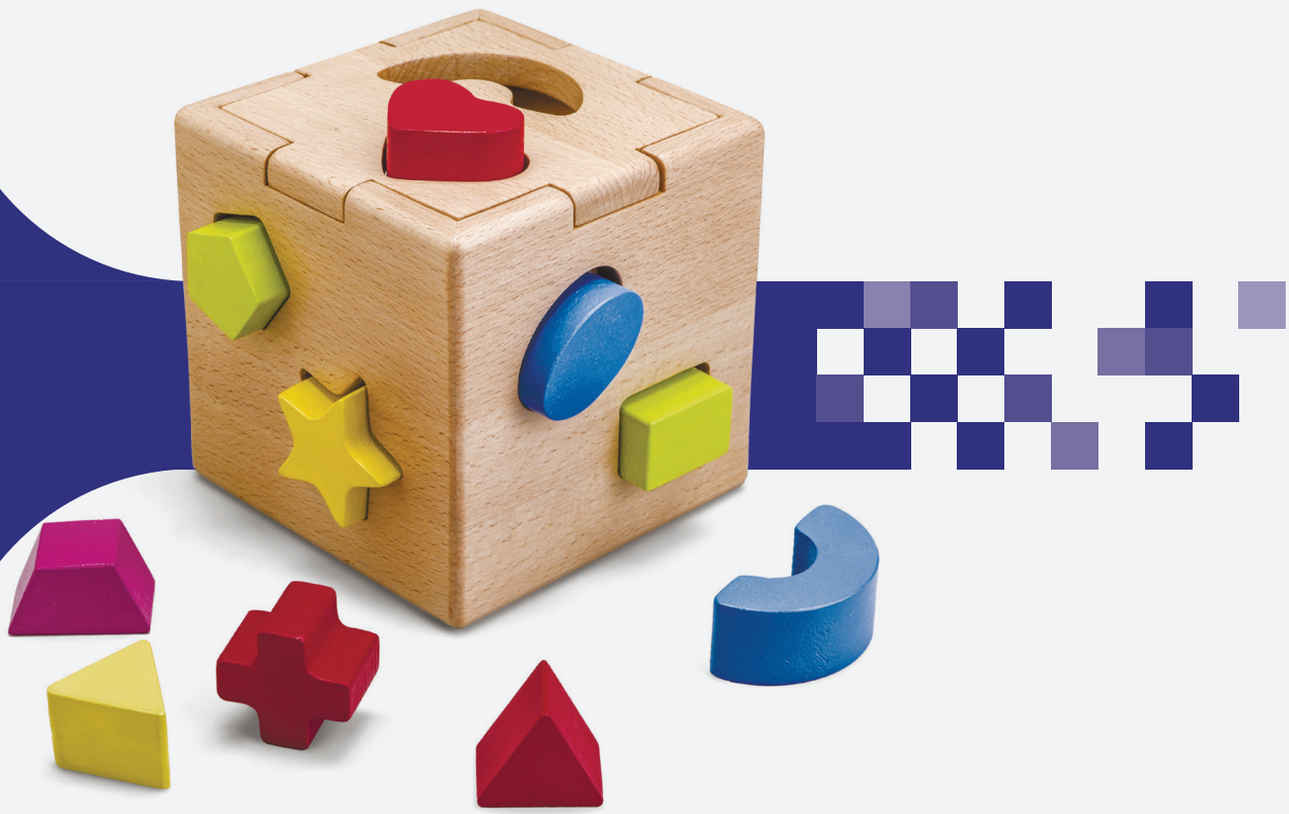
Сервер аутентификации с поддержкой OTP- и U2F-токенов, программных токенов для мобильных устройств



JAS

JaCarta Authentication Server

- Усиленная аутентификация пользователей по одноразовым паролям (OTP)
- Строгая аутентификация пользователей по протоколу U2F
- Обеспечение аутентификации на десктопах, ноутбуках и мобильных устройствах
- Простая интеграция с прикладным ПО по стандартным протоколам
- Высокая производительность (более 1 000 аутентификаций в секунду)

Аладдин

Проблемы использования простых паролей

Аутентификация, т.е. процедура проверки подлинности пользователя, является главным барьером на пути в информационные системы. Самым распространённым методом обеспечения безопасного входа является однофакторная аутентификация, когда в качестве единственного фактора выступает пара "логин/пароль". Очевидно, что главное достоинство этой методики защиты — простота. Одновременно с этим это и её главный недостаток, т.к. пароль можно быстро подобрать.

Не менее 28% от всех инцидентов безопасности в мире стали возможными только из-за того, что администраторы взломанных систем использовали слишком слабые пароли. Использование сильных паролей также не решает проблему — обычно пользователи не могут их запомнить, поэтому чаще всего просто записывают их на стикерах или в блокнотах, которые оставляют рядом со своим рабочим местом.

Решением описанной проблемы является переход на многофакторную аутентификацию с использованием стойких криптографических алгоритмов и инфраструктуры открытых ключей (PKI), однако для многих организаций развёртывание и поддержка PKI является слишком затратной задачей. Альтернативой является использование усиленной аутентификации на основе одноразовых паролей (OTP) или строгой аутентификации на основе открытого протокола FIDO U2F.

Для первого варианта компания "Аладдин Р.Д." предлагает линейку устройств JaCarta PKI, для второго — JaCarta WebPass и JaCarta U2F, работающие с сервером аутентификации JaCarta Authentication Server (JAS).

JaCarta Authentication Server

— надёжное решение для организации усиленной или строгой аутентификации

OTP — одноразовый пароль (One Time Password). Главное преимущество OTP при его сравнении с обычным статическим паролем — невозможность повторного использования.

По этой причине даже если злоумышленник перехватит данные сессии аутентификации, он не сможет использовать скопированный OTP для получения доступа к защищаемой информационной системе.

U2F (Universal 2nd Factor) — открытый протокол двухфакторной аутентификации конечных пользователей онлайн-сервисов, разработанный ведущими мировыми ИТ-компаниями в рамках организации FIDO Alliance.

Применение протокола U2F позволяет организовать строгую двухфакторную аутентификацию по U2F-токену без разворачивания инфраструктуры открытых ключей (PKI).

JAS поддерживает работу как с аппаратными OTP- и U2F-токенами, так и с программными токенами для мобильных устройств (например, "Яндекс.Ключ", Google Authenticator). Применение JAS позволяет обеспечить надёжную защиту доступа к информационным системам и электронным сервисам, а также повысить удовлетворённость и лояльность пользователей из-за упрощения процесса аутентификации.

В зависимости от типа используемых токенов (OTP, U2F, программные) JAS обеспечивает безопасный доступ к следующим системам и сервисам:

- корпоративные системы (CRM, порталы, почта и т.д.), в т.ч. Microsoft SharePoint и Microsoft Outlook Web App;
- Web-приложения, сайты и облачные сервисы;
- системы дистанционного банковского обслуживания (ДБО);
- удалённые рабочие столы: Microsoft Remote Desktop Gateway, VMware Horizon View, Citrix XenApp/XenDesktop;
- VPN-шлюзы;
- самописные приложения.

Встроенные инструменты управления аппаратными и программными токенами значительно упрощают и ускоряют работу системных администраторов и офицеров безопасности.

JAS может использоваться

В государственных и коммерческих организациях, нуждающихся в усилении аутентификации пользователей при доступе к внешним или внутрикорпоративным системам

Разработчиками систем ДБО, корпоративного ПО и онлайн-сервисов

Организациями, заинтересованными в импортозамещении аналогичных продуктов иностранных вендоров

Преимущества

Поддержка аппаратных и программных токенов

JAS позволяет использовать для аутентификации как аппаратные, так и программные токены, что даёт возможность применять разные способы аутентификации для разных пользователей: OTP- и U2F-токены для пользователей десктопов и ноутбуков, программные токены — для мобильных пользователей.

Отечественное ПО

JAS зарегистрирован в Едином реестре российских программ для электронных вычислительных машин и баз данных (№ 2128) и обладает всеми необходимыми функциями для импортозамещения аналогичных разработок иностранных вендоров.

Совместимость

JAS совместим с любыми аппаратными и программными токенами, генерирующими OTP по событию (HOTP, согласно RFC 4226) и по времени (TOTP, согласно RFC 6238), а также любыми U2F-токенами. Для интеграции с прикладным ПО реализована поддержка протоколов RADIUS, REST, WCF, WS-Federation и AD FS, с SMS-шлюзами — HTTP и SMPP.

Поддержка мобильных устройств

JAS поддерживает бесплатные приложения генерации OTP по событию и по времени, в т.ч. "Яндекс.Ключ", Google Authenticator, которые доступны для мобильных устройств на базе операционных систем Google Android, Apple iOS, Microsoft Windows и др. Поддержка SMS-шлюзов позволяет отправлять OTP на мобильные устройства в виде SMS-сообщений.

Доступные цены

Цены на JAS фиксированы в рублях, не зависят от колебаний на валютном рынке и выгодно отличаются от цен на иностранные аналоги. После внедрения JAS оплачивается только техническая поддержка, позволяющая получать консультации технических специалистов компании "Аладдин Р.Д." и все обновления.

Автономность

Для полноценной работы JAS не требуется дополнительное ПО, т.к. в комплект поставки уже включены сервис аутентификации, средства мониторинга, плагины для Microsoft Network Policy Server (NPS) и Microsoft Active Directory Federation Services (AD FS), а также средства управления токенами и пользователями.

Строгая аутентификация без PKI

Поддержка международного стандарта FIDO U2F позволяет построить систему строгой аутентификации без разворачивания PKI и сопутствующих ему издержек.

Производительность

JAS выдерживает значительные нагрузки — свыше 1 000 аутентификаций в секунду на одном сервере, что позволяет использовать его в организациях любого масштаба.

Масштабируемость

Производительность сервера JAS напрямую зависит от производительности процессора (вертикальная масштабируемость).

Надёжность

В JAS реализована поддержка службы кластеров Microsoft Failover Cluster (режим Active/Standby) и репликации базы данных средствами Microsoft SQL Server, что позволяет гарантировать бесперебойность аутентификации.

Лицензирование и поддержка

Лицензирование

- JAS лицензируется только по количеству токенов (как аппаратных, так и программных).
- Цены на лицензии фиксированы в рублях.
- В рамках одной мажорной версии (1.x) срок действия лицензии не ограничен.

Внедрение

- Для ознакомления с JAS доступна демо-версия на 1 месяц.
- Установка и настройка JAS максимально автоматизированы.
- Внедрение и сопровождение JAS могут осуществлять как партнёры компании "Аладдин Р.Д.", имеющие сертифицированных специалистов, так и представители самого разработчика.

Техническая поддержка

- При покупке JAS предоставляется 12 месяцев базовой технической поддержки.
- Сертификат базовой технической поддержки даёт право на:
  - получение всех обновлений продукта (в рамках мажорной версии);
  - получение консультаций по установке и использованию системы;
  - доступ к Базе знаний по JAS и токенам.
- Доступны пакеты технической поддержки на 12, 24 и 36 месяцев.

Технические характеристики

Системные требования

Сервер JAS
– Процессор: Intel Core i3-3xxx
– Оперативная память: от 3 ГБ
– ОС: Microsoft Windows Server 2012 R2 или выше
– Дополнительное ПО: Microsoft SQL Server 2008 (или выше) и Microsoft .NET Framework 4.5

Консоль управления JAS
– Процессор: Intel Core i3-3xxx
– Оперативная память: от 1 ГБ
– ОС: Microsoft Windows Vista SP2 или выше
– Дополнительное ПО: Microsoft .NET Framework 4.5

JAS-плагин для NPS
– Оперативная память: от 2 ГБ
– ОС: Microsoft Windows Server 2008 SP2 или выше
– Дополнительное ПО: Microsoft .NET Framework 4.5, Microsoft Network Policy and Access Services

JAS-плагин для AD FS
– Процессор: 2 GHz Dual-Core и выше
– Оперативная память: см. системные требования к AD FS + дополнительно 1 GB
– ОС: Microsoft Windows Vista SP2 или выше
– Дополнительное ПО: Microsoft .NET Framework 4.5, Active Directory Federation Services Role

Поддерживаемые модели аппаратных токенов

- Любые токены, генерирующие OTP по событию (в т.ч. JaCarta WebPass, eToken PASS, eToken NG-OTP, eToken NG-OTP (Java) и др.)
- Любые токены, генерирующие OTP по времени (в т.ч. eToken PASS и др.)
- Любые U2F-токены (в т.ч. JaCarta U2F)

Поддерживаемые программные токены для мобильных устройств

Любые программные токены, в т.ч. "Яндекс.Ключ", Google Authenticator (для ОС Google Android, Apple iOS, Microsoft Windows и др.)

Поддерживаемые протоколы интеграции с прикладным ПО

- Remote Authentication in Dial-In User Service (RADIUS)
- Representational State Transfer (REST)
- Windows Communication Foundation (WCF)
- Web Services Federation (WS-Federation)
- Active Directory Federation Services

Поддерживаемые протоколы интеграции с SMS-шлюзами

- HTTP (запросы POST и GET)
- Short Message Peer-to-Peer (SMPP)

Поддерживаемые режимы аутентификации

- Только OTP
- OTP + OTP PIN-код
- Доменный пароль + OTP
- Доменный пароль + OTP + OTP PIN-код
- U2F
- SMS

Поддерживаемые алгоритмы генерации OTP

- RFC 4226 + HMAC-SHA-1 (6 символов)
- RFC 4226 + HMAC-SHA-256 (6 символов)
- RFC 4226 + HMAC-SHA-256 (7 символов)
- RFC 4226 + HMAC-SHA-256 (8 символов)
- RFC 6238 + HMAC-SHA-1 (6 цифр)
- RFC 6238 + HMAC-SHA-1 (7 цифр)
- RFC 6238 + HMAC-SHA-1 (8 цифр)
- RFC 6238 + HMAC-SHA-256 (6 цифр)
- RFC 6238 + HMAC-SHA-256 (7 цифр)
- RFC 6238 + HMAC-SHA-256 (8 цифр)
- RFC 6238 + HMAC-SHA-512 (6 цифр)
- RFC 6238 + HMAC-SHA-512 (7 цифр)
- RFC 6238 + HMAC-SHA-512 (8 цифр)

Отказоустойчивость

Microsoft Failover Cluster, модель Active/Standby:
- несколько серверов JAS: синхронизация текущих значений счётчиков;
- несколько серверов Microsoft SQL Server: репликация базы данных средствами Microsoft SQL Server.

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17
Лицензии ФСБ России № 12632Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации услуг ГОСТ Р (РОСС RU.0001.03ГУ00) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
Сертификат соответствия - № РОСС RU.ФК14.К00011 от 20.07.18
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации "Военный Регистр" (РОСС RU.И1975.04ГШ02) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012
Сертификат соответствия - № ВР 21.1.13537-2019 от 25.04.19