

JaCarta PKI

Новое поколение PKI-токенов и смарт-карт
для строгой аутентификации



Для использования
в корпоративных
и государственных
системах

Содержание

Аутентификация.....	3
Требования к технологии и средствам аутентификации.....	4
Назначение.....	6
Модельный ряд.....	7
Для каждой задачи — своё оптимальное решение.....	7
Смарт-карты.....	8
USB-токены.....	9
MicroUSB-токены.....	10
Secure MicroSD-токены.....	10
Сравнение и выбор модели.....	11
Современный дизайн.....	12
Смарт-карты.....	12
USB-токены в корпусе XL.....	13
USB-токены в корпусе Nano – для пользователей ноутбуков.....	14
MicroUSB-токены – для пользователей мобильных устройств.....	15
Безопасный доступ к ресурсам компьютера и сети по токену.....	16
Больше возможностей, больше инноваций.....	17
Выбор модели из семейства JaCarta PKI.....	20
Модели семейства JaCarta PKI.....	21
JaCarta PKI.....	21
JaCarta PKI/BIO.....	22
JaCarta PKI/ГОСТ.....	23
JaCarta PKI/BIO/ГОСТ.....	24
JaCarta PKI/Flash, JaCarta PKI/BIO/Flash.....	25
JaCarta PKI/ГОСТ/Flash, JaCarta PKI/BIO/ГОСТ/Flash.....	26
Смарт-карт ридеры.....	27
Сертификаты.....	29
Технические подробности.....	31
Поддерживаемые криптографические алгоритмы.....	31
Объём Flash-памяти.....	31
Интерфейс.....	31
Для разработчиков и интеграторов.....	32
Доступные программные интерфейсы.....	32
Совместимость.....	32
Централизованное управление жизненным циклом PKI-токенов.....	32
Нам доверяют.....	33

Аутентификация

Так же как "театр начинается с вешалки", безопасность при электронном взаимодействии начинается с ответа на вопрос: "ты кто, и как ты можешь доказать, что ты это ты?".

Классическим примером аутентификации во многих корпоративных и государственных информационных системах является аутентификация пользователей на основе регистрационного имени пользователя (логин) и пароля.

Сегодня мы понимаем, что при современном уровне и характере угроз информационной безопасности (ИБ) привычная всем пара логин-пароль не может обеспечить требуемый уровень безопасности. Для этого в корпоративной системе необходимо применять более надёжные средства аутентификации.

Наши технологии и новейшая линейка продуктов JaCarta PKI помогут построить современную, надёжную и удобную для пользователей систему аутентификации.

Требования к аутентификации

Требования к надёжности, типу, технологии и средствам аутентификации зависят от важности обрабатываемой информации, прав и полномочий администраторов и пользователей системы, вероятности инцидента и определяются на основе анализа рисков возможного ущерба (финансового, репутационного, организационного).

Режим работы администраторов и пользователей – только **внутри периметра** ИБ (в офисе – сотрудники) или **вне** его (удалённые, мобильные пользователи) – сильно влияет на правильный выбор модели используемого средства аутентификации, а также на требования по обеспечению среды, в которой работает пользователь (доверяем мы ей или нет), либо применения средств и технологий, компенсирующих риски работы в недоверенной среде.

Тип аутентификации определяется требуемой надёжностью.



Надёжность аутентификации зависит от целого набора параметров, выбора технологии и средств аутентификации.

Требуемый тип аутентификации

Важность информации	Вероятность и размер возможного ущерба		
	Низкая	Средняя	Высокая
Высокая	●	●	●
Средняя	⚙	●	●
Низкая	⚙	⚙	●

⚙ — Простая аутентификация ● — Усиленная аутентификация ● — Строгая аутентификация

На выбор типа аутентификации сильно влияют права и полномочия пользователя в системе (руководитель, ТОП-менеджер, администратор), а также сценарии работы (удалённый пользователь, мобильный пользователь, работа с домашнего компьютера и пр.).

Для таких пользователей и/или сценариев работы следует выбирать строгую или, в крайнем случае, усиленную аутентификацию.

Требования к технологии и средствам аутентификации



Надёжность аутентификации, в первую очередь, зависит от используемой технологии.

1. Логин-пароль, электронные идентификаторы (Touch Memory и др.) – **низкая** надёжность.

Основная проблема заключается в модели использования паролей: пользователи выбирают простые пароли, которые легко подобрать. Если администратор выставляет требование к использованию сложных длинных паролей, то их сложно запомнить, поэтому пользователи будут записывать их "на бумажках". Пароль нетрудно подглядеть или перехватить.

2. Одноразовые пароли (запрос-ответ) – **средняя** надёжность.

Технология OTP (One-Time-Password) подвержена серьёзному риску – базируется на использовании общего секретного ключа на сервере и в токене, его компрометация приведёт к мгновенной компрометации всех аккаунтов в системе.

Пример: недавний инцидент с OTP-токенами SecureID компании RSA.

3. Строгая аутентификация (с использованием криптографии и PKI-инфраструктуры открытых ключей) – **высокая** надёжность.

Высокая надёжность строгой аутентификации не обеспечивается при использовании цифровых сертификатов/программных токенов с одним фактором аутентификации – знанием пароля.

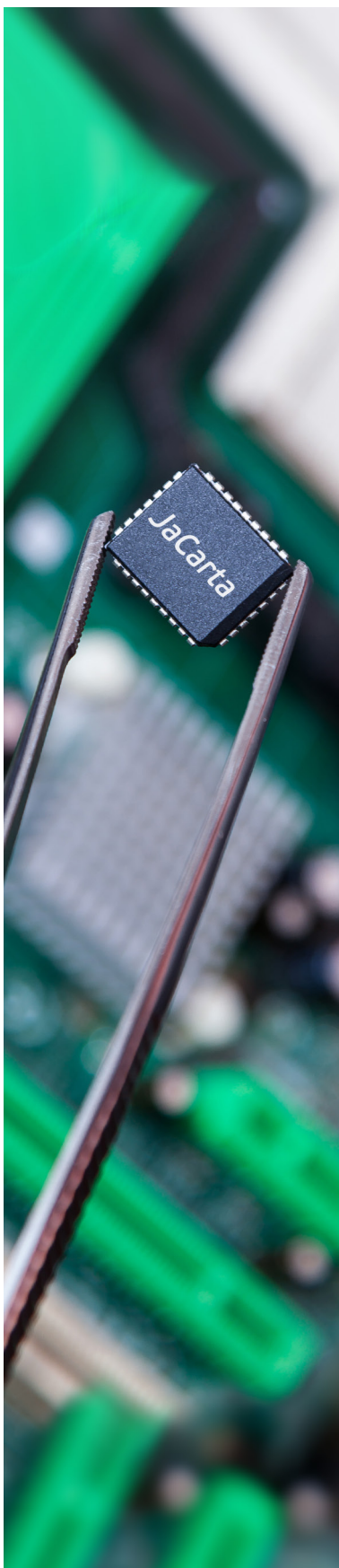
Для обеспечения высокой надёжности строгой аутентификации необходима, как минимум, **двухфакторная аутентификация** (первый фактор – обладание физическим токеном или картой, второй фактор – знание PIN-кода для выполнения криптографических операций внутри токена, необходимых для аутентификации).

В чём основной недостаток программных токенов (ключевых контейнеров) как средств аутентификации? Если злоумышленник завладеет (скопирует, перехватит) программный токен, то рано или поздно он обязательно сможет подобрать к нему пароль и воспользоваться этим токеном от имени его законного владельца.

У аппаратных токенов есть два важных преимущества:

- секретные ключи из аппаратного токена невозможно скопировать, тогда как программный токен легко копируется, причём незаметно;
- количество попыток подбора PIN-кода аппаратного токена ограничено средствами самого токена (как правило, не более 15 попыток, после чего дальнейшие попытки подбора PIN-кода просто невозможны – токен перестаёт "отвечать" на них).

Для программного токена (ключевого контейнера) количество попыток подбора PIN-кода практически не ограничено, может выполняться параллельно на нескольких компьютерах с использованием возможностей современных графических процессоров по высокоэффективному параллельному исполнению одинаковых задач.



При доступе к критически важной информации рекомендуется использовать третий фактор аутентификации – биометрическую идентификацию владельца карты (токена), подтверждающую факт присутствия владельца в момент аутентификации и делающую невозможным использование карты (токена) без её владельца.

Следует отметить возможности применения технологии биометрической идентификации в борьбе с внутренними нарушителями. Ведь результатом классического "подглядывания из-за плеча" может стать PIN-код к смарт-карте коллеги. Однако, если смарт-карта требует помимо PIN-кода ещё и предъявления отпечатка пальца, то воспользоваться полученной информацией (PIN-кодом) и забытой на рабочем месте смарт-картой коллеги злоумышленнику будет просто невозможно.

Надёжность системы с использованием строгой двух- или трёхфакторной аутентификации напрямую зависит от надёжности используемых аппаратных средств (токенов и смарт-карт).

Архитектура и технология используемого в токене или в смарт-карте микроконтроллера должна быть **"Secure by design"** ("сконструирован как безопасный и для целей обеспечения безопасности").

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

Используемый микроконтроллер должен, как минимум, соответствовать профилю безопасности для устройств подобного класса (Smart Card Security User Group – Smart Card Protection Profile) и иметь соответствующее подтверждение (международный сертификат) – Common Criteria с достижением оценочного уровня доверия (EAL) не ниже 4+, а в идеале – соответствовать ещё и профилю защиты Security IC Platform Protection Profile и иметь подтверждение Common Criteria с достигнутым оценочным уровнем доверия - EAL 5+.

Почему? Если средство строгой аутентификации выполнено на микроконтроллере общего применения, эмулирует функциональность смарт-карты (не являясь ею по факту), не имеет специальных встроенных средств защиты от клонирования, взлома и других специальных атак, не имеет международных сертификатов безопасности, значит оно подвержено серьёзным рискам. А следовательно, и вся система.

Если в корпоративной системе планируется использование **юридически значимого электронного документооборота**, то выбор типа аутентификации в системе напрямую влияет на тип применяемой электронной подписи (ЭП):

- простая ЭП – можно использовать простую аутентификацию;
- усиленная ЭП – рекомендуется использовать усиленную или строгую аутентификацию;
- усиленная квалифицированная ЭП (приравняемая к собственноручной подписи) – рекомендуется строгая двухфакторная аутентификация.

Почему? – Потому, что надёжность системы определяется по её самому слабому звену – как доверять электронной подписи, если мы не уверены в том, кто её поставил? Это особенно актуально для удалённых или мобильных пользователей.

*Продукты семейства JaCarta PKI ориентированы на построение **строгой** двух- и трёхфакторной аутентификации.*

Назначение



JaCarta PKI — это новая линейка PKI-токенов для строгой двух- или трёхфакторной аутентификации пользователей в корпоративных системах, безопасного хранения ключевых контейнеров программных СКЗИ*, профилей и цифровых сертификатов пользователей.

JaCarta PKI предназначена для корпоративных пользователей, имеющих развёрнутую инфраструктуру открытых ключей (PKI), при этом поддержка JaCarta PKI в продуктах мировых вендоров обеспечивается штатными средствами.

Однако, если в компании нет развёрнутой PKI-инфраструктуры или настроенного Active Directory, то для организации двухфакторной аутентификации на основе токенов JaCarta PKI существует специальное программное решение JaCarta SecurLogon, позволяющее избежать больших затрат на информационную безопасность.

JaCarta PKI выполнена на современной открытой технологической платформе Java Card с учётом огромного накопленного опыта разработки и внедрения как средств строгой аутентификации, средств электронной подписи, так и инфраструктуры применения смарт-карт и USB-токенов.

JaCarta® является собственной продуктовой линейкой российской компании "Аладдин Р.Д."

Модельный ряд



Функционально они идентичны, но предполагают различные модели использования, разный набор доступных опций (расширение функциональных или эксплуатационных характеристик) и возможностей кастомизации.

Для каждой задачи — своё оптимальное решение

Одно универсальное решение для любых задач, по определению, будет сложнее и хуже, чем набор специализированных, "заточенных" на решение конкретных специфических задач.

Единая и гибкая технологическая платформа позволила нам создать широкую линейку продуктов, оптимизировать их для каждого специфического сегмента, и для каждого такого сегмента предложить лучший продукт и лучшее в своём классе решение.

Линейка PKI-токенов включает **несколько исполнений** и форм-факторов.



Смарт-карты

PKI-карты для корпоративных пользователей



- Для строгой двухфакторной аутентификации пользователей в корпоративной сети, безопасного доступа к информационным ресурсам предприятия, приложениям.
- Для строгой двухфакторной аутентификации, но вместо PIN-кода используется биометрическая идентификация владельца карты (для упрощения жизни ТОП-менеджеров и руководства компаний).
- Для строгой трёхфакторной аутентификации пользователей с использованием биометрической идентификации владельца карты при доступе к критически важным ресурсам (использование карты возможно только в присутствии её владельца).
- Для работы с системами электронного документооборота (хранение ключевого контейнера программных СКЗИ на карте – отчуждаемый носитель или как персональное средство ЭП с неизвлекаемым ключом ЭП).

Электронное удостоверение



- Для пропуска в помещения (визуальная идентификация и наличие RFID-метки).
- Для контроля рабочего времени (при интеграции со СКУД и/или JMS).
- Для безопасного доступа к системам компании (строгая аутентификация и биометрическая идентификация).
- Для обеспечения юридической значимости (персональное средство ЭП – полное соответствие 63-ФЗ).
- Для начисления заработной платы сотрудниками (платёжное приложение MasterCard/VISA).

Электронное удостоверение сотрудника на "зарплатной карте"



- Для получения заработной платы на карту и оплаты товаров и услуг – полнофункциональная чиповая международная платёжная карта MasterCard/VISA.
- Для строгой двух- или трёхфакторной аутентификации в корпоративной сети и получения доступа к информационным ресурсам предприятия (PKI).
- Для прохода на территорию предприятия (по встроенной RFID-метке) или льготного (предоплаченного) проезда сотрудников на городском транспорте (метро, автобусы).
- Для работы с системами электронного документооборота (опция).

По правилам платёжных систем такие карты должны эмитироваться банками.

USB-токены

PKI-токены для корпоративных пользователей

В корпусе Nano



- USB-токен в миниатюрном корпусе Nano **для пользователей ноутбуков.**

В корпусе XL



- **Для строгой двухфакторной аутентификации** пользователей в корпоративной сети, безопасного доступа к информационным ресурсам предприятия, приложениям.

Опционально может быть использована **биометрическая идентификация** владельца токена вместо PIN-кода или дополнительно, в качестве третьего фактора аутентификации.

В рамках проекта в PKI-токен может быть имплантирована RFID-метка для интеграции с корпоративной СКУД.

- **Для работы с системами электронного документооборота** (хранение ключевого контейнера программных СКЗИ в токене – отчуждаемый носитель или как **персональное средство ЭП** с неизвлекаемым ключом ЭП).

Комбинированные PKI-токены с дополнительной Flash-памятью

В корпусе XL



- **Для строгой двухфакторной аутентификации** пользователей в корпоративной сети, безопасного доступа к информационным ресурсам предприятия, приложениям.

Опционально может быть использована биометрическая идентификация владельца токена.

- **Для работы с системами электронного документооборота** (хранение ключевого контейнера программных СКЗИ в токене – отчуждаемый носитель или как персональное средство ЭП с неизвлекаемым ключом ЭП).

- **Для загрузки операционных систем, виртуальных машин** с предварительно установленным и настроенным набором приложений из доверенного источника – эталонного образа CD-ROM раздела Flash-памяти токена.

- **Для хранения данных** в Flash-памяти токена.

Flash-память разбита на два раздела: CD-ROM для доверенных программ и неизменяемых данных и Flash-диск (перезаписываемая область) для пользовательских данных.

MicroUSB-токены



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

- Для строгой двухфакторной аутентификации и электронной подписи при работе в корпоративных сетях (PKI), на Web-порталах и облачных сервисах.
- Для работы с системами электронного документооборота (хранение ключевого контейнера программных СКЗИ в токене – отчуждаемый носитель или как средство ЭП с неизвлекаемым ключом ЭП).
- Возможность работы на стандартных персональных компьютерах и ноутбуках через адаптер MicroUSB-to-USB.

Secure MicroSD-токены*



Комбинированные MicroSD-токены с ЭП для мобильных пользователей (BYOD)

- Для строгой двухфакторной аутентификации и электронной подписи при работе в корпоративных сетях (PKI), системах электронного документооборота, на Web-порталах.
- Для безопасного хранения ключей VPN, ключевых контейнеров, приложений и пользовательских данных (как модуль безопасности для мобильных платформ на базе Google Android, Microsoft Windows, Linux).
- Для работы с системами электронного документооборота (хранение ключевого контейнера программных СКЗИ в токене – отчуждаемый носитель или как персональное средство ЭП с неизвлекаемым ключом ЭП).

Один Secure MicroSD-токен для разных устройств

- Для работы на планшете, смартфоне, ноутбуке или персональном компьютере корпоративным 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.

Сравнение и выбор модели

	Смарт-карта	USB		MicroUSB	MicroSD
		Nano	XL		
Строгая аутентификация при подключении к корпоративным ресурсам предприятия (PKI)	●	●	●	●	●
Биометрическая идентификация владельца (опция BIO)	●	⚙	⚙	●	⚙
Обратная совместимость с продуктами компании Aladdin	●	●	●	●	●
Хранение ключевых контейнеров программных СКЗИ (КриптоПро CSP, VipNetCSP и др.)	●	●	●	●	●
Персональное средство ЭП с неизвлекаемым ключом ЭП (опция ГОСТ)	●	●	●	●	●
Дополнительная Flash-память для ОС, виртуальных машин, приложений и данных (опция Flash)	●	●	●	●	●

⚙ — Опция, доступна только в рамках согласованного проекта

● / ● — Недоступно/доступно для данного исполнения

Современный дизайн



Смарт-карты

Смарт-карты JaCarta PKI, как и платёжные карты Premium-класса, могут иметь эксклюзивный строгий дизайн. На чёрную пластиковую карту, имеющую матовую поверхность, устанавливается чип с палладиевыми контактами серебристого цвета. Смарт-карта рассчитана на интенсивное ежедневное использование.



Номер модели и серийный номер карты выдавлены с помощью эмбоссе-ра и также имеют серебристый цвет.



Для работы с картой понадобится любой стандартный **PC/SC-совместимый ридер** (считыватель смарт-карт).

Карта также может иметь нужный Вам тип **RFID-метки** (до двух в одной карте!) для интеграции с Вашей системой доступа в помещения (СКУД) и пр.

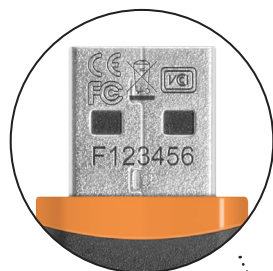


Кастомизация. Карты также можно заказывать в привычном белом пластике, печатать на них самостоятельно, либо заказать печать по согласованному дизайну у нас. Чипы при этом могут устанавливаться как с позолоченными контактами, так и с серебристыми (палладиевыми).



USB-токены в корпусе XL

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

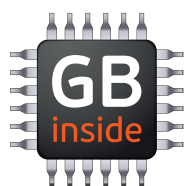


Лазерная гравировка уникального серийного номера ключа на металлическом разъёме делает невозможным подмену или стирание номера



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

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



Токен со встроенной Flash-памятью стал заметно компактнее. Благодаря новой архитектуре теперь он работает быстрее и меньше греется при интенсивной работе с Flash-памятью. Токены с дополнительной Flash-памятью (с голубой вставкой) имеют голубой светодиод, остальные – красный.

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

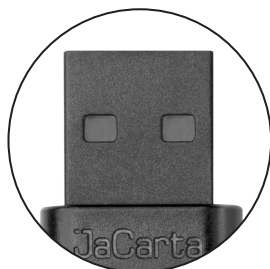


Кастомизация – для интеграции с системой СКУД в токен (в корпусе XL) можно добавить несколько **RFID-меток**. Тогда Ваш токен может стать ещё и ключом от офиса или пропуском на парковку.

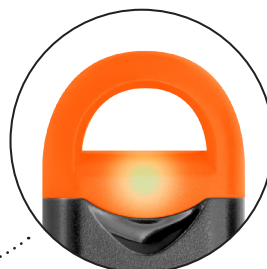


USB-токены в корпусе Nano – для пользователей ноутбуков

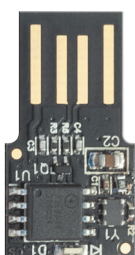
Для пользователей, часто работающих "в походных условиях", предназначена модель USB-токена в миниатюрном корпусе Nano. Уникальная запатентованная конструкция и стильный запоминающийся дизайн в виде навесного замка – у пользователей он хорошо ассоциируется с безопасностью!



Ресурс пластикового разъёма – 5,000 подключений, что соответствует примерно 5 годам активной эксплуатации (4 раза в день в течение 260 рабочих дней в году)



Удобство подключения и отсоединения токена от компьютера, надёжная фиксация его в разъёме.



Надёжная конструкция – очень важна при использовании токена в дорожных условиях.

Причина большинства поломок USB-устройств – отдельный разъём, припаиваемый к печатной плате токена. Здесь же разъём и плата токена – одно целое, сломать его в этом месте теперь практически невозможно.

Контактная группа USB-разъёма и самого токена здесь едины, а надёжность соединения внутри USB-разъёма обеспечивает пластиковая оправка, являющаяся частью корпуса токена. На ней же с помощью лазерной гравировки нанесён уникальный серийный номер токена.



Кастомизация.

Все токены имеют выделенное место на корпусе для размещения логотипа. Строго и дорого смотрится лазерная гравировка логотипа. Цветной логотип можно нанести методом тампо-печати. Он будет иметь повышенную стойкость к истиранию за счёт специальной микроструктуры корпуса токена и технологии нанесения краски.



Миниатюрные размеры – при подключении к ноутбуку токен выступает всего на 2 см, поэтому риск его механического повреждения минимален. Он никогда не будет мешать подключению других устройств, даже если разъёмы расположены очень близко, а устройство имеет неприлично большие размеры (как, например, в случае с GSM-модемами).



MicroUSB-токены – для пользователей мобильных устройств

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.

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.
- **Удобство в использовании для конечного пользователя** – пользователь применяет простой PIN-код или входит по отпечатку пальца.

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 уникальных биометрических характеристик (отпечаток пальца) для входа в ОС Microsoft Windows, домен или для доступа к сетевым информационным ресурсам
- Возможность использования цифровых сертификатов

Больше возможностей, больше инноваций



Больше памяти

Новые карты и токены JaCarta PKI имеют больше защищённой памяти для хранения ключевых контейнеров, цифровых сертификатов, профилей и данных.

Базовая модель JaCarta PKI имеет **объём доступной защищённой памяти ~50 Кб** – практически неограниченное количество ключей, ключевых контейнеров и сертификатов!

Быстрее

Благодаря новой архитектуре, используемой в USB-токенах с дополнительной Flash-памятью, **скорость работы** с ней достигла 18.8 Мб/с при чтении и 10.5 Мб/с при записи.

При этом существенно снижены энергопотребление и выделение тепла.

Удобнее

Установка драйвера для USB-токенов (и наших смарт-карт ридеров) в современных ОС (Microsoft Window Vista/7/2008/8/8.1, Linux, Mac OS X) **не требуется**, они работают через встроенный в эти ОС стандартный CCID-драйвер.

Ещё надёжнее

USB-токены JaCarta PKI имеют **повышенную пыле- и влагозащищённость**. Допускается хранение и использование токенов в постоянно пыльных или влажных помещениях.

Ещё безопаснее

Все семейство JaCarta PKI 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, при низких температурах и пониженной влажности воздуха.

Токены и смарт-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.



Больше новых функций

Гибкий набор требуемых функций обеспечивается за счёт широкого модельного ряда, нескольких форм-факторов, предназначенных **для разных сценариев** использования, набором **дополнительных опций** и возможностей **кастомизации**.

Расширить функциональность смарт-карт и токенов JaCarta также можно за счёт оперативной разработки и загрузки новых Java-приложений, которые будут исполняться процессором карты или токена.

Открытая архитектура и **промышленные стандарты** позволят **сделать это!**

Удобное управление

Для управления жизненным циклом всех токенов и смарт-карт JaCarta на предприятии можно использовать систему управления JaCarta Management System (JMS).

Совместимость и многоплатформенность

При проектировании новой платформы JaCarta наши инженеры уделяли огромное внимание поддержке новых карт и токенов не только **на различном "железе"**, **в различных ОС** (Microsoft Window, MAC OS X, Linux, Apple iOS, Google Android и др.), в приложениях ведущих вендоров (преимущественно **штатными средствами**), но и **преимственности** и **совместимости** с продуктами, ранее выпущенными компанией Aladdin, с существующей инсталляционной базой смарт-карт, токенов, приложений и систем управления.

Теперь и для мобильных платформ

Наличие в линейке JaCarta PKI первого в отрасли MicroUSB-токена, а также Secure MicroSD-токенов позволяет использовать функции стро-гой аутентификации практически на всех современных мобильных платформах - Apple iOS, Google Android, Linux, Microsoft Windows. При этом никаких ограничений по функциональности нет – все функции, доступные на Microsoft Windows/Linux/MAC OS X, будут доступны и на мобильных платформах.

Смарт-картами JaCarta PKI теперь можно пользоваться практически на всех современных мобильных платформах, включая и самую закрытую из всех – Apple iOS. Для этого достаточно приобрести специализированный карт-ридер, который также может работать и на Apple, и на Google Android, и на Microsoft Windows.

Аппаратная реализация национальной криптографии

JaCarta, как **универсальная платформа**, поддерживает полный набор как "западной" криптографии, так и российской и обеспечивает формирование усиленной квалифицированной ЭП с неизвлекаемым ключом ЭП. В отличие от программных СКЗИ, срок хранения закрытого ключа составляет **3 года** с возможностью регенерации самим пользователем.

Платформа, на которой сделано семейство JaCarta, также поддерживает украинскую (ДСТУ 4145-2002) и казахстанскую/СНГ националь-



ную криптографию (ГОСТ 34.310-2004).

Поддержка биометрии

Реализованная в продукте технология идентификации человека по отпечаткам пальца (Biometric Match-On-Card) может использоваться для:

- повышения удобства работы – вместо ввода PIN-кода при аутентификации и работы с электронной подписью (КриптоПро CSP);
- повышения надёжности аутентификации (как третий фактор);
- предотвращения использования карты/токена другим лицами.

Визуализация подписываемого документа

JaCarta предоставляет дополнительный сертифицированный программный интерфейс, который позволяет встроить токен в любое программное или программно-аппаратное решение с соблюдением всех требований закона "Об электронной подписи":

- визуализация подписываемого/подписанного электронного документа пользователю;
- формирование ЭП только после получения подтверждения от пользователя.

Доступность для любых компаний

Специальное программное решение JaCarta SecurLogon позволит организовать двухфакторную аутентификацию на основе токенов JaCarta PKI в любой компании, даже в той, в которой нет развёрнутой PKI-инфраструктуры или настроенного Active Directory. Это идеальное решение для простого и быстрого перехода от обычных паролей к более надёжным способам аутентификации на предприятии при небольших затратах на информационную безопасность.

Легендарная надёжность и качество

Наши токены до сих пор по 10-13 лет прекрасно работают у многих корпоративных и государственных заказчиков, заслуженно став синонимом качества.

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.

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.

Выбор модели из семейства JaCarta PKI

Модель, форм-фактор		Строгая аутентификация	Биометрическая идентификация	Обратная совместимость	Хранение ключевых контейнеров	Электронная подпись (по ГОСТу)	Дополнительная Flash-память
JaCarta PKI	USB-токен	●		⚙	●		
	Смарт-карта	●		⚙	●		
	MicroUSB-токен	●			●		
	Secure MicroSD						
JaCarta PKI/BIO	USB-токен	●	⚙		●		
	Смарт-карта	●	●		●		
	Secure MicroSD						
JaCarta PKI/ГОСТ	USB-токен	●			●	●	
	Смарт-карта	●			●	●	
	MicroUSB-токен	●			●	●	
	Secure MicroSD						
JaCarta PKI/BIO/ГОСТ	USB-токен	●	⚙		●	●	
	Смарт-карта	●	●		●	●	
	Secure MicroSD						
JaCarta PKI/Flash	USB-токен	●			●		●
	Смарт-карта						
	Secure MicroSD	●			●		●
JaCarta PKI/BIO/Flash	USB-токен	●	⚙		●		●
	Смарт-карта						
	Secure MicroSD	●	⚙		●		●
JaCarta PKI/ГОСТ/Flash	USB-токен	●			●	●	●
	Смарт-карта						
	Secure MicroSD	●			●	●	●
JaCarta PKI/BIO/ГОСТ/Flash	USB-токен	●	⚙		●	●	●
	Смарт-карта						
	Secure MicroSD	●	⚙		●	●	●

● — поддерживаемая функциональность

⚙ — возможная функциональность для данного форм-фактора, обеспечивается на заказ и требует предварительного согласования

Чёрным цветом выделены базовые (рекомендованные) модели, серым — выпускаемые на заказ под согласованные с компанией "Аладдин РД." проекты, жирным выделены рекомендуемые форм-факторы для каждой модели.

Модели семейства JaCarta PKI



MicroUSB-токен



USB-токен в корпусе Nano



USB-токен в корпусе XL



Смарт-карта

JaCarta PKI

USB-токен/MicroUSB-токен/смарт-карта для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ, профилей и паролей.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Хранение ключевых контейнеров практически для всех программных СКЗИ (КриптоПро CSP, VipNet CSP и др.).
- Сертификат соответствия ФСТЭК России № 2799 (средство аутентификации и безопасного хранения данных для Microsoft Windows и Linux).

Особенности

JaCarta PKI – базовая, или основная, модель семейства. Её функциональности обычно бывает достаточно для 60–70% выполняемых проектов.

Выпускается в трёх базовых форм-факторах: USB-токен (в корпусе XL и Nano), MicroUSB-токен и смарт-карта (чёрный пластик, чип с палладиевыми контактами).

Если предполагается использование смарт-карты или токена JaCarta PKI вместе с продуктами, ранее выпущенными компанией Aladdin, или в уже созданной инфраструктуре с имеющимися в эксплуатации продуктами компании, то следует выбрать опцию "Обратная совместимость с продуктами Aladdin".

Эту опцию не рекомендуется использовать для новых проектов, где нет необходимости обеспечивать совместимость с ранее выпущенными продуктами компании Aladdin.

MicroUSB-токен рекомендуется использовать для пользователей мобильных устройств под управлением ОС Google Android, Microsoft Windows и Linux (телефоны, смартфоны, планшеты, терминальное оборудование и др.).

Рекомендуется

Для работы со смарт-картами со стационарного компьютера рекомендуется использовать офисные карт-ридеры ASEDrive IIIe USB, с ноутбуками – компактные ASEDrive III USB Mini.

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



USB-токен в корпусе XL



Смарт-карта

JaCarta PKI/BIO

Смарт-карта/USB-токен для строгой двух- и трёхфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ, профилей и паролей.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Биометрическая идентификация владельца карты (токена) по отпечаткам пальцев (Match-On-Card), может использоваться в дополнение к PIN-коду или вместо него.
- Хранение ключевых контейнеров практически для всех программных СКЗИ (КриптоПро CSP, VipNet CSP и др.).
- Сертификат соответствия ФСТЭК России № 2799.

Особенности

JaCarta BIO выполнена на базе модели JaCarta PKI с дополнительной опцией поддержки биометрии.

Рекомендуется использовать в проектах, где необходимо кардинально снизить риски получения несанкционированного доступа к критически важной информации, не допустить использования карт в отсутствие их владельцев (неотчуждаемость носителя), снизить время аутентификации, упростить жизнь руководству и ТОП-менеджерам, избавив их от ввода сложных паролей и их периодической смены.

Основным (рекомендуемым) форм-фактором JaCarta PKI/BIO является смарт-карта.

USB-токены также могут работать с биометрией, однако понадобится предварительное тестирование используемых сканеров (например, встроенных в ноутбуки или клавиатуры) на предмет совместимости.

Рекомендуется

Для работы с биометрией рекомендуется использовать смарт-карт-ридеры со встроенным сканером отпечатков пальцев ASEDrive BIO (ASEDrive IIIe Bio Combo, ASEDdrive IIIe Bio Combo Swipe).

Для работы с биометрией также могут использоваться другие современные полупроводниковые сканеры (не оптические!), встроенные в карт-ридеры, клавиатуры с карт-ридером, некоторые ТОПовые модели ноутбуков.



MicroUSB-токен



USB-токен в корпусе Nano



USB-токен в корпусе XL



Смарт-карта

JaCarta PKI/ГОСТ

PKI-токен/смарт-карта для работы с усиленной квалифицированной электронной подписью и строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам, безопасного хранения ключей, ключевых контейнеров программных СКЗИ и профилей.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП.
- Сертификаты соответствия ФСБ России № СФ/124-2380, СФ/121-2270 и СФ/121-2350.
- Сертификат соответствия ФСТЭК России № 2799.

Особенности

Модель JaCarta PKI/ГОСТ ориентирована на компании, развернувшие инфраструктуру открытых ключей (PKI) и внедряющие систему юридически значимого электронного документооборота.

Выпускается в трёх базовых форм-факторах: USB-токен (в корпусе XL и Nano), MicroUSB-токен смарт-карта (чёрный пластик, чип с палладиевыми контактами).

MicroUSB-токен рекомендуется использовать для пользователей мобильных устройств под управлением ОС Google Android, Microsoft Windows и Linux (телефоны, смартфоны, планшеты, терминальное оборудование и др.).

Рекомендуется

Использовать дополнительный программный интерфейс, который позволяет встроить токен в любое программное или программно-аппаратное решение с соблюдением всех требований закона об ЭП.

Для работы со смарт-картами со стационарного компьютера рекомендуется использовать офисные карт-ридеры ASEDrive IIIe USB, с ноутбуками – компактные ASEDrive III USB Mini.

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

JaCarta PKI/BIO/ГОСТ



USB-токен в корпусе XL



Смарт-карта

Смарт-карта/USB-токен для работы с электронной подписью в системах электронного документооборота и строгой двух- и трёхфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ, профилей и паролей.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП.
- Биометрическая идентификация владельца карты (токена) по отпечаткам пальцев (Match-On-Card), может использоваться в дополнение к PIN-коду или вместо него.
- Хранение ключевых контейнеров практически для всех программных СКЗИ (КриптоПро CSP, VipNet CSP и др.), а также использования в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов (в т.ч. КриптоПро CSP, VipNet CSP, Lissi CSP в режиме ЭП с неизвлекаемым ключом).
- Сертификаты соответствия ФСБ России № СФ/124-2380, СФ/121-2270 и СФ/121-2350.
- Сертификат соответствия ФСТЭК России № 2799.

Особенности

Модель JaCarta PKI/BIO/ГОСТ сделана на базе модели JaCarta PKI/ГОСТ с дополнительной опцией поддержки биометрии. Она ориентирована на компании, развернувшие инфраструктуру открытых ключей (PKI) и внедряющие систему юридически значимого электронного документооборота.

Рекомендуется использовать в проектах, где необходимо кардинально снизить риски получения несанкционированного доступа к критически важной информации, гарантировать физическое присутствие подписанта документа в момент совершения операции (неотчуждаемость носителя от его владельца), снизить время аутентификации, упростить жизнь руководству и ТОП-менеджменту, избавив их от ввода и периодической смены сложных паролей.

Основным (рекомендуемым) форм-фактором JaCarta PKI/BIO/ГОСТ является **смарт-карта**.

USB-токены также могут работать с биометрией, однако понадобится предварительное тестирование используемых сканеров (например, встроенных в ноутбуки) на предмет совместимости.

Рекомендуется

Использовать дополнительный программный интерфейс, который позволяет встроить токен в любое программное или программно-аппаратное решение с соблюдением всех требований закона об ЭП.

Для работы с биометрией рекомендуется использовать считыватели смарт-карт со встроенным сканером отпечатков пальцев ASEDrive BIO.



USB-считыватель с MicroSD



USB-токен в корпусе XL

JaCarta PKI/Flash, JaCarta PKI/BIO/Flash

Комбинированный PKI-токен с дополнительной Flash-памятью для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ, профилей и паролей.

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

Модель JaCarta PKI/BIO/Flash имеет дополнительную опцию поддержки биометрической идентификации владельца токена по отпечаткам пальцев (технология Match-On-Card), которая может использоваться в дополнение к PIN-коду или вместо него.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Хранение ключевых контейнеров практически для всех программных СКЗИ (КриптоПро CSP, VipNet CSP и др.).
- Flash-память объёмом 2, 4 и 8 Гб.
- Сертификат соответствия ФСТЭК России № 2799 (средство аутентификации и безопасного хранения данных для Microsoft Windows и Linux).

Особенности

Эту модель рекомендуется использовать для удалённых (мобильных) пользователей, администраторов, когда необходимо снизить риски получения несанкционированного доступа к критически важной информации при работе из недоверенной среды, использования в качестве удобного средства доступа в корпоративную сеть и служебной Flash-карты.

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).

Рекомендуется

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



USB-считыватель с MicroSD



Считыватель с MicroSD



USB-токен в корпусе XL

JaCarta PKI/ГОСТ/Flash, JaCarta PKI/BIO/ГОСТ/Flash

Комбинированный PKI-токен с дополнительной Flash-памятью для работы с усиленной квалифицированной электронной подписью в системах электронного документооборота и строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ, профилей и паролей.

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

Модель JaCarta PKI/BIO/ГОСТ/Flash имеет дополнительную опцию поддержки биометрии для идентификации владельца токена по отпечаткам пальцев (технология Match-On-Card), которая может использоваться в дополнение к PIN-коду или вместо него.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Формирование и проверка усиленной квалифицированной электронной подписи с неизвлекаемым ключом ЭП.
- Хранение ключевых контейнеров практически для всех программных СКЗИ (КриптоПро CSP, VipNet CSP и др.).
- Flash-память объёмом 2, 4 и 8 Гб.
- Сертификат соответствия ФСБ России № СФ/124-2380, СФ/121-2270 и СФ/121-2350.
- Сертификат соответствия ФСТЭК России № 2799 (средство аутентификации и безопасного хранения данных для Microsoft Windows и Linux).

Особенности

Эту модель рекомендуется использовать для удалённых (мобильных) пользователей, администраторов, когда необходимо снизить риски получения несанкционированного доступа к информации и к ЭП при работе из недоверенной среды, использования в качестве удобного средства доступа в корпоративную сеть, персонального средства ЭП и служебной Flash-карты.

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).

Рекомендуется

Использовать дополнительный программный интерфейс, который позволяет встроить токен в любое программное или программно-аппаратное решение с соблюдением всех требований закона об ЭП.

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

Смарт-карт ридеры

Использование смарт-карт подразумевает применение смарт-карт ридеров.

19-летний опыт работы компании "Аладдин Р.Д." на этом рынке позволил качественно проработать предложение для каждого сценария применения и предложить лучшее, что есть на рынке.

Для использования в офисе



ASEDrive IIIe USB

- Подключение – к USB-порту
- Повышенная надёжность и долговечность контактной группы, не портящей внешний вид карты
- Поддержка карт с эмбоссированием
- Цвет: светлый (бежевый), чёрный (опция)
- CCID-совместимый (установка драйвера устройства не требуется)
- Поддерживаемые платформы: Microsoft Windows, Linux, Mac OS X
- Выпускается компанией "Аладдин Р.Д." по лицензии и технологии компании Athena Smartcard Solutions (Япония)

Для использования с ноутбуками (для мобильных пользователей)



ASEDrive III USB Mini

- Подключение – к USB-порту (через отсоединяемый кабель)
- Лёгкий и компактный, чуть больше самой смарт-карты
- Поддержка карт с эмбоссированием
- Цвет: чёрный
- CCID-совместимый (установка драйвера устройства не требуется)
- Поддерживаемые платформы: Microsoft Windows, Linux, Mac OS X
- Выпускается компанией "Аладдин Р.Д." по лицензии и технологии компании Athena Smartcard Solutions (Япония)

Клавиатура со смарт-карт ридером и сканером отпечатков пальцев



ASEDrive IIIe Bio Keyboard

- Подключение – к USB-порту
- Сканер – полноразмерная полупроводниковая матрица (Touch)
- Загрузка смарт-карты – вертикальная
- Поддержка карт с эмбоссированием
- Цвет: чёрный, светлый (опция)
- CCID-совместимый карт-ридер (установка драйвера устройства не требуется)



ASEDrive IIIe Bio Combo

Ридер со встроенным сканером отпечатков пальцев для топ-менеджеров

- Подключение – к USB-порту
- Сканер – полноразмерная полупроводниковая матрица (Touch)
- Загрузка смарт-карты – вертикальная
- Поддержка карт с эмbossированием
- Цвет: чёрный
- CCID-совместимый (установка драйвера устройства не требуется)



ASEDrive IIIe Bio Combo Swipe

Ридер со встроенным сканером отпечатков пальцев для офисных сотрудников

- Подключение к USB-порту
- Сканер отпечатков пальцев со swipe-сенсором
- Загрузка смарт-карты горизонтальная
- Поддержка карт с эмbossированием
- Цвет: чёрный
- CCID-совместимый (установка драйвера устройства не требуется)



iR-301UL

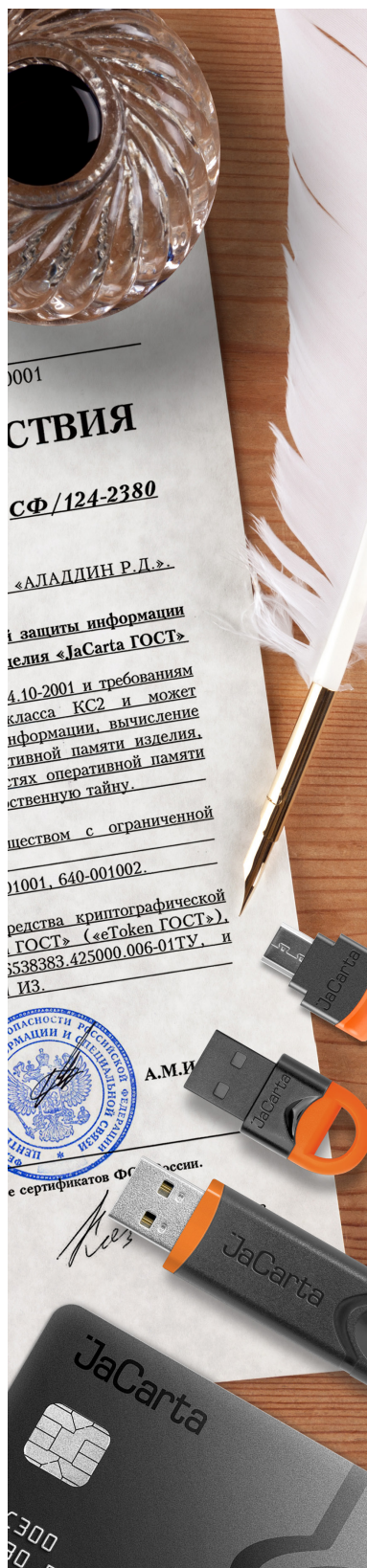
Смарт-карт ридер для мобильной платформы Apple iOS

- Apple iOS – для работы с картой с российской криптографией Jailbreak не требуется
- При подключении к компьютеру работает как обычный CCID-совместимый карт-ридер (установка драйвера устройства не требуется)
- Поддержка карт с эмbossированием
- Сертифицирован по EMV Level 1 (Pay&Sign), может использоваться для работы с платёжными картами
- Производится OEM-партнёром компании "Аладдин Р.Д." – Feitian Technologies
- Встроенное программное обеспечение считывателя (Firmware) поддерживает работу с картами с российской криптографией "на борту" и отличается от стандартной, предлагаемой компанией Feitian



iR-301U

Сертификаты



- **Сертификат соответствия ФСТЭК России № 2799** подтверждает, что смарт-карты и токены семейства JaCarta PKI являются средством аутентификации и безопасного хранения пользовательских данных.

Действие сертификата распространяется на Microsoft Windows XP/Vista/7/8/2003/2008 и Linux (RedHat, Ubuntu, CentOS, "Циркон" и др. дистрибутивы, соответствующие спецификации Linux Standard Base 3.1).

Смарт-карты и токены JaCarta PKI могут использоваться в ИСПДн до 1-го класса включительно.

- **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, утвержденным 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".
- **Сертификат соответствия ФСБ России № СФ/121-2270** подтверждает, что смарт-карты и USB-токены (имеющие в названии опцию ГОСТ) соответствуют требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 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/124-2380** подтверждает, что реализованная в смарт-картах и токенах (имеющих в названии /ГОСТ) 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.
- **Международные сертификаты безопасности**, допускающие ввоз и эксплуатацию JaCarta PKI 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** (устройства не являются источником электромагнитных помех, которые могут повлиять на работу другого электронного оборудования, и полностью соответствует международным требованиям в части уровня электромагнитных помех радиоустройствам).

- **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.
- **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).
- **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 влажных помещениях.

Технические подробности



Поддерживаемые криптографические алгоритмы

Для моделей PKI, BIO:

- AES (длины ключей 128, 192, 256 бит)
- DES (длина ключа 56 бит)
- 3DES (длины ключей 112 и 168 бит)
- RSA (длины ключей 512, 1024, 2048)
- Криптография на эллиптических кривых (длины ключей 160, 192 бит)
- Аппаратная генерация ключей для RSA
- Алгоритмы согласования ключей: алгоритм Диффи-Хеллмана, алгоритм Диффи-Хеллмана на эллиптических кривых
- Функции хэширования: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- Генератор последовательностей случайных чисел

Для моделей с опцией "Обратная совместимость с продуктами Aladdin":

- 3DES (длина ключа 168 бит)
- RSA (длина ключа 1024 и 2048)
- Аппаратная генерация ключей для RSA
- Функции хэширования: SHA-1 (160 бит)
- Генератор последовательностей случайных чисел

Для моделей с опцией ГОСТ:

- 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)
- 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 PKI 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 X	Apple iOS	Google Android
PKI	APDU PKCS #11 (#7, #10) MS CAPI (CSP, CNG)	APDU PKCS #11 (#7, #10)				
BIO	PKCS #11 (#7, #10)					
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)	PKCS #11 (#7, #10)	PKCS #11 (#7, #10)

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

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 PKI-токенов

- JaCarta Management System (JMS) – система управления полностью поддерживающая работу с JaCarta, а так же с eToken.
- SafeNet Authentication Manager (SAM) – только для моделей с обратной совместимостью с продуктами компании Aladdin

Нам доверяют

Российская компания "Аладдин Р.Д." является признанным экспертом и лидером рынка средств строгой двух-факторной 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.

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 – награда от Аппарата Совета Безопасности РФ, Комитета Государственной Думы по безопасности.



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/ИСО 9001-2011
 Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00079 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.

