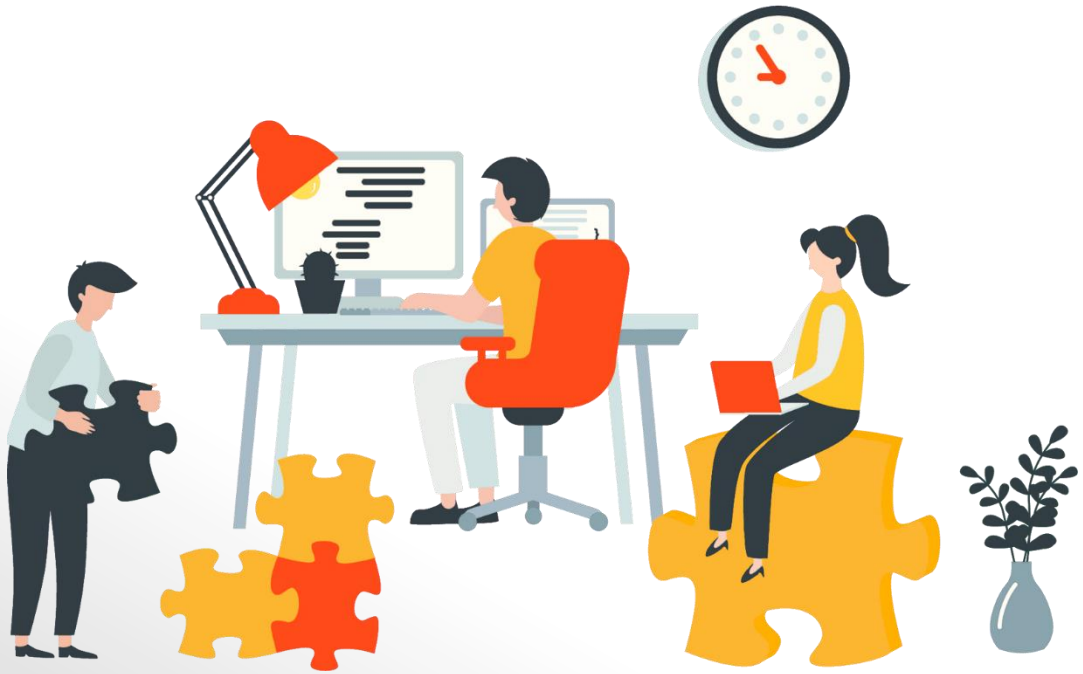
Замещение Microsoft CA

Технологии аутентификации, безопасный удалённый доступ и защита данных



Сергей Шалимов,
Руководитель направления по работе с технологическими партнерами "Аладдин Р.Д."

Потребности ИС в текущих условиях

- На данный момент более 90% ИС построены на Microsoft Active Directory и используют Microsoft Certificate Service из состава Windows Server в качестве сервиса генерации и управления цифровыми сертификатами (сертификаты доступа, PKI инфраструктура);
- Необходимо применить усилия, чтобы изолировать центр доменной инфраструктуры (а соответственно и сам Центр Сертификации) от атаки извне, он связан с каждым рабочим местом, с IDM системами, внутренними порталами и сервисами и т.д.;
- Отсутствие патчей безопасности для Windows Server;
- Отсутствие уверенности в отказоустойчивости при атаках извне (помним Ирак, когда отключалось оборудование и ПО по командам из США), а это критическая часть ИС.

Как вывод: необходим перевод ядра доменной инфраструктуры (домена безопасности) на отечественное ПО и установка отечественного ПО управления цифровыми сертификатами.

Аладдин

Продуктовый портфель

Защита доступа к данным

- **JaCarta** – линейка USB-токенов и смарт-карт для аутентификации и электронной подписи
- **JaCarta Management System** – система управления жизненным циклом аппаратных носителей JaCarta
- **Aladdin Enterprise Certification Authority** – центр управления жизненным циклом цифровых сертификатов
- **Aladdin SecurLogon** – мультизадачное средство 2ФА для Linux
- **JaCarta Authentication Server** (JAS) – автономный высокопроизводительный сервер аутентификации по OTP
- **Aladdin LiveOffice** – средство дистанционной работы

Защита данных при хранении и обработке

- **Secret Disk Linux** – СКЗИ для защиты данных на дисках ПК в ОС Linux
- **Крипто БД** —система предотвращения утечек информации из высокопроизводительных систем управления базами данных (СУБД)
- **JaCarta SF** – защищённый USB-флеш накопитель (ЗМНИ)

Аладдин

Aladdin Enterprise Certificate Authority (Aladdin eCA)

Построение доменов безопасности

Аладдин

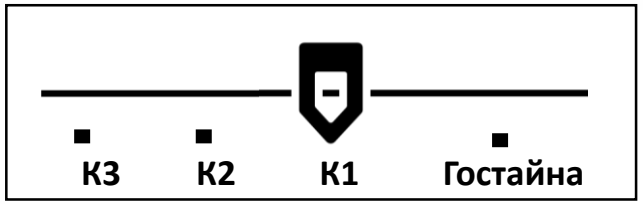
Aladdin eCA

Что это и для кого?

Aladdin Enterprise Certificate Authority (Aladdin eCA) – сервер на базе отечественных ОС, обеспечивающий управление цифровыми сертификатами пользователей и технических средств информационной системы (выпуск, распространение, аннулирование, приостановка, возобновление)

Предназначен для замены Microsoft CA в корпоративных и государственных информационных системах:

- ГИС до 1-го класса защищённости включительно;
- ИСПДн до 1-й категории включительно;
- Объектов КИИ до 1-ой категории включительно:
- АСУ ТП на критически важных объектах, потенциально опасных объектах до 1-го класса защищённости включительно.



Aladdin eCA

Основные возможности

Предназначен как для малых так и для крупных территориально распределенных ИС и высоконагруженных сервисов ЦОД

- **создания иерархии ЦС** с распределением политик безопасности и автоматизацией развертывания;
- **все функциональные роли** (Root_CA, Sub_CA, Policy, RA, CDP, DB, Web Enrolment) могут быть **разнесены по** отдельным **нодам;**
- удобная Web-консоль и ролевая модель:
  - организации точки распространения CRL, службы OCSP и т.д.;
  - публикация сертификатов;
  - удобный выпуск сертификатов пользователям Web-enrolment;
- **поддержка шаблонов** и выпуск сертификатов серверам
- поддержка отечественных СУБД Postgres Pro и Jatoba;
- **возможность подключения HSM** при помощи интерфейса PKCS#11;
- **интеграция с доменами** отечественных производителей **Samba DC, FreeIPA, ALD Pro**

Aladdin eCA

Схема применения

Импортозамещение

Подходы и проблемы

Практика прошлых лет в действующих ИС - уже не работает!

- Сохраняется структура леса/домена на базе Microsoft AD и CA
- Замещаются **только клиентские ОС** и офисный пакет
- Замещаются периметровые СЗИ и СКЗИ

➢ Что дальше делать с серверной стороной и текущей PKI?

Проектирование ИС с чистого листа - не всегда это возможно!

- Структура леса/домена создается с нуля
- Клиентские ОС:
  - Только Linux - выбирают домены FreeIPA, ALDPro
  - Микс Windows/Linux - выбирают Samba DC

➢ Как обеспечить SSO и 2ФА, где взять Linux PKI для доменов на Samba, FreeIPA, ALD Pro?

Аладдин

Методика внедрения

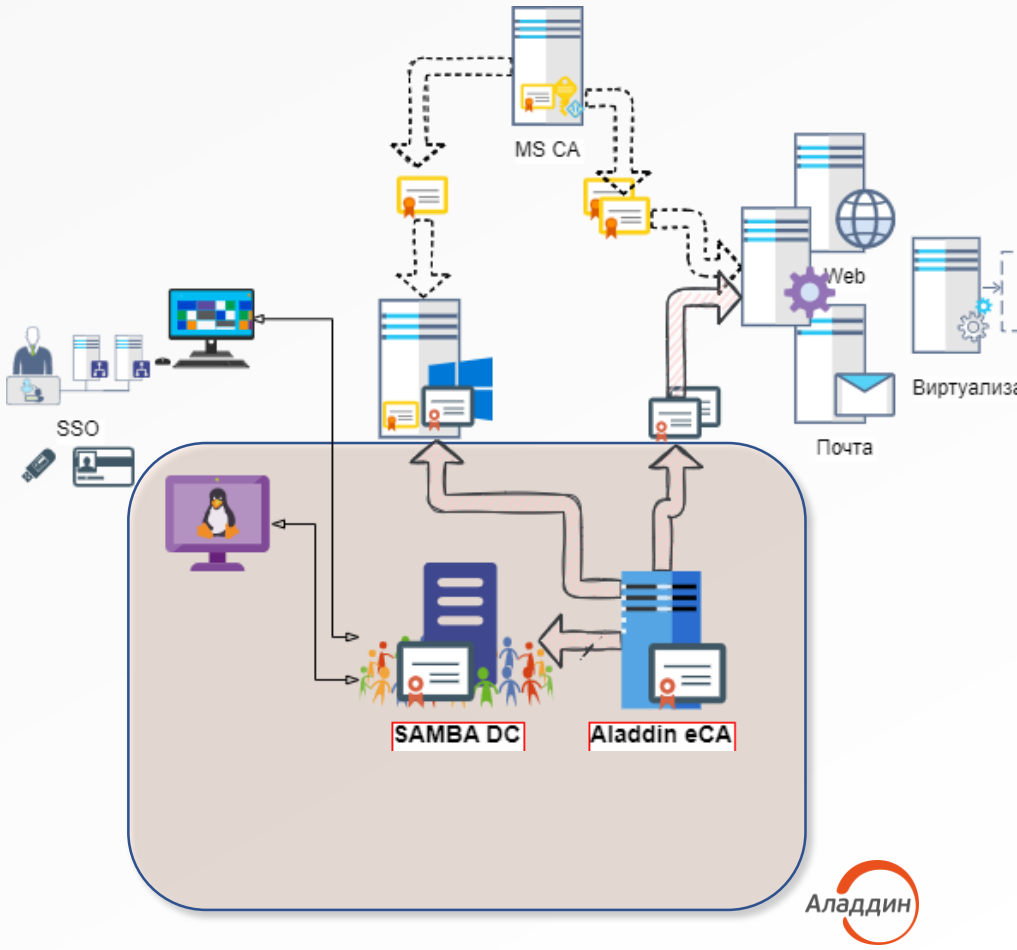
Особенности миграции сервисов LDAP и PKI в действующих ИС

План миграции:

- Временно сохраняется структура леса/домена на базе Microsoft AD
- Рядом разворачивается новый домен на базе Samba DC
- Разворачивается в параллель Aladdin eCA
- Выпускаются сертификаты для Windows и Linux KDC с обоих CA
- По мере окончания срока действия сертификаты выпускаются новым CA

В итоге:

- Отсутствуют риски остаться без ИС в результате отключения сервисов Microsoft
- Бесшовная и плавная миграцию LDAP и PKI без резкого отключения AD
- Получаем реально независимую инфраструктуру домена безопасности с сохранением SSO

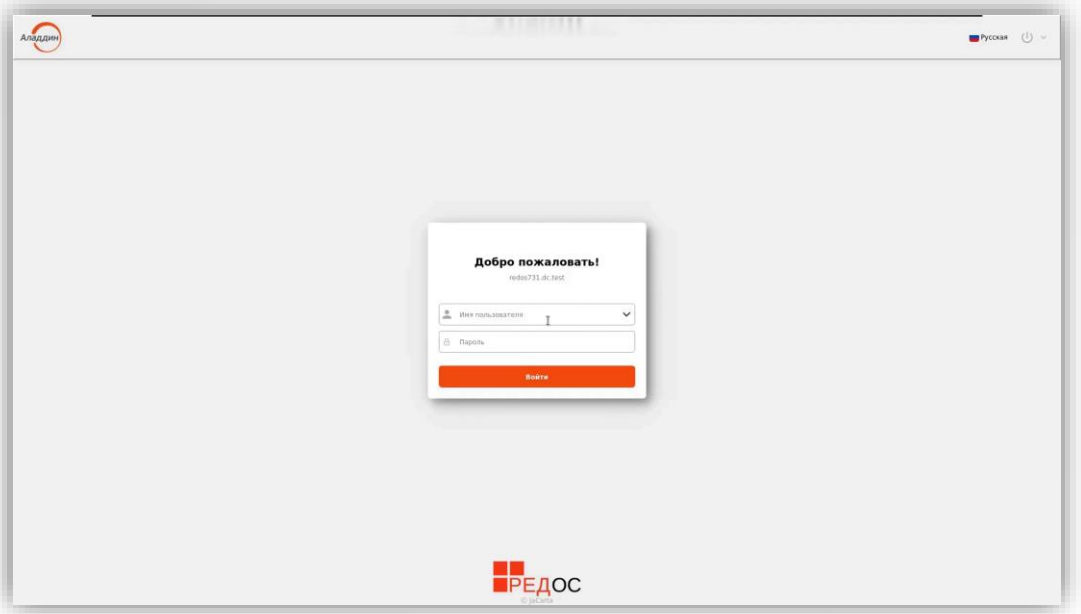


Aladdin SecurLogon для Linux

Организация SSO (единый вход) на отечественных ОС

Локальная и доменная 2ФА без PKI

- **Вместо** простого **пароля используется автоматически сгенерированная сложная последовательность** (до 63 символов), хранящихся в защищённой области электронного ключа JaCarta. В случае установки в политиках безопасности функции автоматической смены пароля на средстве аутентификации, к примеру, раз в день — задача подбора пароля становится и вовсе невыполнимой
- **Пользователю не нужно запоминать сложные пароли и периодически их менять**. Нужно всего лишь запомнить короткий PIN-код, который защищён от подбора
- При данном сценарии нет необходимости поддерживать УЦ
- Конфигурирование и защита SSH и RDP подключений



Локальная и доменная 2ФА в связке с CA

- Aladdin SecurLogon является удобным решением для перехода от простых паролей к двухфакторной аутентификации **с использованием любых цифровых сертификатов,** хранящихся в защищённой области электронного ключа JaCarta
- Aladdin SecurLogon помогает облегчить создание гетерогенных сетей в уже существующих системах с развёрнутой PKI, так и создание новых ИС только на базе отечественных ОС
- Поддерживает работу с Aladdin eCA, MSCA

Автоматическая конфигурация АРМ

- Домены: Microsoft AD, FreeIPA, Samba DC
- РЕД ОС 7.2 (7.3), Astra Linux 1.6 SE (1.7 SE), Альт 8 СП, Альт 9
- Автоматизация развертывания 20 минут на 1000 АРМ
- На сертификации по требованиям ОУД-2 ФСТЭК

Аладдин

Удалённый доступ

Обзор решений и возможностей

Аладдин

Удалённый доступ

Наиболее востребованные сценарии и технологии

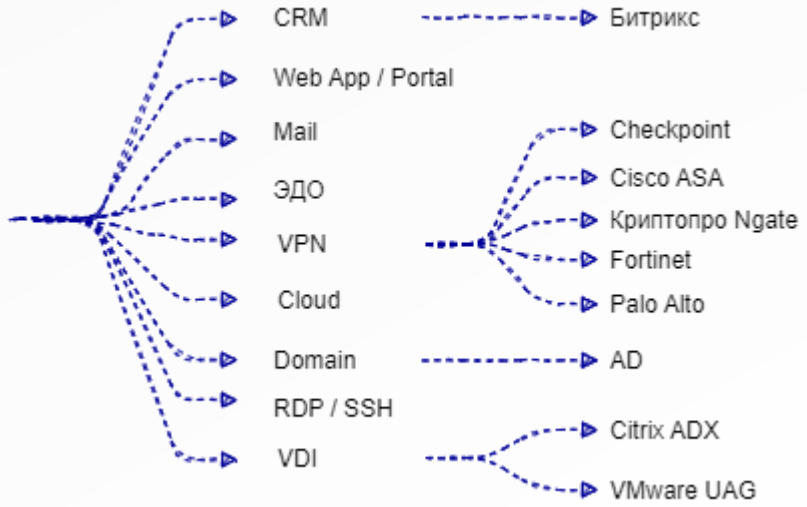
Одноразовые пароли

JaCarta Authentication Server (JAS) + **Aladdin 2FA** – автономный высокопроизводительный сервер аутентификации по OTP и Push

Цифровые сертификаты

JaCarta - USB токены и смарт карты

Aladdin LiveOffice (ALO) – замена корпоративного ноутбука (доверенная ОС, серт/ VPN, 2ФА и ЭП в одном устройстве)



Защита данных

Обзор решений и возможностей

Аладдин

Secret Disk Linux

Основная информация о продукте

Secret Disk Linux обеспечивает криптографическую защиту информации в среде Linux

- Шифрование виртуальных дисков
- Прозрачное шифрование информации
- Встроенный модуль шифрования Secret Disk Crypto Engine
- Магма, Кузнечик, Эхинацея ГОСТ Р 34.12-2018 , ГОСТ 34.13-2018
- 2ФА пользователей на базе алгоритма ЭП ГОСТ Р 34.10-2018
- Поддержка ОС Astra Linux 1.6 (Смоленск) Обновление 6.
- Поддержка ядра ОС: generic
- Поддержка файловой системы EXT4

Экспериментальные возможности:

- Поддержка ядра Astra Linux в режиме hardened
- Поддержка мандатного режима PARSEC
- Поддержка пользователей домена Astra Linux Domain

Аладдин

Крипто БД

Важнейшие задачи, решаемые продуктом

Надёжная защита информации в СУБД

- **Сертифицированное** СКЗИ для защиты данных в базе
- Зашифровываются таблицы или отдельные столбцы
- Реализованы методы "прозрачного" шифрования

Разграничение прав доступа пользователей

- В системе реализована двухфакторная аутентификация

Аудит и мониторинг действий пользователей

- Доступ к данным учитывается в защищенном журнале

Защита от Администратора СУБД

- Админ имеет доступ к таблицам
- Все попытки доступа фиксируются

ORACLE DATABASE

Microsoft SQL Server

PostgreSQL

TIBERO DataBase

Аладдин

Спасибо!

Будь собой в электронном мире!®

Для запроса дополнительной информации прошу обращаться напрямую или на общий ящик команды, будем рады поделиться опытом и помочь!

Построение системы 2ФА на базе отечественных ОС

- Инфраструктура открытых ключей
- Удаленное подключение сотрудников
- Централизованное управление защищенными носителями информации

Интеграция системы 2ФА в ИТ-инфраструктуру

- Обеспечение связи с доменами на базе SambaDC, FreeIPA, ALD Pro и др.
- Обеспечение связи с бизнес приложениями

Помощь в миграции инфраструктуры с Windows на Linux

- Разработка плана миграции (на базе готовых отработанных методик)

Контакты:

Шалимов Сергей
+7 (977) 280 84 12
linux@aladdin.ru
www.aladdin-rd.ru

Аладдин