JaCarta ГОСТ

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

Персональное средство электронной подписи
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 помогут быть собой в электронном мире.

JaCarta ГОСТ – будь собой в электронном мире!

Версия	1.0
Редакция от	04.04.2014
Листов	30

Телефон +7 (495) 223-00-01 • Факс +7 (495) 646-64-40 • aladdin@aladdin-rd.ru • www.aladdin-rd.ru

Содержание

1. 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 скреплённого 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.

1.1. 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 защищённый 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 ЭП.** Этот вид ЭП характеризуется применением надёжных криптографических алгоритмов, она позволяет определить лицо, подписавшее документ, и обнаружить внесение изменений в подписанный документ. Основное применение - внутренние системы, интегрированные с PKI, 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.

1.2. 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 недосягаем 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-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/EC - о порядке использования электронных подписей в Европейском Сообществе).

1.3. 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 Р34.10-2001, ГОСТ Р34.11-94 (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/124-1671 от 11 мая 2011 г.).

Аппаратная реализация сертифицированных криптографических алгоритмов позволяет безопасно формировать ЭП на "борту" электронного ключа. В отличие от программных СКЗИ, срок

действия закрытого ключа увеличивается до 3 лет с возможностью перегенерации пользователем.

Технологическая платформа JaCarta позволяет использовать ЭП в самых разных информационных системах. Благодаря одному электронному ключу пользователь имеет возможность безопасно работать с электронным документооборотом, 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.

2. Назначение

JaCarta ГОСТ – это **первое и пока единственное персональное средство** усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП, полностью соответствующее всем требованиям 63-ФЗ и Приказа ФСБ № 796 к средствам ЭП. Выпускается в виде смарт-карты, USB- 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 отчётности;
- 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 Windows, Linux, Mac OS, но и с мобильными устройствами – планшетами, смартфонами на базе Apple iOS, Android, 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 **перегенерации его самим пользователем**);

- использование в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов.

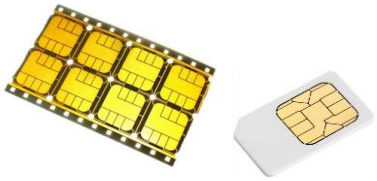
3. Модельный ряд

При проектировании линейки JaCarta ГОСТ наши инженеры учли накопленный 15-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 надёжностных.

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**.**

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

Смарт-карты	USB-токены	Secure MicroSD-токен
		
	В миниатюрном корпусе Nano для массовых B2C- и-G2C-проектов	Для мобильных, встраиваемых (embedded) и M2M-устройств
		
Для проектов «ЭП на платёжной карте»	В корпусе Mini для B2B- и G2B-проектов	
		
Модули смарт-карт с ЭП «на борту»	В привычном корпусе XL с дополнительной флеш-памятью	Secure MicroSD-токен с USB-считывателем для подключения к ноутбуку или ПК

4. 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 отчётности, 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 отчётности, 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.

5. USB-токены с электронной подписью

Для пользователей систем ЭДО и электронных сервисов

В корпусе Mini
для B2B-проектов

- Для использования в СЭД, сдачи электронной отчётностии пр. в качестве персонального средства ЭП с неизвлекаемым ключом ЭП.
- Для сохранения преемственности с существующими системами поддерживается хранение ключевого контейнера в токене для всех программных СКЗИ.
- Позиционирование: для B2B-проектов, там, где требуется периодическое использование токена, и очень важно, чтобы он всегда был под рукой и готов к работе (поэтому так важны надёжность и защищённость токена от пробоя статическим электричеством, влаги, пыли, поломки в "походных" условиях).
- Токен имеет повышенную эксплуатационную надёжность, защиту от пробоя статическим электричеством, пыле- и влагозащищённость.

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.

С дополнительной флеш-памятью в корпусе XL
для корпоративных
пользователей

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

6. 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 Android, Windows, Linux).
- Для СЭД в качестве персонального средства ЭП с неизвлекаемым ключом ЭП.

Один Secure MicroSD-токен для разных устройств

Для работы на планшете, смартфоне, ноутбуке или персональном компьютере пользователям достаточно иметь всего один Secure MicroSD-токен и подключать его через переходники-адаптеры:

- к USB-порту (как обычный USB-токен);
- к слоту для SD-карты памяти.

7. Сравнение моделей

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

○ /● - Недоступно/доступно для данного исполнения

8. Конструктивные особенности

8.1. USB-токены в корпусе Mini – для юридических лиц

Токены в корпусах Mini предназначены для периодического использования в системах сдачи электронной отчётности, дистанционного банковского обслуживания, электронных торгов, электронного декларирования товаров, перемещаемых через границу и пр.

Очень важно, чтобы такие токены всегда были под рукой – в сумке, в кармане. Именно поэтому они имеют повышенную прочность, пыле-, влагозащищённость, защиту USB-разъёмов (токена и компьютера), меньший риск повреждения статическим электричеством.

При работе в «походных» условиях риск поломки такого токена минимален, ведь он выступает из разъёма ноутбука всего на 2 см.

Сдвижной колпачок, защищающий и очищающий USB-разъём от соринок и жировых пятен, на боковой поверхности имеет лазерную гравировку уникального серийного номера ключа.

USB-разъём токена имеет упрощённую конструкцию — пластиковую основу для контактной группы без О-образной оправки, фиксирующей токен в разъёме.

Необнаруживаемое вскрытие корпуса практически исключено, попытка вскрытия приводит к видимым дефектам.

Токен имеет заметный зелёный индикатор режима работы, а для крепления к токену бирки, брелока или обычных ключей случит небольшое металлическое кольцо и гибкий поводок-петля. Поэтому он не будет теряться.

Повышенные меры по обеспечению пыле и влаго-защищённости – токен может использоваться в постоянно пыльных и влажных помещениях, допускается длительное погружение в воду на глубину до 1 м, может работать даже в погруженном в пресную воду состоянии (соответствует требованиям стандарта IP58, Category 2).

8.2. USB-токены в корпусе Nano – для физических лиц

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

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

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.

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.

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

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.

Базовые цвета: белый, жёлтый, красный, синий, розовый, малиновый, фиолетовый, зелёный, оранжевый.

Примеры:

8.3. 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.

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

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.

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

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

8.4. Смарт-карты

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

Чип может поставляться с привычными позолоченными контактами.

Встроенная RFID-метка – в смарт-карту может быть имплантирована радиочастотная метка (RFID), используемая на предприятиях в системах контроля и управления доступом (СКУД) в помещения, учёта рабочего времени сотрудников и пр. (см. «Доступные опции»).

9. 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 и формату квалифицированного сертификата.

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 перегенерации 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).

10. 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.

11. Поддержка мобильных платформ

11.1. 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 карт-ридер с разъёмом Apple Dock (30-pin) или Lightning (8-pin).

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 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.

11.2. Android, Windows Phone 8

Считыватель, используемый для подключения смарт-карт к Apple iOS, имеет дополнительный разъём Micro USB, через который может подключаться как к ПК, так и к Android-устройствам.

SECURE MICROSD С ЭЛЕКТРОННОЙ ПОДПИСЬЮ «НА БОРТУ»

JaCarta ГОСТ, выполненная в виде привычной карточки MicroSD, делает возможным использование сертифицированной российской криптографии на мобильных платформах на базе Android, Windows или Linux.

Такой Secure MicroSD-токен через USB-ридер или MicroSD→SD адаптер можно использовать и на обычном компьютере.

12. Надёжность и качество

При разработке и производстве нового поколения токенов JaCarta наши инженеры учли весь накопленный опыт и сделали их ещё лучше, ещё надёжнее.

Более того, компания «Аладдин Р. Д.» сертифицировала свою систему управления качеством продукции в соответствии требованиям международного стандарта менеджмента качества ГОСТ Р ИСО 9001-2011 (ISO 9001:2011), а производство - в соответствии с международным стандартом экологической безопасности ISO 14001:2004.

13. 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)

14. Модели семейства JaCarta ГОСТ

14.1. JaCarta ГОСТ

Первое и **пока единственное** 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.
- Доступная защищённая память ~32 КБ.
- Сертификат соответствия ФСБ России СФ/124-1671 (действие сертификата распространяется на изделия "JaCarta ГОСТ" на основании письма № 149/3/2/1-1016 от 03.08.2011 г.).
- Сертификат соответствия ФСБ 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 двух базовых форм-факторах: USB-токен (в корпусах Nano и Mini) и смарт-карта.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Для удобства пользователей JaCarta ГОСТ компания «Аладдин Р. Д.» разработала программный комплекс **JC-GOSTClient**, в состав которого входят: утилита администрирования, библиотеки PKCS#11 v2.30 (draft) и PKI-расширений, поставщики криптографии JaCarta CSP, Java Cryptographic Provider (JCP), драйвер для Microsoft Windows XP.

Спецификация 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:

- jcpkcs11 (основная) - реализует взаимодействие с устройством;
- jcpkcs11x – PKI-расширение для работы с цифровыми сертификатами и Удостоверяющими центрами;

Кроме того, доступна библиотека jcpkcs11v — 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.

Смарт-карта

USB-токен в корпусе Nano

USB-токен в корпусе Mini

14.2. JaCarta ГОСТ/Flash, JaCarta MicroSD ГОСТ

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.

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

Характеристики JaCarta ГОСТ/Flash, JaCarta 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;
- доступная защищённая память ~32 КБ;
- флеш-память объёмом 2, 4 и 8 ГБ;

- сертификат соответствия ФСБ России СФ/124-1671 (действие сертификата распространяется на изделия JaCarta ГОСТ на основании письма № 149/3/2/1-1016 от 03.08.2011 г.);
- 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 Android, Windows, Linux, а также на обычных ноутбуках и стационарных компьютерах (с использованием USB-ридера).

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Для удобства пользователей JaCarta ГОСТ компания «Аладдин Р. Д.» разработала программный комплекс **JC-GOSTClient**, в состав которого входят: утилита администрирования, библиотеки PKCS#11 v2.30 (draft) и PKI-расширений, поставщики криптографии JaCarta CSP, Java Cryptographic Provider (JCP), драйвер для Microsoft Windows XP.

Спецификация 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:

- jcpkcs11 (основная) - реализует взаимодействие с устройством;
- jcpkcs11x – PKI-расширение для работы с цифровыми сертификатами и Удостоверяющими центрами;

Кроме того, доступна библиотека jcpkcs11v — GUI-расширение для отображения и подтверждения пользователем подписываемых данных, а также для отображения проверяемых данных.

Для работы с флеш-памятью предназначена утилита **JaCarta Flash**, с помощью которой при необходимости можно для разбить дополнительную флеш-память токена на два раздела: CD-ROM и Flash, а также записать ISO-образ диска в CD-ROM область.

РЕКОМЕНДАЦИИ

Для использования Secure MicroSD-токена на ноутбуке или персональном компьютере рекомендуется приобрести USB-считыватель или переходник MicroSD→SD.

USB-токен в корпусе XL

Secure MicroSD

15. Сертификаты

- **Сертификат соответствия ФСБ России СФ/124-1671**, 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.

  Действие данного сертификата распространяется на JaCarta ГОСТ на основании письма № 149/3/2/1-1016 от 03.08.2011 г.

- **Сертификат соответствия ФСБ России № СФ/121-2270**, подтверждающий, что смарт-карты и USB-токены (имеющие в названии опцию ГОСТ) 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).

  Микроконтроллер защищён и может противостоять всем известным на сегодняшний день атакам: клонирование, взлом, физические, логические, статистические, переборные, стрессовые, с использованием специальных зондов, по питанию и пр.

- **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 радио-устройствам).

- **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 PKI 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.

16. 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 Secure MicroSD	Через любой разъём/коннектор для подключения карт памяти формата MicroSD

17. 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.

Архитектура системного ПО и основные принципы:

- **мультиплатформенность**:
  - поддержка разных ОС (32/64): Windows, Linux, Mac OS;
  - поддержка разных архитектур: x86, ARM, RISC;
  - поддержка мобильных платформ: Apple iOS, Android, Windows 8;
- **одинаковое высокоуровневое API** для всех платформ, всех используемых чипов и устройств, единый SDK;
- **полный набор стандартных интерфейсов**: APDU (PC/SC), PKCS#11 (#7, #10), MS CAPI (CSP, CNG), Java Cryptographic Provider (JCP);
- дополнительный **сертифицированный программный интерфейс для визуализации** подписываемого документа в решениях наших партнёров;
- **полный набор функций**, необходимых для полноценной работы с СКЗИ, удостоверяющими центрами, квалифицированными сертификатами X.509, биометрией (дополнительного ПО не требуется);
- **совместимость** с существующей инсталляционной базой программных СКЗИ — все модели JaCarta поддерживают хранение ключевых контейнеров программных СКЗИ (КриптоПро CSP, VipNet CSP и др.);
- **удобство перехода** на новые модели с аппаратной поддержкой российской криптографии — JaCarta обеспечивает одновременную поддержку двух режимов работы с CSP: хранение ключевого контейнера и работу с неизвлекаемым ключом ЭП;
- **встроенная поддержка** аппаратных средств работы с ЭП в недоверенной среде (считывателей смарт-карт с визуализацией).

18. Базовые решения

Кроме интерфейсов для работы со смарт-картами и токенами мы предлагаем и готовые технологические решения:

- аутентификация и ЭП для веб-порталов и облачных сервисов;
- аутентификация и ЭП для мобильных платформ Apple iOS, Android;
- АРМ для работы с удостоверяющим центром КриптоПро УЦ;
- решения технологических партнёров компании (подробнее на сайте - http://www.aladdin-rd.ru/solutions/partners/).

19. О компании

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

Многие продукты, решения и технологии компании занимают доминирующее положение на российском рынке. За 18 лет работы практически каждый выводимый на рынок продукт компании заслуживал особого внимания и становился лидером в своём сегменте.

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

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

В 2012 г. компания «Аладдин Р. Д.» сертифицировала свою систему управления качеством продукции в соответствии требованиям международного стандарта менеджмента качества ГОСТ Р ИСО 9001-2008 (ISO 9001:2008), в 2013 – прошла аудит и подтвердила сертификат.

Позиции компании на российском рынке:

- входит в ТОП-3 (№ 2) — рынок аппаратных решений ИБ;
- входит в ТОП-20 (№ 11) — крупнейшие компании на рынке ИБ;
- Входит в ТОП-100 (№ 79) — крупнейшие ИТ-компании России.

Лист регистрации изменений

Версия документа	Изменения
1.0	Исходная версия документа

Телефон: +7 (495) 223-00-01
Факс: +7 (495) 646-64-40
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (бессрочно), № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12 и № 24530 от 25.02.14
Microsoft Silver OEM Hardware Partner, Oracle Gold Partner, Apple Developer
Сертификат соответствия СМК ГОСТ Р ИСО 9001-2011