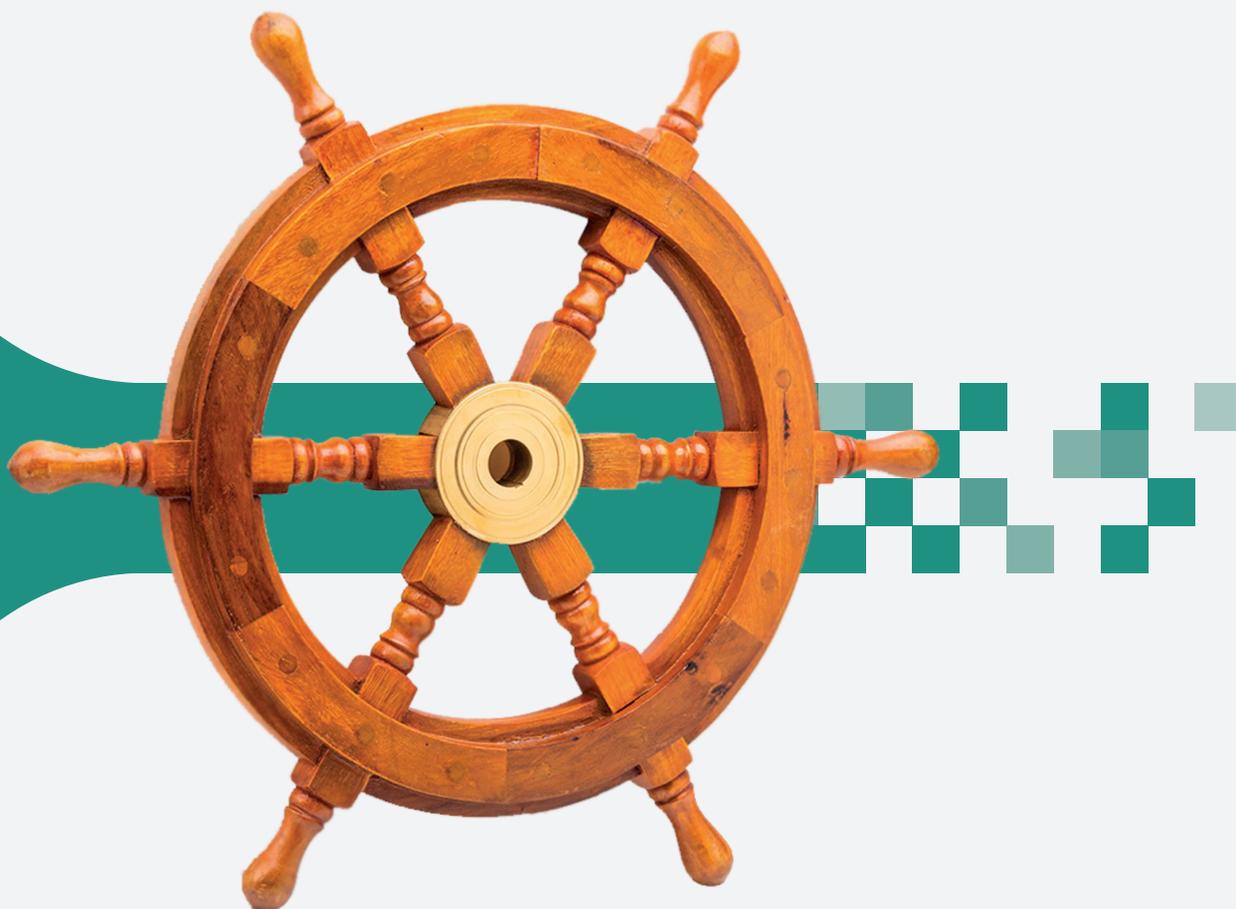


Корпоративная система учёта и управления жизненным циклом средств аутентификации



JMS

JaCarta Management System

- ▶ Поддержка USB-токенов и смарт-карт различных производителей
- ▶ Учёт СКЗИ по требованиям ФСБ России
- ▶ Развитый аудит действий сотрудников и администраторов
- ▶ Низкая стоимость внедрения и поддержки
- ▶ Сертификат ФСТЭК России



Необходимость автоматизации работы с токенами

Любая организация, использующая большое количество USB-токенов и смарт-карт для обеспечения двухфакторной аутентификации сотрудников и работы с электронной подписью (ЭП), сталкивается со значительными затратами на их администрирование (учёт, управление, соблюдение требований регуляторов, координация работы территориально-распределённых филиалов).



Задача учёта

Какой токен был выдан, кому, в каком подразделении или филиале компании?

Какие функции можно выполнять с помощью этого токена (доступ к корпоративным системам, Web-порталам, работа с ЭП и т. д.)?

Какие ключи и цифровые сертификаты хранятся в токене, когда заканчивается срок их действия?



Задача управления

К какой из систем даёт доступ этот токен? Как быстро отменить или предоставить доступ?

Какие политики организации исполняются? Как быстро применить изменения в случае их смены?

Какие права имеет каждая из групп пользователей? Достаточно ли их?

Как быстро выпустить сертификаты большим группам пользователей? Что делать, если они находятся в разных филиалах?

Как обеспечить актуальность данных о пользователях и их сертификатов (например, при смене фамилии после заключения брака)?



Соблюдение требований регуляторов

63-ФЗ "Об электронной подписи"
152-ФЗ "О персональных данных"
Приказ ФСБ России № 66
Приказ ФАПСИ № 152
Постановление Правительства Российской Федерации № 1119
Приказ ФСТЭК России № 21 и № 17
Приказ ФСБ России и ФСТЭК России №№ 416/189
Стандарты Банка России

Поэкземплярный учёт лицензий на средства криптографической защиты информации (СКЗИ), дистрибутивов СКЗИ, поэкземплярный и персонифицированный учёт токенов

В случае, если на предприятии используется несколько сотен или тысяч токенов, учёт и управление ими занимает значительную часть рабочего времени ИБ-отдела и стоит ощутимых денег. Таким образом, автоматизация процесса учёта и управления токенами необходима организациям, в которых:

- используется более 100 USB-токенов и смарт-карт;
- есть необходимость в обеспечении соблюдения политик информационной безопасности или требований регуляторов;
- имеющиеся средства аутентификации используются в нескольких филиалах.



Средние и крупные предприятия и корпорации



Банки и другие финансовые организации



Государственные учреждения, министерства и ведомства

Назначение JaCarta Management System

JMS – корпоративная система учёта и управления жизненным циклом USB-токенов и смарт-карт различных производителей (JaCarta, eToken и др.). С её помощью можно автоматизировать типовые операции при работе с USB-токенами и смарт-картами, обеспечить гибкую настройку политик их использования, а также централизованно управлять доступом к корпоративным системам.

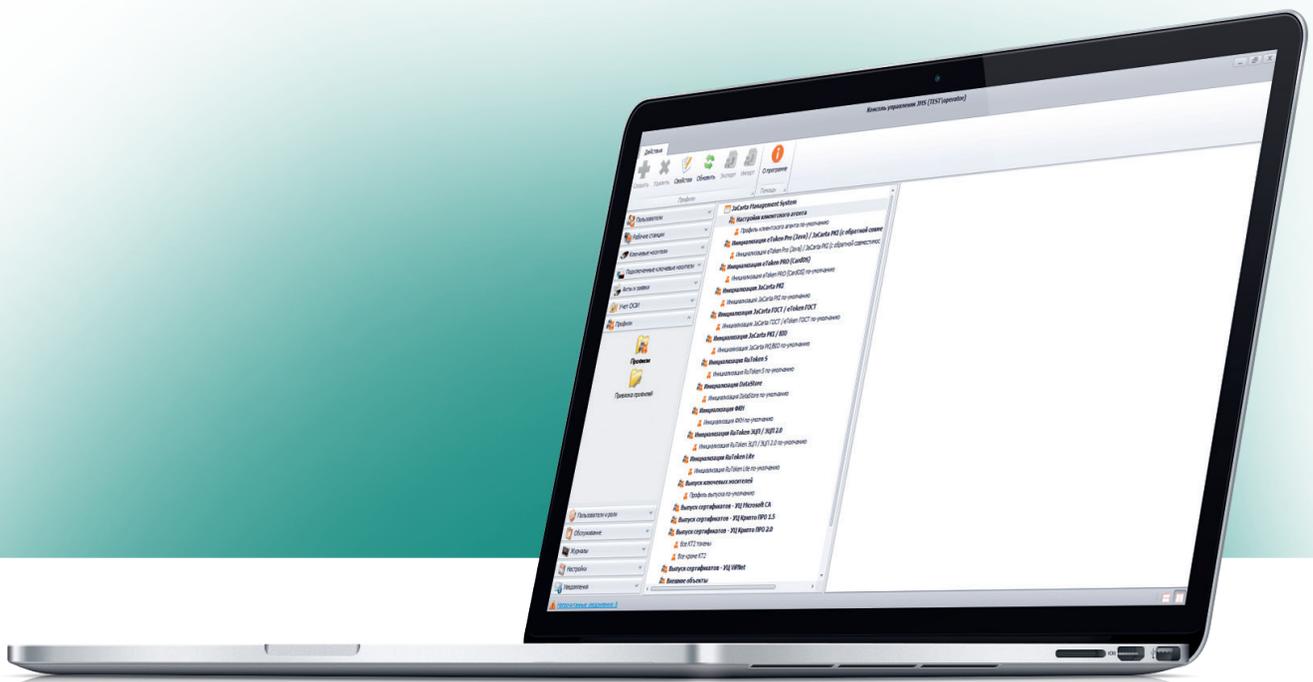
Встроенные в JMS средства построения отчётов и печати документов позволяют отслеживать состояние устройств и максимально автоматизировать подготовку документов, связанных с их жизненным циклом.

Автоматическая синхронизация USB-токенов и смарт-карт с базой JMS и популярными Удостоверяющими центрами даёт возможность мгновенно приводить содержимое всего парка USB-токенов и смарт-карт в актуальное состояние.

Единый реестр отечественного ПО

JMS – первая система управления токенами, включенная в Единый реестр отечественного ПО (№ 311) и рекомендуемая к закупкам государственными предприятиями и органами власти. Организации, имеющие в обороте 200 и более различных цифровых сертификатов, ведущие ручной учёт и управление, вынуждены нанимать дополнительного специалиста для ведения такой работы.

© Gartner, 2011 (G00226426)



Возможности



Автоматический учёт токенов

JMS позволяет автоматизировать учёт всех токенов, в т.ч. сертифицированных СКЗИ. Учитываются владелец, номер, модель и срок службы токенов, а также объекты на токене и рабочие станции, использующие токены.



Управление жизненным циклом токенов

JMS позволяет управлять всем жизненным циклом токенов от выдачи до отзыва вместе со всеми связанными с ними объектами (цифровые сертификаты, ключи, метки АПМДЗ и др.).



Управление политиками безопасности

С помощью JMS можно централизованно управлять политиками безопасности в отношении токенов, при этом изменения в политиках применяются практически моментально.



Возможность работы без аппаратных токенов

JMS позволяет производить выпуск сертификатов (контейнеров) не на токен, а непосредственно в реестр ПК. Т.е. пользователь теперь может работать без токена. Кроме того, на всех ПК, на которых установлен клиент JMS, можно в автоматическом режиме собирать информацию о сертификатах в личном хранилище пользователя, личном хранилище ПК и в файлах файловой системы. Все найденные сертификаты учитываются в системе и срок их действия можно контролировать, оперативно обновляя истекающие сертификаты в соответствии с настройками администратора. Администратор также имеет возможность дистанционно удалить нежелательные сертификаты на ПК пользователя.



Подготовка и печать документов

JMS может формировать и выводить на печать заявки на выдачу, замену и отзыв токенов или цифровых сертификатов, максимально упрощая формирование документов, связанных с жизненным циклом токенов.



Аудит действий пользователей и администраторов

JMS ведёт журнал действий пользователей и администраторов с удобными механизмами поиска и сортировки, помогающий диагностировать неисправности и разбирать конфликтные ситуации.



Синхронизация с внешними системами

JMS может автоматически отслеживать изменения во внешних системах (например, Microsoft Active Directory, в Удостоверяющем центре), в т.ч. изменение атрибутов пользователей (например, при смене фамилии), перевыпускать сертификаты и обновлять их на токенах.



Поддержка филиальной структуры

JMS позволяет отслеживать перемещение токенов между филиалами и распределять права по администрированию серверов JMS между ИТ-специалистами штаб-квартиры и филиалов. Возможен выпуск сертификатов группе пользователей, распределённых по разным филиалам.



Сервис самообслуживания для пользователя

JMS позволяет сотруднику самостоятельно совершать операции с токенами (выпуск, отключение, синхронизация, блокирование, разблокирование, замена) без обращения в ИТ- или ИБ-отдел.



Резервное копирование

JMS сохраняет копии выпущенных объектов, что позволяет гарантировать их сохранность, а также перевыпускать токены со старыми сертификатами.



Создание отчётов

В JMS реализована настраиваемая подсистема построения отчётов по токенам, пользователям, СКЗИ, ключевым документам и рабочим станциям. Доступно построение отчётов как по отдельным подразделениям, так и по всей филиальной сети.

Консоль управления

Удобно



Консоль управления JMS предоставляет удобный и интуитивно-понятный графический интерфейс для администрирования пользователей, токенов, сертификатов, СКЗИ, политик безопасности и планов обслуживания. Все функции по управлению и учёту токенов сосредоточены в одном месте, что избавляет от необходимости работы в нескольких не связанных между собой приложениях.

Для большего удобства управления JMS может использоваться упрощённый режим Консоли управления JMS, скрывающий все объекты и элементы управления, на которые у оператора нет прав. Этот режим может применяться для комфортной работы специалистов бюро пропусков и локальных администраторов, которым не требуются все возможности JMS.

Безопасно



Консоль управления JMS является полноценным приложением для Microsoft Windows, что гарантирует её быструю и бесперебойную работу, а также исключает проблемы совместимости с новыми версиями браузеров и снижения уровня безопасности из-за использования ActiveX-компонент или плагинов для работы с токенами (по сравнению с Web-клиентами).

Доступ к объектам и операциям в консоли управления определяется полномочиями конкретного администратора в соответствии с назначенной ему ролью. Передача данных между Сервером JMS и Консолью управления JMS осуществляется в зашифрованном виде с помощью протокола HTTPS (SSL и TLS, в т.ч. версии 1.2).



РусГидро

"...Применение современных технологий от "Аладдин Р.Д." не только позволяет эффективно и выгодно решить задачу по обеспечению информационной безопасности систем холдинга, но и обеспечивает максимум удобства для сотрудников. Выбор в пользу JMS также обусловлен тем, что использование комплексного решения, созданного на основе продуктов и технологий от одного разработчика, решает большое количество как организационных, так и технических и эксплуатационных вопросов".

Анатолий Иванов,
заместитель директора
Департамента по специальным видам
работ и защиты информации
ОАО "РусГидро"



"...Успешное сотрудничество ПФР с "Аладдин Р.Д." длится уже на протяжении многих лет. Это стало возможным благодаря надёжности и универсальности применения решений, разработанных компанией, которые обеспечивают высокий уровень защиты информации и возможность интеграции в информационную систему ПФР. Проект, реализуемый в Пенсионном Фонде России, является своевременным и актуальным, с учётом государственного курса на импортозамещение и сотрудничества с российскими производителями..."

Андрей Косарев,
руководитель проекта внедрения JMS
Департамента по обеспечению
информационной безопасности
Пенсионного Фонда России

Выгоды и преимущества

Отечественное ПО



JMS – первая система управления жизненным циклом токенов, зарегистрированная в Едином реестре отечественного ПО (№ 311) и рекомендуемая к закупкам государственными предприятиями и органами власти (при наличии отечественного решения структуры, финансируемые из российского бюджета, не могут приобретать аналогичное по функциям импортное ПО).

Повышение эффективности организации



Внедрение JMS позволяет повысить эффективность работы ИБ-отдела и организации в целом. Это достигается за счёт автоматизации работы с токенами, значительного сокращения числа человеческих ошибок, а также снижения времени простоя сотрудников, вызванных поломкой токенов или истечением срока действия цифровых сертификатов.

Уникальные функции



В JMS реализован ряд уникальных функций, позволяющих значительно упростить работу с токенами, сократить количество ошибок и повысить эффективность работы ИТ-отдела и сотрудников. Среди них:

- автоматический учёт СКЗИ в соответствии с требованиями ФСБ России;
- автоматическое ведение реестра токенов;
- автоматическое обновление сертификатов при изменении личных данных пользователей;
- поддержка многофункциональных токенов;
- пакетная регистрация токенов JaCarta;
- выпуск и управление сертификатами пользователей в реестр ПК без использования токенов;
- учёт сертификатов в личном хранилище пользователей и компьютеров;
- взятие под управление имеющихся токенов и объектов на них;
- сохранение перевыпускаемых сертификатов;
- учёт перемещения токенов между подразделениями организации;
- управление токенами внешних пользователей (вне Active Directory);
- работа нескольких серверов JMS в автономном режиме;
- распределение полномочий администраторов в филиальной сети;
- создание кастомизированных запросов ко всем поддерживаемым Удостоверяющим центрам;
- простая миграция с SAM и TMS, в т.ч. с возможностью параллельной работы обеих систем (JMS и SAM/TMS) с сохранением всех данных и настроек.

Обеспечение соответствия требованиям законодательства России



Возможности JMS по учёту всех СКЗИ (как аппаратных, так и программных) и ключевых документов, согласно требованиям ФСБ России, а также СЗИ, согласно требованиям ФСТЭК России, позволяют соблюсти все требования российского законодательства. JMS также сертифицирована ФСТЭК России и может применяться для защиты информации в ИСПДн до 1 уровня включительно, в ГИС до 1 уровня защиты включительно, а также при создании АС до уровня защищённости 1Г включительно.

Быстрое внедрение



За счёт автоматизации процесса установки и настройки, а также ряда уникальных возможностей, таких, как пакетная регистрация и взятие под управление выпущенных ранее токенов, внедрение JMS максимально сжато во времени. По опыту Пенсионного Фонда России после тестирования и настройки JMS в пилотной зоне процесс внедрения системы в каждом из филиалов ПФР в среднем занимал всего 3 рабочих дня.

Масштабируемость и производительность



JMS спроектирована как высокопроизводительная и масштабируемая система, позволяющая вести учёт и управление более чем 1 млн токенов и расположенных на них объектов без ощутимой деградации производительности. Поддерживается работа в кластере и в виртуальных средах, а также автономная работа серверов JMS в организациях с территориально-распределённой структурой, испытывающих дефицит пропускной способности каналов.

Простой интерфейс для пользователя и администратора



JMS предоставляет современный и интуитивно-понятный интерфейс как для администраторов и офицеров безопасности (Консоль управления JMS — позволяет управлять всеми токенами, пользователями, рабочими станциями и политиками безопасности, а также строить отчёты и осуществлять обслуживание системы), так и для пользователей (Клиент JMS — позволяет синхронизировать токены и использовать функции самообслуживания). В системе также реализован Web-based личный кабинет пользователя, обладающий дружелюбным интерфейсом.

Поддержка имеющейся инфраструктуры открытых ключей



Система JMS позволяет брать под управление токены, которые использовались в организации до её внедрения, а также сохранять сертификаты и ключи токенов, которые выводятся из эксплуатации. Также в системе реализована поддержка всех популярных Удостоверяющих центров. Это позволяет обеспечить преемственность со старой инфраструктурой и избежать проблем, вызванных переходом на новую систему управления токенами.

Собственный каталог пользователей



Если в организации нет Active Directory или другого источника информации о пользователях, JMS позволяет создавать собственный каталог пользователей с нужными атрибутами и иерархией пользователей, настраиваемый через Консоль управления JMS. К разным ветвям иерархии можно привязывать профили пользователей, что позволяет быстро присваивать и изменять желаемые политики безопасности.

Низкая стоимость владения



Лицензирование JMS максимально прозрачно, а цены фиксированы в рублях и не зависят от колебаний курсов на валютном рынке. В базовую поставку JMS уже включены все необходимые функции для полноценной автоматизации учёта и управления токенами. Дополнительные возможности лицензируются отдельно, что позволяет оптимизировать затраты и спланировать постепенное развитие системы. После внедрения JMS оплачивается только техническая поддержка, позволяющая получать консультации технических специалистов компании "Аладдин Р.Д." и все обновления системы.

Токены и система управления от одного разработчика



"Аладдин Р.Д." — единственный российский вендор, производящий как собственные средства аутентификации и ЭП (токены JaCarta), так и систему управления ими (JMS). В случае их совместного использования заказчик получает:

- максимально упрощённый процесс логистики, внедрения и предоставления технической поддержки;
- снижение затрат на поиск разрозненных поставщиков, а также тестирование и поддержку не связанных между собой решений и продуктов;
- снижение совокупных затрат на поддержку инфраструктуры аутентификации и ЭП;
- гарантированную совместимость продуктов и надёжность их работы;
- быстрый выпуск обновлений и поддержку всех новых моделей токенов JaCarta;
- возможность влиять на дальнейшее развитие JMS и токенов JaCarta, предлагая новые функции;
- полноценную поддержку распространённых токенов и смарт-карт других производителей, позволяющую внедрять систему в гетерогенные (в смысле используемых токенов) информационные инфраструктуры.

Гибкость в настройке и модификации



Вместе с JMS предоставляется открытый интерфейс прикладного программирования (API), позволяющий интегрировать её с другими информационными системами. Например, обеспечить управление пользователями JMS из другой системы, организовать экспорт списка пользователей и рабочих станций в JMS и т. д.

Лицензирование и поддержка



Лицензирование

- JMS лицензируется только по количеству пользователей, токенами которых управляет система.
- Цены фиксированы в рублях.
- В рамках одной версии срок действия лицензии не ограничен.
- Лицензии можно докупить поштучно.



Техническая поддержка

- При покупке JMS предоставляется 12 месяцев базовой технической поддержки.
- Сертификат базовой технической поддержки даёт право на:
 - получение всех обновлений продукта в рамках мажорной версии (3.x);
 - получение консультаций по установке и использованию системы;
 - доступ к Базе знаний по JMS, а также токенам JaCarta и eToken.
- Доступны пакеты технической поддержки на 12, 24 и 36 месяцев.
- Возможно приобретение расширенного пакета технической поддержки, включающего индивидуализированный набор дополнительных услуг.



Внедрение

- Для знакомства с JMS доступна полнофункциональная версия на 1 месяц.
- Установка и настройка JMS максимально автоматизированы.
- Внедрение и сопровождение JMS могут осуществлять как авторизованные партнёры компании "Аладдин Р.Д.", так и представители самого разработчика.



Обучение

- В Учебном Центре "Информзащита" проводится учебный курс "Построение и эксплуатация инфраструктуры аутентификации на основе продуктов: электронные ключи JaCarta и система управления JaCarta Management System".
- Курс ориентирован на системных архитекторов, системных администраторов, администраторов информационной безопасности и специалистов служб технической поддержки.
- По результатам тестирования слушателям могут быть выданы сертификаты "Инженер по внедрению JMS" и "Специалист по эксплуатации JMS".



Дополнительные опции

- Поддержка технологии биометрической идентификации.
- Поддержка УЦ КриптоПро 1.5/2.0, ViPNet 4.6, Notary- PRO 2.7.
- Импорт данных пользователей из УЦ КриптоПро 1.5 или 2.0.
- Учёт СКЗИ.
- Поддержка токенов сторонних производителей.

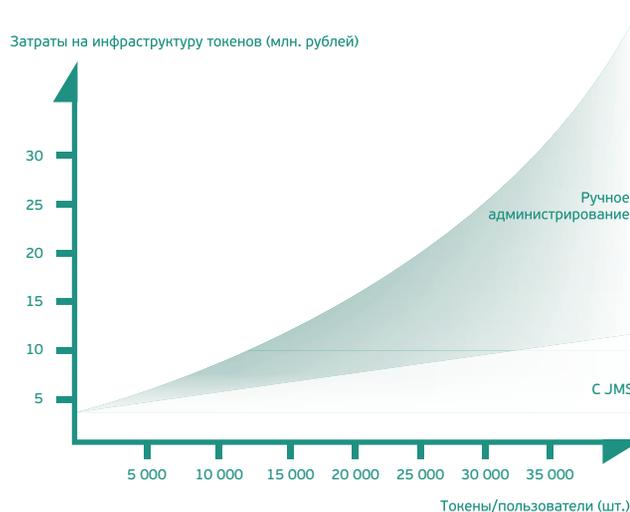
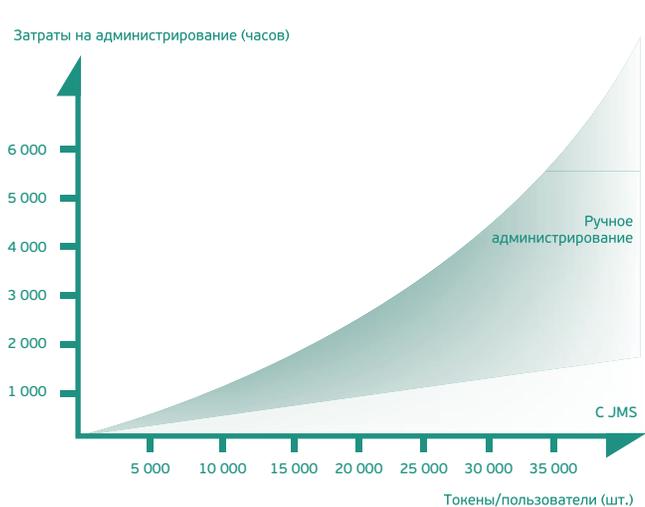
Экономический эффект от внедрения JMS

Благодаря своим возможностям JMS повышает качество и скорость работы ИТ- и ИБ-служб организации, сокращая временные и эксплуатационные затраты на внедрение и поддержку средств аутентификации и ЭП.

Ниже указано время выполнения наиболее частых операций по учёту и управлению токенами в ручном режиме и с использованием JMS, а также рассчитана экономия трудозатрат администратора ИБ после внедрения JMS.

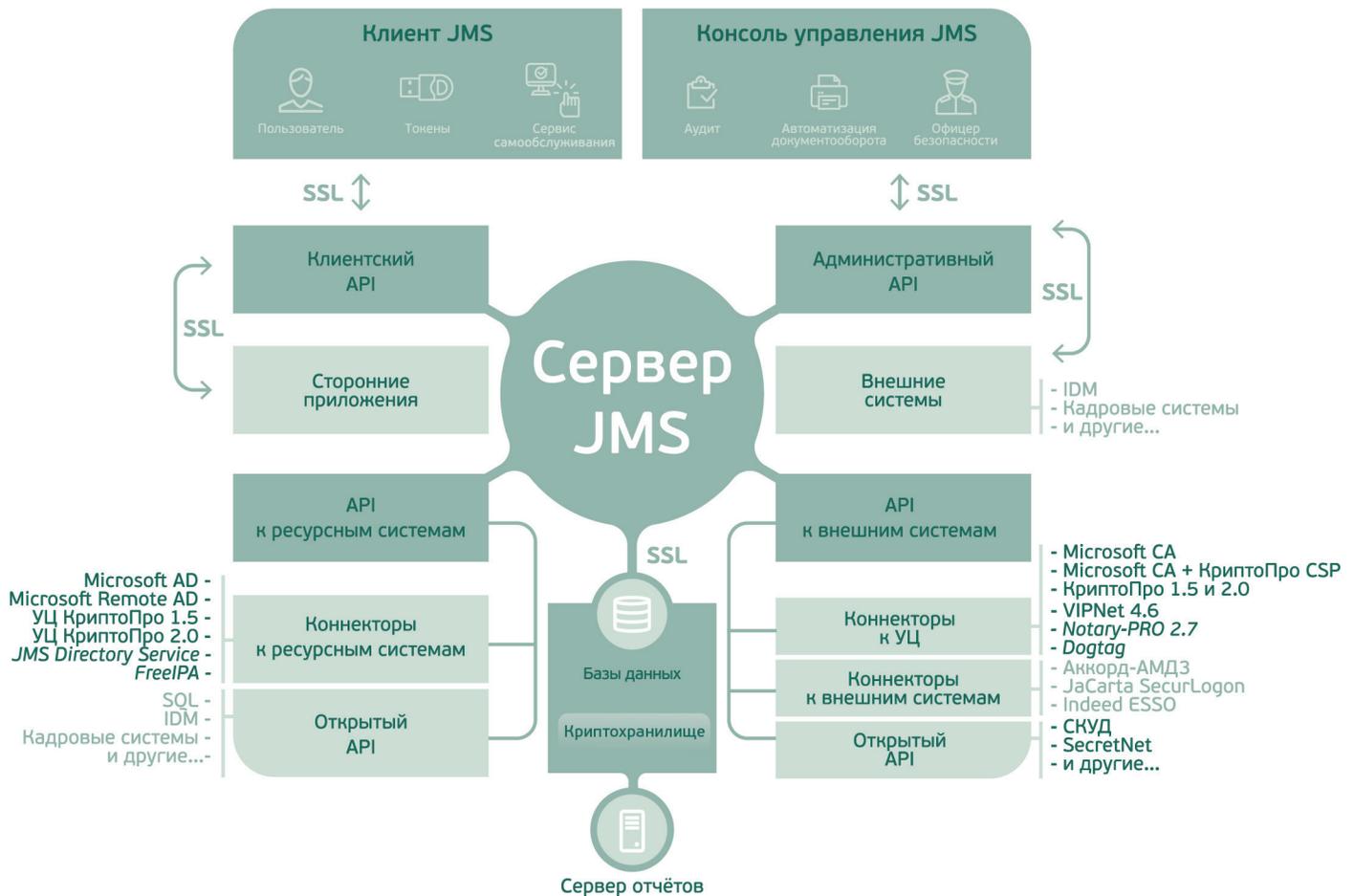
Операция	При использовании 100 токенов			При использовании 1000 токенов		
	Вручную	С JMS	Экономия времени	Вручную	С JMS	Экономия времени
Выпуск токена и 2 сертификатов (аутентификация + ЭП) одному сотруднику	2 мин.	1 мин.	в 2 раза	2 мин.	1 мин.	в 2 раза
Выпуск токена и 2 сертификатов (аутентификация + ЭП) всем сотрудникам компании	100 × 2 мин. = 3 ч. 20 мин.	5 мин.*	в 40 раз	1 000 × 2 мин. = 33 ч. 20 мин.	5 мин.*	в 400 раз
Отзыв токена и 2 сертификатов (аутентификация + ЭП) у одного сотрудника	2 мин.	30 сек.	в 4 раза	2 мин.	30 сек.	в 4 раза
Отзыв токена и 2 сертификатов (аутентификация + ЭП) у всех сотрудников компании	100 × 2 мин. = 3 ч. 20 мин.	5 мин.*	в 40 раз	1 000 × 2 мин. = 33 ч. 20 мин.	5 мин.*	в 400 раз
Выпуск дополнительного сертификата всем сотрудникам компании	100 × 1 мин. = 1 ч. 40 мин.	5 мин.*	в 20 раз	1 000 × 1 мин. = 16 ч. 40 мин.	5 мин.*	в 200 раз
Перевыпуск сертификатов всем сотрудникам компании при истечении срока службы	100 × 2 мин. = 3 ч. 20 мин.	2 мин.*	в 100 раз	1 000 × 2 мин. = 33 ч. 20 мин.	2 мин.*	в 1000 раз
Удалённая разблокировка PIN-кода токена	2 мин.	30 сек.	в 4 раза	2 мин.	30 сек.	в 4 раза
Средний эффект от внедрения JMS	Снижение в 10 раз			Снижение в 15 раз		

* При массовом обслуживании пользователей время администратора JMS тратится только на первоначальную настройку или изменение профилей выпуска токенов и сертификатов, а также привязку их к пользователям. Дальнейшая ручная работа не требуется, что экономит время администратора и снижает вероятность ошибок.



Для получения методики расчёта экономического эффекта от внедрения JMS обращайтесь к представителям компании "Аладдин Р.Д." или её партнёрам.

Архитектура



- **Сервер JMS** – ядро JMS, осуществляющее централизованное управление учётными записями пользователей, токенами, политиками и т. д. Может быть установлен в одном экземпляре или в составе кластера. Поддерживается виртуализация и резервное копирование закрытых ключей, баз данных и настроек системы.
- **База данных JMS** – обеспечивает централизованное хранение информации об учётных записях пользователей JMS, токенах, объектах, выпущенных на токенах, политиках, настройках JMS и т. д. Значимая информация хранится в Криптохранилище.
- **Криптохранилище** – виртуальный объект (область базы данных), где хранятся критически важные данные (закрытые ключи, PIN-коды и т. д.). Криптохранилище создаётся в процессе первоначальной настройки конфигурации JMS.
- **Консоль управления JMS** – консоль администратора, позволяющая регистрировать пользователей, выполнять операции с токенами пользователей, настраивать профили выпуска, создавать и редактировать глобальные группы JMS, выполнять планы обслуживания. Доступ к объектам и операциям в консоли управления определяется полномочиями конкретного администратора в соответствии с назначенной ему ролью.
- **Клиент JMS** – клиентский агент JMS на стороне пользователя, который выполняет функцию синхронизации содержимого токена с данными на сервере, а также позволяет пользователю выполнять ряд операций с токеном в рамках сервиса самообслуживания (выпуск, разблокировка, замена).
- **JMS Server API** – открытый API для разработки коннекторов к УЦ и ресурсным системам, собственного клиентского ПО, а также для интеграции с другими ИТ- и ИБ-системами предприятия.

Клиент JMS

- Полноценное приложение (по сравнению с конкурирующими решениями, использующими Web-интерфейс):
 - обеспечивается быстрая и бесперебойная работа за счёт функционирования в ОС Microsoft Windows;
 - не требуется снижения безопасности браузеров для работы с токенами (например, применяя ActiveX компоненты или плагины);
 - не нужно беспокоиться о совместимости приложения с новой версией браузера.
- Предоставляет пользователю удобный и интуитивно-понятный графический интерфейс.
- Доступно развёртывание с помощью групповых политик (Microsoft GPO).
- В рамках проекта доступна возможность использования клиента для Linux и других встраиваемых систем и решений (M2M, IoT).

Поддержка филиальной структуры

- Доступно закрепление пользователей, токенов и объектов на них за конкретным филиалом, что позволяет отслеживать перемещения токенов в филиальной сети.
- При низкой пропускной способности каналов между филиалами и головным офисом серверы JMS могут работать в автономном режиме с возможностью управления каждым из них из единой консоли.
- Встроенный механизм ролей и полномочий позволяет распределить обязанности по управлению серверами JMS между офицерами безопасности головного офиса и филиалов организации, а также делегировать права другим ИТ-специалистам.
- Поддержка консолидированных отчётов по группам филиалов или всей филиальной сети позволяет отслеживать состояние и использование всех имеющихся токенов.

Минимальная зависимость от Microsoft Active Directory (AD)

- Не требуется модифицировать и расширять схему AD, т.к. все необходимые данные копируются и хранятся в собственной базе данных JMS.
- В качестве источника информации о пользователях может применяться не только AD, но и внешние источники (УЦ, кадровые системы, базы данных Microsoft SQL Server, FreeIPA, JMS Directory Service (собственная база данных JMS) и т. д.).

Масштабируемость и отказоустойчивость

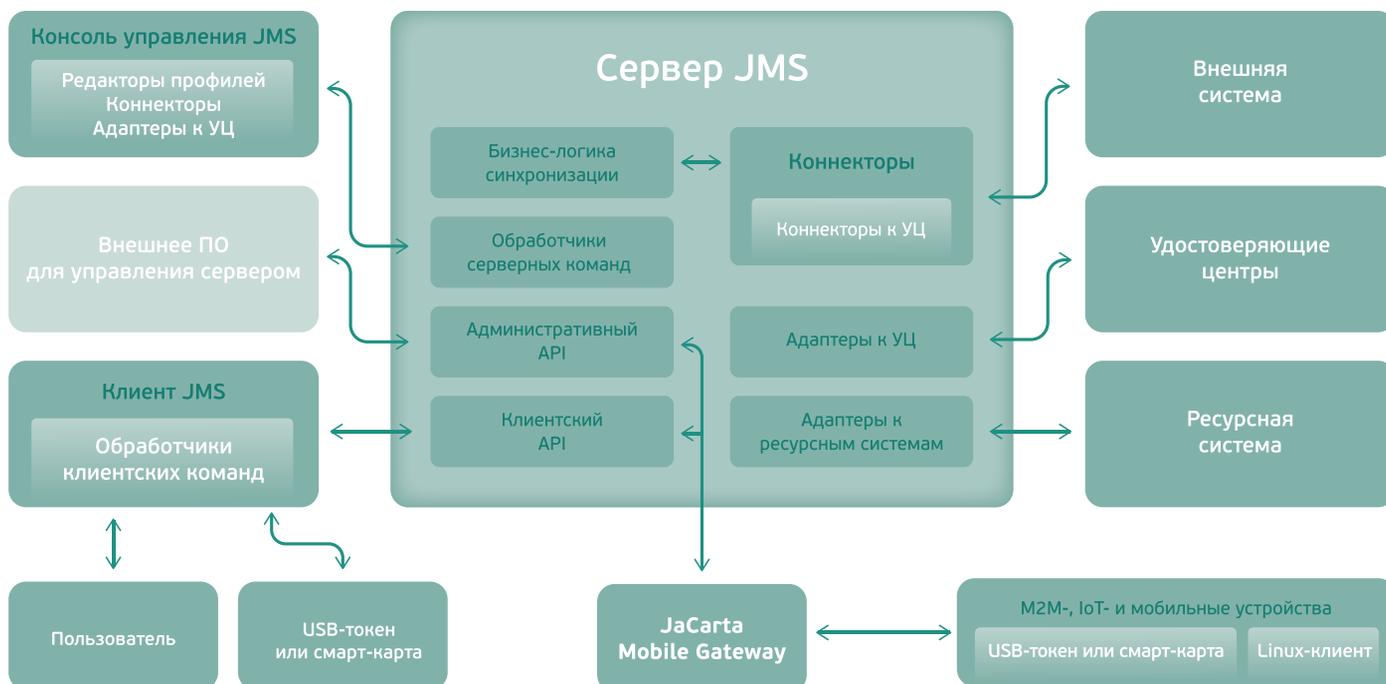
- Поддержка виртуализации (VMware ESX и ESXi, Microsoft Hyper-V).
- Поддержка распространённых балансировщиков нагрузки.
- Поддержка кластерных технологий (NLB), обеспечивающих:
 - балансировку нагрузки между серверами JMS при внедрении в крупных организациях;
 - отказоустойчивость серверов JMS, работающих с общей базой данных (начиная с версии Microsoft SQL Server Standard);
 - катастрофоустойчивость при разнесении серверов и баз данных JMS по разным площадкам (рекомендуется версия Microsoft SQL Server Enterprise с поддержкой функции AlwaysOn).

Безопасность и надёжность

- Каналы "Сервер JMS – Клиент JMS" и "Сервер JMS – Консоль управления JMS" шифруются с помощью HTTPS (SSL/TLS).
- Все значимые данные хранятся в Криптохранилище с доступом по цифровому сертификату.
- К пользователям и администраторам JMS применяется ролевая модель с делегированием полномочий.
- Реализован механизм принудительной смены PIN-кода пользователя.

Возможности расширения

JMS предоставляет открытый серверный API, обеспечивающий дополнительные возможности по расширению функциональности системы с помощью добавления новых модулей, разработки коннекторов к УЦ и ресурсным системам.



- Для интеграции JMS с внешней системой в сценариях, когда JMS является ведущей системой, необходимо разработать "коннектор". Коннектор к внешней системе позволяет в автоматическом режиме управлять данными, которые внешней системе требуется разместить на токене.
- Для интеграции JMS с новым типом УЦ необходимо разработать "адаптер к УЦ", который является расширением для встроенного в JMS коннектора – коннектора к УЦ. Коннектор к УЦ реализует общую логику работы с УЦ, а взаимодействие с конкретным типом УЦ коннектор осуществляет через адаптеры.
- Для интеграции JMS с внешней системой, которая будет являться источником учётных записей пользователей и рабочих станций, необходимо разработать адаптер к ресурсной системе.

Возможности масштабирования

В таблице указаны требования к оборудованию и ПО в зависимости от количества пользователей JMS.

Кол. пользователей	Узлы кластера	Сервер JMS				Сервер СУБД				Пропускная способность канала JMS – SQL Мбит/с	Редакция Microsoft SQL Server
		Процессор	ОЗУ	Диск	Процессор	ОЗУ	Диск				
		Ядра	ГГц	ГБ	Ядра	ГГц	ГБ				
<1 000	1	<4	3	4	<100	<4	3	<32	<200	<100	Express/Standard
1 000 – 10 000	2	4-24*	3	4-24*	~100	4-24	3	32–160	200	100-500	Standard
>10 000	2 и выше	>24*	3	>24*	>100	>24	3	>160	>200	>500	Enterprise

* указаны суммарные аппаратные требования на все узлы кластера

Примечания:

- Если предполагается развёртывание системы в нескольких географически удалённых филиалах, рекомендации из таблицы должны применяться для каждой инсталляции в соответствии с количеством пользователей в конкретном филиале.
- При любом варианте установки рекомендуется использовать отказоустойчивый сервер СУБД с файлом базы данных на сетевом хранилище.

Требования к специалистам по внедрению

Специалисты, занимающиеся внедрением JMS, должны удовлетворять следующим требованиям к квалификации:

- иметь базовые представления о PKI и её использовании в информационных системах масштаба предприятия;
- иметь навыки установки и настройки ПО в среде Microsoft Windows;
- иметь навыки администрирования локальных сетей на основе клиентских и серверных ОС Microsoft Windows и службы каталогов AD;
- понимать особенности реализации PKI на основе УЦ Microsoft CA, КриптоПро и др.;
- пройти учебный курс "Построение и эксплуатация инфраструктуры аутентификации на основе продуктов: электронные ключи JaCarta и система управления JMS" (желательно).

Сертификация



Сертификат ФСТЭК России № 3355 удостоверяет, что ПО JMS является программным средством управления средствами аутентификации, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей" (Гостехкомиссия России, 1999) – по 4 уровню контроля и технических условий.

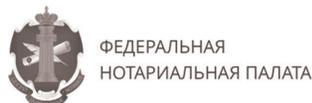
Сертификат позволяет использовать JMS для защиты информации в ИСПДн до 1 уровня включительно, в государственных информационных системах до 1 уровня защиты включительно, а также при создании автоматизированных систем до уровня защищённости 1Г включительно.

Технические характеристики

Параметр	Описание		
Системные требования к серверу JMS	ОС <ul style="list-style-type: none"> • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 	СУБД <ul style="list-style-type: none"> • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 • Microsoft SQL Server 2008 	
Системные требования к АРМ пользователей (Клиент JMS, Консоль управления JMS)	Microsoft <ul style="list-style-type: none"> • Microsoft Windows 10 • Microsoft Windows 8, 8.1 • Microsoft Windows 7 SP1 • Microsoft Windows Vista SP2 • Microsoft Windows XP SP3 (32-бит), SP2 (64-бит) • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2003 R2 SP2 • Microsoft Windows Server 2003 SP2 	Linux <ul style="list-style-type: none"> • Для M2M, IoT- и мобильных устройств (через JaCarta Mobile Gateway) 	
Модели поддерживаемых токенов	JaCarta <ul style="list-style-type: none"> • JaCarta-2 ГОСТ • JaCarta-2 PKI/ГОСТ • JaCarta-2 PKI/BIO/ГОСТ • JaCarta-2 PRO/ГОСТ • JaCarta LT • JaCarta PKI • JaCarta PKI/Flash • JaCarta PRO • JaCarta ГОСТ • JaCarta ГОСТ/Flash • JaCarta PKI/BIO • JaCarta PKI/ГОСТ • JaCarta PKI/ГОСТ/Flash • JaCarta PKI/BIO/ГОСТ • JaCarta PRO/ГОСТ • JaCarta CryptoPro (КриптоПро ФКН CSP) 	eToken <ul style="list-style-type: none"> • eToken 5110 • eToken 5105 • eToken 5100 • eToken 4100 • eToken ГОСТ • eToken PRO • eToken PRO (Java) • eToken PRO Anywhere • eToken NG-Flash (Java) • eToken NG-OTP (Java) без OTP-функциональности 	Рутокен <ul style="list-style-type: none"> • Рутокен ЭЦП 2.0 • Рутокен ЭЦП • Рутокен S • Рутокен Lite ESMART <ul style="list-style-type: none"> • ESMART Token • ESMART Token ГОСТ Другие <ul style="list-style-type: none"> – по запросу
Поддерживаемые УЦ	<ul style="list-style-type: none"> • Microsoft CA с КриптоПро CSP • Microsoft CA • КриптоПро 2.0 • КриптоПро 1.5 	<ul style="list-style-type: none"> • ViPNet 4.6 • Notary-PRO 2.7 • Dogtag 	
Поддерживаемые СКЗИ (функция "Учёт СКЗИ")	Любые программные и программно-аппаратные СКЗИ		
Базы учётных данных пользователей и рабочих станций	<ul style="list-style-type: none"> • Microsoft Active Directory • Microsoft Remote Active Directory • УЦ КриптоПро 2.0 • УЦ КриптоПро 1.5 • FreeIPA • Собственная база данных JMS Directory Service • Другие (за счёт разработки коннекторов, предоставляется SDK с примерами) 		
Масштабирование	<ul style="list-style-type: none"> • От 100 до 1 000 000 токенов (использование JMS для учёта и управления менее чем 100 токенами нецелесообразно) 		
Виртуализация	VMware <ul style="list-style-type: none"> - ESX - ESXi Microsoft Hyper-V		

Параметр	Описание
Отказоустойчивость и надёжность	<ul style="list-style-type: none"> • Поддержка кластерных технологий (NLB) • Резервное копирование настроек и базы данных системы • Резервное копирование закрытых ключей и сертификатов
Территориальные ограничения	Нет (ограничения есть только при использовании сертифицированных СКЗИ)
Необходимость наличия лицензий на распространение JMS	Нет (лицензия ФСБ России на распространение СКЗИ требуется при продаже токенов с поддержкой российской криптографии, например, JaCarta-2 ГОСТ, eToken ГОСТ, Рутокен ЭЦП)
Локализация (поддерживаемые языки)	<ul style="list-style-type: none"> • Русский (по умолчанию) • Английский • Другие (по запросу)
Возможность добавления других моделей токенов	Есть (по запросу)

Среди наших клиентов



Российская компания "Аладдин Р.Д." является признанным экспертом и лидером рынка средств строгой двухфакторной аутентификации пользователей в корпоративных ресурсах, на Web-порталах и в облачных сервисах. Многие продукты, решения и технологии компании занимают доминирующее положение на российском рынке и применяются лидерами ключевых отраслей экономики.

За более чем 20 лет работы практически каждый выводимый на рынок продукт компании заслуживал особого внимания и становился лидером в своём сегменте. Во многих коммерческих и государственных организациях продукты и решения компании "Аладдин Р.Д." фактически стали корпоративным стандартом.



+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 21.1.1.13537-2019 от 25.04.19

© 1995-2019, ЗАО "Аладдин Р.Д.". Все права защищены.