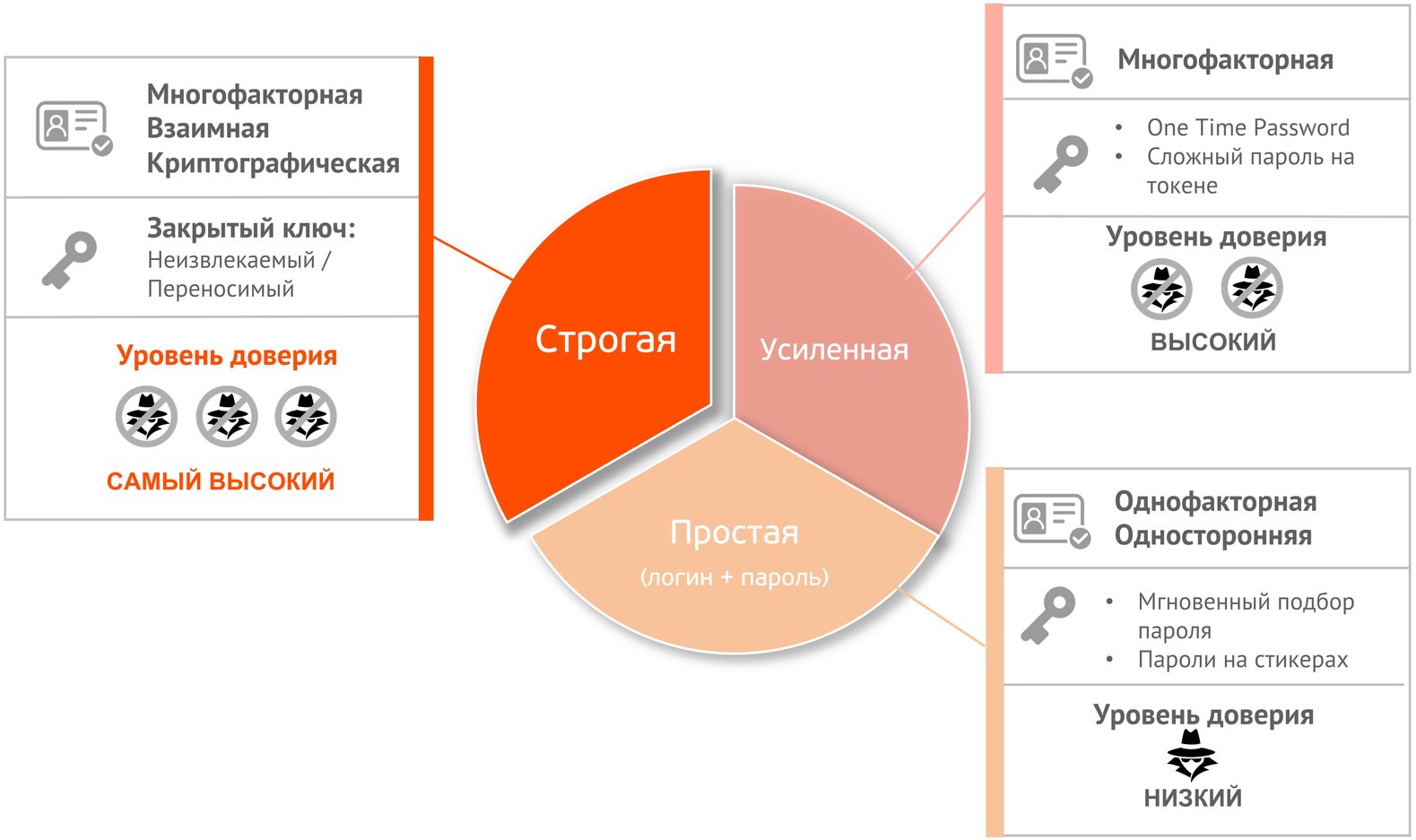
- Позволяет
  - Работать параллельно с действующим Microsoft CA
  - Импортировать и использовать действующие шаблоны сертификатов Microsoft CA, создавать новые
  - Одновременно работать с различными службами каталогов (как Windows, так и Linux)
  - Интегрироваться с различными внешними системами через REST API
    - IdM, IAM, IGA, SIEM, JMS и др.
  - Использовать различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды
  - Ролевая модель и делегирование 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
  - Обеспечить строгую двухфакторную аутентификацию (в т.ч. под Linux)

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

Инфраструктура открытых ключей и сертификаты

Аутентификация пользователей информационной системы



Строгая аутентификация необходима для

- администраторов ИС
- дистанционных пользователей
- обеспечения классов защиты КС1, КС2

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

АНОНС

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)!

Комплексный подход в построении защищенной ИС

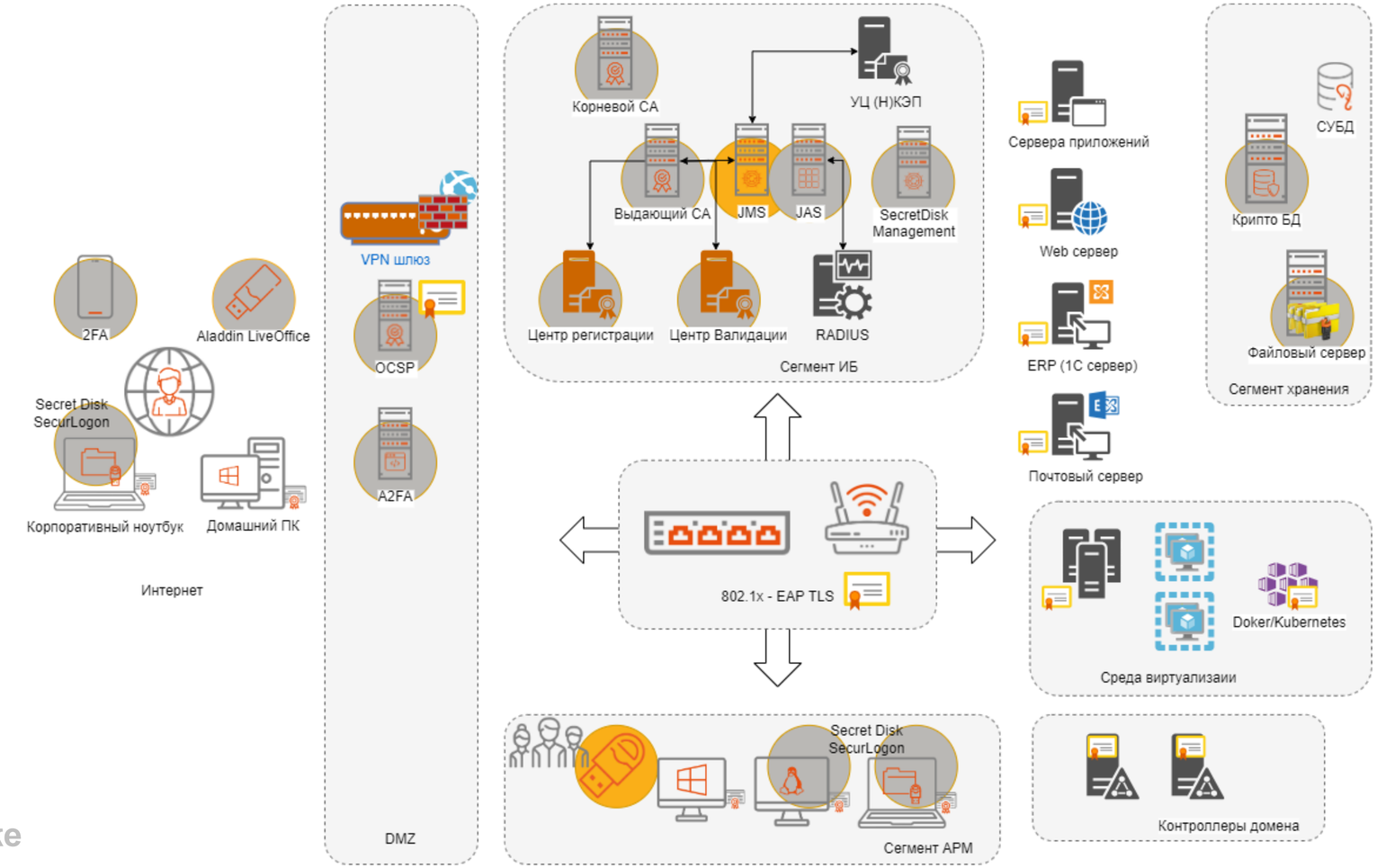
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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

Усиленная аутентификация
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- 2FA
- Aladdin SecurLogon
- Аутентификация по OTP / PUSH / SMS

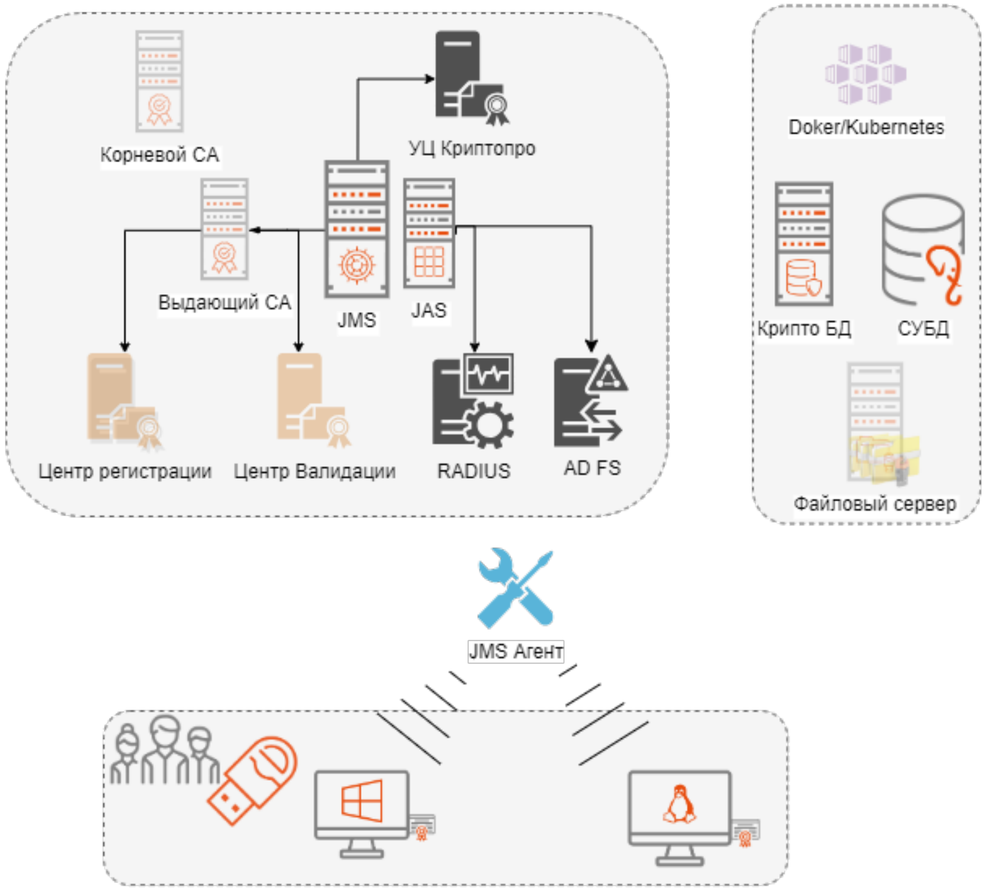
Дистанционная работа («удаленка»)
- Aladdin LiveOffice

Защита данных при хранении и обработке
- КриптоБД
- SecretDisk Linux
- Защита данных от утечек
- Централизованное управление (v2.0 ноябрь)



JaCarta Management System - управления жизненным циклом электронных ключей

- **Инвентаризация и управление ЖЦ usb-токенов и смарт карт**
  - Связь токена с учетной записью пользователя
  - Электронный реестр выданных токенов, актов передачи и т.д.
  - Управление выпуском/отзывом (политики пин-кодов, параметров инициализации, уведомлений и т.д.)
  - Разблокировка заблокированных пользователями токенов и смарт карт в режиме “запрос-ответ” или автоматическом режиме
  - Взятие под управление электронных ключей сторонних вендоров
- **Запись на ЭК необходимых сертификатов и ключевых контейнеров**
  - Aladdin eCA, Microsoft CA, УЦ Microsoft CA, КриптоПро 2.0, ViPNet 4.6, Notary-PRO 2.7
  - Microsoft AD, freeIPA, Samba DC, ALDPro, УЦ КриптоПро 2.0, собственного каталога учётных данных пользователей (JDS)
  - Связывание учётных записей пользователей из разных ресурсных систем по совпадающему атрибуту
- **Управление профилями учётных записей на usb-токенах/картах**
  - используя ПО SecurLogon для записи (логин, пароль) на электронный ключ и обеспечения 2ФА без необходимости строить PKI
- **Ведение поэкземплярного учёта СКЗИ**
- в соответствии с приказом ФАПСИ №152 от 13.06.2001. Экспорт отчёта в распространённые форматы.



Комплексный подход в построении защищенной ИС

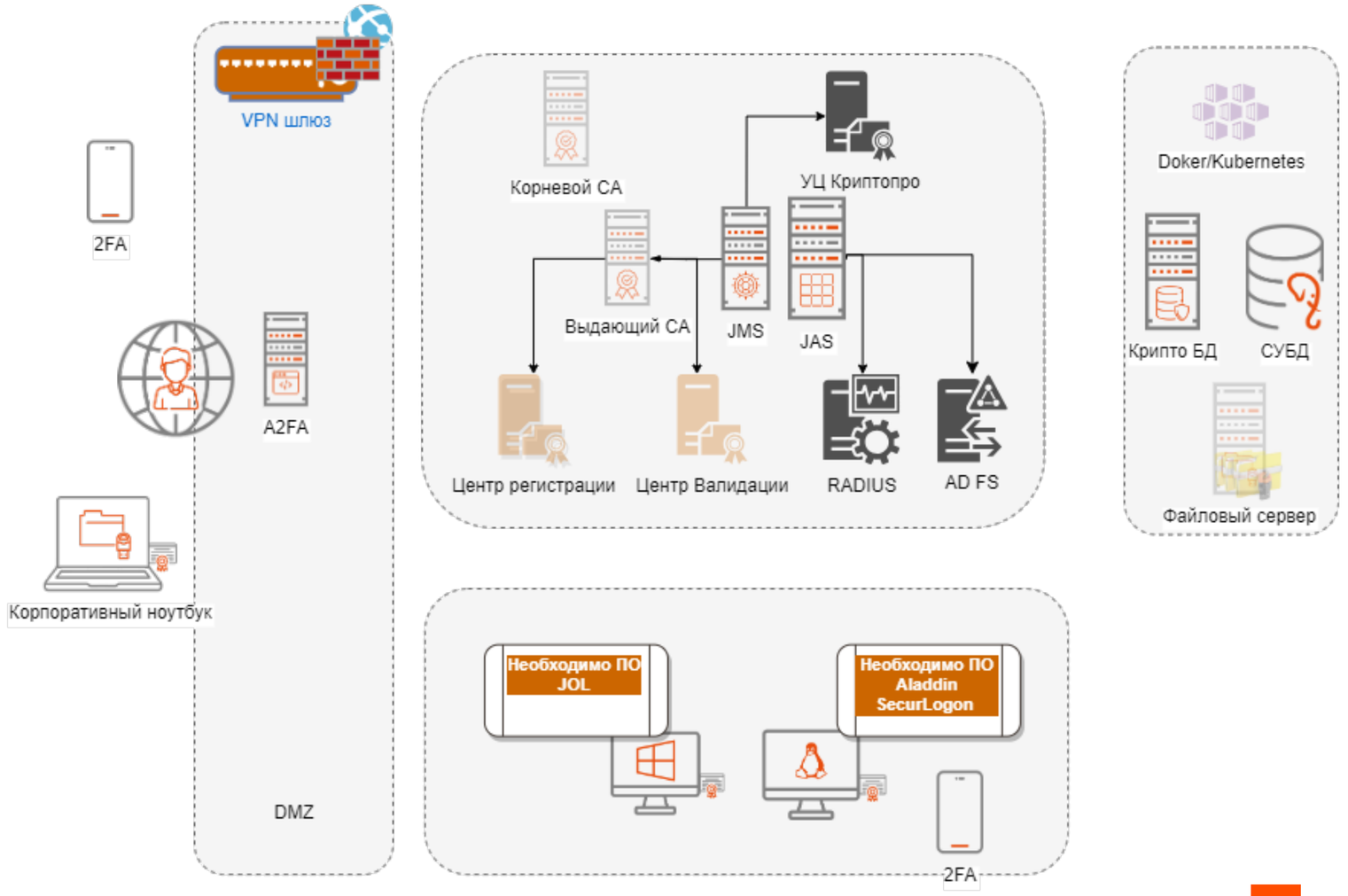
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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

Усиленная аутентификация
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- 2FA
- Aladdin SecurLogon
- Аутентификация по OTP / PUSH / SMS

Дистанционная работа («удаленка»)
- Aladdin LiveOffice

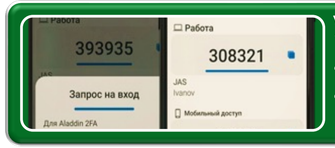
Защита данных при хранении и обработке
- КриптоБД
- SecretDisk Linux
- Защита данных от утечек
- Централизованное управление (v2.0 ноябрь)



Уровни зрелости ИС и надежности технологии аутентификации

Строгая аутентификация (Token-based 2FA)

- Аппаратные токены смарт карты с неизвлекаемыми ключами
- JaCarta PKI, Aladdin LiveOffice



Усиленная аутентификация (App-based 2FA)

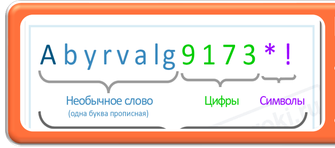
- Логин/пароль + приложение аутентификатор на смартфоне или аппаратный генератор OTP
- Приложение Aladdin 2FA в связке с сервером JAS (генератор OTP и PUSH)

Усиленная аутентификация (SMS-based 2FA)

- Логин/пароль + SMS с одноразовым паролем (OTP)
- JAS (интеграция с sms-шлюзом)

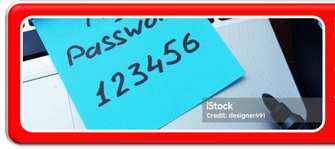
Простая аутентификация – уникальный сложный пароль (Password Manager)

- Уникальный пароль для каждого сервиса, хранение его в парольном менеджере
- Длинный, сложный пароль - LastPass, 1Password, Яндекс, SecurLogon



Простая аутентификация – НЕ уникальный, сложный пароль (Quality Password)

- Единый для всех сервисов, но сложный и длинный пароль с спец символами, не содержит личную информацию
- Пример Sa!@#$%-17baRaw



Простая аутентификация – уникальный простой пароль (Unique Password)

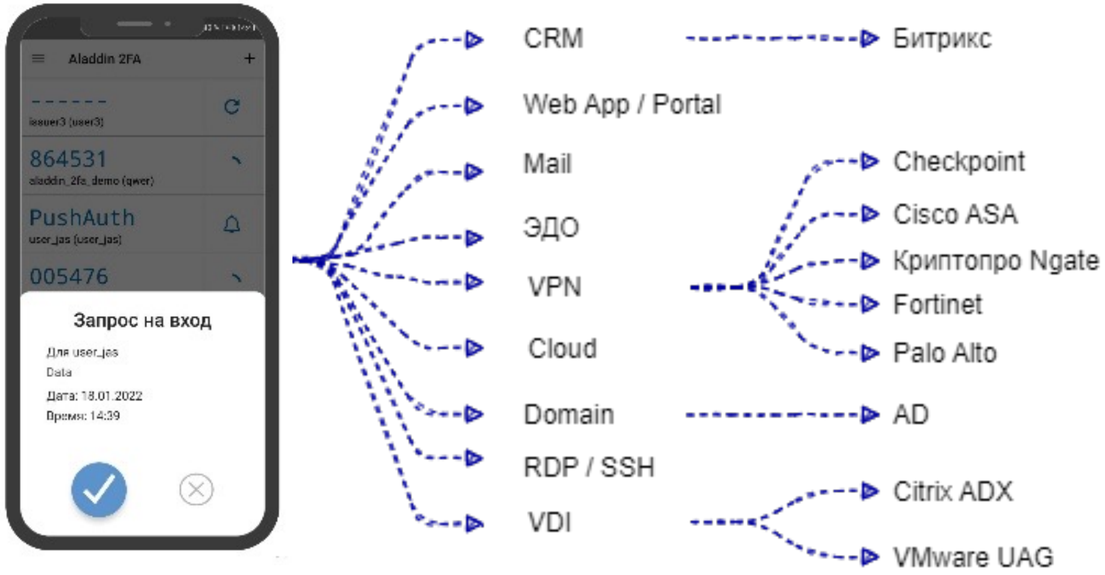
- Уникальный для каждого сервиса, но простой, короткий или содержащий личную информацию
- Пример пароля – galinamail1, galinapizza1

Простая аутентификация – «золотой» пароль (Shared Password)

- Единый и простой пароль для всех ваших сервисов и интернет ресурсов
- Пример пароля – qwerty123

JaCarta Authentication Server (JAS) – сервер усиленной аутентификации

- **Усиленная аутентификация** пользователей по одноразовым паролям (PUSH/OTP/SMS)
- **Строгая аутентификация** пользователей по протоколу U2F (разработка FIDO Alliance)
- **Аутентификации на десктопах, ноутбуках:**
  - Windows требуется ПО JAS OTP Logon (JOL)
  - Linux требуется ПО Aladdin SecurLogon
- **Простая интеграция с прикладным ПО по стандартным протоколам:**
  - RADIUS
  - REST
  - WCF
  - ADFS
- **Высокая производительность** (более 5,000 аутентификаций в секунду)
- **Личный кабинет пользователя**, позволяющий реализовать все операции с программными аутентификаторами от самостоятельного выпуска до блокировки
- **Сервис безопасной передачи секрета** (вектора инициализации) программных аутентификаторов и собственное мобильное приложение Aladdin 2FA



OTP (One Time Password) — одноразовый пароль.

Главное преимущество OTP при его сравнении с обычным статическим паролем — невозможность повторного использования.

Комплексный подход в построении защищенной ИС

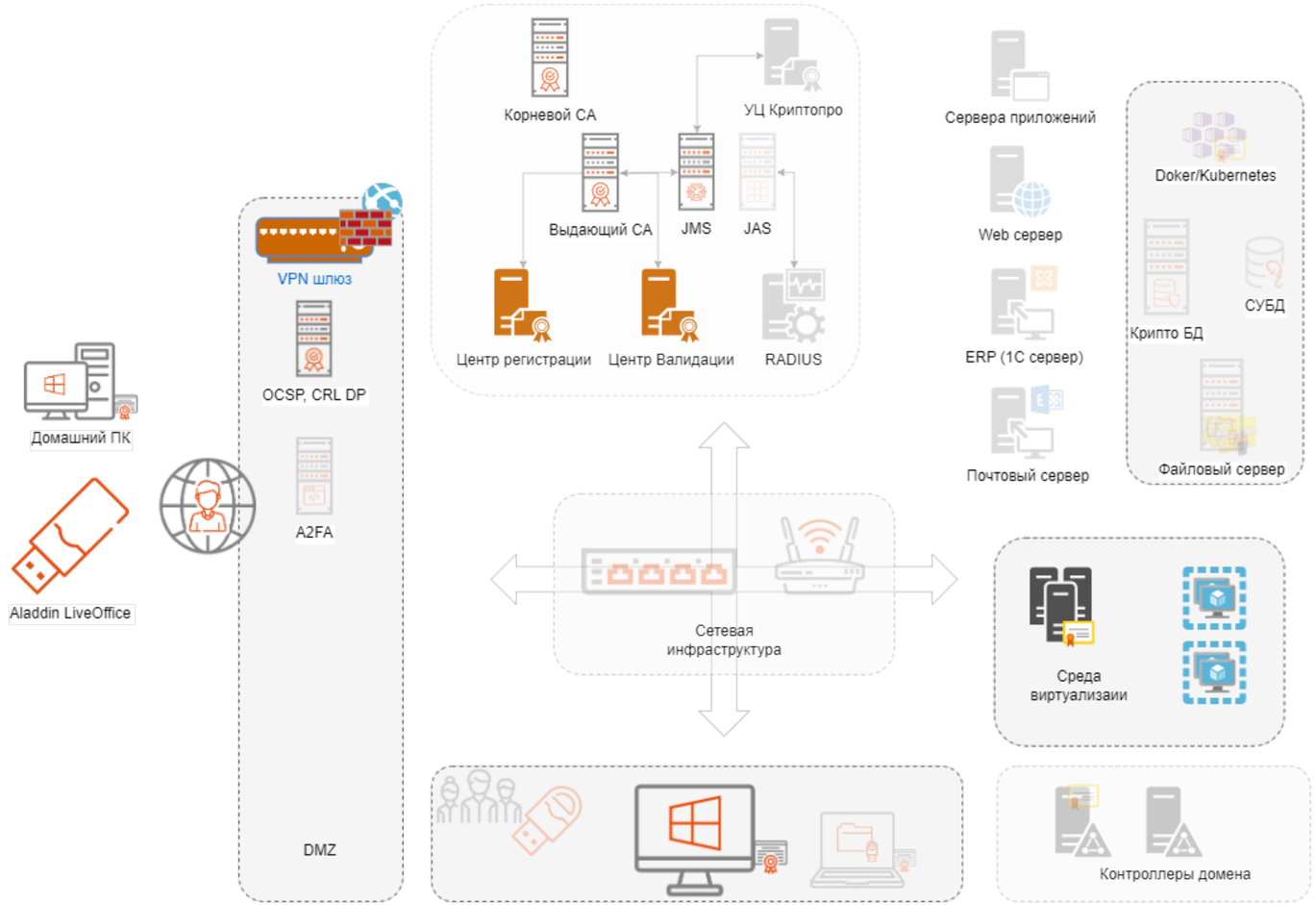
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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

Усиленная аутентификация
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- 2FA
- 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 (v2.0 ноябрь)



Aladdin LiveOffice

✓ **Существенная экономия бюджета на организацию дистанционной работы**

✓ **Безопаснее, чем служебный ноутбук**

Служебный ноутбук

Стоимость: 1 : 7

Специализированное средство LiveOffice

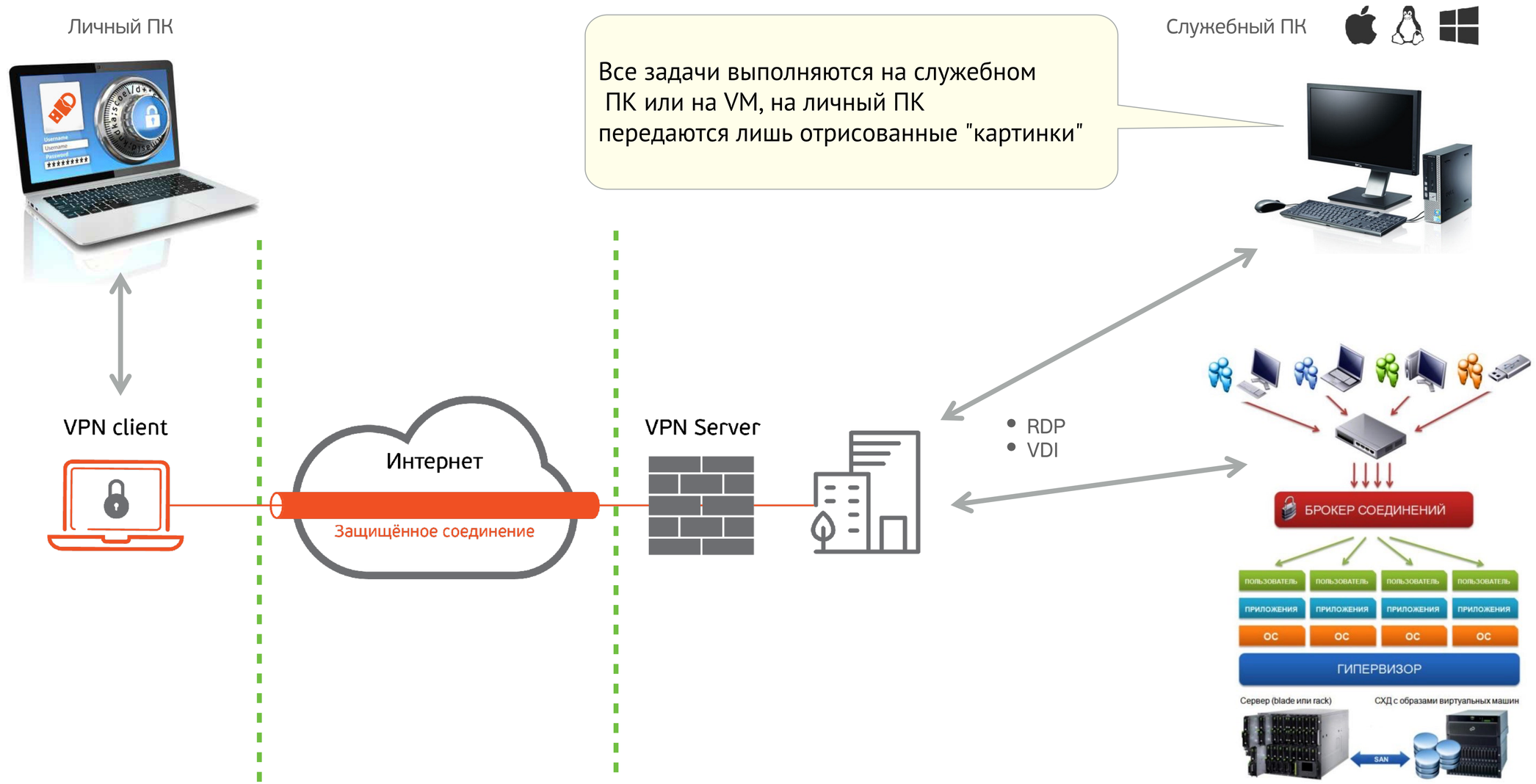
- Необходимо установить сертифицированные средства защиты и программное обеспечение:
  - Средство доверенной загрузки
  - ОС
  - Антивирус
  - Средство 2ФА (USB-токен, S/C)
  - Средство идентификации и авторизации СВТ
  - VPN
  - Средство прозрачного шифрования дисков
  - Межсетевой экран
  - Средства мониторинга и контроля удалённого доступа
- Необходимо обеспечить их совместимость

- Все необходимое для работы уже на борту
- Используется личное СВТ (организация на платит за него)
- Экономия бюджета в 5-10 раз

  или

  За те же деньги можно обеспечить средствами дистанционной работы 5-10 сотрудников
- **Поверхность для атаки здесь существенно меньше, информация хранится и обрабатывается на рабочем ПК, на устройстве не хранится**

Как это работает



Aladdin LiveOffice

- 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

Aladdin LiveOffice

- 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)

Комплексный подход в построении защищенной ИС

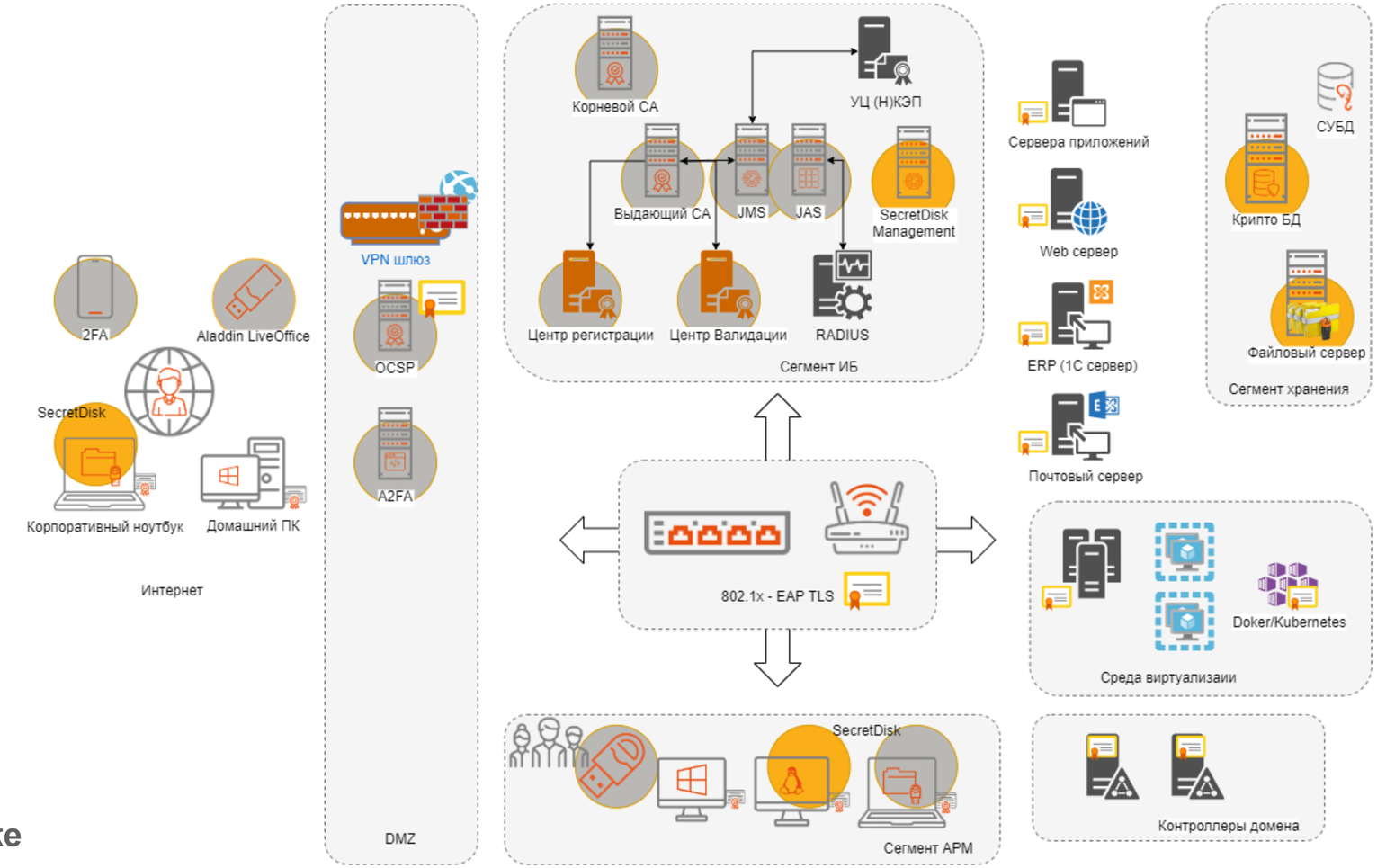
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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

Усиленная аутентификация
- JaCarta Authentication Server 4 Linux
- Сервер A2FA
- 2FA
- 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 (v2.0 ноябрь)



Secret Disk

- 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
  - Сокрытие 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)

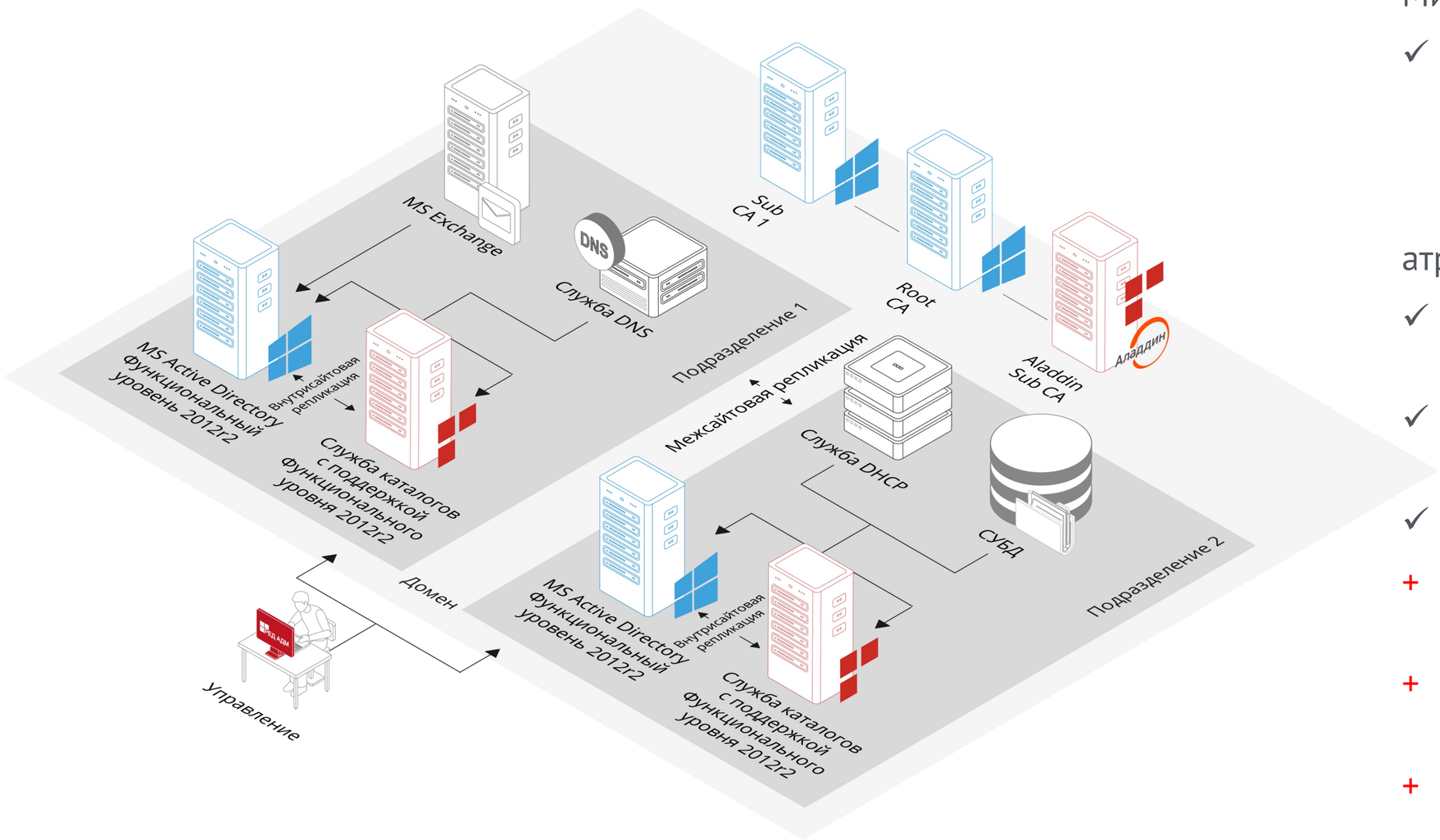
- Персональная версия
- Для серверов (приложений, файловых)
- С централизованным управлением (Enterprise)
- Версия под Linux - имеет сертификат МО для работы с ГТ ("СС")

Крипто БД

- 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

РЕД АДМ + Aladdin eCA – комплексный сценарий миграции



Миграция:

- ✓ Репликация с MS AD 2003, 2008R2, 2012R2, 2016:
  - структуры домена
  - пользователей (пароли, атрибуты)
- ✓ Двухсторонняя репликация групповых политик
- ✓ Поддержка работы геторогенной инфраструктуры (Windows, Linux)
- ✓ Шаблоны сертификатов
- \+ Плавный вывод из ИС продуктов Microsoft без остановки сервисов
- \+ Не требуется строить новый отдельный домен/лес
- \+ Бесшовная миграция PKI

Дмитрий Шуралев

АО "Аладдин Р.Д."

Аладдин - будь собой в электронном мире!

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.