

JaCarta ГОСТ

Новая линейка смарт-карт,
USB-, MicroUSB- и Secure MicroSD-токенов



Содержание

JaCarta ГОСТ.....	3
Новая линейка смарт-карт, USB-, MicroUSB- и Secure MicroSD-токенов.....	3
Электронная подпись.....	4
Виды электронной подписи.....	4
Технологии безопасного формирования электронной подписи.....	5
Технологическая платформа JaCarta.....	6
Назначение.....	7
Модельный ряд.....	8
Secure MicroSD-токены с электронной подписью.....	9
MicroUSB-токены с электронной подписью.....	9
USB-токены с электронной подписью.....	9
Сравнение моделей.....	10
Смарт-карты с электронной подписью.....	10
Конструктивные особенности.....	11
MicroUSB-токены.....	11
USB-токены в корпусе Nano.....	12
USB-токены в корпусе XL.....	13
Смарт-карты.....	14
Аппаратная реализация национальной криптографии.....	15
Безопасность.....	15
Безопасный доступ к ресурсам компьютера и сети по токenu.....	16
Поддержка мобильных платформ.....	17
Apple iOS.....	17
Google Android.....	18
Упаковка и полезные аксессуары.....	19
Модели семейства JaCarta ГОСТ.....	20
JaCarta ГОСТ.....	20
JaCarta ГОСТ/Flash.....	21
Сертификаты.....	22
Технические подробности.....	24
Объём Flash-памяти.....	24
Интерфейс.....	24
Для разработчиков и интеграторов.....	25
Доступные программные интерфейсы.....	25
Совместимость.....	25
Централизованное управление жизненным циклом токенов.....	25
О компании.....	26

JaCarta ГОСТ

Новая линейка смарт-карт, USB-, MicroUSB- и Secure MicroSD-токенов

Персональное средство электронной подписи (ЭП) от лидера российского рынка — компании "Аладдин Р.Д.":

- аппаратная реализация российской криптографии;
- формирование усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП;
- строгая аутентификация пользователей;
- безопасное хранение ключей, паролей, цифровых сертификатов;
- сертификат соответствия ФСБ России.

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 ГОСТ помогут быть собой в электронном мире.



JaCarta ГОСТ —
будь собой в электронном мире!

Электронная подпись



С развитием информационных технологий электронная подпись (ЭП) стала привычным атрибутом нашей жизни. ЭП позволяет придать электронному документу юридическую силу, равную юридической силе собственноручно подписанного и скрепленного печатью бумажного документа. С одной стороны, такие нововведения призваны облегчить процесс электронного взаимодействия и расширить возможности информационных систем. С другой стороны, важно соблюдать все требования безопасности и действовать в соответствии с законодательством, дабы избежать ситуаций, когда юридическая сила документа может быть оспорена в силу неправомерного использования того или иного аналога собственноручной подписи.

Виды электронной подписи

Действующий 63-ФЗ "Об электронной подписи" от 6 апреля 2011 г. устанавливает три вида ЭП в зависимости от решаемых задач и областей применения.

- **Простая ЭП.** Наименее защищенный вид ЭП, к которому не предъявляется каких-либо существенных ограничений и требований по безопасности. Тем не менее, в силу своей простоты и удобства часто применяется и для подтверждения финансовых транзакций. Например, вводя свой PIN-код при использовании банковской карты, Вы, фактически, подтверждаете операцию простой ЭП.
- **Усиленная неквалифицированная ЭП.** Этот вид ЭП характеризуется применением надежных криптографических алгоритмов, она позволяет определить лицо, подписавшее документ, и обнаружить внесение изменений в подписанный документ. Основное применение – внутренние системы, интегрированные с РКІ, такие, как электронная почта, корпоративные порталы, системы электронного документооборота и т.д.
- **Усиленная квалифицированная ЭП.** Данный вид ЭП отличается тем, что её создание и проверка должны осуществляться сертифицированными средствами ЭП. Достоинством квалифицированной электронной подписи является признание в качестве аналога собственноручной подписи во всех информационных системах без дополнительных условий.

Для усиленной ЭП и усиленной квалифицированной ЭП применяются решения на основе асимметричной криптографии с использованием пар открытых и закрытых* ключей шифрования. Для того чтобы подписывать электронные документы, пользователю необходимо иметь закрытый ключ подписи и сертификат соответствующего ему открытого ключа.



Технологии безопасного формирования электронной подписи

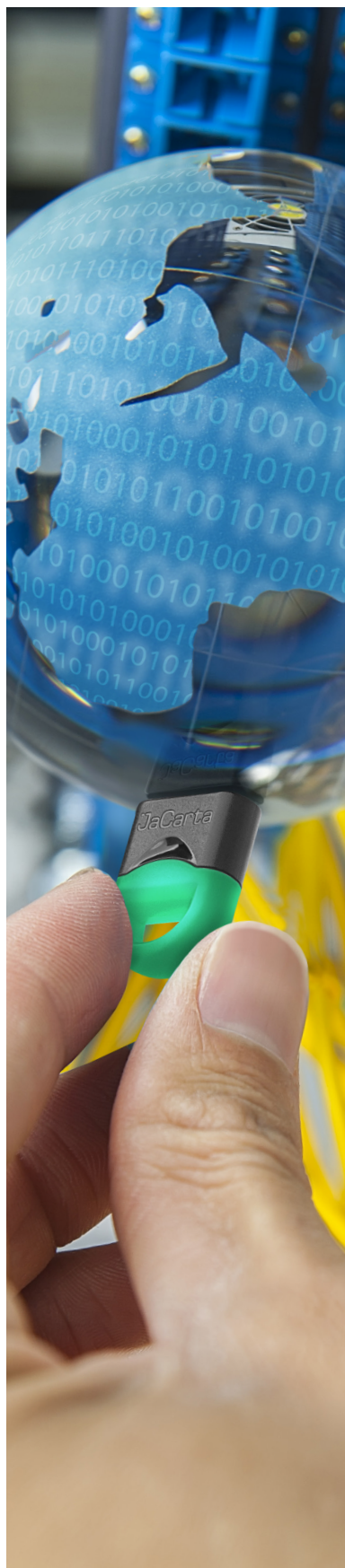
Как для собственноручной подписи нужна авторучка, так и для ЭП необходим соответствующий инструментарий. Изначально в роли средства ЭП выступали обычные компьютеры, на которых выполнялись соответствующие программы. Однако это неудобно и очень небезопасно – Вы никогда не можете быть уверены, что компьютер не заражён вредоносным вирусом или трояном, который может похитить пароли, ключи шифрования или выполнить транзакцию без Вашего ведения. К тому же, доступ к компьютеру могут иметь посторонние лица. Конечно, существуют и средства защиты от мошенников – обычно используются пароли, рекомендуется хранить секретные ключи ЭП на внешних устройствах, но всё это становится неэффективно по мере развития хакерских технологий и уже не может остановить киберпреступников.

Мы предлагаем средство ЭП не в виде программы для компьютера, а в виде миниатюрного персонального устройства (специализированного защищённого компьютера) – электронного ключа. Размеры этого компьютера – считанные миллиметры, что позволяет размещать его в стандартных пластиковых карточках, миниатюрных USB-устройствах (токены) и даже внутри карты памяти формата MicroSD. Это и есть то самое средство ЭП, которое всегда можно носить с собой.

Мы особенно позаботились о том, чтобы его нельзя было ни вскрыть, ни извлечь из него информацию, ни другим способом вмешаться в его функционирование. Секретный ключ ЭП является неизвлекаемым и недостижимым для злоумышленника. Используются также и традиционные меры защиты – пароли. Если Вы потеряете данное средство ЭП, то без знания Вашего личного пароля воспользоваться им невозможно.

Только аппаратные решения – электронные ключи (смарт-карты, USB-, MicroUSB- и Secure MicroSD-токены) на основе специализированного защищённого микроконтроллера в состоянии надёжно защитить закрытый криптографический ключ пользователя.

Также стоит отметить, что JaCarta ГОСТ является безопасным устройством класса Secure Signature Creation Device и полностью соответствует международным требованиям к устройствам для создания подписи (Директива 1999/93/ЕС - о порядке использования электронных подписей в Европейском Сообществе).



Технологическая платформа JaCarta

Любой электронный ключ JaCarta может быть использован для формирования усиленной ЭП, однако в линейке есть семейство электронных ключей, которое объединено общим названием **JaCarta ГОСТ**. Название подчёркивает существенную особенность этих устройств – в них реализованы российские криптографические алгоритмы, в соответствии с которыми формируется и проверяется ЭП, – ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 (скоро появятся и более современные алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012). Качество данных решений подтверждается сертификатом соответствия требованиям ФСБ России к средствам криптографической защиты информации класса КС2 (сертификат соответствия № СФ/124-2380 от 11 мая 2014 г.) и средствам электронной подписи (сертификат соответствия № СФ/121-2270 от 12 декабря 2013 г.).

Аппаратная реализация сертифицированных криптографических алгоритмов позволяет безопасно формировать ЭП на "борту" электронного ключа. В отличие от программных средств криптографической защиты информации (СКЗИ), срок действия закрытого ключа увеличивается до 3 лет с возможностью регенерации пользователем.

Технологическая платформа JaCarta позволяет использовать ЭП в самых разных информационных системах. Благодаря одному электронному ключу пользователь имеет возможность безопасно работать с системами электронного документооборота, платёжными системами, аутентифицироваться в облачных сервисах, участвовать в электронных торгах и др. Пользоваться электронным ключом можно не только со стационарного компьютера или ноутбука, но и со смартфона или планшета, который всегда под рукой!

Теперь электронный ключ JaCarta ГОСТ представляет собой универсальное решение, подходящее для разных информационных систем и типов устройств.

Назначение



JaCarta ГОСТ — это первое и пока единственное на российском рынке персональное средство усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП, полностью соответствующее всем требованиям 63-ФЗ и Приказа ФСБ России № 796 к средствам ЭП. Выпускается в виде смарт-карты, USB-, MicroUSB- и Secure MicroSD-токена.

В состав комплекта может входить интерфейсное ПО, имеющее встроенные функции визуализации подписываемых и проверяемых документов, контроля срока действия ключей ЭП и пр.

Линейка продуктов JaCarta ГОСТ предназначена для обеспечения юридической значимости действий пользователей при использовании различных электронных сервисов:

- дистанционное банковское обслуживание (ДБО);
- электронные торговые площадки;
- сдача электронной отчетности;
- электронное декларирование грузов, перемещаемых через границу;
- публичные или корпоративные Web-порталы и облачные сервисы, например, Портал гос. услуг;
- системы корпоративного/ведомственного электронного документооборота (СЭД).

JaCarta ГОСТ является недорогим, простым, надёжным и удобным в использовании устройством, ориентированным на применение как в массовых проектах (B2C/G2C – для физических лиц), так и для корпоративных пользователей (B2B/G2B – для юридических лиц).

JaCarta ГОСТ может использоваться не только с различными компьютерами, работающими под управлением Microsoft Windows, Linux, Mac OS, но и с мобильными устройствами – планшетами, смартфонами на базе Apple iOS, Google Android, Microsoft Windows 8.

Решаемые задачи:

- формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП;
- визуализация подписываемого/подписанного электронного документа;
- строгая взаимная двухфакторная аутентификация пользователей Web-порталов и облачных сервисов (с использованием ЭП);
- генерация ключей, формирование и проверка электронной подписи с неизвлекаемым ключом ЭП при работе с криптопровайдерами КриптоПро CSP, VipNet CSP, Signal-COM CSP, Lissi CSP, JaCarta CSP;
- безопасное хранение ключевой информации и цифровых сертификатов;
- хранение закрытого ключа ЭП (срок действия составляет 3 года, с возможностью регенерации его самим пользователем);
- использование в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов.

Модельный ряд



Разные исполнения и форм-факторы функционально идентичны, но предполагают различные модели использования, разный набор доступных опций и возможностей кастомизации

При проектировании линейки JaCarta ГОСТ наши инженеры учли накопленный 20-летний опыт, и для каждого сегмента, для каждого сценария использования смогли оптимизировать как набор технических и функциональных параметров, так и крайне важных для массового использования – эксплуатационных и надёжных.

Теперь линейка **JaCarta ГОСТ** является **лучшим предложением на рынке**: по инновационности и используемым новейшим технологиям (Java Card), по подтверждённой безопасности (в частности, невозможности клонирования) и соответствию требованиям российского законодательства, по возможностям использования.

Линейка JaCarta ГОСТ включает **несколько исполнений** и форм-факторов.



Secure MicroSD-токен

Для мобильных, встраиваемых (embedded) и M2M-устройств



MicroUSB-токен

Для пользователей мобильных устройств под управлением ОС Google Android, Microsoft Windows и Linux



USB-токены

В миниатюрном корпусе Nano для массовых B2C- и G2C-проектов
В привычном корпусе XL с дополнительной flash-памятью



Смарт-карты

Для проектов "ЭП на платёжной карте"
Модули смарт-карт с ЭП "на борту"

Secure MicroSD-токены* с электронной подписью



Комбинированные MicroSD-токены с ЭП для мобильных пользователей

- Для безопасного хранения ключей VPN, ключевых контейнеров, приложений и пользовательских данных, для работы с ЭП (как модуль безопасности для мобильных платформ на базе Google Android, Microsoft Windows, Linux).
- Для СЭД в качестве персонального средства ЭП с неизвлекаемым ключом ЭП.

MicroUSB-токены с электронной подписью



Первый в отрасли MicroUSB-токен для мобильных устройств

- Для систем ЭДО в качестве персонального средства ЭП с неизвлекаемым ключом ЭП
- Для безопасного хранения ключей VPN, приложений и пользовательских данных, для работы с ЭП (как модуль безопасности для мобильных платформ на базе Google Android, Microsoft Windows, Linux)

USB-токены с электронной подписью



Для пользователей систем ЭДО и электронных сервисов

В корпусе Nano для B2C-/G2C-проектов

- Позиционирование: для массовых B2C- и G2C-проектов.
- Миниатюрный недорогой USB-токен для физических лиц – пользователей различных электронных сервисов: систем интернет-банкинга, для работы с Порталом гос. услуг и пр.

Для корпоративных пользователей

В корпусе XL

- Позиционирование: для корпоративных пользователей.
- Для строгой двухфакторной аутентификации пользователей в корпоративной сети, безопасного доступа к информационным ресурсам предприятия, приложениям.
- Для работы с ЭП в системах электронного документооборота (СЭД) и дистанционного банковского обслуживания (ДБО).

В корпусе XL с дополнительной flash-памятью

- Позиционирование: для корпоративных пользователей, работы в СЭД, пользователей систем ДБО.
- Комбинированный USB-токен с дополнительной flash-памятью для работы электронной подписью в СЭД.
- Flash-память может быть разбита на два раздела: CD-ROM для доверенных ОС, виртуальных машин, программ и неизменяемых данных и flash-диск (перезаписываемая область) для пользовательских данных.



* Поддержка только для Google Android версий 4.1–4.3. Secure MicroSD-токен не поддерживается в Google Android версии 4.4 из-за ограничений прав доступа к внешним носителям, которые были введены Google в этой версии ОС.

Смарт-карты с электронной подписью

Для пользователей систем ЭДО и электронных сервисов



- Для строгой двухфакторной **аутентификации** пользователей и усиленной квалифицированной **электронной подписи** при работе в системах электронного документооборота, ДБО, сдачи электронной отчетности, на Web-порталах и в "облачных" сервисах.

Платёжные карты с электронной подписью, карты "Электронное правительство"



- Полнофункциональная **чиповая платёжная карта MasterCard или VISA** и усиленная квалифицированная электронная подпись для работы с Порталом гос. услуг (www.gosuslugi.ru), системами интернет-банкинга, системами электронной отчетности, счет-фактурами и другими электронными и облачными сервисами, требующими юридическую значимость.
- Для социальных проектов** в карту может быть встроен бесконтактный чип (RFID), например, для проезда в транспорте и допуска на социальные объекты.
- По правилам платёжных систем такие карты должны эмитироваться банками. Могут выдаваться, например, в рамках зарплатных проектов.



Модули смарт-карт с электронной подписью "на борту"

- Для M2M- и embedded-решений**, где требуется электронная подпись для передаваемых данных (для использования в качестве встраиваемого модуля безопасности).
- Для производителей карт** и Персобюро.

Сравнение моделей

	Secure MicroSD	MicroUSB	USB		Смарт-карта
			Nano	XL	
Персональное средство ЭП с неизвлекаемым ключом ЭП	●	●	●	●	●
Хранение ключевых контейнеров программных СКЗИ (КриптоПроCSP, VipNetCSP и др.)	●	●	●	●	●
Дополнительная Flash-память для ОС, виртуальных машин, приложений и данных (опция/Flash)	●	●	●	●	●

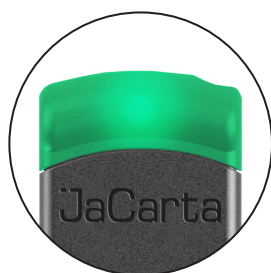
- — Недоступно для данного исполнения
● — Доступно для данного исполнения

Конструктивные особенности



MicroUSB-токены

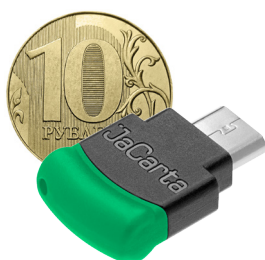
MicroUSB-токены предназначены для пользователей мобильных/носимых устройств под управлением ОС Google Android, Microsoft Windows и Linux.



Удобный яркий колпачок – не позволит оставить токен подключенным к устройству. Яркость светодиода подобрана так, чтобы не слепить в темноте и быть заметной даже при ярком солнечном свете. Колпачок обеспечивает удобное подключение и отключение токена от мобильного устройства.



Миниатюрный карабин (в комплекте) – позволяет крепить токен на связке с ключами, быстро отсоединять от неё при подключении его к планшету или смартфону, а после использования – быстро возвращать обратно.



Оптимальные размеры – токен не сильно выступает за пределы корпуса планшета/телефона при подключении. Он никогда не будет мешать при работе и не позволит забыть его подключенным к мобильному устройству.

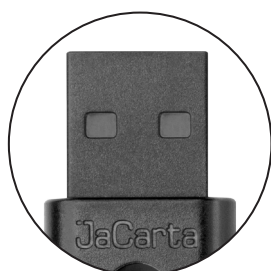


Строгий стильный дизайн – чёрный матовый корпус с выступающим ярким цветным колпачком отлично смотрится с любым планшетом или смартфоном. Разные модели (с разными функциями) различаются цветом колпачка.

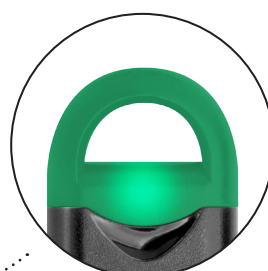


USB-токены в корпусе Nano

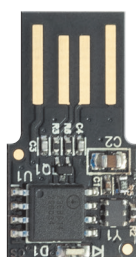
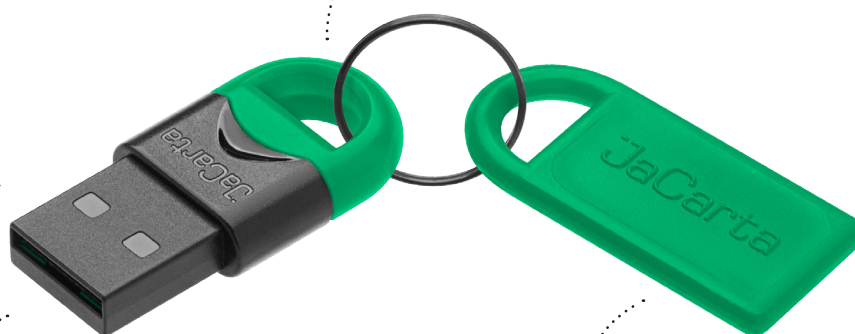
Токены в миниатюрном пластиковом корпусе Nano имеют оптимальный размер: если токен делать ещё меньше, то пользователи гарантированно будут забывать их подключенными в порт компьютера.



Привычный металлический **USB-разъём** заменён на пластиковый, являющийся продолжением корпуса токена.



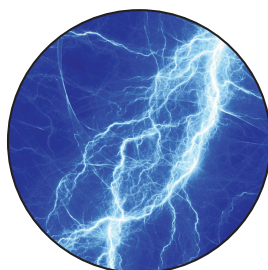
Удобство подключения и отсоединения токена от компьютера обеспечивается за счёт пластиковой дужки (как у навесного замка), надёжная фиксация токена в разъёме.



Надёжная запатентованная конструкция – разъём и плата токена – одно целое, сломать его в этом месте практически невозможно. Да и при подключении к компьютеру он выступает из него всего на 2 см.



Для того чтобы токен не терялся (ведь он такой маленький!) и Вы всегда могли идентифицировать нужный, мы предлагаем целый спектр цветных **пластиковых брелоков** с металлическим колечком.



Повышенная надёжность (живучесть) токена обеспечивается за счёт снижения риска пробоя статическим электричеством (отсутствуют металлические детали, открытые контактные проводники в USB-разъёме закрыты пластиковой оправкой – частью корпуса).

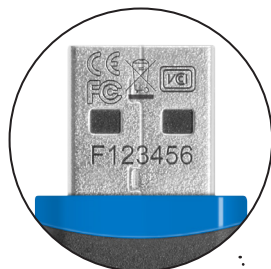


Кастомизация – токены в корпусе Nano могут выпускаться с цветной вставкой и пластиковым брелоком в Вашем фирменном цвете. На брелоке предусмотрено место и для Вашего логотипа.



USB-токены в корпусе XL

USB-токен JaCarta выпускается в стильном чёрном корпусе XL. Он рассчитан на интенсивное ежедневное использование корпоративными пользователями. Поэтому он имеет надёжный металлический разъём и удлинённый корпус для удобного подключения токена к компьютеру, соседние провода и разъёмы не мешают.

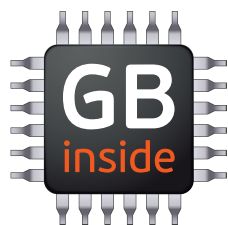
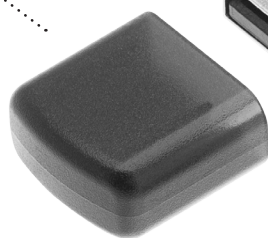


Лазерная гравировка уникального серийного номера ключа на металлическом разъёме делает невозможным подмену или стирание номера.



Яркость и цвет световой индикации работы токена подобраны так, чтобы не слепить пользователя, когда он работает в условиях слабой освещённости (например, в транспорте), и хорошо заметен при ярком офисном или солнечном свете.

Для защиты разъёма USB от попадания пыли, влаги, мелких твёрдых частиц служит съёмный пластиковый колпачок.



Токен со встроенной Flash-памятью стал заметно компактнее. Благодаря новой архитектуре теперь он работает быстрее и меньше греется при интенсивной работе с Flash-памятью.

Корпус имеет достаточно широкое **отверстие под кольцо** для бирки, брелока и для удобного крепления токена на связке с ключами.



Кастомизация – токены могут выпускаться с цветной вставкой в Вашем фирменном цвете. На корпусе предусмотрено место и для Вашего логотипа.



Смарт-карты

Смарт-карты могут поставляться как в фирменном стиле (чёрный пластик с серебряным эмбоссированием номера модели и уникального серийного номера карты, чип с палладиевыми контактами серебристого цвета), так и в виде "белого пластика" для самостоятельной печати на карте, с высококачественной полноцветной печатью по согласованному дизайну.



Чипы могут устанавливаться как с позолоченными контактами, так и с серебристыми (палладиевыми).



Возможность нанесения ID-номера (для идентификации и учёта токена на предприятии) и/или номера чипа. Нанесение осуществляется методом эмбоссирования, что делает невозможным подмену или стирание номера. Можно менять формат и расположение номеров, а также наносить любые символы (например, для нанесения ФИО сотрудника).



Встроенная RFID-метка

в смарт-карту может быть имплантирована радиочастотная метка (RFID), используемая на предприятиях в системах контроля и управления доступом (СКУД) в помещениях, учёта рабочего времени сотрудников и пр.



Кастомизация – при поставке смарт-карты в белом пластике доступна возможность нанесения изображений (например, логотипа и элементов стиля) на одну или обе стороны смарт-карты.

Аппаратная реализация национальной криптографии



JaCarta ГОСТ спроектирован в соответствии с требованиями ФСБ России к шифровальным криптографическим средствам по уровню КС2, предназначенным для защиты информации, не содержащих сведений, составляющих государственную тайну, требованиям ФСБ России к средствам квалифицированной подписи.

При формировании и проверке электронной подписи в JaCarta ГОСТ выполняются все требования 63-ФЗ к средствам усиленной и квалифицированной электронной подписи (в части визуализации подписываемого/проверяемого документа, невозможности использования закрытого ключа, срок действия которого уже истёк, контроля целостности ПО и т.п.).

В отличие от программных СКЗИ **срок действия закрытого ключа** для JaCarta ГОСТ составляет **3 года** с возможностью регенерации самим пользователем, причём дистанционно, без визита в Ваш офис, без использования специализированных АРМов и дополнительного ПО.

Поддерживаемые криптографические алгоритмы:

- ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка ЭП);
- ГОСТ Р 34.11-94 (функция хэширования);
- ГОСТ 28147-89 (симметричное шифрование данных в памяти);
- алгоритм Диффи-Хеллмана (выработка ключа парной связи в соответствии с RFC 4357).

Платформа JaCarta также поддерживает украинскую (ДСТУ 4145-2002) и казахстанскую/СНГ национальную криптографию (ГОСТ 34.310-2004).

Безопасность



Семейство JaCarta ГОСТ выполнено на **защищённых смарт-карточных чипах**, имеющих специальную защиту и на аппаратном, и на программном уровнях (Secure by design), что позволяет успешно противостоять всем известным угрозам безопасности, методам взлома и клонирования.

Главным критерием для нас при выборе чипов является их **подтверждённая** физическая защищённость и гарантированная безопасность.

USB-токены имеют **повышенную защищённость от пробоя** статическим электричеством (до 15 киловольт), что крайне важно при эксплуатации в зимних условиях, низких температурах и пониженной влажности воздуха.

Токены и карты **не оказывают влияния** на работу электронного оборудования, чувствительного к электромагнитным излучениям и помехам (например, медицинское оборудование), а также сами **имеют повышенную защищённость** от воздействия на них электромагнитных излучений и помех.

Безопасный доступ к ресурсам компьютера и сети по токenu



JaCarta SecurLogon позволяет повысить уровень безопасности при входе на локальный компьютер и в корпоративную сеть под управлением ОС Microsoft Windows за счёт простого и быстрого перехода от авторизации по логину и паролю к двухфакторной аутентификации на основе токена.

Для функционирования JaCarta SecurLogon нет необходимости в покупке дорогостоящего серверного оборудования для развёртывания Active Directory и собственного Удостоверяющего центра для выпуска сертификатов пользователей. Вместо сертификатов SecurLogon генерирует сложные пароли (до 63-х символов), которые записываются на токен. Решение помогает автоматизировать выполнение пользователями требований и регламентов ИБ в компании.

Преимущества

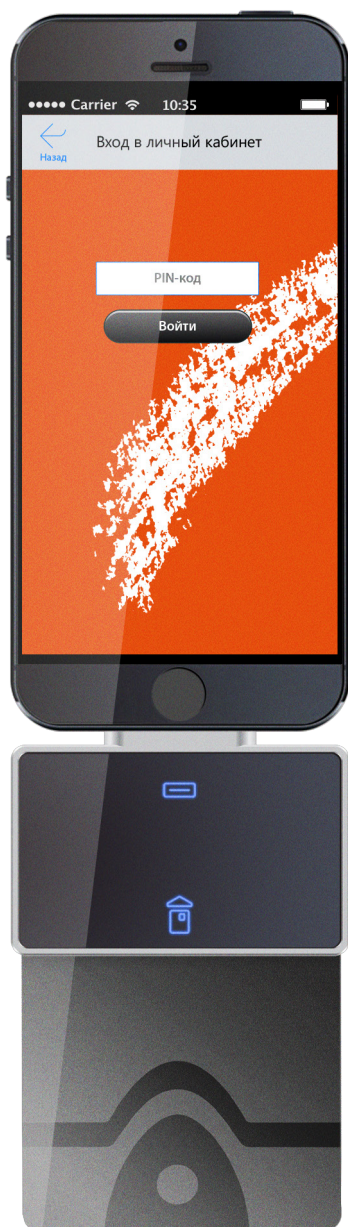
- **Организация двухфакторной аутентификации без Active Directory и/или Microsoft CA.** Использование JaCarta SecurLogon не требует настройки Active Directory, развёртывания PKI-инфраструктуры и покупки дорогостоящего серверного оборудования и ПО.
- **Невозможность подбора пароля.** Программное решение позволяет генерировать и записывать на токен случайные длинные, сложные и устойчивые ко взлому и перебору пароли для доступа в компьютер или сеть.
- **Настоящий сложный пароль не известен и не виден пользователю.** JaCarta SecurLogon позволяет генерировать пароли заданной длины, сохранять их в памяти смарт-карты или USB-токена и подставлять в хранилище учётных данных таким образом, что пользователь даже не знает своего пароля, а потому не может записать его и скомпрометировать. Пользователю лишь остаётся запомнить свой PIN-код.

Основные функции

- Двухфакторная аутентификация пользователей на локальном (не подключенном к сети) компьютере и в домене Microsoft Windows с помощью токенов и смарт-карт JaCarta и eToken
- Возможность блокировки компьютера при временном отсутствии сотрудника на рабочем месте
- Возможность использования цифровых сертификатов

Поддержка мобильных платформ

Apple iOS



Смарт-картами JaCarta ГОСТ теперь можно пользоваться практически на всех современных мобильных платформах, включая и самую закрытую из всех – Apple iOS. Для этого достаточно приобрести специализированный смарт-карт ридер* с разъёмом 30-pin или Lightning.

Что это даёт?

- Не нужно делать Jailbreak.
- Возможность распространения приложений через AppStore, т.к. криптография содержится на отчуждаемом носителе – карте, а приложение содержит только вызовы.

Приложения для Apple iOS представляют собой монолитный код. Если приложение использует программно реализованную криптографию, то оно классифицируется как СКЗИ. Следовательно, на него распространяются все ограничения – запрет на экспорт, распространение через Интернет (с американского сайта Apple, ограничения Apple и американского законодательства на распространение приложений, содержащих криптографию).

- Сокращение сроков вывода продукта на рынок (криптография на карте уже имеет сертификат, разработчикам предоставляется SDK с примерами и средства отладки).
- Минимальное влияние при установке обновлений и новых версий ОС.

Криптографические функции реализованы на карте, а не в iOS-приложении. Внесение изменений в приложение не влияет на реализацию криптографии на карте.

- Соответствие требованиям законодательства – ЭП формируется в персональном сертифицированном устройстве пользователя (на смарт-карте).
- Удобство и упрощение режима эксплуатации – одна карта, один считыватель смарт-карт для всех используемых устройств и платформ.

Для планшетов iPad предлагается вариант кожаного чехла со встроенным считывателем смарт-карт.

* Для работы со смарт-картой на мобильных устройствах под управлением Apple iOS также можно использовать беспроводной смарт-карт ридер, изображённый на следующей странице.

Google Android

Для работы со смарт-картой JaCarta ГОСТ на мобильных устройствах под управлением ОС Google Android удобно использовать беспроводной смарт-карт ридер. Для подключения смарт-карты к мобильным устройствам ридер использует технологию Bluetooth.



Беспроводной смарт-карт ридер работает с мобильными устройствами под управлением Google Android и Apple iOS



MicroUSB- и Secure MicroSD-токены с электронной подписью "на борту"

JaCarta ГОСТ, выполненная в виде MicroUSB-токена или привычной карточки MicroSD, делает возможным использование сертифицированной российской криптографии на мобильных платформах на базе Google Android.

Для подключения MicroUSB- или Secure MicroSD-токена к обычному компьютеру под управлением Microsoft Windows, Mac OS X и Linux можно использовать специализированные USB-ридеры или адаптеры MicroUSB-to-USB/MicroSD-to-USB.

Упаковка и полезные аксессуары



Чтобы Вы могли сосредоточиться на главном и не отвлекаться на ряд мелочей, порой не менее важных при запуске нового проекта, мы подготовили типовую индивидуальную упаковку для токенов и смарт-карт, типовые инструкции для пользователей, а также целый набор полезных аксессуаров: кольца для крепления токенов на связке с ключами, цветные брелоки, чтобы пользователям и администраторам было легче находить и идентифицировать свои токены и т.п.

На базе типовой индивидуальной упаковки можно быстро сделать новую, в Вашем фирменном стиле.



Типовой упаковочный конверт



Типовая VIP-упаковка (коробка)

Модели семейства JaCarta ГОСТ

JaCarta ГОСТ



MicroUSB-токен



USB-токен в корпусе Nano



USB-токен в корпусе XL



Смарт-карта

Первое и пока единственное на российском рынке персональное средство усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП, полностью соответствующее всем требованиям 63-ФЗ и Приказа ФСБ России № 796 к средствам ЭП.

- Формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП.
- Хранение ключевых контейнеров для КриптоПро CSP, VipNet CSP и других программных СКЗИ.
- Сертификат соответствия ФСБ России № СФ/124-2380.
- Сертификат соответствия ФСБ России № СФ/121-2270, подтверждающий, что JaCarta ГОСТ является средством электронной подписи.
- Сертификат соответствия ФСБ России № СФ/121-2350, подтверждающий, что JaCarta ГОСТ является персональным средством электронной подписи.
- В составе комплекта может быть поставлено интерфейсное ПО, имеющее встроенные функции визуализации подписываемых и проверяемых документов, контроля срока действия ключей ЭП и пр.

Особенности

JaCarta ГОСТ выпускается в трёх базовых форм-факторах: USB-токен (в корпусе Nano), MicroUSB-токен и смарт-карта.

Программное обеспечение

Для удобства пользователей JaCarta ГОСТ компания "Аладдин Р. Д." разработала программный комплекс **"Единый клиент JaCarta"**.

Наличие спецификаций PKCS#11 определяет высокоуровневый платформонезависимый унифицированный интерфейс взаимодействия программ с внешними криптографическими устройствами: USB-токенами, смарт-картами, картами Secure MicroSD и пр. Интерфейс PKCS#11 является рекомендуемым при работе с устройством и реализуется библиотеками:

- jscrks11 (основная) – реализует взаимодействие с устройством;
- jscrks11x – PKI-расширение для работы с цифровыми сертификатами и Удостоверяющими центрами.

Кроме того, доступна библиотека jscrks11v — GUI-расширение для отображения и подтверждения пользователем подписываемых данных, а также для отображения проверяемых данных.

Рекомендации

Для работы со смарт-картами со стационарного компьютера рекомендуется использовать офисные считыватели смарт-карт ASEDrive IIIe, с ноутбуками – компактные ASEDrive Mini, с мобильными устройствами – iR301-U и bR301.

JaCarta ГОСТ/Flash



Secure MicroSD



USB-токен в корпусе XL

Комбинированный токен с дополнительной Flash-памятью и российской криптографией "на борту" для строгой аутентификации пользователей и формирования усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП при работе с Web-порталами и облачными сервисами, в системах электронного документооборота, декларирования, ДБО и с др. электронными сервисами.

Flash-память может быть разбита на два раздела: CD-ROM для доверенных ОС, виртуальных машин, программ и неизменяемых данных и flash-диск (перезаписываемая область) для пользовательских данных.

Характеристики JaCarta ГОСТ/Flash, JaCarta Secure MicroSD ГОСТ:

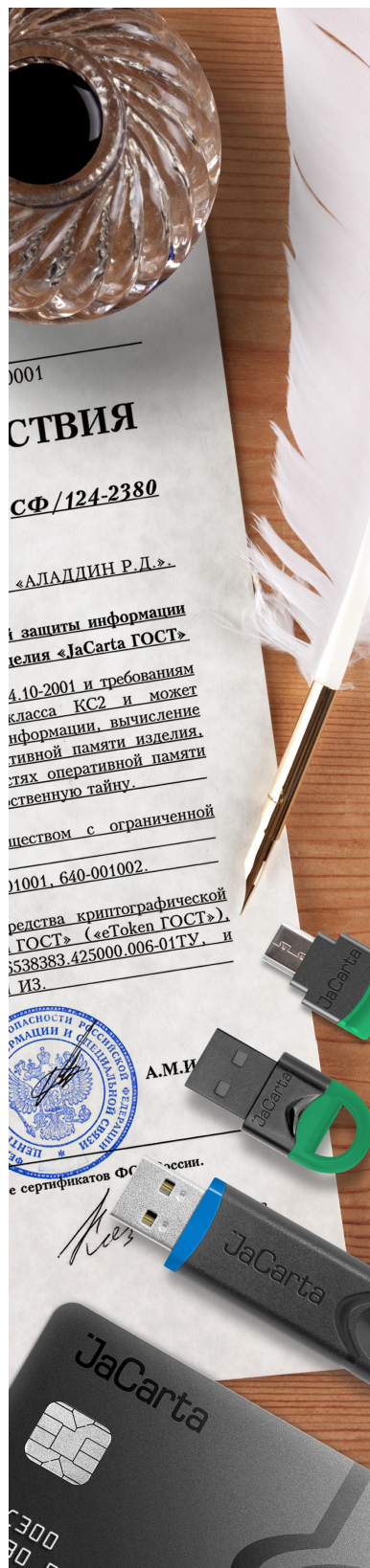
- формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП;
- хранение ключевых контейнеров для КриптоПро CSP, VipNet CSP и других программных СКЗИ;
- flash-память объемом 2, 4 и 8 Гб;
- сертификат соответствия ФСБ России № СФ/124-2380, подтверждающий, что JaCarta ГОСТ является СКЗИ класса КС2;
- сертификат соответствия ФСБ России № СФ/121-2270, подтверждающий, что JaCarta ГОСТ является средством электронной подписи;
- сертификат соответствия ФСБ России № СФ/121-2350, подтверждающий, что JaCarta ГОСТ является персональным средством электронной подписи;
- в составе комплекта может быть поставлено интерфейсное ПО, имеющее встроенные функции визуализации подписываемых и проверяемых документов, контроля срока действия ключей ЭП и пр.

Особенности

Выпускается в двух форм-факторах: USB-токен (в стандартном корпусе XL) и Secure MicroSD-токен.

Secure MicroSD-токен предназначен для мобильных пользователей и может использоваться в планшетах и телефонах на базе Google Android, Microsoft Windows, Linux, а также на обычных ноутбуках и стационарных компьютерах (с использованием USB-ридера).

Сертификаты



- **Сертификат соответствия ФСБ России № СФ/124-2380**, подтверждающий, что реализованная в смарт-картах и токенах российская криптография соответствует ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к средствам криптографической защиты информации класса КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну. Срок действия закрытого ключа ЭП – до трёх лет.
- **Сертификат соответствия ФСБ России № СФ/121-2270**, подтверждающий, что смарт-карты и USB-токены соответствуют требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 № 796, установленным для класса КС2, и могут использоваться для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с Федеральным законом от 6 апреля 2011 г. № 63 "Об электронной подписи".
- **Сертификат соответствия ФСБ России № СФ/121-2350** подтверждает, что дополнительный программный интерфейс "Криптотокен ЭП", входящий в состав продуктовой линейки JaCarta ГОСТ, соответствует требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 и класса КС2, и может использоваться для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".
- **Common Criteria EAL 4+** – международный сертификат на используемые в устройствах JaCarta микроконтроллер (чип) и операционную систему на соответствие профилю безопасности Smart Card Security User Group – Smart Card Protection Profile.

Архитектура и технология используемого в JaCarta ГОСТ микроконтроллера - Secure by design (сконструирован как безопасный и для целей обеспечения безопасности).
- **Common Criteria EAL 5+** – международный сертификат на используемые в устройствах JaCarta микроконтроллер (чип) и операционную систему на соответствие профилю защиты Security IC Platform Protection Profile, версия 1.0. Оценка соответствия выполнена по методике Common Criteria (версия 3.1, ревизия 3). Достигнутый уровень доверия – EAL 5+ (усиленный).

- **Международные сертификаты безопасности**, допускающие ввоз и эксплуатацию JaCarta на территории стран – членов ЕС:
 - **RoHS** (отсутствие в устройствах опасных для здоровья веществ – свинца, кадмия, ртути, шестивалентного хрома и бромидных соединений);
 - **CE** (разрешение для ввоза и применения устройств на территории стран – членов ЕС);
 - **FCC** (устройство не является источником электромагнитных помех, которые могут повлиять на работу другого электронного оборудования, и полностью соответствует международным требованиям в части уровня электромагнитных помех радиоустройствам).
- **Электромагнитная безопасность** — сертификат № 1242202 Федерального агентства по техническому регулированию и метрологии на соответствие требованиям нормативных документов ГОСТ Р 51317.4.2-2010:
 - устройства имеют повышенную защищённость от пробоя статическим электричеством (до 15 киловольт) и соответствует требованиям ГОСТ Р 51317.4.2-2010;
 - устройства не оказывают влияния на работу электронного оборудования, чувствительного к электромагнитным излучениям и помехам (например, медицинское оборудование) и соответствует требованиям ГОСТ Р 51318.22-99;
 - устройства имеют повышенную защищённость от воздействия электромагнитных излучений и помех и соответствует требованиям ГОСТ Р 51318.22-99.
- **Сертификат пыле- и влагозащищённости устройства** (степень защиты IP58): USB-токены JaCarta ГОСТ соответствуют требованиям международного и российского стандартов IEC 60529 (ГОСТ 14254-96, DIN 40050, МЭК 529:1989) и являются пыле- и влагозащищёнными устройствами, допускается их использование в постоянно пыльных и постоянно влажных помещениях.

Технические подробности



Поддерживаемые криптографические алгоритмы:

- ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка ЭП);
- ГОСТ Р 34.11-94 (функция хэширования);
- ГОСТ 28147-89 (симметричное шифрование – для данных, содержащихся в областях оперативной памяти изделия);
- алгоритм Диффи-Хеллмана (выработка ключа парной связи в соответствии с RFC 4357).

Каждое устройство JaCarta ГОСТ имеет встроенный генератор последовательностей случайных чисел.

Объём Flash-памяти

Для USB-токенов с опцией Flash	2/8 ГБ
Для Secure MicroSD	4 ГБ

Интерфейс

Для USB-токенов	USB 2.0 Full speed (12 Мбит/с)
Для смарт-карт	ISO 7816-3: — T=0 (для опции EMV-совместимость); — T=1 (используется по умолчанию).
Для MicroUSB-токенов	Через адаптер MicroUSB-to-USB 2.0 Full speed (12 Мбит/с)
Для Secure MicroSD	Через любой разъём/коннектор для подключения карт памяти формата MicroSD

Для разработчиков и интеграторов

Для использования линейки JaCarta ГОСТ в собственном прикладном или системном ПО разработчикам предоставляется широкий набор программных интерфейсов, позволяющих встроить любые устройства JaCarta гарантированно качественно и в самые короткие сроки.

Доступные программные интерфейсы

Приложение (функциональность)	Microsoft Windows	Linux x86	Linux ARM	Mac OS	Apple iOS	Google Android
ГОСТ	APDU PKCS #11 (#7, #10) MS CAPI (CSP, CNG) Java Crypto Provider (JCP) Криптотокен ЭП*	APDU PKCS #11 (#7, #10) Криптотокен ЭП*	APDU PKCS #11 (#7, #10)	APDU PKCS #11 (#7, #10)	APDU PKCS #11 (#7, #10)	APDU PKCS #11 (#7, #10)

* Дополнительный **сертифицированный программный интерфейс для визуализации** подписываемого документа в соответствии с требованиями 63-ФЗ (статья 12).

Совместимость

Подтверждённая совместимость с существующей инсталляционной базой программных СКЗИ.

- Все модели JaCarta поддерживают хранение ключевых контейнеров программных СКЗИ (КриптоПро CSP, VipNet CSP и др.)

Централизованное управление жизненным циклом токенов

- JaCarta Management System (JMS) – система управления средствами аутентификации и ЭП, полностью поддерживающая работу с JaCarta, а также с eToken
- SafeNet Authentication Manager (SAM) – только для моделей с обратной совместимостью с продуктами компании Aladdin

О компании

Российская компания "Аладдин Р. Д." является признанным экспертом и лидером рынка средств ЭП и аутентификации пользователей в корпоративных ресурсах, на Web-порталах и в облачных сервисах.

Многие продукты, решения и технологии компании занимают доминирующее положение на российском рынке. За 20 лет работы практически каждый выводимый на рынок продукт компании заслуживал особого внимания и становился лидером в своём сегменте.

Продукты компании "Аладдин Р. Д." неоднократно были удостоены званий "Продукт года", "Лучший инновационный продукт", "Лучший продукт в области информационной безопасности", "Прорыв года", а компания – награда от Аппарата Совета Безопасности РФ, Комитета Государственной Думы по безопасности.

Во многих компаниях, банках и Федеральных структурах продукты и решения компании "Аладдин Р. Д." стали стандартом де-факто.

В 2012 г. компания "Аладдин Р. Д." сертифицировала свою систему управления качеством продукции на соответствие требованиям международного стандарта менеджмента качества ГОСТ Р ИСО 9001:2008 (ISO 9001:2008), в 2013 г. – прошла аудит на соответствие новому стандарту ГОСТ ISO 9001:2011, а в 2014 г. подтвердила результаты.

Позиции компании на российском рынке:

- входит в ТОП-3 — рынок аппаратных решений ИБ;
- входит в ТОП-20 — крупнейшие компании на рынке ИБ;
- входит в ТОП-100 — крупнейшие ИТ-компании России.

