Клиент для Linux с поддержкой усиленной и строгой аутентификации с PKI

Aladdin SecurLogon

- Простой и быстрый переход к двух- и трехфакторной аутентификации в Linux
- Полноценная поддержка PKI
- Работа с различными доменами
- Работа в гетерогенных средах (Windows и Linux)
- Полноценная замена Microsoft Smart Card Logon на отечественных ОС

Аладдин

Клиент для Linux с поддержкой 2FA/3FA – усиленной и строгой аутентификации, PKI. Отечественная замена Microsoft Smart Card Logon. Решение для простого и быстрого перехода к двухфакторной аутентификации в Linux при входе в операционную систему и доступе к сетевым ресурсам по USB-токенам и смарт-картам JaCarta

Сценарии применения

Aladdin SecurLogon позволяет настроить двухфакторную аутентификацию для следующих сценариев:

Локальная 2ФА без PKI

- Вместо пароля используется автоматически сгенерированная сложная последовательность до 63 символов, хранящаяся в защищённой области электронного ключа JaCarta
- Пользователю не нужно запоминать сложные пароли и периодически их менять. Нужно всего лишь запомнить короткий PIN-код, который защищён от подбора

Сетевая 2ФА без PKI

- Сетевая 2ФА по логину и паролю, которые записываются в закрытый раздел токена или смарт-карты
- Работа в доменах на базе Microsoft AD, Samba DC или FreeIPA
- В данном сценарии не нужно поддерживать УЦ
- Использование OTP, SMS, PUSH

Локальная 2ФА с PKI

- ОС аутентифицирует пользователя с использованием цифровых сертификатов, хранящихся в защищённой области электронного ключа JaCarta
- Можно использовать как самоподписанный сертификат, так и сертификат, выпущенный с помощью УЦ

Сетевая 2ФА с PKI

- Упрощает создание гетерогенных сетей в уже существующих системах с развёрнутой PKI и ИС на базе Linux
- Поддерживает работу с MSCA, AeCA, DogTAG

Преимущества применения Aladdin SecurLogon

› Повышение безопасности подключения к ИС

- Повышает общий уровень безопасности за счёт перехода от системы простых паролей к двухфакторной аутентификации (2ФА)
- При извлечении пользователем USB-токена или смарт-карты компьютер блокируется автоматически, что минимизирует риск несанкционированного доступа к ПК или его использования недобросовестными третьими лицами
- Автоматическая генерация и смена сложного пароля (до 63 символов): пользователь не имеет доступа к паролю, а значит, не сможет записать или скомпрометировать его

› Удобство для пользователя

- Простой PIN-код вместо сложного пароля: пользователю не требуется заучивать сложные пароли и периодически их менять. Нужно лишь запомнить короткий PIN-код, который защищён от подбора
- Гибкие настройки политик входа – вместо пароля можно использовать электронный ключ (ЭК)
- Безопасное подключение к удалённому рабочему столу (RDP), используя данные из защищённого раздела ЭК

› Автоматизация работы администратора

- Гибкие возможности настройки и сценариев применения: поддержка гетерогенных сетей с PKI / без PKI, различных доменов и УЦ
- Поддержка отечественных ОС – Astra Linux, РЕД ОС, Альт

› Сертификаты

- Средство двухфакторной аутентификации “Aladdin SecurLogon” в государственном реестре системы сертификации средств защиты информации.
- Сертификат соответствия №4809 выдан 8 мая 2024 года. Сертификация во ФСТЭК России на соответствие УД-4.
- Aladdin SecurLogon разработан РФ, зарегистрирован в Едином реестре отечественного ПО - № 10043 запись от 02.04.2021

› Задачи импортозамещения и санкционной независимости

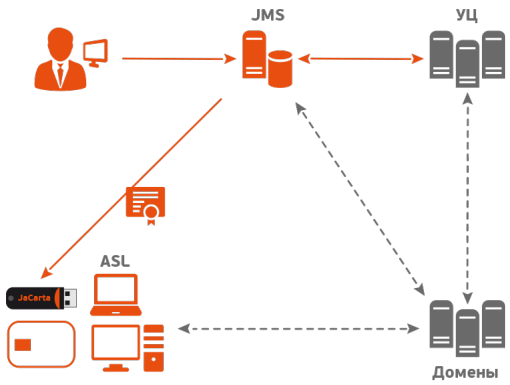
Клиент для Linux с поддержкой усиленной и строгой аутентификации и PKI - Aladdin SecurLogon разработан РФ, зарегистрирован в Едином реестре отечественного ПО - №10043 запись от 02.04.2021

› Какие продукты зарубежных вендоров способен заместить Aladdin SecurLogon?

Вендор	Продукт
Microsoft	MS Smart Card Logon
SAFENET	SafeNet Authentication Service
SafeNet	eToken Network Logon

Aladdin SecurLogon в сетевой аутентификации с использованием PKI

Организация 2ФА для входа в операционную систему, расположенную в сетевом домене



› Генерация сертификата

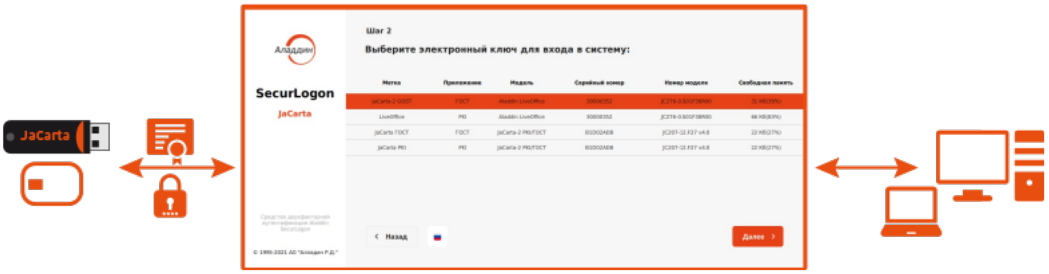
- Администратор безопасности через консоль управления JaCarta Management System (JMS) создаёт на смарт-карте или USB-токене закрытый ключ и формирует GSR-запрос
- JMS передаёт GSR-запрос в удостоверяющий центр (УД)
- УД возвращает в JMS сертификат пользователя
- JMS записывает полученный сертификат пользователя в защищённую память электронного ключа (ЭК) JaCarta
- ЭК передаётся пользователю

› Аутентификация

- Электронный ключ JaCarta пользователь подключает к своему рабочему ПК с настроенным Aladdin SecurLogon и инициирует запрос на аутентификацию для входа в домен
- Сервер отправляет пользователю набор данных с запросом их подписать
- Пользователь вводит PIN-код для доступа к закрытому ключу
- Подписанный запрос передаётся на сервер
- Сервер проверяет подпись и в случае успеха аутентифицирует пользователя
- Aladdin SecurLogon в локальной аутентификации
- Вариант настройки 2ФА для входа в локальную операционную систему

Aladdin SecurLogon в локальной аутентификации

Вариант настройки 2ФА для входа в локальную операционную систему



› Настройка

- Администратор безопасности с помощью Aladdin SecurLogon генерирует сертификат или профиль пользователя и сохраняет сгенерированную информацию на защищённый раздел USB-токена или смарт-карты
- Если нет развёрнутой PKI, то при генерации профиля пользователя задаётся периодичность смены пароля
- Регулярная генерация и замена паролей на новые происходят автоматически без участия пользователя

› Аутентификация

- Полученный электронный ключ JaCarta пользователь подключает к своему рабочему ПК с настроенным Aladdin SecurLogon и вводит PIN-код
- Данные из защищённого раздела электронного ключа JaCarta сопоставляются с данными ОС – в зависимости от выбранной политики входа и способа аутентификации это может быть сложный пароль или цифровой сертификат
- При успешной аутентификации пользователю предоставляется доступ к его рабочему столу

Совместимость

Вендор	Значение
Поддерживаемые операционные системы	Поддерживаемые ОС: • Astra Linux Special Edition, версия 1.7 • Альт 8 СП Рабочая станция, версия 8.1 • Альт Рабочая станция, версия 10 • РЕД ОС 7.3
Поддерживаемые домены	• Microsoft AD • FreeIPA • Samba DC • ALD PRO
Поддерживаемые УЦ	• Aladdin Enterprise CA • MSCA
Поддерживаемые модель USB-токенов и смарт-карт	• JaCarta 2 ГОСТ • JaCarta PRO • JaCarta PRO/ГОСТ • JaCarta-2 PRO/ГОСТ • JaCarta PKI • JaCarta PKI/Flash • JaCarta PKI/ГОСТ/Flash • JaCarta-2 PKI/ГОСТ • JaCarta PKI/ГОСТ • JaCarta SF/ГОСТ • Aladdin LiveOffice • eToken PRO (Java)

Aladdin SecurLogon обеспечивает

- Автоматизацию настройки 2ФА для:
  - входа в локальную операционную систему (с PKI или по профилю пользователя)
  - входа в операционную систему, расположенную в сетевом домене (с PKI или по профилю пользователя)
  - безопасного подключения к удалённому рабочему столу (RDP) - при этом удалённые компьютеры необязательно должны находиться в одном домене
- Настройки OTP, PUSH, SMS
- Переход на отечественные операционные системы и использование многофакторной аутентификации
- Построение сложных гетерогенных сетей за счёт гибкой архитектуры и поддержки наиболее популярных технологий аутентификации
- Полноценную поддержку PKI, двух- и трёхфакторную строгую аутентификацию пользователей в ОС на базе Linux, в смешанных гетерогенных средах
- 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
  - этот пароль хранится в защищённой памяти токенов JaCarta, в соответствии с установленными политиками безопасности он может автоматически меняться, например, раз в день, после каждого использования
  - после ввода правильного ПИН-кода токена SecurLogon использует этот пароль для доменной и/или локальной аутентификации на отдельно стоящих АРМах. При этом пользователь свой пароль не знает, следовательно, не сможет его скомпрометировать
- Усиленную аутентификацию пользователей с использованием одноразовых паролей (OTP) или виртуального токена на мобильном устройстве
- Применение политик входа на основе принадлежности пользователя к группе безопасности (только токен, токен или пароль, только пароль)
- Аутентификацию любым из методов на отдельно стоящих АРМ или АРМ в одноранговых сетях (workgroup)
- Дополнительные сервисные функции, позволяющие до входа в ОС разблокировать токен, сменить ПИН-код пользователя, кастомизировать окно приветствия и др.
- Групповое развёртывание и удалённую настройку с рабочего места администратора
- Полноценную альтернативу Microsoft Smart Card Logon на отечественных ОС на базе Linux
- Защиту удалённых соединений (RDP)

О компании

Аладдин – ведущий российский вендор – разработчик и производитель

- ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов
- средств аутентификации и электронной подписи для обеспечения информационной безопасности и защиты данных.

Компания работает на рынке с апреля 1995 г.

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, 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".

В 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.

Основные направления деятельности

- Информационная безопасность, PKI
- Многофакторная аутентификация, обеспечение безопасного доступа к информационным ресурсам предприятия
- Организация безопасной дистанционной работы сотрудников и контрагентов организаций при использовании ими недоверенных средств вычислительной техники
- Средства электронной подписи
- Защита данных (на дисках, съёмных носителях, в базах данных)

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин — ведущий российский вендор-разработчик и производитель
ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры

https://t.me/aladdinrd
https://vk.com/aladdinrd

01/2024