Ключевые компоненты для построения безопасной доверенной ИТ-инфраструктуры.

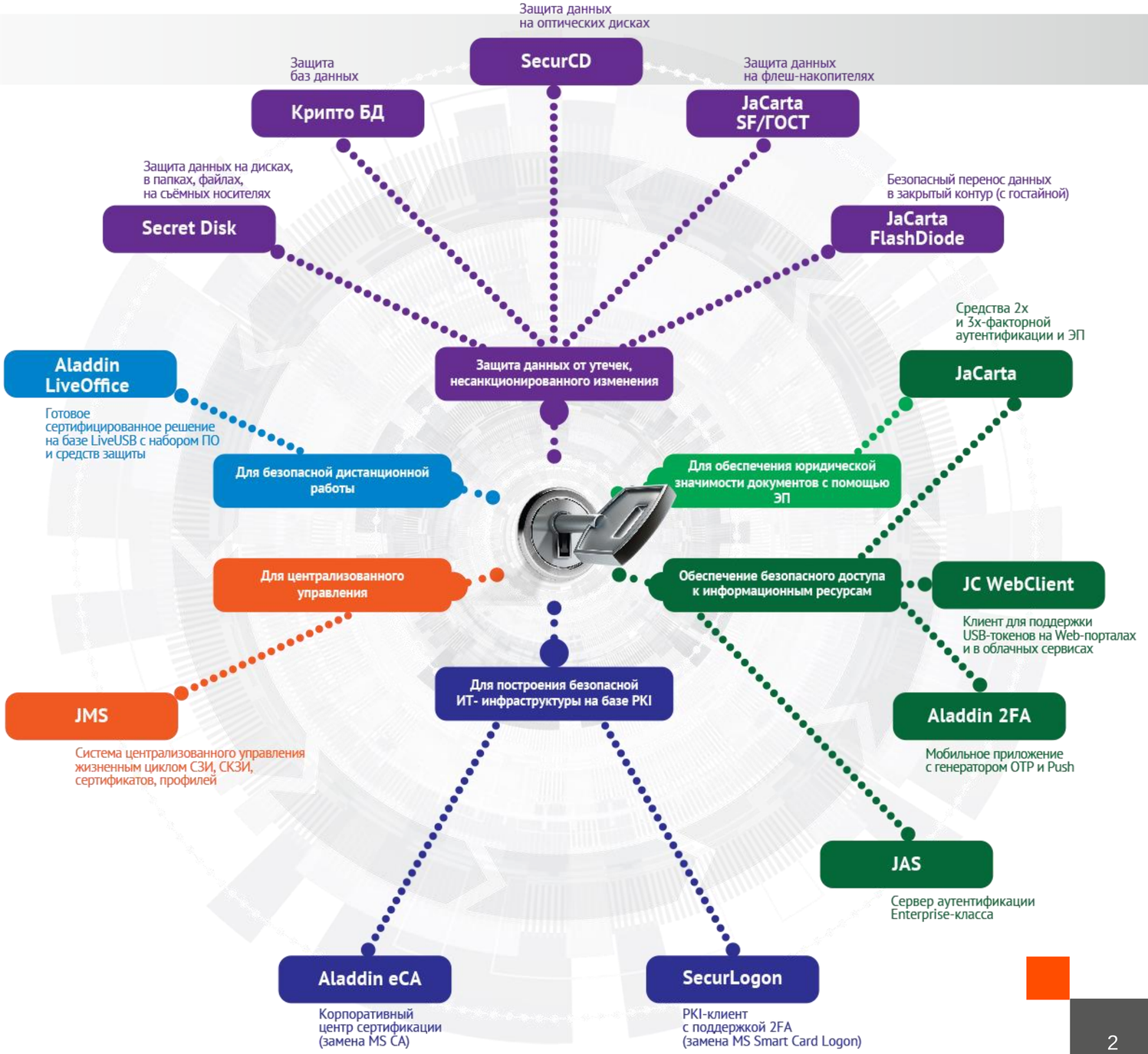
Денис Полушин

АО "Аладдин Р.Д."

ведущий российский вендор-разработчик и производитель

- ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры

- средств аутентификации и электронной подписи

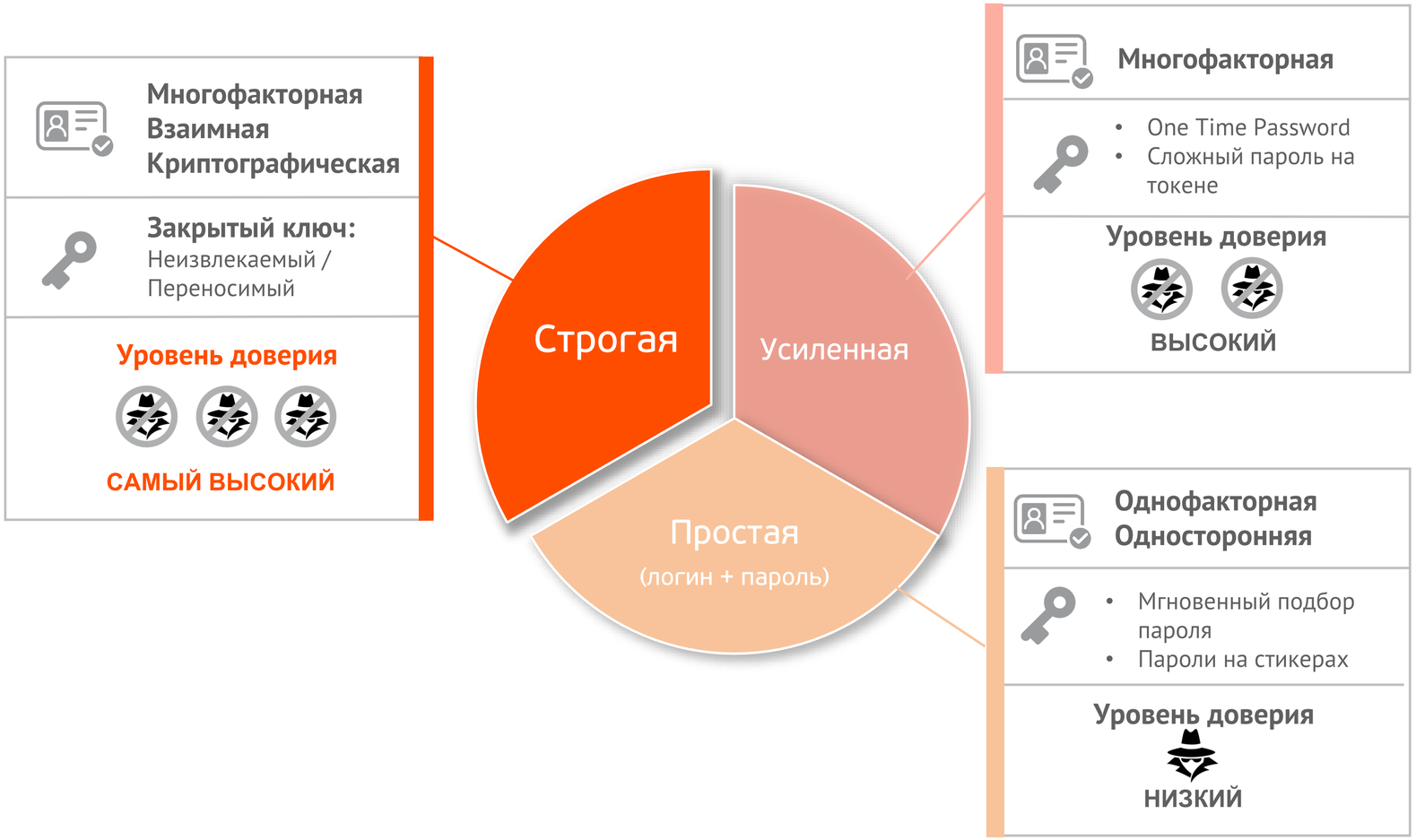


Нац. стандарты по идентификации и аутентификации

- 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

Логин-пароль

Давно уже не актуальная технология!

5 часов на подбор пароля t~pbE#0u

8 символов, цифры, прописные и строчные буквы, специальные символы

Или 39 минут на оборудовании AWS за 39$

Обычно вот так:

- длина не 8, а 6 символов
- смена пароля раз в 42 дня
- позволяют пользователям самим менять пароли, как итог – 3 «золотых» пароля
- пароль от корп. ПК используют для заказа пиццы

Если увеличить длину и почаще менять?

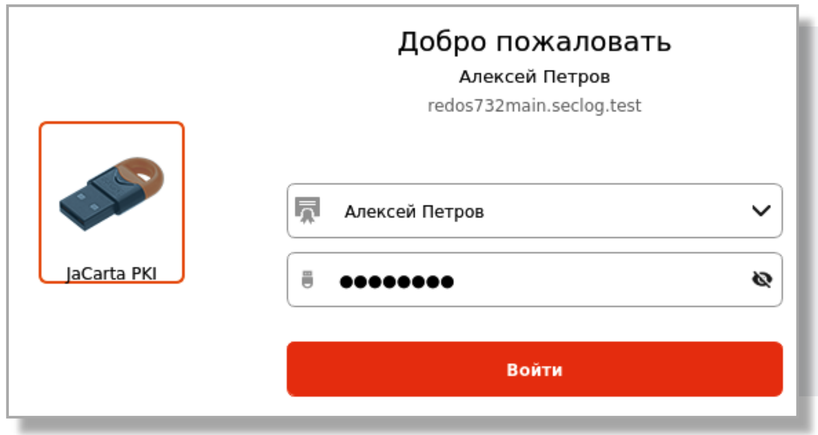
- на рабочем столе файлик с паролями, фотка в телефоне, стикеры и т.д.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	3 secs
7	Instantly	Instantly	15 secs	51 secs	4 mins
8	Instantly	3 secs	13 mins	52 mins	5 hours
9	Instantly	1 mins	11 hours	2 days	2 weeks
10	Instantly	34 mins	3 weeks	5 months	3 years
11	1 sec	15 hours	3 years	24 years	300 years
12	14 secs	2 weeks	200 years	1k years	20k years
13	2 mins	1 year	9k years	91k years	2m years
14	24 mins	29 years	483k years	6m years	118m years
15	4 hours	800 years	25m years	251m y	9bn years
16	2 days	20k years	1bn years	22bn y	697bn years
17	2 weeks	518k years	68bn years	1tn years	54tn years
18	5 months	13m years	4tn years	84tn years	4qd years

Оборудование хакера

- Домашний компьютер и топовая видеокарта
- Доступ к базам хэшей https://haveibeenpwned.com/

Источник - https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=footer



Aladdin SecurLogon
Поддержка средств 2ФА на клиентах Linux

- Сложные пароли (63 символа)
- Для пользователей не использующих PKI

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

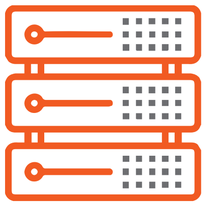
Инфраструктура открытых ключей и сертификаты

Зачем нужны сертификаты в ИС?

Строгая аутентификация

- ✓ Сотрудников внутри ИС
- ✓ Администраторов ИС
- ✓ Дистанционных сотрудников (интернет)
- ✓ Внешних пользователей

Доверие к инфраструктуре



- ✓ Web-серверы
- ✓ Маршрутизаторы
- ✓ Межсетевые экраны
- ✓ Контроллеры домена

Подключенные устройства

- ✓ Мобильные устройства
- ✓ АСУ ТП

Корпоративная электронная подпись

- ✓ Email, S/MIME
- ✓ внутренний ЭДО

Проблемы перехода на отечественное ПО

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

- 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 сервисов MS - очень большие**

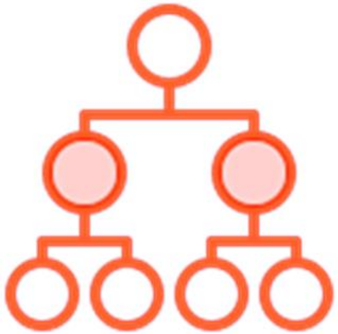
Проблемы перехода на отечественное ПО

Проблема №2

- Как обеспечить миграцию действующей PKI?
  - 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 перехода на отечественное ПО

Проблема №3

- Импортозамещаемся, переходим на отечественные ОС (Linux)
  - Одномоментно перейти на отечественные ОС и отказаться полностью от Windows большинство владельцев ИС не смогло
  - В мире Linux свои службы каталогов и домены безопасности (Samba DC, FreeIPA, ALD Pro, РЕД АДМ, Альт Домен)

✓ **Корпоративный СА 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 перехода на отечественное ПО

Проблема №5

- Обеспечить привычные сценарии с **автоматизацией** выпуска сертификатов

Aladdin Enterprise CA

Корпоративный центр сертификации

- ключевой компонент

для построения корпоративной PKI на Linux

В Реестре отечественного ПО №2021663130

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

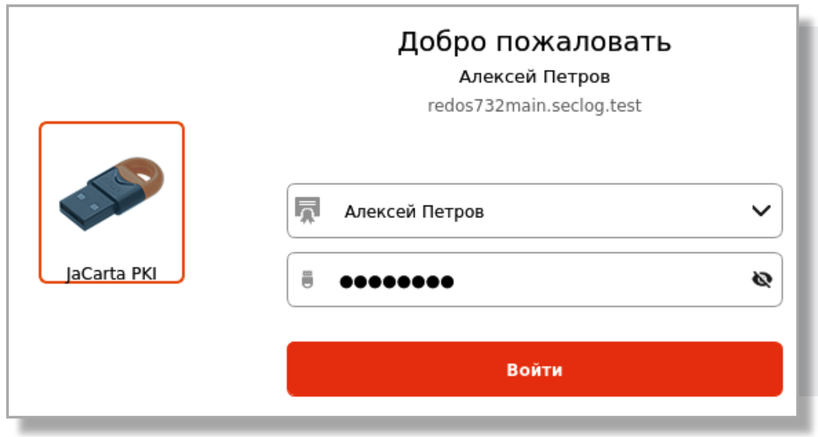
Импортозамещение: Microsoft Certificate Services (MS CA)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

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**
    - **РЕД АДМ (промышленная редакция)**
    - **Альт Домен**
    - **ALD Pro**
    - **Samba DC**
    - **FreeIPA**
  - + 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
  - + 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

✓ **Замена для Microsoft Certificate Services (MS CA)**



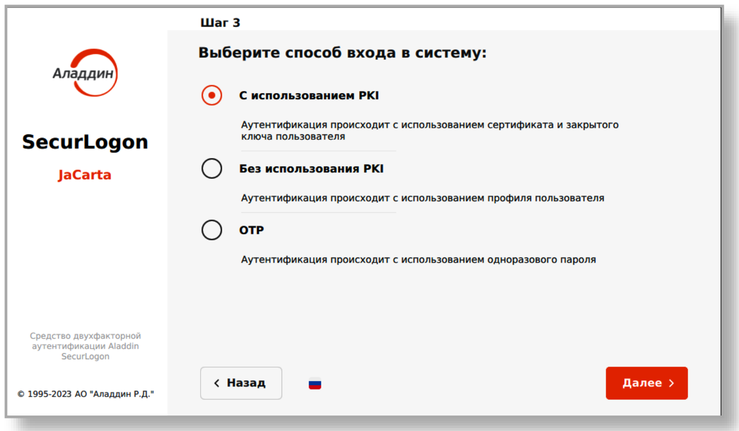
Aladdin SecurLogon
PKI-клиент и поддержка сертификатов в Linux
- замена MS SmartCard Logon

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

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**



Комплексный подход в построении защищенной ИС

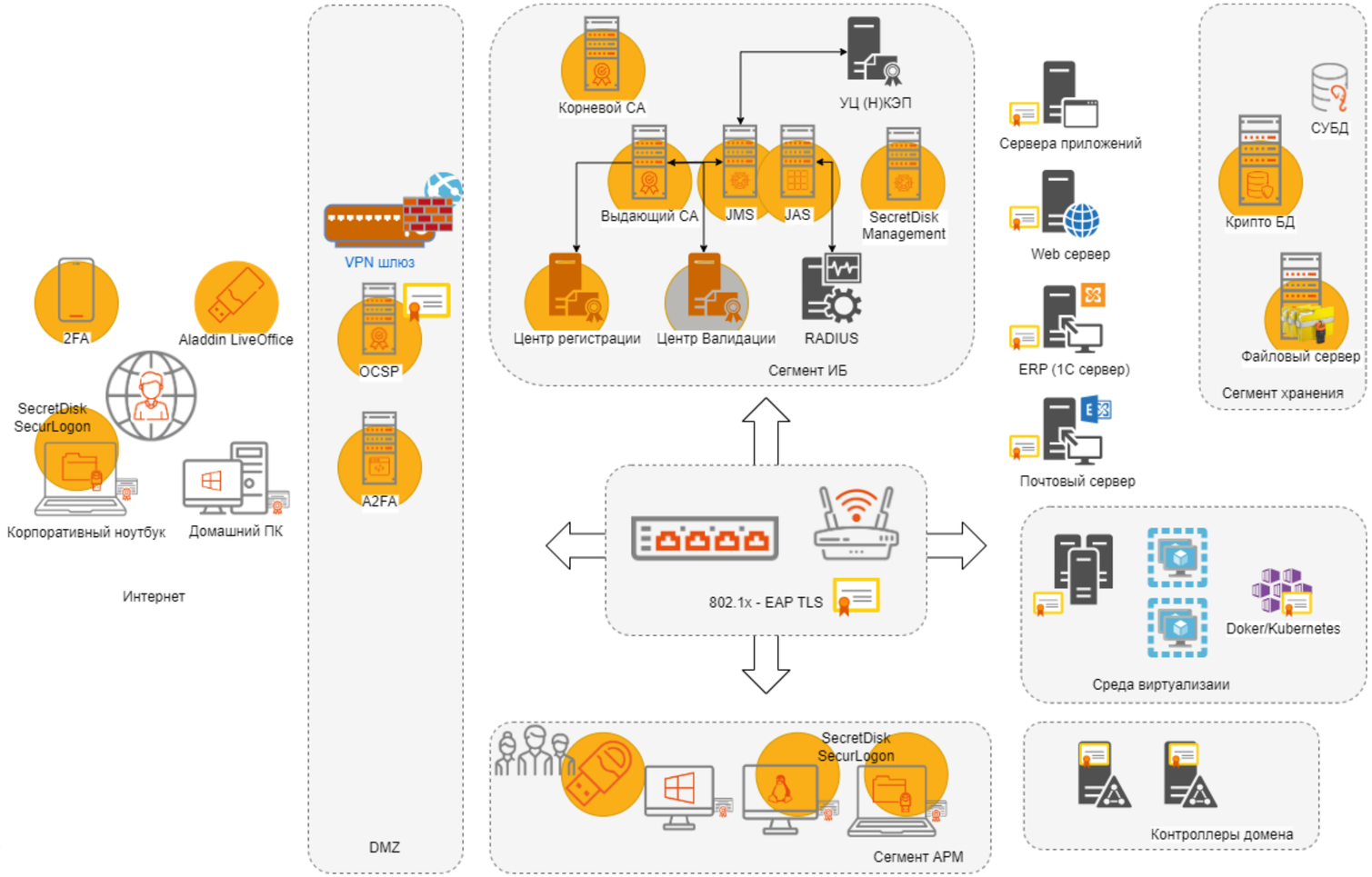
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Комплексный подход в построении защищенной ИС

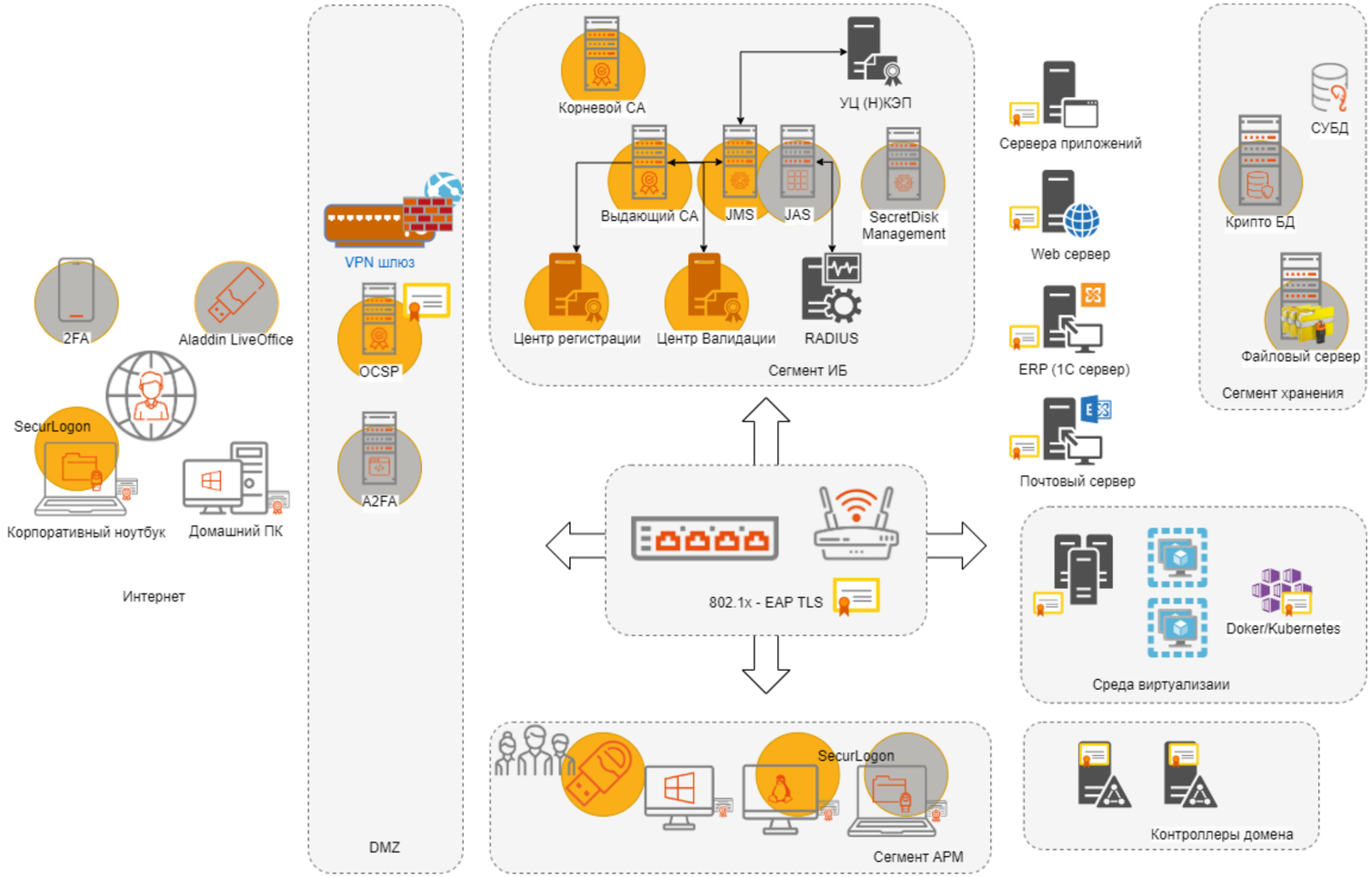
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Комплексный подход в построении защищенной ИС

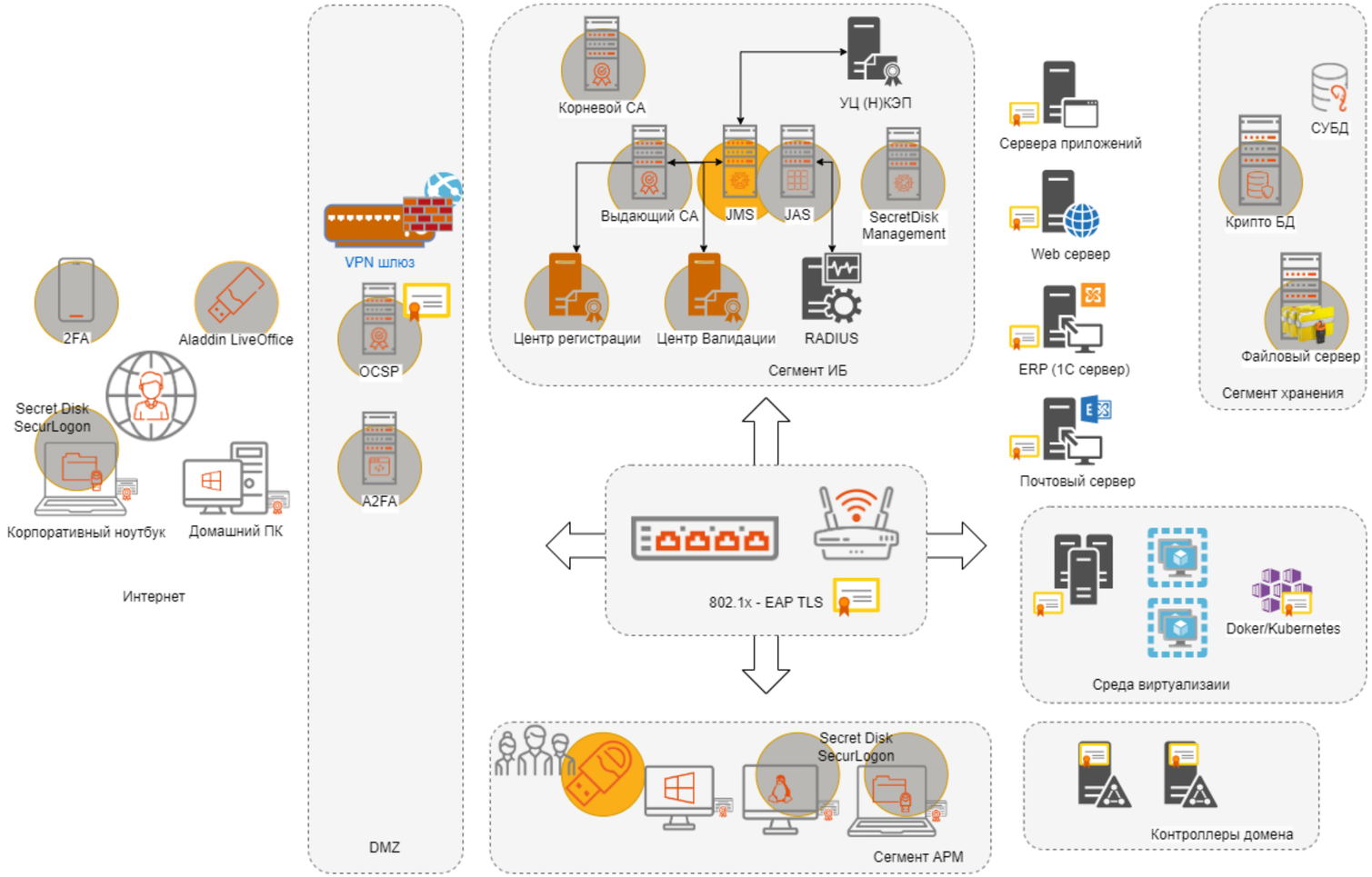
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Комплексный подход в построении защищенной ИС

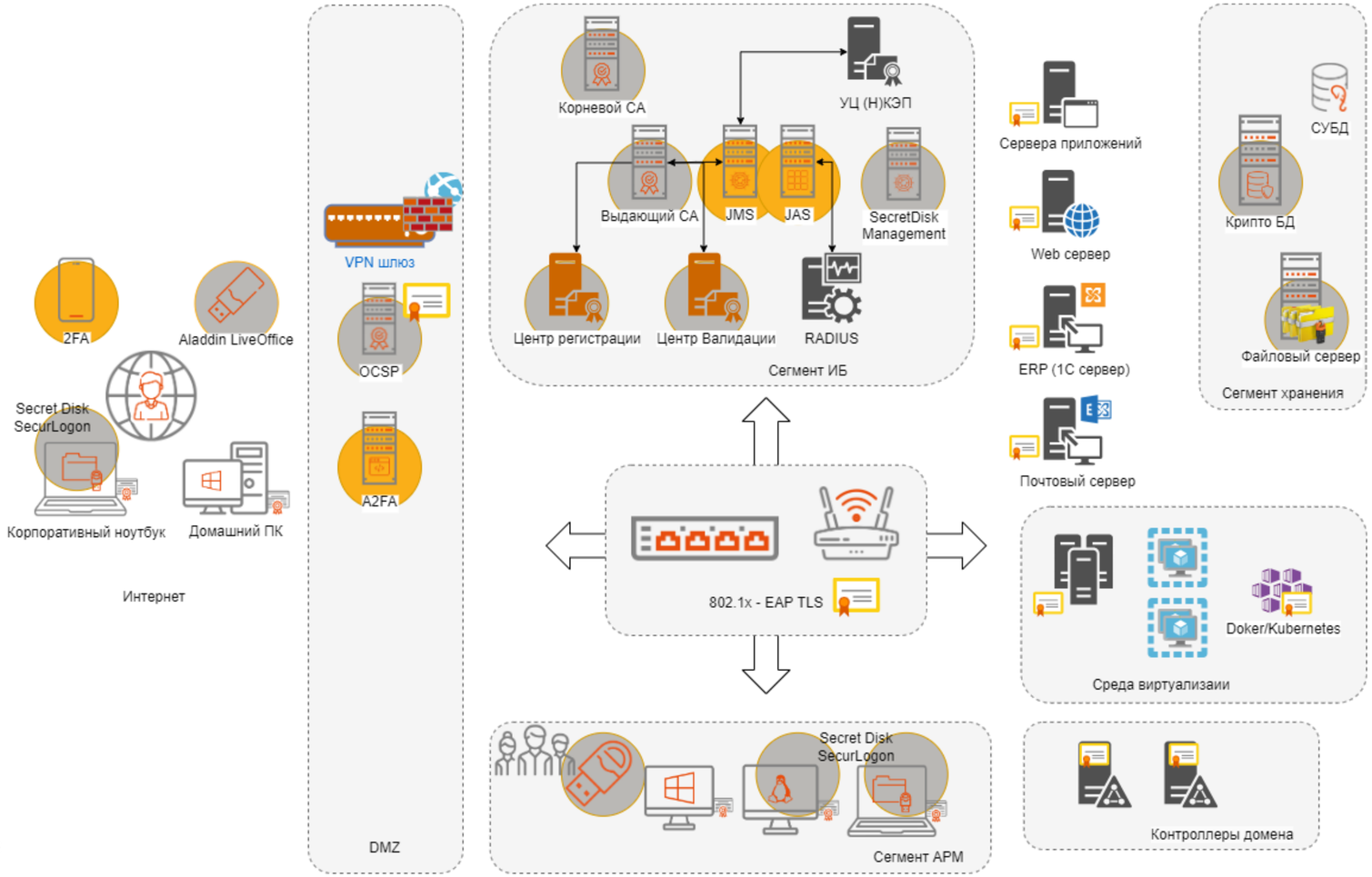
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Комплексный подход в построении защищенной ИС

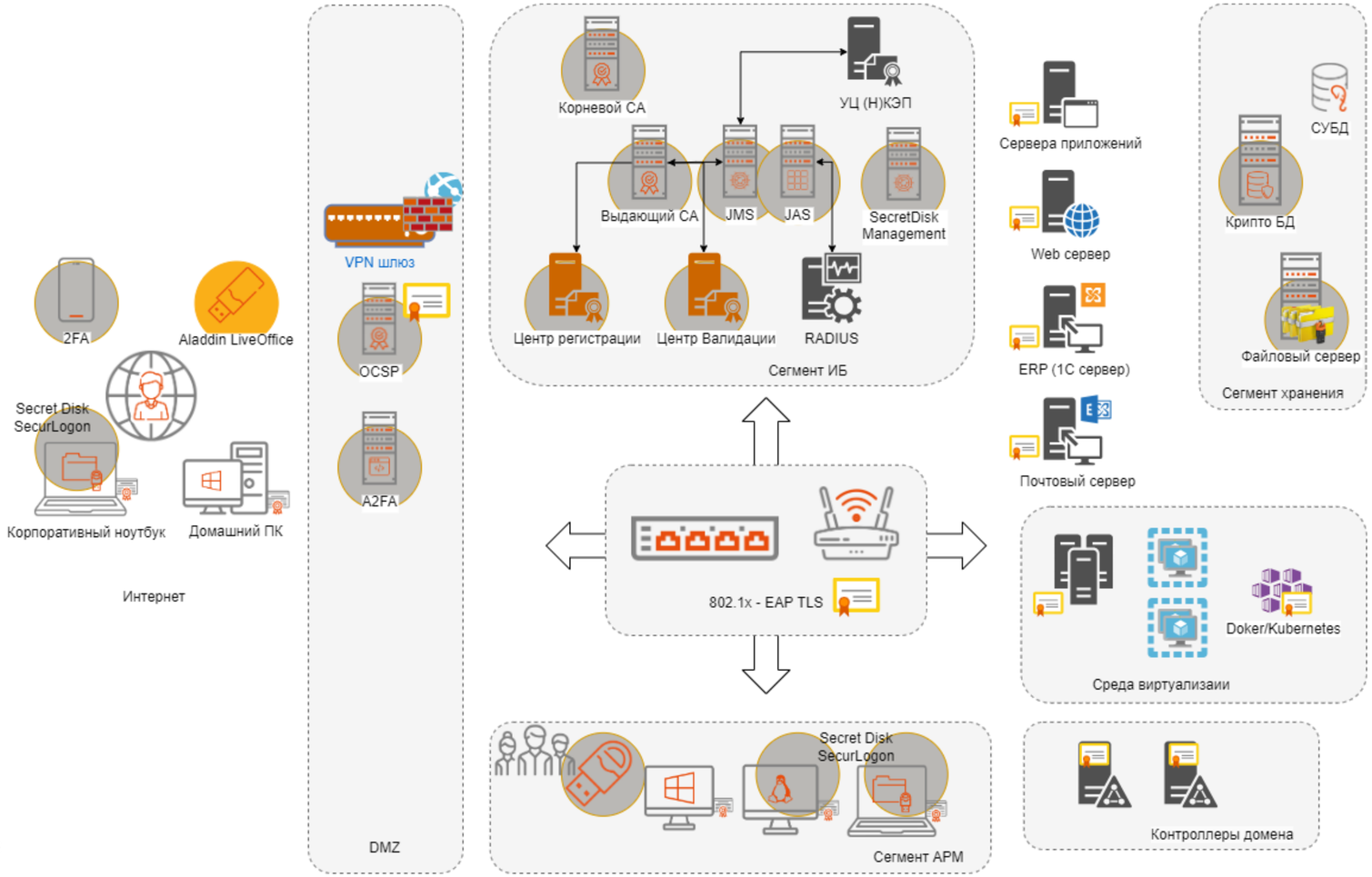
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Комплексный подход в построении защищенной ИС

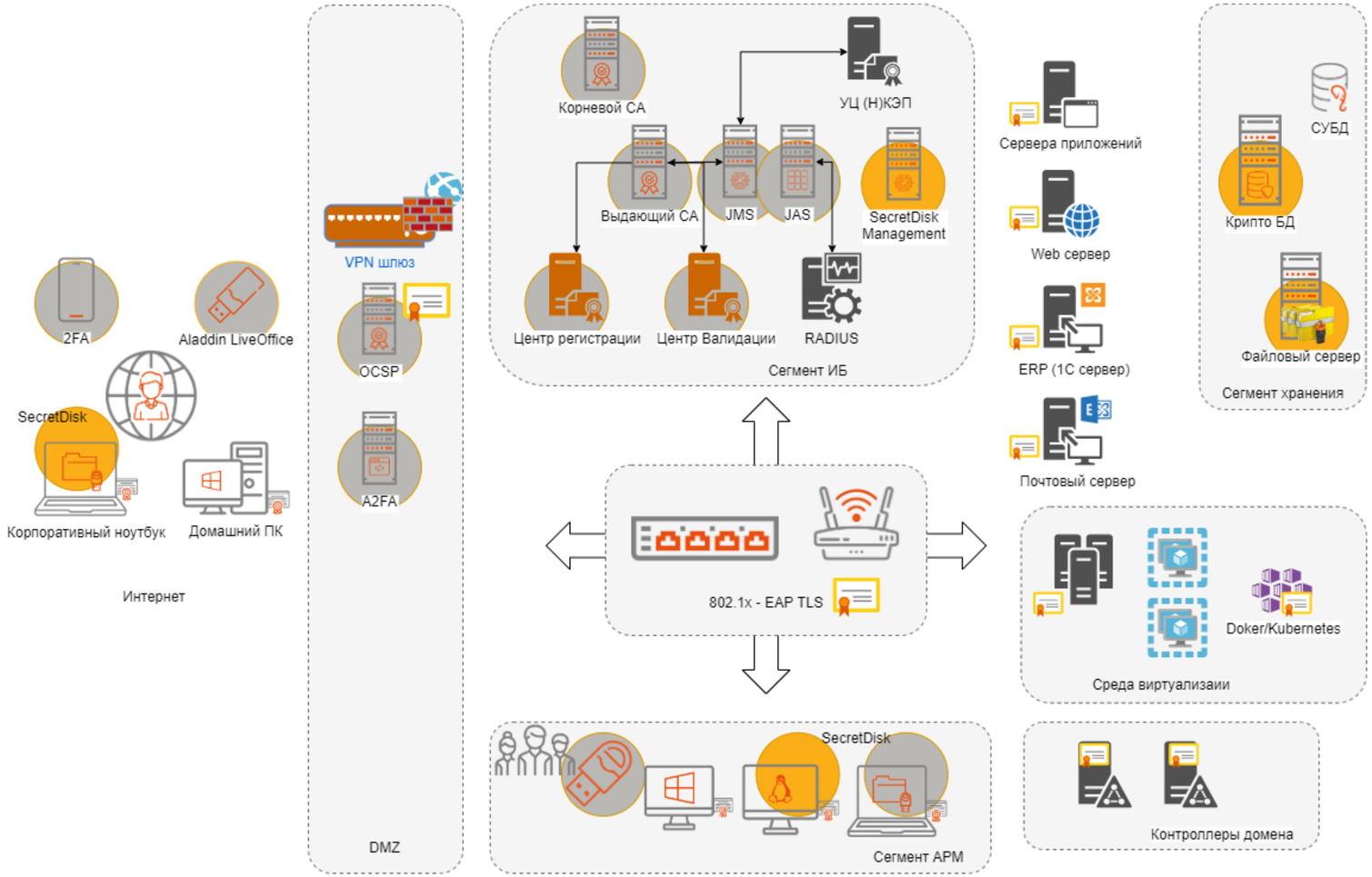
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Комплексный подход в построении защищенной ИС

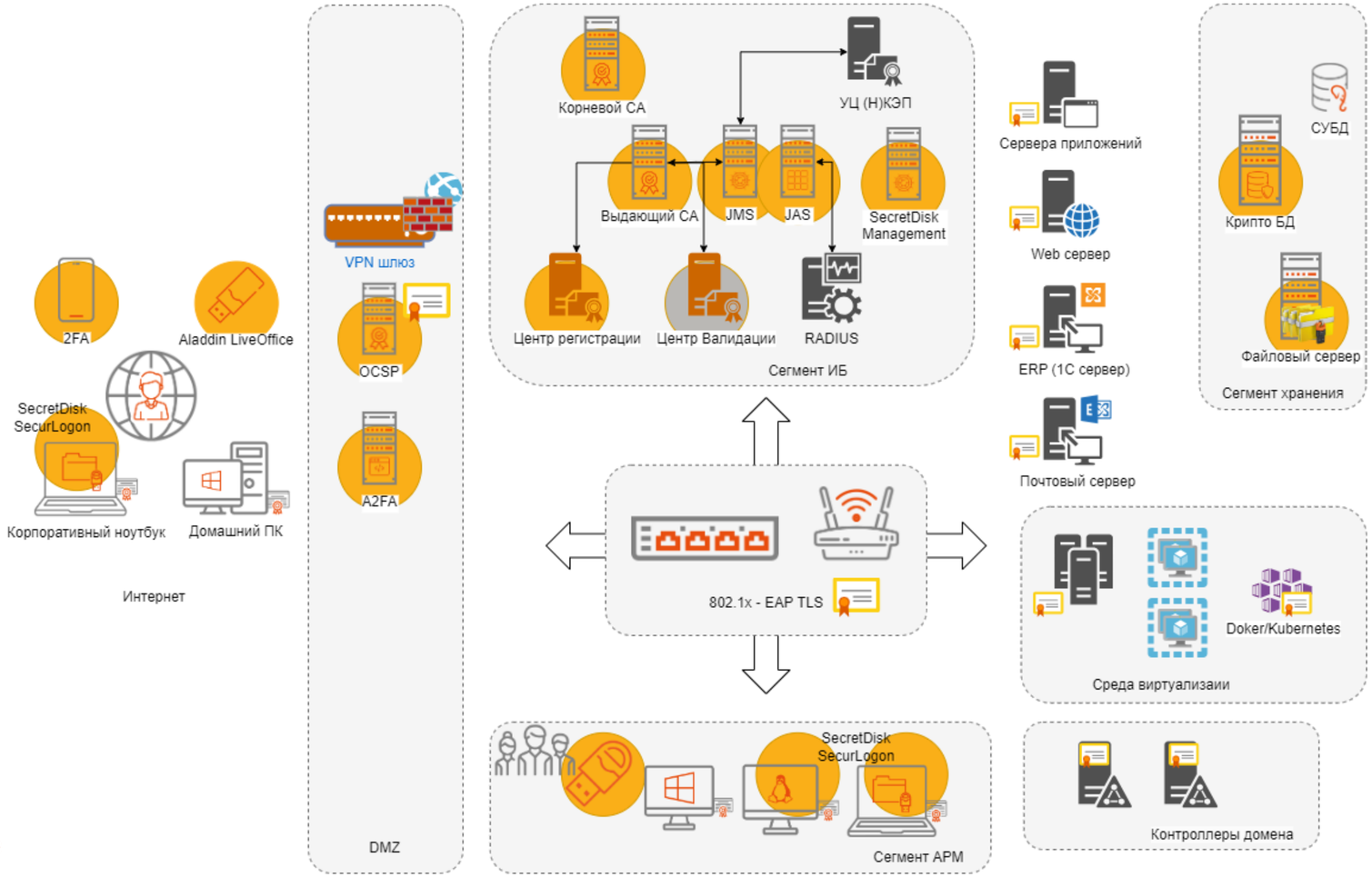
PKI корпоративного уровня
- Aladdin Enterprise CA (root, sub)
- Центр валидации, регистрации
- Aladdin SecurLogon
- Строгая аутентификация пользователей
- Сертификаты серверов и компьютеров

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)



Решения по импортозамещению

Денис Полушин

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.