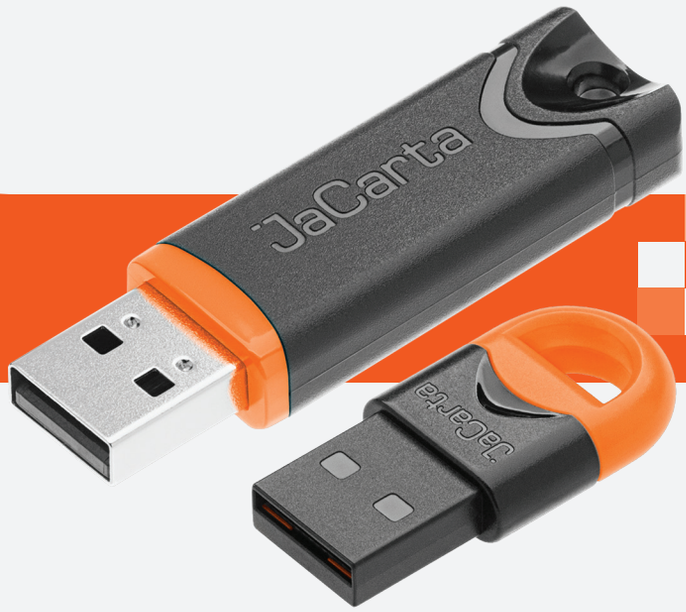
Сертифицированное средство электронной подписи и СКЗИ



JaCarta-2 ГОСТ

- Аппаратная поддержка новых российских криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012
- Полноценное СКЗИ с широким набором криптографических функций
- Средство строгой двухфакторной аутентификации для безопасного доступа в информационные системы, Web-порталы и облачные сервисы
- Безопасное хранение пользовательских данных

Аладдин

Строгая аутентификация и электронная подпись с использованием новых российских криптоалгоритмов

Новое поколение USB-токенов, смарт-карт и модулей безопасности с аппаратной поддержкой ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012

Устройства JaCarta-2 ГОСТ предназначены для использования в качестве сертифицированного средства

Электронной подписи и полноценного СКЗИ* в системах электронного документооборота (ЭДО), дистанционного банковского обслуживания (ДБО) и др. для обеспечения юридической значимости и неотказуемости действий пользователей, а также для обеспечения целостности и конфиденциальности передаваемых данных.

Строгой двухфакторной аутентификации для безопасного доступа пользователей или терминального оборудования в информационные системы, портальные и облачные сервисы.

Безопасного хранения ключевых контейнеров программных СКЗИ, пользовательских данных, сертификатов, паролей и других объектов.

Для обеспечения совместимости с существующими системами и плавного перехода на использование нового российского стандарта ЭП устройства JaCarta-2 ГОСТ поддерживают как старые криптографические алгоритмы ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001, так и новые — ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.

* СКЗИ — средство криптографической защиты информации (СКЗИ "Криптотокен 2 ЭП" в составе изделия JaCarta-2 ГОСТ).

USB-токены

смарт-карты

модули

микросхемы

Возможности

"Белый список" команд и функций

JaCarta-2 ГОСТ имеет "белый список" разрешённых команд и функций, которыми можно безопасно пользоваться из прикладного ПО:

- аппаратная генерация ключей для ЭП (неизвлекаемый закрытый ключ ЭП не выходит за пределы устройства), для шифрования и вычисления имитовставки, для внешних нужд и других СКЗИ;
- хэширование по ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012;
- шифрование, вычисление имитовставки по ГОСТ 28147-89;
- формирование и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- генерация случайных чисел;
- HMAC — контроль целостности передаваемых сообщений и диверсификации ключей;
- работа с папками и файлами в памяти устройства (без доступа к ключам).

Некоторые конкурирующие продукты не имеют "белых списков" криптографических функций и программных интерфейсов для встраивания в прикладное ПО.

Встраивание СКЗИ, не имеющих "белых списков", фактически является созданием нового СКЗИ из компонентов другого (сертифицированного как законченное изделие), а эта деятельность требует специальной лицензии на разработку шифросредств.

Сертифицировано по новым требованиям ФСБ России

Устройства JaCarta-2 ГОСТ сертифицированы по новым требованиям ФСБ России и являются функционально законченными и криптографически безопасными средствами, допускающими легитимное встраивание в другое прикладное ПО.

Предназначено для встраивания

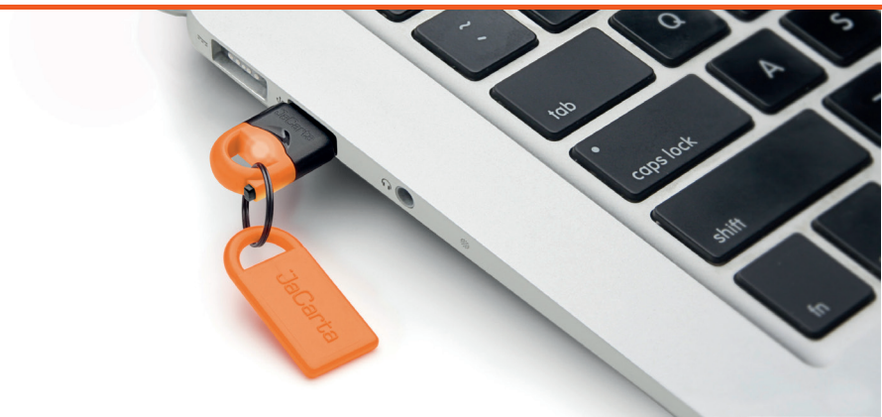
СКЗИ в составе JaCarta-2 ГОСТ предназначено для безопасного встраивания в прикладное ПО. Обязательная в таких случаях проверка оценки влияния (корректность встраивания СКЗИ) при использовании разрешённых функций из "белого списка" становится простой формальной процедурой.

Для встраивания предоставляется комплект разработчика (SDK), включающий библиотеки с разрешёнными для использования высокоуровневыми интерфейсами под разные аппаратные платформы и операционные системы (ОС), подробные примеры с множеством типовых сценариев использования средства ЭП и СКЗИ.

Автоматическое построение защищённого канала

В состав сертифицированного СКЗИ входит интерфейсная криптобиблиотека (ИКБ), предназначенная для работы на стороне хоста (персональный компьютер, сервер или терминальное оборудование) и реализующая:

- набор криптографических алгоритмов и протоколов, включая выработку и согласование сеансовых ключей;
- автоматическое построение защищённого канала с аппаратным устройством JaCarta-2 ГОСТ, что позволяет безопасно передавать команды и данные по открытому каналу;
- быстрое хэширование и шифрование данных (со скоростью работы основного процессора хоста, более мощного и производительного, чем в устройствах JaCarta-2 ГОСТ).



Возможности

Работа с доверенными объектами

К доверенным объектам относятся ключи проверки ЭП. С их помощью проверяется доверие к сертификатам открытых ключей абонентов, с которыми ведётся обмен зашифрованными и/или подписанными сообщениями.

Срок жизни доверенных ключей — 15 лет, закрытых ключей — 3 года, что существенно сокращает стоимость владения устройств JaCarta-2 ГОСТ по сравнению с программными СКЗИ со сроком действия ключей 1 год.

Повышенный ресурс и "живучесть"

Устройства JaCarta-2 ГОСТ проектировались с учётом возможностей применения в различных автоматизированных системах (M2M, IoT, АСУ ТП и пр.) и имеют повышенный ресурс по количеству циклов записи в EEPROM и выполняемых операций ЭП.

Количество операций формирования ЭП составляет не менее 10 млн.

Больше доступной памяти

В новой линейке JaCarta-2 ГОСТ появилась модель с увеличенным объёмом защищённой памяти — теперь для безопасного хранения ключей, кодов авторизации, сертификатов и других объектов доступно до 114 КБайт энергонезависимой памяти (EEPROM).

Дополнительный PIN-код на операцию формирования ЭП

JaCarta-2 ГОСТ позволяет установить второй (дополнительный) PIN-код для операций формирования ЭП.

Устройство может быть сконфигурировано так, что при входе в систему (для строгой двухфакторной аутентификации) пользователь должен ввести один PIN-код, а при проведении финансовых транзакций или при подписании электронных документов — другой PIN-код, разрешающий формирование ЭП.

Новые механизмы разблокирования устройств

Защита от атак на PIN-код — если раньше администратор забывал, не устанавливал или случайно блокировал свой PIN-код, то сбросить забытый PIN-код пользователя было нельзя, и такое заблокированное устройство можно было выбрасывать. В новом поколении устройств JaCarta-2 ГОСТ PIN-код администратора заменён ключом администратора безопасности — случайно или умышленно заблокировать его теперь нельзя.

Защита от блокирования устройства при подборе PIN- и PUK-кодов с задержкой по времени — если пользователь (или кто-то другой, например, злоумышленник или вирус) неверно ввёл и PIN-, и PUK-коды заданное число раз, то по прошествии установленного промежутка времени пользователь самостоятельно сможет восстановить своё устройство, просто введя правильное значение PIN-кода.

Возможность удалённого разблокирования — если пользователь забыл PIN-код своего устройства, то теперь он может позвонить или написать своему администратору и попросить его сгенерировать одноразовый код разблокирования устройства.

Возможность самостоятельного разблокирования — при инициализации устройства администратор может установить и сообщить пользователю специальный PUK-код, с помощью которого он получит возможность самостоятельно разблокировать устройство.

Быстрее

При формировании ЭП значение хэш-функции от подписываемого документа теперь вычисляется с использованием программной библиотеки (ИКБ), являющейся частью сертифицированного СКЗИ и работающей на стороне хоста (персональный компьютер, сервер, терминал).

Это означает, что время подписи, большая часть которого тратится на вычисление хэша для объёмных документов, теперь кардинально сокращается, поскольку хэш вычисляется не на микроконтроллере устройства JaCarta-2 ГОСТ, а на более производительном процессоре хоста.

Благодаря возможности использования защищённого канала выполнение операций хэширования на хосте не приводит к снижению уровня безопасности.

Шифрование также выполняется с использованием ИКБ на хосте. Благодаря этому JaCarta-2 ГОСТ позволяет шифровать объёмные документы без существенных задержек.

Безопасное администрирование

Для инициализации устройств JaCarta-2 ГОСТ при их вводе в эксплуатацию, разблокирования, изменения парольной политики, установки, смены PIN- и PUK-кодов, работы с доверенными объектами, вывода из эксплуатации и сброса к заводским настройкам (например, при выдаче их другим пользователям) предназначен новый АРМ администратора безопасности.

Приобретение АРМ администратора безопасности является полезной, но не обязательной опцией.

Возможность расширения функциональности устройств

Использование технологии Java Card позволяет добавлять необходимую функциональность в устройства JaCarta-2 ГОСТ без необходимости повторной сертификации СКЗИ в ФСБ России. В микроконтроллер с сертифицированным СКЗИ можно загружать другие Java-апплеты, реализующие функции PKI, биометрической идентификации и др.

Защита от взлома и клонирования

Все устройства JaCarta-2 ГОСТ:

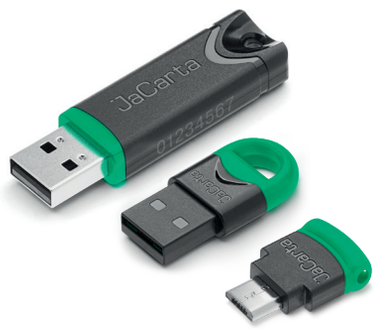
- выполнены на базе защищённых смарт-карточных чипов, имеющих встроенные средства защиты от всех известных атак, методов взлома и клонирования, прошедших сертификацию в международных лабораториях по CAST и EMV (по требованиям для платёжных систем);
- полностью соответствуют международным требованиям к устройствам для создания усиленной квалифицированной ЭП (Qualified Signature Creation Device).

Поддерживаемые ОС

- Microsoft Windows
- Apple macOS
- Linux
- МСВС 3.0, 5.0

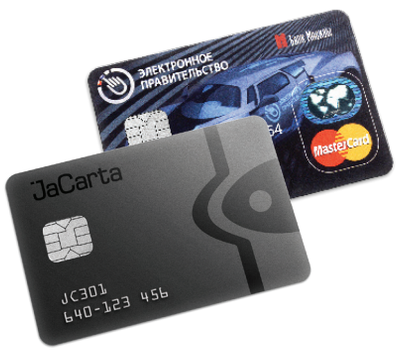
Модельный ряд

Устройства JaCarta-2 ГОСТ выпускаются в различных форм-факторах и исполнениях



USB-токены

В классическом корпусе (XL), миниатюрном (Nano) или с MicroUSB-разъёмом



Смарт-карты

В т.ч. с поддержкой бесконтактного интерфейса NFC. Могут использоваться при выпуске платёжных, социальных и других видов карт с аппаратной поддержкой сертифицированной российской криптографии "на борту" (например, платёжная карта "Мир" с транспортным приложением "Тройка"и средством ЭП)

Модули безопасности

Микросхемы для монтажа на печатную плату. Могут использоваться в различном терминальном, навигационном и другом встраиваемом оборудовании, включая устройства для M2M и АСУ ТП

Комбинированные модели

Функциональность устройств JaCarta-2 ГОСТ может быть расширена — на их базе выпускается целая линейка комбинированных моделей, доступных во всех исполнениях и форм-факторах (USB-токены, смарт-карты, модули безопасности).

Модель	Описание
JaCarta-2 PKI/ГОСТ	Реализована дополнительная поддержка зарубежной криптографии, которая используется для строгой двухфакторной аутентификации при доступе к защищённым корпоративным ресурсам организации с использованием PKI. Совместима с моделью JaCarta PKI.
JaCarta-2 PKI/BIO/ГОСТ	Реализована дополнительная поддержка зарубежной криптографии и биометрическая идентификация пользователя по отпечаткам пальцев с вычислением "на карте" (Match-On-Card), которая используется для замены PIN-кода вводом отпечатка пальца или для строгой трёхфакторной аутентификации при доступе к защищённым корпоративным ресурсам предприятий. Совместима с моделью с JaCarta PKI/BIO.
JaCarta-2 PRO/ГОСТ	Реализована дополнительная поддержка зарубежной криптографии, которая используется для строгой двухфакторной аутентификации при доступе к защищённым корпоративным ресурсам предприятий. Совместима с устройствами JaCarta PRO и eToken PRO (Java) и может работать с ними в одной инфраструктуре без внесения каких-либо изменений.

Сферы применения

USB-токены

- Системы дистанционного банковского обслуживания (ДБО)
- Системы электронного документооборота (ЭДО)
- Электронные торговые площадки (ЭТП)
- Системы сдачи электронной отчётности (Федеральная Налоговая Служба, Пенсионный Фонд России и др.)
- Системы таможенного декларирования
- Порталы государственных услуг
- Web-приложения, корпоративные порталы и облачные сервисы

Смарт-карты

Электронное удостоверение сотрудника
В одной карте возможно совмещение нескольких важных и часто используемых функций:

- пропуск на территорию предприятия, электронный ключ для прохода в помещения (визуальная идентификация и встроенная RFID-метка для интеграции со СКУД);
- средство аутентификации при доступе к корпоративным (служебным) системам;
- средство ЭП сотрудника.

Платёжная карта НСПК "Мир"
В одной карте НСПК "Мир" со встроенным NFC-модулем можно совместить функции:

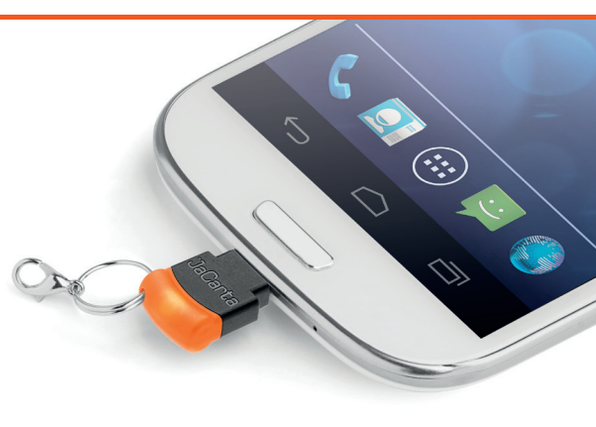
- платёжной (зарплатной) карты;
- средства ЭП (для ДБО, для работы с порталами госуслуг и другими электронными сервисами);
- транспортного приложения, например, "Тройка".

Модули безопасности

Модули безопасности предназначены для встраивания в различное электронное оборудование в качестве сертифицированного модуля безопасности, обеспечивающего конфиденциальность, некорректируемость, юридическую значимость и подтверждение подлинности источников данных и команд.

Модули безопасности могут применяться:

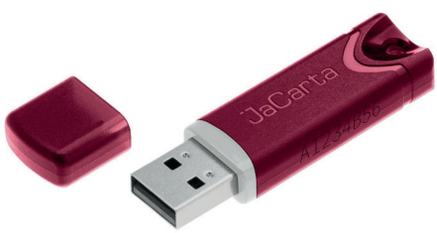
- в различном терминальном, навигационном, телематическом и прочем оборудовании;
- для Интернета вещей (IoT);
- для межмашинного взаимодействия (M2M);
- в автоматизированных системах управления технологическими процессами (АСУ ТП).



Надёжность и качество

При разработке и производстве нового поколения устройств JaCarta-2 ГОСТ был учтён более чем 20-ти летний опыт работы компании. Система управления качеством продукции компании сертифицирована по требованиям российского и международного стандарта менеджмента качества ГОСТ Р ИСО 9001 2011 (ISO 9001:2015), а производства — в соответствии с требованиями российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.

Защищённый служебный носитель JaCarta SF/ГОСТ



- Доступ к данным на USB-диске возможен только аутентифицированным пользователям и только на авторизованных компьютерах
- Защита от внутреннего, внешнего нарушителей, от администраторов
- Сертификат МО России
- Выполняет требования Профиля ФСТЭК России к средствам отчуждения информации на съёмных носителях

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17
Лицензии ФСБ России № 12632Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации услуг ГОСТ Р (РОСС RU.0001.03ГУ00) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
Сертификат соответствия - № РОСС RU.ФК14.К00011 от 20.07.18
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации "Военный Регистр" (РОСС RU.И1975.04ГШ02) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012
Сертификат соответствия - № ВР 21.1.13537-2019 от 25.04.19