

JaCarta ГОСТ

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



Для электронных
сервисов

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 РД."

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 бумажного документа.

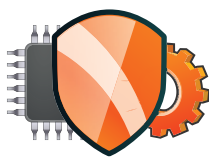
С одной стороны, такие нововведения призваны облегчить процесс электронного взаимодействия и расширить возможности информационных систем. С другой стороны, важно соблюдать все требования безопасности и действовать в соответствии с законодательством, дабы избежать ситуаций, когда юридическая сила документа 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 защищённый вид ЭП, но и имеющий ограниченную сферу применения – в основном для подтверждения каких-либо действий, не имеющих значительных финансовых или юридических последствий;
- **усиленная ЭП** – характеризуется применением криптографических алгоритмов, позволяет определить лицо, подписавшее документ, и обнаружить внесение изменений в подписанный документ. Основное применение – внутренние корпоративные системы, интегрированные с РКИ, например, электронная почта, корпоративные порталы, системы электронного документооборота и т.д.;
- **усиленная квалифицированная ЭП (УКЭП)** – создание и проверка должны осуществляться сертифицированными средствами ЭП, а цифровой сертификат должен быть выдан уполномоченным Удостоверяющим центром. УКЭП является аналогом собственноручной подписи, и она должна приниматься любыми информационными системами без дополнительных условий и ограничений.

Основное назначение новой линейки JaCarta ГОСТ – это формирование усиленной квалифицированной электронной подписи (с неизвлекаемым ключом ЭП) при работе с Web-порталами и облачными сервисами, в системах электронного документооборота, ДБО, для использования в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов.



Технологии безопасного формирования ЭП

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 в том, что компьютер не заражён вредоносным ПО, которое может похитить пароли, ключи или выполнить транзакцию без Вашего ведома. К тому же, доступ к компьютеру могут получить и злоумышленники.

Мы предлагаем "средство ЭП" не в виде программы для компьютера, а в виде миниатюрного персонального устройства, выполненного на базе специализированного защищённого смарт-карточного микроконтроллера. Это и есть Ваше персональное средство ЭП, которое всегда можно носить с собой.

Если Вы потеряете своё средство ЭП, то без знания Вашего личного пароля воспользоваться им будет невозможно.



Невозможность клонирования

Ряд продуктов для формирования ЭП, предлагаемых на российском рынке, выполнен на недорогих микроконтроллерах общего применения, в которых отсутствуют специальные встроенные средства защиты от клонирования, взлома и других атак. Несмотря на наличие сертификатов соответствия (реализованной в них криптографии принятым стандартам), такие средства подвержены серьёзным рискам.

Линейка JaCarta ГОСТ выполнена на защищённом смарт-карточном чипе, имеющем специальные средства защиты от клонирования и всех известных атак. Продукт прошёл полное тестирование в ведущих мировых лабораториях и разрешён для использования в международных платёжных системах VISA и MasterCard.



Сертифицированная российская криптография

В семействе JaCarta есть целая линейка, объединённая 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).

Аппаратная реализация российских алгоритмов позволяет безопасно формировать ЭП "на борту" электронного ключа. В отличие от программных СКЗИ, срок действия закрытого ключа ЭП – до 3 лет с возможностью его регенерации самим пользователем.

JaCarta ГОСТ соответствует требованиям ФСБ России:

- к средствам криптографической защиты информации класса КС2 (сертификат соответствия № СФ/124-2380);
- к средствам ЭП в соответствии с 63-ФЗ и приказом ФСБ России № 796 (сертификат соответствия № СФ/121-2270 и № СФ/121-2350).

JaCarta ГОСТ — будь собой в электронном мире!

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 России № 796 к средствам ЭП.

Линейка 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 Microsoft Windows, Linux, Mac OS X, но и с мобильными устройствами – планшетами, смартфонами на базе Apple iOS, Google Android, Microsoft Windows 8.

JaCarta ГОСТ является безопасным устройством класса Secure Signature Creation Device и полностью соответствует международным требованиям к устройствам для создания подписи (Директива 1999/93/EC).

Решаемые задачи

- Строгая взаимная двухфакторная аутентификация пользователей Web-порталов и облачных сервисов (с использованием ЭП)
- Формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом 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
- Хранение ключевых контейнеров для программных СКЗИ КриптоПро CSP, VipNet CSP и др.
- Хранение пользовательских данных (пароли, коды доступа, настройки и пр.) в защищённой PIN-кодом памяти токена
- Использование в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов
- Реализация требований, предъявляемых к средствам электронной подписи (Статья 12 закона 63-ФЗ), в частности:
 - визуализация подписываемого/подписанного электронного документа;
 - формирование ЭП только после получения подтверждения от пользователя.

Модельный ряд

При проектировании линейки JaCarta ГОСТ наши инженеры учли накопленный 20-летний опыт и для каждого сегмента и сценария использования смогли оптимизировать набор технических, функциональных, эксплуатационных и надёжностных параметров.

Теперь линейка JaCarta ГОСТ является лучшим предложением на рынке: по инновационности и используемым новейшим технологиям (Java Card), по подтверждённой безопасности (в частности, невоз-

можности клонирования) и соответствию требованиям российского законодательства по возможностям использования.

Линейка JaCarta ГОСТ включает несколько функционально идентичных исполнений и форм-факторов, предполагающих различные варианты использования, разный набор доступных опций и возможностей кастомизации.

USB-токены с ЭП



В корпусе Nano для B2C/G2C-проектов

- 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.



В корпусе XL с дополнительной Flash-памятью для корпоративных пользователей

- Для корпоративных пользователей для работы в СЭД, для пользователей систем ДБО. Комбинированный USB-токен с дополнительной Flash-памятью для работы с электронной подписью в системах электронного документооборота

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.

MicroUSB-токены с ЭП



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)

Secure MicroSD-токены с ЭП



Secure MicroSD-токены* с ЭП для мобильных пользователей

- 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)
- Для систем 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

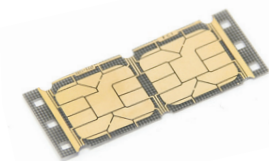
* Поддержка только для Google Android 4.1-4.3. Secure MicroSD-токен не поддерживается в Google Android версии 4.4 из-за ограничений прав доступа к внешним носителям, которые были введены Google в этой версии ОС.

Смарт-карты с ЭП



Для пользователей систем ЭДО и электронных сервисов

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



Модули смарт-карт с ЭП "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



Платёжные карты с ЭП, карты "Электронное правительство"

- Полнофункциональная чиповая платёжная карта MasterCard или VISA с ЭП для работы с Порталом гос.услуг (www.gosuslugi.ru), системами интернет-банкинга, системами электронной отчетности, счёт-фактурами 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
- Проведены испытания в международных лабораториях FIME и Bright Sight, получен сертификат EMVCo

Для работы со смарт-картами мы предлагаем целую линейку смарт-карт ридеров, включая модели для мобильных устройств и модели с биометрическим сканером.

Сравнение моделей

	Смарт-карта	USB		MicroUSB	Secure MicroSD
		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

Безопасный доступ к ресурсам компьютера и сети по токenu



JaCarta SecurLogon — простой и быстрый переход от обычных паролей к двухфакторной аутентификации при входе в ОС Microsoft Windows, в домен и доступе к сетевым ресурсам по токenu JaCarta. Для работы не требуется разворачивать Active Directory, создавать собственный Удостоверяющий центр для выпуска сертификатов пользователей (внедрять PKI-инфраструктуру).

Преимущества JaCarta SecurLogon

- **Организация двухфакторной аутентификации без Active Directory и/или Microsoft CA.** Использование JaCarta SecurLogon не требует настройки Active Directory, развёртывания PKI-инфраструктуры и закупки дорогостоящего серверного оборудования и ПО.
- **Невозможность подбора пароля.** Программное решение позволяет генерировать на токене случайные длинные, сложные и устойчивые ко взлому и перебору пароли для доступа в компьютер или сеть. На подбор сложного пароля в 30-63 символа у злоумышленника уйдут годы.
- **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 компрометировать. Пользователю лишь остаётся запомнить свой простой и короткий PIN-код.

Поддержка мобильных платформ

iOS

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. Для работы с ЭП на iOS-устройствах также можно использовать беспроводной смарт-карт ридер.



Google Android

Для работы со смарт-картой JaCarta ГОСТ на мобильных устройствах под управлением ОС Google Android удобно использовать беспроводной смарт-карт ридер, который использует для подключения Bluetooth-интерфейс.



MicroUSB- и Secure MicroSD-токены с ЭП "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.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
 Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
 Система менеджмента качества компании соответствует требованиям стандарта ISO/IEC 9001:2011
 Сертификат СМК ГОСТ Р ИСО 9001:2011 № РОСС RU.ИСТ72.Н00079 от 29.07.14
 Microsoft Silver OEM Hardware Partner, Microsoft Silver Cloud Platform Partner, Apple Developer
 Названия других технологий, продуктов и компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

Microsoft Partner Silver OEM Hardware Apple Developer





© 1995-2015
ЗАО "Аладдин РД."
Все права защищены

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