Аладдин РД

JaCarta PKI

Смарт-карты, USB- и MicroUSB-токены
для строгой аутентификации
в корпоративных системах

"Не решив задач надёжной идентификации и аутентификации пользователя, не дав ему удобных и надёжных средств, обеспечивающих юридическую значимость его действий в Сети, эффективно работать, взаимодействовать, развиваться в современном электронном мире уже просто нельзя.

Наши технологии и линейка продуктов JaCarta помогут быть собой в электронном мире".

Сергей Груздев,
генеральный директор "Аладдин Р.Д."

Аутентификация

Что необходимо для надёжной (строгой) аутентификации?

Применение инфраструктуры открытых ключей

Для обеспечения строгой аутентификации нужно использовать криптографию и инфраструктуру открытых ключей (PKI). Другие методы и технологии способны обеспечить лишь простую или усиленную аутентификацию.

Минимум два фактора аутентификации

Первый фактор — обладание физическим USB-токеном или смарт-картой (далее — токеном), второй фактор — знание PIN-кода для выполнения криптографических операций внутри токена, необходимых для аутентификации.

Неотчуждаемость токена от его владельца

При доступе к критически важной информации рекомендуется использовать третий фактор аутентификации — биометрическую идентификацию владельца токена, подтверждающую факт присутствия владельца в момент аутентификации и делающую невозможным использование токена без его владельца.

Для топ-менеджеров и руководителей биометрическая идентификация может использоваться вместо PIN-кода (как второй фактор).

Подтверждённая невозможность клонирования токена

Если средство аутентификации выполнено на микроконтроллере общего назначения, эмулирует функциональность смарт-карты, не имеет специальных встроенных средств защиты от клонирования, взлома и других специальных атак, не имеет международных сертификатов безопасности, значит оно подвержено серьёзным рискам информационной безопасности. Следовательно, этим рискам подвержена и вся корпоративная информационная система, так как она безопасна настолько, насколько безопасно её самое слабое звено.

JaCarta PKI — семейство надёжных устройств для строгой двух- или трёхфакторной аутентификации

Компания "Аладдин Р.Д." предлагает надёжные и недорогие устройства для обеспечения строгой двух- или трёхфакторной аутентификации — токены семейства JaCarta PKI.

Все модели линейки JaCarta PKI выполнены на смарт-карточном защищённом микроконтроллере "Secure by design" (сконструирован как безопасный, для целей обеспечения безопасности) и поддерживаются в продуктах мировых вендоров штатными средствами.

Токены JaCarta PKI прошли сертификацию в международных лабораториях. Полученные сертификаты удостоверяют, что используемые в них микроконтроллеры и операционная система соответствуют профилям безопасности Security IC Platform Protection Profile и Java Card™ System Protection Profile (достигнутый уровень доверия — EAL 5+).

Назначение

Токены семейства JaCarta PKI предназначены для строгой двухфакторной аутентификации в корпоративных системах, Web-приложениях и облачных сервисах, а также безопасного хранения ключей, ключевых контейнеров криптопровайдеров и средств криптографической защиты информации (СКЗИ), профилей и паролей пользователей. Предназначены для использования совместно с PKI.

Токены семейства JaCarta PKI являются недорогими, простыми, надёжными и удобными в использовании устройствами, ориентированными на применение как в массовых проектах для физических лиц (B2C/G2C), так и для корпоративных пользователей (B2B/G2B). Они могут использоваться не только с персональными компьютерами, работающими под управлением Microsoft Windows, Linux или Apple macOS, но и с мобильными устройствами — планшетами и смартфонами на базе Apple iOS, Google Android и Microsoft Windows.

Решаемые задачи

- Безопасный доступ пользователей в корпоративные системы, Web-приложения, сайты и облачные сервисы.
- Хранение ключевых контейнеров криптопровайдеров и программных СКЗИ (КриптоПро CSP, ViPNet CSP и др.) для обеспечения юридической значимости действий пользователей.
- Хранение пользовательских данных (сертификаты, пароли, коды доступа, настройки и пр.) в защищённой PIN-кодом памяти токена.

Комбинированные модели

Помимо основной модели — JaCarta PKI, — Заказчикам также доступны комбинированные токены, сочетающие в себе несколько функций:

- JaCarta-2 PKI/ГОСТ и JaCarta PKI/ГОСТ — для работы с электронной подписью (ЭП), строгой двухфакторной аутентификации и безопасного хранения ключевых контейнеров;
- JaCarta PKI/BIO — для строгой двух- или трёхфакторной аутентификации с применением биометрической идентификации пользователя (по отпечатку пальцев) и безопасного хранения ключевых контейнеров;
- JaCarta-2 PKI/BIO/ГОСТ и JaCarta PKI/BIO/ГОСТ — для работы с ЭП, строгой двух- или трёхфакторной аутентификации с применением биометрической идентификации пользователя (по отпечатку пальцев) и безопасного хранения ключевых контейнеров.

Сертификаты

Токены JaCarta PKI имеют сертификаты соответствия ФСТЭК России № 3449 и ФСТЭК России № 2799, которые подтверждают, что они вместе с ПО "Единый клиент JaCarta" и сопутствующим клиентским ПО являются средством аутентификации и безопасного хранения пользовательских данных и могут применяться для защиты информации в информационных системах персональных данных (ИСПДн) до 1 уровня защищённости включительно и при создании автоматизированных информационных систем (ИС) до класса защищённости 1Г включительно.

Комбинированные модели, имеющие функциональность для работы с ЭП, также сертифицированы ФСБ России как СКЗИ и средство ЭП класса КС1 и КС2 (сертификаты соответствия № СФ/124-3112 для моделей JaCarta-2 ГОСТ и № СФ/111-2750 для моделей JaCarta ГОСТ).

Токены JaCarta PKI являются безопасным устройством класса Qualified Signature Creation Device и полностью соответствуют международным требованиям к устройствам для создания ЭП ("Положение и регламент электронной идентификации и доверенных служб для электронных транзакций на внутреннем рынке ЕС № 910/2014").

В линейке токенов JaCarta ГОСТ реализованы криптографические алгоритмы ГОСТ 28147-89, ГОСТ Р 34.10-2001 и ГОСТ 34.11-94. В JaCarta-2 ГОСТ к указанным выше криптографическим алгоритмам добавлены новые алгоритмы — ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

Варианты исполнения

USB-токены в корпусах XL и Nano

- **Для строгой двух- или трёхфакторной аутентификации** в корпоративной сети и получения доступа к информационным ресурсам предприятия.
- **Для безопасного хранения пользовательских данных** (сертификаты, пароли, коды доступа, настройки и т.д.).
- **Для хранения ключевых контейнеров** криптопровайдеров и программных СКЗИ с целью обеспечения юридической значимости действий пользователя (для работы с СЭД, ДБО и т.д.).
- **Для прохода на территорию предприятия** по встроенной RFID-метке (только для токенов в корпусе XL).

MicroUSB-токены

- **Для пользователей мобильных устройств** под управлением ОС Google Android, Microsoft Windows и Linux (смартфоны, планшеты, терминальное оборудование и др.).
- **Для строгой двухфакторной аутентификации** в корпоративной сети и получения доступа к информационным ресурсам предприятия.
- **Для безопасного хранения пользовательских данных** (сертификаты, коды доступа, настройки и т.д.).
- **Для хранения ключевых контейнеров** криптопровайдеров и программных СКЗИ с целью обеспечения юридической значимости действий пользователя (для работы с СЭД, ДБО и т.д.).

Смарт-карты

- **Для строгой двух- или трёхфакторной аутентификации** в корпоративной сети и получения доступа к информационным ресурсам предприятия.
- **Для безопасного хранения пользовательских данных** (сертификаты, пароли, коды доступа, настройки и т.д.).
- **Для хранения ключевых контейнеров** криптопровайдеров и программных СКЗИ с целью обеспечения юридической значимости действий пользователя (для работы с СЭД, ДБО и т.д.).

- **Для визуальной идентификации сотрудников** (возможно нанесение на поверхность карты фотографии сотрудника, ФИО, должности и других данных).
- **Для прохода на территорию предприятия** (по встроенным RFID-меткам) или льготного (предоплаченного) проезда сотрудников на городском транспорте (метро, автобусы, трамваи и т.д.).
- **Для получения заработной платы** на карту и оплаты товаров и услуг с помощью платёжных систем MasterCard, VISA или "Мир".

Модули смарт-карт

- **Для межмашинного взаимодействия** (M2M) и встраиваемых решений, где требуется аутентификация при передаче данных (для использования в качестве встраиваемого модуля безопасности).
- **Для производителей карт и Персобюро.**

Выбор модели из семейства JaCarta PKI

	JaCarta PKI			JaCarta PKI/BIO		JaCarta-2 PKI/ГОСТ и JaCarta PKI/ГОСТ			JaCarta-2 PKI/BIO/ ГОСТ и JaCarta PKI/BIO/ГОСТ	
	USB	MUSB	Smart Card	USB	Smart Card	USB	MUSB	Smart Card	USB	Smart Card
Строгая аутентификация	●	●	●	●	●	●	●	●	●	●
Усиленная аутентификация*	○	○	○	○	○	○	○	○	○	○
Биометрическая идентификация				□	●				□	●
Хранение ключевых контейнеров	●	●	●	●	●	●	●	●	●	●
Средство ЭП						●	●	●	●	●
Работа с мобильными устройствами		●	●		●		●	●		●
Встраивание RFID-метки	○		○	○	○	○		○	○	○
Визуальная кастомизация	○	○	○	○	○	○	○	○	○	○

* — При использовании лицензии JaCarta SecurLogon

● — Базовая функциональность ○ — Дополнительная функциональность (доступна за дополнительную плату)

□ — Функциональность, реализуемая в рамках проекта (требует предварительного согласования)

Нам доверяют

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.

Продукты, решения и технологии компании занимают доминирующее положение на российском рынке. Во многих компаниях, банках и Федеральных структурах продукты и решения компании "Аладдин Р.Д." стали стандартом де-факто.

Преимущества

Безопасность

- Токены JaCarta PKI выполнены на специализированном микроконтроллере, что позволяет обеспечить защиту от клонирования, взлома, физических, логических, статистических, переборных и стрессовых атак, атак с использованием специальных зондов и т.д.
- Аппаратная реализация криптоалгоритмов позволяет исключить риск компрометации закрытого ключа вредоносными программами или злоумышленниками, так как он формируется и хранится внутри токена.
- Все модели токенов JaCarta PKI прошли тестирование в ведущих мировых лабораториях и разрешены для использования в международных платёжных системах VISA и MasterCard, а также Национальной системе платёжных карт "Мир".
- Токены JaCarta PKI не оказывают влияния на работу электронного оборудования, чувствительного к электромагнитным излучениям и помехам (например, медицинского), а также сами имеют повышенную защищённость от воздействия электромагнитных излучений и помех.

Удобный графический интерфейс

Для работы с различными моделями токенов JaCarta PKI достаточно установить Единый Клиент JaCarta, объединяющий в себе всё необходимое для их настройки. Также поддерживается работа с токенами eToken PRO, eToken PRO (Java) и eToken ГОСТ. Для продвинутых пользователей и администраторов доступен расширенный режим интерфейса.

Гибкая лицензионная и ценовая политика

В линейку токенов JaCarta PKI входит большое количество моделей, которые могут одновременно сочетать в себе до четырёх функций (двух- и трёхфакторная аутентификация, ЭП, хранение данных). При приобретении токенов Заказчик может выбрать и оплатить только те функции, которые ему действительно нужны. Это позволяет подобрать оптимальное предложение с точки зрения функциональности, стоимости и удобства использования.

Совместимость с популярными криптопровайдерами и программными СКЗИ

Все модели JaCarta поддерживают хранение ключевых контейнеров распространённых криптопровайдеров и программных СКЗИ (КриптоПро CSP, ViPNet CSP и др.), что обеспечивает совместимость с существующей инсталляционной базой программных СКЗИ.

Быстрое внедрение

Внедрение токенов JaCarta PKI не требует дополнительных усилий и работ по интеграции, так как они штатно поддерживаются в любой существующей PKI и имеют более 150 сертификатов совместимости с программными продуктами отечественных и зарубежных вендоров.

Электронная подпись с любых устройств

При использовании сертифицированных криптоконтейнеров программных СКЗИ или при применении комбинированных моделей JaCarta PKI/ГОСТ пользователь может удалённо работать с ЭП на разных устройствах: десктопе, ноутбуке, планшете или смартфоне (на базе Apple iOS или Google Android). Это позволяет обеспечить постоянную доступность работы с ЭП на внешних Web-порталах (например, на Портале государственных услуг), в системах ДБО, системах сдачи электронной отчётности, в "облачных" и других электронных сервисах.

Соответствие международным стандартам

Токены JaCarta PKI прошли сертификацию в международных лабораториях. Полученные сертификаты допускают ввоз и эксплуатацию этих токенов на территории стран-членов ЕС (RoHS, CE, FCC), а также удостоверяют, что используемые в них микроконтроллеры и операционная система соответствуют профилям безопасности Security IC Platform Protection Profile и Java Card™ System Protection Profile (достигнутый уровень доверия — EAL 5+).

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 (JaCarta Management System). В результате 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 PKI и ЭП;
- гарантированную совместимость продуктов и надёжность их работы;
- быстрый выпуск обновлений и поддержку всех моделей токенов JaCarta;
- возможность участвовать в разработке JMS и токенов JaCarta, предлагая реализацию новых функций.

Кастомизация

"Аладдин Р.Д." может адаптировать токены JaCarta PKI к потребностям Заказчиков. Внешний вид изделий кастомизируется путём нанесения логотипа, изменения цвета корпуса, колпачка, брелока и т.д. В некоторые модели токенов может быть имплантирована радиочастотная метка (RFID), используемая в системах контроля и управления доступом, учёта рабочего времени и т.д.

Дополнительные опции

JaCarta SecurLogon® — двухфакторная аутентификация без развёртывания инфраструктуры открытых ключей

JaCarta SecurLogon® —программно-аппаратное решение, позволяющее осуществить простой и быстрый переход от обычных паролей к двухфакторной аутентификации при входе в ОС Microsoft Windows или доступе к сетевым ресурсам за счёт использования токенов JaCarta.

Вместо сертификатов JaCarta SecurLogon генерирует сложные пароли (до 63-х символов), которые записываются на токен, поэтому для его работы не требуется разворачивать Active Directory или создавать собственный Удостоверяющий центр. Всё что нужно — приобрести токены JaCarta, установить на рабочие места Единый Клиент JaCarta и активировать в нём JaCarta SecurLogon.

Если в памяти токена имеется сертификат пользователя и соответствующий закрытый ключ, JaCarta SecurLogon может работать и с PKI, позволяя использовать их для входа в домен Microsoft Windows или сетевой ресурс вместо логина и пароля. В результате можно обеспечить плавный переход от парольной аутентификации к строгой двухфакторной аутентификации с использованием цифровых сертификатов.

Вход в систему или сервис осуществляется после ввода PIN-кода. Так как пользователь не знает настоящий пароль, он не может записать и скомпрометировать его. Поддержка биометрической идентификации позволяет заменить ввод PIN-кода на сканирование отпечатка пальца.

Решение JaCarta SecurLogon сертифицировано ФСТЭК России по 4 уровню контроля недекларированных возможностей (сертификат № 3575).

JaCarta Management System — централизованное управление жизненным циклом токенов

JaCarta Management System (JMS) — специализированная система управления жизненным циклом токенов JaCarta, eToken и др. Применение JMS позволяет автоматизировать типовые операции при работе с токенами разных производителей, обеспечить гибкую настройку политик использования токенов, а также даёт возможность централизованно управлять доступом к корпоративным системам.

Встроенные средства построения отчётов и печати документов позволяют отслеживать состояние инфраструктуры токенов и максимально автоматизировать документооборот, связанный с их жизненным циклом. Отличительной особенностью JMS является автоматический учёт СКЗИ и ключевых документов, а также автоматическое формирование нормативной документации по каждому событию, связанному с их учётом.

JMS — первая система управления жизненным циклом токенов, включенная в Единый реестр отечественного ПО (№ 311) и рекомендуемая к закупкам государственными и муниципальными органами власти (при наличии отечественного решения государственные структуры не могут приобретать аналогичное по функциям импортное ПО).

JMS сертифицирована ФСТЭК России по 4 уровню контроля отсутствия недекларированных возможностей (сертификат № 3355).

JC-WebClient — строгая аутентификация и электронная подпись для Web-приложений и облачных сервисов

JC-WebClient — единая технология работы с токенами JaCarta в Web-приложениях и облачных сервисах. Применение JC-WebClient позволяет легко реализовать:

- строгую двухфакторную взаимную аутентификацию пользователя и Web-сервера;
- формирование и проверку усиленной квалифицированной ЭП с использованием российских криптоалгоритмов;
- формирование и проверку усиленной ЭП с использованием западных криптоалгоритмов;
- шифрование данных, передаваемых между клиентским ПК и Web-сервером.

JC-WebClient работает со всеми популярными браузерами на всех платформах (Microsoft Windows, Apple macOS, Linux) и устанавливается при первом посещении защищаемого Web-ресурса, далее не требует каких-либо действий пользователя.

Для встраивания предлагается комплект разработчика JC-WebClient v. 3 SDK, который включает в себя подробное руководство и исчерпывающий перечень примеров с исходными кодами.

JC-Mobile — строгая аутентификация и электронная подпись для пользователей мобильных приложений

JC-Mobile — решение, позволяющее организовать безопасный доступ сотрудников, партнёров и клиентов к сервисам организации с мобильных устройств, обеспечить юридическую значимость подписываемых электронных документов и производимых операций, а также гарантировать безопасное хранение ключей и цифровых сертификатов на отчуждаемом модуле безопасности (смарт-карте или MicroUSB-токене).

JC-Mobile поддерживает мобильные устройства на базе Apple iOS, Google Android и Microsoft Windows. Кроме этого, токены JaCarta в составе решения можно подключать к десктопам и ноутбукам на базе Microsoft Windows, Apple macOS или Linux через специальные адаптеры или смарт-карт ридеры.

Apple iOS

Для применения смарт-карт JaCarta PKI с мобильными устройствами на базе Apple iOS достаточно приобрести специализированный смарт-карт ридер с разъёмом 30-pin или Lightning (Jailbreak не нужен!) , либо беспроводной смарт-карт ридер.

Google Android

JaCarta, выполненная в виде MicroUSB-токена, делает возможным использование сертифицированной российской криптографии на мобильных платформах на базе Google Android (если они имеют MicroUSB-разъём). Для этой цели также можно использовать смарт-карты JaCarta (с помощью беспроводного смарт-карт ридера с подключением по Bluetooth-интерфейсу).

Технические характеристики

Параметр	Описание
Микроконтроллер	Защищённый смарт-карточный чип, имеющий специальную сертифицированную защиту и на аппаратном, и на программном уровнях (Secure by design), что позволяет успешно противостоять всем известным угрозам безопасности, методам взлома и клонирования
Размер EEPROM-памяти на чипе	80 Кбайт (114 Кбайт по отдельному запросу)
Поддерживаемые операционные системы	**Microsoft** • Microsoft Windows 10 • Microsoft Windows 8.1 • Microsoft Windows 8 • Microsoft Windows 7 SP1 • Microsoft Windows Vista SP2 • Microsoft Windows XP SP3 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2003 SP2 **Linux** **Apple macOS/OS X** **Apple iOS** **Google Android**
Поддерживаемые криптографические алгоритмы	• AES (длины ключей 128, 192, 256 бит) • DES (длина ключа 56 бит) • 3DES (длины ключей 112 и 168 бит) • RSA (длины ключей 512, 1024, 2048) • криптография на эллиптических кривых (длины ключей 160, 192 бит) • аппаратная генерация ключей для RSA и криптографии на эллиптических кривых • алгоритмы согласования ключей: алгоритм Диффи-Хеллмана, алгоритм Диффи-Хеллмана на эллиптических кривых • функции хэширования: SHA-1, SHA-224 (эллиптические кривые), SHA-256, SHA-384, SHA-512 • генератор последовательностей случайных чисел
Доступные программные интерфейсы	**Для функциональности PKI** • Microsoft Windows — APDU, PKCS #11, MS CAPI (CSP, CNG) • Linux — APDU, PKCS #11 • Linux ARM — APDU, PKCS #11 • Apple macOS — APDU, PKCS #11 • Apple iOS — APDU, PKCS #11 (JC-Mobile) • Google Android — APDU, PKCS #11 (JC-Mobile) **Для функциональности BIO** • Microsoft Windows — PKCS #11 **Для функциональности ГОСТ (СКЗИ "Криптотокен ЭП")** • Microsoft Windows — APDU, PKCS #11, Криптотокен ЭП[1], JavaScript (JC-WebClient) • Linux — APDU, PKCS #11, Криптотокен ЭП, JavaScript (JC-WebClient) • Linux ARM — APDU, PKCS #11 • Apple macOS — APDU, PKCS #11, JavaScript (JC-WebClient) • Apple iOS — APDU, PKCS #11 (JC-Mobile) • Google Android — APDU, PKCS #11 (JC-Mobile) **Для функциональности ГОСТ (СКЗИ "Криптотокен 2 ЭП")** • Microsoft Windows — Интерфейсная криптобиблиотека[2] (APDU), PKCS #11 • Linux — Интерфейсная криптобиблиотека (APDU), PKCS #11 • Apple macOS — Интерфейсная криптобиблиотека (APDU), PKCS #11

[1] Сертифицированный программный интерфейс для визуализации подписываемого документа в соответствии с требованиями Статьи 12 63-ФЗ при применении JaCarta ГОСТ.

[2] Сертифицированный программный интерфейс для работы с устройствами JaCarta-2 ГОСТ.

Параметр	Описание
Аппаратные интерфейсы	Для USB-токенов: USB 2.0 Full speed (12 Мбит/с), разъём USB Type A Для смарт-карт: ISO 7816-3: • T=0 (для опции EMV-совместимость); • T=1 (используется по умолчанию). Для MicroUSB-токенов: Разъёмы Micro-B или Micro-AB. Подключение к ПК через адаптер MicroUSB-to-USB 2.0 Fullspeed (12 Мбит/с)
Совместимость с программными СКЗИ	Подтверждённая совместимость с существующей инсталляционной базой программных СКЗИ. Все модели JaCarta PKI поддерживают хранение ключевых контейнеров криптопровайдеров и программных СКЗИ (например, КриптоПро CSP)
CCID-совместимость	Установка драйвера устройства для современных ОС (Microsoft Windows Vista и выше, Linux, Apple macOS) не требуется
Возможность встраивания радиометки (RFID)	Есть (только для смарт-карт и USB-токенов в корпусе XL)
Пыле- и влагозащищённость	Есть у USB-токенов в корпусе XL и Nano (степень защиты IP56)
Необходимость наличия лицензий на распространение шифросредств	Есть для моделей JaCarta-2 PKI/ГОСТ, JaCarta-2 PKI/BIO/ГОСТ, JaCarta PKI/ГОСТ и JaCarta PKI/BIO/ГОСТ, так как в их составе используются сертифицированные СКЗИ (при их распространении требуется лицензия ФСБ России на распространение СКЗИ)
Сертификация	**Сертификаты соответствия ФСТЭК России № 3449 и ФСТЭК России № 2799** подтверждают, что токены семейства JaCarta вместе с ПО "Единый клиент JaCarta" и сопутствующим клиентским ПО являются средством аутентификации и безопасного хранения пользовательских данных и соответствуют требованиям по 4 уровню контроля недекларированных возможностей (НДВ 4) и требованиям Технических условий. **Сертификат ФСТЭК России № 3575** подтверждает, что JaCarta SecurLogon является программно-техническим средством защиты от несанкционированного доступа к информации и соответствует требованиям по 4 уровню контроля недекларированных возможностей (НДВ 4) и требованиям Технических условий. **Сертификат ФСТЭК № 3355** подтверждает, что ПО JaCarta Management System является программным средством управления средствами аутентификации и соответствует требованиям по 4 уровню контроля недекларированных возможностей (НДВ 4) и требованиям Технических условий. **Сертификат соответствия ФСБ России № СФ/124-3112** подтверждает, что СКЗИ "Криптотокен 2 ЭП" в составе JaCarta-2 ГОСТ соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, а также требованиям к СКЗИ класса КС1 и КС2 и требованиям к средствам ЭП класса КС1 и КС2. **Сертификат ФСБ России № СФ/111-2750** подтверждает, что персональное средство электронной подписи "Криптотокен ЭП", предназначенное для использования совместно с СКЗИ "Криптотокен" в составе изделия JaCarta ГОСТ (eToken ГОСТ), соответствует требованиям к средствам ЭП по классам КС1 и КС2 и может использоваться для реализации функций ЭП в соответствии с 63-ФЗ "Об электронной подписи" от 6 апреля 2011 года. **Common Criteria EAL 5+** — международный сертификат на используемые в устройствах JaCarta микроконтроллер (чип) и операционную систему на соответствие профилям безопасности Security IC Platform Protection Profile и Java Card™ System Protection Profile (достигнутый уровень доверия — EAL 5+). **Международные сертификаты безопасности**, допускающие ввоз и эксплуатацию JaCarta на территории стран-членов ЕС (RoHS, CE, FCC). **Электромагнитная безопасность** — изделие JaCarta ГОСТ соответствует требованиям ГОСТ Р 51317.4.2-2010, ГОСТ Р 51318.22-99 и ГОСТ Р 51318.22-99, а также требованиям Технического регламента Таможенного союза "Электромагнитная совместимость технических средств" (декларация о соответствии ТС N RU Д-RU.AB49.B.05350 от 06.09.2016 г., Протокол сертификационных испытаний № 8908EM-LAB09/16 от 02.09.2016 г., ТУ 46538383.40 3000.002ТУ). **Сертификат пыле- и влагозащищённости устройства** — степень защиты IP56: допускается использование в постоянно пыльных и постоянно влажных помещениях. **Сертификат Роспотребнадзора** — подтверждает, что изделие JaCarta безопасно для здоровья человека и соответствует санитарно-эпидемиологическим и гигиеническим требованиям, утвержденным решением Комиссии Таможенного союза № 299 от 28.05.2010 г.

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17.
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17.
Лицензия Министерства обороны РФ № 1384 от 22.08.16.
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011.
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15.
Apple Developer.

+7 (495) 223-00-01 aladdin@aladdin-rd.ru **Web**: www.aladdin-rd.ru

ID: 6012-060917