Аладдин

Новое в JMS

Обзор основных изменений
обновлённого продукта

JaCarta Management System
версии 3.7

aladdin.ru

JaCarta Management System — корпоративная система управления жизненным циклом средств аутентификации и электронной подписи с интегрированным производительным сервером усиленной аутентификации 2FA. Обновлённый продукт предоставляет пользователям ряд новых возможностей за счёт реализации новых и оптимизации привычных функций.

Интеграция с сервером аутентификации JaCarta Authentication Server (JAS)

Функциональность ранее автономного высокопроизводительного 2FA-сервера глубоко интегрирована в JMS 3.7, что выводит его на новый уровень и позволяет использовать в крупных Enterprise-инфраструктурах.

- Высокопроизводительный 2FA-сервер JAS в процессе аутентификации обеспечивает пользователям второй фактор защиты.
- Все привычные для администраторов JMS инструменты управления электронными ключами и сертификатами распространяются на OTP- и U2F-токены, программные аутентификаторы для мобильных устройств, а также SMS.
- В качестве OTP-токенов могут использоваться как популярные приложения для двухфакторной аутентификации (Яндекс.Ключ, Google Authenticator, Microsoft Authenticator), так и разработанное компанией "Аладдин Р.Д." - Aladdin 2FA. Использование мобильного приложения от "Аладдин Р.Д." решает проблему безопасной передачи секрета в процессе активации мобильного приложения.
- Серверы JMS и JAS используют единую базу данных (Microsoft SQL), что позволяет сократить издержки на администрирование и повысить удобство эксплуатации.
- В систему аудита продукта добавлен журнал событий аутентификации, регистрируемых сервером JAS.
- Поддержка стандартных протоколов и открытый API дают возможность интеграции JAS с популярными серверами доступа сторонних вендоров. Глубокая экспертиза и наработанный опыт взаимодействия с многочисленными программными и программно-аппаратными комплексами третьих изготовителей позволяет специалистам компании "Аладдин Р.Д." и партнёров встроить JAS практически в любую инфраструктуру.

Поддержка тонких клиентов на Linux, Windows и macOS

В состав обновлённого продукта включен компонент JMS Web Manager (JWM), реализующий сервис, который обеспечивает работу Web-клиента JMS в операционных системах семейств Linux, Windows и macOS.

Из коробки поддержаны токены и смарт-карты JaCarta PKI, JaCarta ГОСТ, JaCarta PKI/ГОСТ, JaCarta-2 PKI, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ.

Поддержка PostgreSQL

В качестве альтернативы по-прежнему поддерживаемой СУБД MS SQL новая версия JMS может использовать PostgreSQL.

Работа с Удостоверяющими центрами в режиме offline

Новая версия JMS позволяет в процессе выпуска сертификатов взаимодействовать с УЦ в режиме offline. Данный режим особенно актуален для УЦ, находящихся в изолированном защищённом сегменте сети.

Интеграция с "КриптоПро DSS"

JaCarta Management System поддерживает сервис "облачной" электронной подписи "КриптоПро DSS". Администратору из консоли JMS доступна возможность настройки и управления пользовательскими профилями DSS. JMS обеспечивает автоматизацию всех сценариев, обычно выполняемых оператором "КриптоПро DSS" вручную, и тем самым значительно сокращает объём рутинных работ.

В процессе автоматизации работы с ключевыми контейнерами, сертификатами и другими информационными объектами системы "КриптоПро DSS" в JMS задействованы те же механизмы, что и в работе с физическими носителями (USB-токенами и смарт-картами). Выпуск сертификатов для пользователей возможен как на Удостоверяющем центре "КриптоПро УЦ 2.0", подключенном к DSS, так и с помощью стороннего УЦ.

Поддержка КриптоПро CSP 5.0

Список поддерживаемых криптопровайдеров пополнился новой версией КриптоПро CSP 5.0. Важной особенностью работы с данным криптопровайдером является возможность генерирования с его помощью неизвлекаемых ключей внутри токена JaCarta-2 ГОСТ.

Возможности JMS по поэкземплярному учёту СКЗИ распространяются на данный криптопровайдер и обеспечивают соответствие требованиям ФСБ России.

Интеграция с SIEM-системами

JaCarta Management System 3.7 предоставляет возможность выгрузки регистрируемых в системе событий на Syslog-сервер. Можно выгружать события, генерируемые как JMS, так и JAS. В зависимости от категории и важности событиям присваивается степень критичности (статус). Благодаря детальной классификации событий администратор имеет возможность фильтровать для выгрузки только события из интересующих его категорий. Существуют следующие статусы событий:

- "Информационные";
- "Предупреждения";
- "Ошибки";
- "Критические ошибки".

Обновлённая схема лицензирования

Продукт JMS доступен в двух вариантах, определяемых типом лицензии.

JMS Enterprise Edition

- Лицензия соответствует типовой конфигурации продукта, обеспечивающей автоматизацию администрирования средств аутентификации и ЭП для организаций масштаба предприятия.
- Ориентирована на корпоративных пользователей, для которых важно обеспечить максимальную автоматизацию жизненного цикла как сертификатов, так и электронных ключей – носителей данных сертификатов. В качестве носителей сертификатов могут выступать также рабочие станции (случай выпуска сертификата в личное хранилище пользователя).
- Стоимость лицензии определяется числом пользователей, использующих один или более носитель.

JMS CA Edition

- Лицензия соответствует специальной конфигурации продукта, предназначенной для предприятий, использующих JMS для выпуска большого числа электронных ключей и сертификатов без необходимости их администрирования на протяжении всего жизненного цикла. Примером подобных предприятий могут служить Удостоверяющие центры или организации, использующие системы ДБО.
- Стоимость лицензии фиксирована для определённого периода использования продукта и не зависит от числа пользователей, использующих один или более носитель.

Лицензия JMS Enterprise Edition может как не иметь ограничений по сроку действия, так и быть ограниченной одним годом. В первом случае для получения технической поддержки и бесплатного обновления версий потребуется регулярно приобретать техническую поддержку. Во втором – новую лицензию придётся приобретать для обеспечения функционирования продукта. Стоимость технической поддержки включена.

Лицензия JMS CA Edition всегда ограничена одним годом.

Новые возможности для Удостоверяющих центров

Начиная с версии 3.7, JMS предоставляет Удостоверяющим центрам и другим организациям, выпускающим большое количество сертификатов на электронные ключи без необходимости дальнейшего управления жизненным циклом последних, следующие дополнительные возможности:

- собственная ресурсная система JMS (JMS Directory Service – JDS) для кастомизации шаблонов выпускаемых сертификатов;
- реализация "из коробки" специфичных для УЦ сценариев выпуска электронных ключей;
- автоматизация выпуска сертификатов в режиме offline для аккредитованных УЦ, находящихся в изолированных защищённых сегментах сети;
- облегчённая версия интерфейса, упрощённая процедура конфигурирования;
- расширенные возможности подсистемы печати заявок, актов, сертификатов.

Возможности работы с ресурсными системами

Отключение ресурсных систем

Реализована возможность отключения дополнительных ресурсных систем, работающих совместно с основной (Active Directory).

Разделение связанных ресурсных систем

При одновременном использовании нескольких ресурсных систем (например, Active Directory и КриптоПро УЦ) JMS позволяет связать данные из их учётных записей в одну по общему атрибуту (e-mail, табельный номер и др.), имеющемуся в обеих базах данных. Начиная с версии 3.7, в JMS появилась возможность выполнения обратной операции – после проведения необходимых настроек с объединёнными учётными записями, они вновь могут быть разделены.

Поддержка смарт-карт ридеров линейки JCR

JMS автоматически определяет подключенные смарт-карт ридеры производства компании "Аладдин Р.Д." и предоставляет возможности автоматизации их учёта. Зарегистрированное устройство может быть закреплено за сотрудником. Все ридеры учитываются и отображаются на отдельном экране консоли управления JMS с удобными механизмами поиска, фильтрации и сортировки.

Повышение удобства использования продукта

Новая версия JMS стала существенно удобнее в использовании. Ниже представлен краткий перечень улучшений и новых возможностей.

- Проверка сертификатов, используемых для подписи запросов и подключения к УЦ, на актуальность по спискам отзыва.
- Настройка для сервера JAS принудительной доменной аутентификации с помощью NPS-плагина. Имя домена можно указать в настройках NPS-плагина, при аутентификации оно подставляется автоматически, и пользователю в таком случае достаточно ввести только свой логин и пароль.
- Возможность выбора в процессе настройки параметров аутентификации формата имени пользователя из UPN- или FQDN-форматов.
- Копирование профиля с возможностью редактирования полей освобождает администратора от необходимости создавать в каждой из групп профили с нуля и заново прописывать все настройки и политики.
- Поиск по профилям в консоли управления JMS. Функция особенно полезна в организациях, где для работы необходимо создавать большое число профилей, например, в Удостоверяющих центрах.
- Отказ от создания аутентификатора при выпуске ключевого носителя (прежде создавался всегда). Организациям, не использующим внутреннюю аутентификацию JMS по ключевому носителю, это позволяет сократить время на выпуск токена и сэкономить место на нём.
- Добавление других типов приложений для токена в созданные ранее профили.
- Скрытие неиспользуемых администратором элементов интерфейса в Консоли управления JMS. Эта функция позволяет существенно разгрузить упомянутый выше интерфейс.

Оптимизация работы и повышение производительности системы

Для администратора реализована функция "Ограничение типов клиентских событий". Она позволяет администратору выбирать из разнообразных типов событий, генерируемых JMS-клиентом, только те, которые нужно сохранить в журналах JMS и, соответственно, базе данных. Прочие события игнорируются, тем самым предотвращая разрастание БД и замедление скорости работы системы.

Общая оптимизация работы с токенами позволяет выпускать их намного быстрее, чем в предыдущих версиях JMS. Для ряда популярных моделей токенов скорость выпуска повысилась более чем в 2 раза.