

# РУТОКЕН®

## РОССИЙСКОЕ СРЕДСТВО АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ИНФОРМАЦИИ



- Безопасное хранение ключей шифрования и ЭЦП, паролей и цифровых сертификатов
- Надежная аппаратная аутентификация при доступе к защищенным ресурсам
- Российские криптографические алгоритмы и международные стандарты безопасности



совместная разработка компаний «Актив» и «АнКАД»

# РУТОКЕН®

Сделан в России, сделан для России



Электронный идентификатор Рутокен — персональное устройство доступа к информационным ресурсам, полнофункциональный аналог смарт-карты, выполненный в виде USB-брелока. Рутокен предназначен для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и ЭЦП.

**Новый уровень информационной безопасности.** Современные сетевые операционные системы содержат мощные средства для обеспечения информационной безопасности, применение Рутокен позволяет использовать эти возможности в полную силу. Вход в сеть, защита электронной переписки и шифрование данных могут осуществляться на основе цифровых сертификатов, хранящихся в защищенной памяти Рутокен. При этом существенно повышается защищенность сети и удобство работы пользователей.

**Эlegantное решение проблемы слабых паролей.** При использовании Рутокен не нужно запоминать длинные и сложные пароли, они хранятся в токене. Множество разных паролей, ключей шифрования, сертификатов могут содержаться в памяти токена, пользователь должен помнить только один PIN-код.

**Удобство и универсальность.** Для несведущего человека Рутокен — просто красивый брелок для ключей. Это легкое, прочное устройство. Использовать Рутокен удобно и просто. У большинства современных компьютеров USB-порт выведен на переднюю панель. Один токен может одновременно использоваться различными приложениями.

**Защищенность.** Информация хранится в защищенной файловой системе Рутокен. Существуют три уровня доступа — гость, пользователь и администратор. Доступ к памяти защищен PIN-кодами. Если пользователь потерял токен, то нашедший его злоумышленник не сможет им воспользоваться. Корпус Рутокен имеет защиту от механического воздействия: его невозможно снять, не разрушив при этом.

**Уникальность.** Каждый Рутокен имеет 32-битный уникальный номер, доступный только для чтения. Все содержимое файловой системы шифруется на основе данных, индивидуальных для каждого экземпляра устройства.

**Корпоративное использование.** Рутокен может выступать как единое устройство для доступа ко всем ресурсам корпоративной сети: надежная двухфакторная аутентификация пользователей; хранение в памяти Рутокен ключей шифрования, паролей и сертификатов; защита электронной почты (ЭЦП, шифрование); сокращение организационных затрат (например, чтобы лишить сотрудника прав доступа к ресурсам сети, достаточно просто изъять его токен).

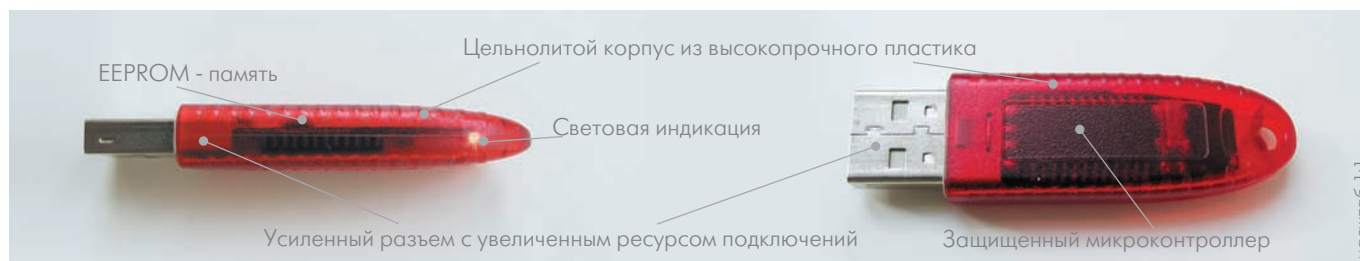
**Реальная криптография.** Рутокен содержит аппаратную реализацию российского алгоритма шифрования ГОСТ 28147-89. Ключи шифрования могут быть созданы самим токеном без возможности экспорта за его пределы.

**Поддержка промышленных стандартов.** Рутокен поддерживает стандарт PC/SC, стандарты PKCS#11, MS CryptAPI, X.509. Это позволяет без труда встраивать Рутокен в уже существующие системы безопасности.

**Российский токен.** Рутокен разработан и производится в Москве. В нем используются российские стандарты шифрования. Это позволяет создавать на базе идентификаторов Рутокен системы информационной безопасности в соответствии с российским законодательством. Рутокен — единственное средство аутентификации, сертифицированное ФСБ РФ.

# Подробная техническая информация

## Обзор технических характеристик и ПО Рутокен



### Основные характеристики

- Базирован на защищенном микроконтроллере
- Интерфейс USB (USB 1.1 / USB 2.0)
- EEPROM память: 32, 64 и 128 Кб
- Габаритные размеры: 58x16x8 мм
- Масса: 6,3 г
- Поддерживаемые операционные системы:
  - Windows 7/2008/Vista/2003/XP/2000/ME/98
  - Linux, Mac OS X
- Поддержка стандартов:
  - ISO/IEC 7816
  - PC/SC
  - Microsoft Crypto API и Smartcard API
  - PKCS#11
- 32-битовый уникальный серийный номер
- Возможность присвоения токenu символического имени для упрощения его визуальной идентификации
- Индивидуальная маркировка каждого токена. Наносится на боковую поверхность корпуса, удаление невозможно без видимых повреждений поверхности

### Поддержка ГОСТ 28147-89

- Аппаратная реализация российского алгоритма шифрования ГОСТ 28147-89
- Шифрование внешних данных по ГОСТ 28147-89 в любом из 3 режимов:
  - простая замена
  - гаммирование
  - гаммирование с обратной связью
- Выработка 32-битовой имитовставки по ГОСТ 28147-89
- Генерация 256-битовых случайных чисел
- Защищенное хранение ключей шифрования ГОСТ 28147-89 в объектах данных без возможности их экспорта из токена
- Возможность импорта ключей шифрования ГОСТ 28147-89

### Файловая система Рутокен

- Встроенная файловая система по стандарту ISO/IEC 7816
- Прозрачное шифрование всей файловой системы по ГОСТ 28147-89 на основе данных, уникальных для каждого экземпляра Рутокен
- Объекты данных для security-ориентированных операций
- Свойства, права доступа и атрибуты безопасности для каждого объекта файловой системы Рутокен: папки, файла и объекта данных
- Количество создаваемых папок и уровень их вложенности ограничивается только объемом памяти
- Предопределенные папки для объектов данных разных типов для повышения удобства использования
- Автоматический поиск объекта данных в памяти токена на основе типа и имени объекта

### Аутентификация и конфиденциальность

- 2-факторная аутентификация (по факту наличия Рутокен и по факту предъявления PIN-кода)
- PIN-коды Пользователя и Администратора
- Ограничение числа попыток аутентификации с предъявлением PIN-кода
- Разграничение прав Пользователя и Администратора
- Возможность назначения 3-х разных политик смены PIN-кода Пользователя

### Дополнительные возможности

- Поддержка стандарта X.509 и международных криптоалгоритмов
- Защищенное хранение ключей асимметричного шифрования и ЭЦП, цифровых сертификатов
- Возможность использования Рутокен для асимметричного шифрования данных и для работы с цифровыми сертификатами из любых smartcard-приложений, поддерживающих стандарт PC/SC



# РУТОКЕН®

для Microsoft® Windows® 2000/XP/2003/Vista/2008



Рутокен для Windows — это готовое решение, которое позволяет за короткий срок внедрить аппаратную авторизацию пользователей и защиту электронной переписки в сетях на базе Windows 2000/XP/2003/Vista/2008. Решение построено на применении встроенных инструментов безопасности Windows и электронных идентификаторов Рутокен в качестве носителей ключевой информации.

Данный продукт могут использовать любые организации и предприятия, информационная структура которых построена на базе сетей Microsoft Windows. Для развертывания и последующей эксплуатации решения Рутокен для Windows не требуется привлечения сторонних специалистов и приобретения дополнительного оборудования и программного обеспечения третьих фирм. Все необходимые настройки сети может выполнить штатный системный администратор предприятия, следуя подробным инструкциям, содержащимся в Руководстве по внедрению Рутокен для Windows.

## Комплект поставки

- CD с программным обеспечением и электронной документацией
- Печатное руководство «Приступая к работе»
- Рутокен 32 Kb
- Лицензия на использование продукта в пределах одной организации

## Системные требования

### Серверная часть

- Windows 2000/2003/2008 Server, настроенный как контроллер домена, с установленными Службами Интернета(IIS)
- Exchange Server, интегрированный с Active Directory\*

### Клиентская часть

- Операционная система Windows 2000/XP Pro/Vista
- Свободный USB-порт
- Почтовый клиент Microsoft Outlook\*

\* — необходимо для работы с защищенной электронной почтой

## Авторизация пользователей в сетях и на рабочих станциях

- Вход в домен по предъявлению токена
- Подключение к терминальному серверу по предъявлению токена
- Блокирование сессии пользователя после отсоединения токена

## Безопасность электронной переписки

- Электронная цифровая подпись почтовых сообщений
- Шифрование почтовых сообщений

## Защищенный удаленный доступ к корпоративным и информационным ресурсам

- Безопасное подключение к сетям VPN
- Безопасная связь с защищенными веб-ресурсами

## Надежное хранение и безопасное использование паролей, ключей шифрования и ЭЦП

- Применение Рутокен в качестве защищенного хранилища ключевой информации пользователя информационной системы

Вся ключевая информация хранится в защищенной памяти Рутокен. Пользователю не нужно запоминать сложные, длинные пароли, нужно лишь подключить Рутокен к USB-порту компьютера и ввести PIN-код. После отсоединения токена рабочая сессия автоматически блокируется. Использовать Рутокен просто, обучение персонала займет минимум времени.



# РУТОКЕН RF<sup>®</sup>

Пропуск в помещение + доступ к данным  
USB-токен со встроенной RFID-меткой



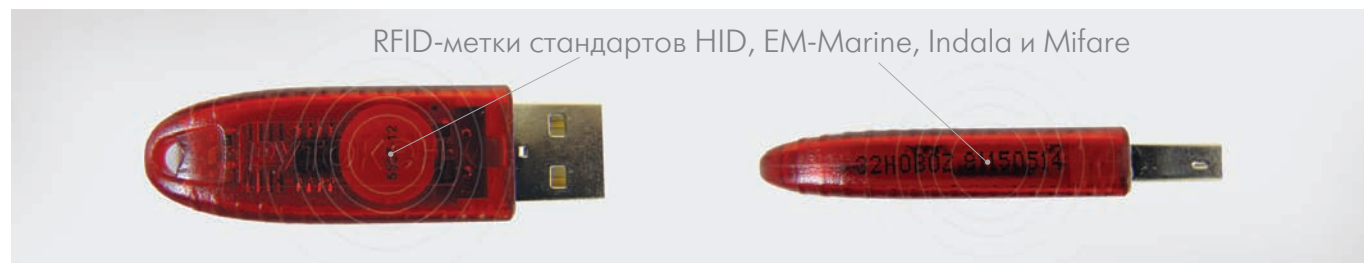
Рутокен RF — это USB-токен со встроенной радиочастотной меткой (RFID-меткой). Он предназначен для доступа пользователей к информационным ресурсам компьютера и для физического доступа в здания и помещения.

Рутокен RF объединяет возможности, предоставляемые USB-токенами, смарт-картами и бесконтактными электронными пропусками:

- Строгая двухфакторная аутентификация при доступе к компьютеру и защищенным информационным ресурсам
- Безопасное хранение криптографических ключей и цифровых сертификатов
- Применение в системах контроля и управления доступом, в системах учета рабочего времени и аудита перемещений сотрудников
- Использование в виде пропуска для электронных проходных



Рутокен RF представляет собой бюджетное, простое в эксплуатации комбинированное устройство идентификации. Бесконтактный пропуск для выхода из помещения и средство доступа в компьютерную сеть объединены в одном брелоке. Система безопасности может быть сконфигурирована так, что сотрудник просто физически не сможет оставить доступ к конфиденциальной информации. Для выхода из помещения необходимо предъявить Рутокен RF, а при отключении идентификатора от USB-порта компьютера пользовательская сессия автоматически блокируется.



Рутокен RF обладает всеми возможностями «обычных» электронных идентификаторов Рутокен и совместим с готовыми решениями на основе Рутокен.

Рутокен RF прекрасно подходит для любых предприятий и организаций, которые хотят повысить комплексную безопасность за счет использования единого устройства доступа в помещения и к данным на компьютерах.

RFID-метки стандарта EM-Marine — наиболее распространенные метки в России. На сегодняшний день, считыватели, совместимые с ними, установлены в большинстве существующих систем контроля доступа (СКД). RFID-технологии стандарта HID широко применяются в крупных компаниях и корпорациях. В большинстве случаев, если в вашей организации есть СКД — она поддерживает Рутокен RF.

# Рутокен в массовых проектах

Сотни тысяч идентификаторов Рутокен используются по всей России. Благодаря высокому качеству и конкурентоспособной цене российские USB-токены востребованы в массовых проектах, масштабы которых измеряются многими тысячами пользователей. В этих проектах Рутокен используются для аутентификации, хранения и использования ключей электронной цифровой подписи. Для многих наших партнеров и заказчиков мы поставляем токены в индивидуальном исполнении.



## Компания СКБ Контур, проект Контур-Экстерн

«Контур-Экстерн» — крупнейшая по охвату абонентов в России система передачи электронной отчетности предприятий во все государственные контролирующие органы, разработанная федеральной IT-компанией СКБ Контур. Компания владеет самым крупным по количеству выданных сертификатов ЭЦП удостоверяющим центром в стране. Уже более 100 тыс. абонентов «Контур-Экстерн» используют Рутокен.



## Альфа-Банк, проект Альфа-Директ

«Альфа-Директ» — многофункциональная система интернет-трейдинга, разработанная специалистами Альфа-Банка. ЭЦП является важным фактором, обеспечивающим высокий уровень безопасности совершения операций в системе. Все финансово значимые приказы клиентов подписываются электронной цифровой подписью.



## БТА Банк

В ООО «БТА Банк» (Россия) успешно завершён проект внедрения дистанционных сервисов обслуживания юридических лиц. Основным элементом хранения секретных ключей ЭЦП и кодов аутентификации удаленного обслуживания БТА Банка является электронный идентификатор Рутокен.



## Электронная Москва

ОАО «Электронная Москва» создано в целях активного внедрения современных информационных технологий, дальнейшего развития информационно-коммуникационной инфраструктуры города Москвы, обеспечения доступа москвичей к сформированным информационным ресурсам. Удостоверяющий центр ОАО «Электронная Москва» является Уполномоченным удостоверяющим центром органов исполнительной власти города Москвы.

Идентификаторы Рутокен широко используют в своих крупных проектах наши партнеры: Крипто-Про, Цифровые технологии, Такском, SecurIT, Роста, Газинформсервис и другие. Масштабные проекты были развернуты в АКБ «Союз», группе компаний «Связной», «ИНГ БАНК». Идентификаторы Рутокен активно применяются в государственных проектах, использующих технологии ЭЦП. Среди них Казначейство РФ, Верховный суд РФ, Минздравсоцразвития РФ, Электронное правительство Республики Татарстан, Управление печати Республики Башкортостан, Администрация Калужской области и многие другие.

# Сертифицированная продукция

Продукция Рутокен имеет сертификаты ФСТЭК и ФСБ. Наличие сертификатов обеспечивает широкому спектру государственных заказчиков возможность успешного прохождения аттестации рабочих мест сотрудников, которые по роду своей деятельности имеют доступ к информации ограниченного характера. Сертифицированная продукция Рутокен предназначена для коммерческих организаций, чья политика в области информационной безопасности формируется в соответствии с отраслевыми и национальными стандартами. Сертифицированные идентификаторы Рутокен и программное обеспечение Рутокен будут полезны в проектах, связанных с защитой персональных данных.

## Сертификат №СФ/124-0999 ФСБ России

Выдан: 10 мая 2007 г. Действителен до: 10 мая 2010 г.

Сертификат удостоверяет, что аппаратно-программное средство криптографической защиты информации (СКЗИ) «Rutoken» в составе согласно формуляру КБЖД.468244.033 ФО соответствует требованиям ГОСТ 28147-89 и требованиям ФСБ России к СКЗИ класса КС2 и может использоваться для шифрования и имитозащиты информации, не содержащей сведений, составляющих государственную тайну.

## Сертификат №1461 ФСТЭК России

Выдан: 18 сентября 2007 г. Действителен до: 18 сентября 2010 г.

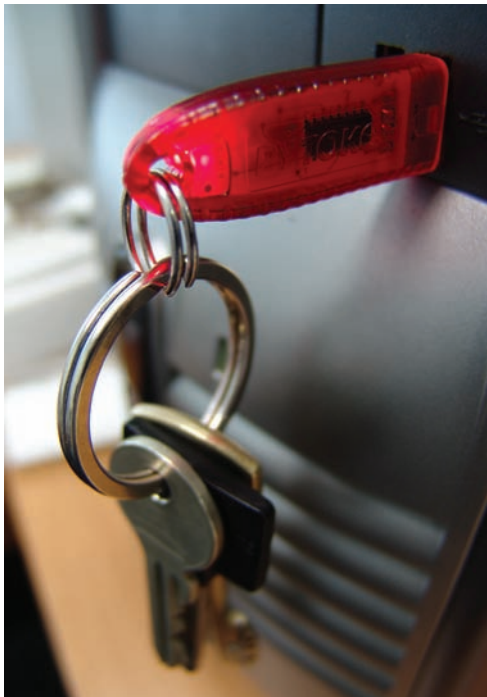
Настоящий сертификат удостоверяет, что в системном программном обеспечении (микропрограмме) Rutoken нет программных закладок и недеklarированных возможностей. Сертификат соответствия по 3-му уровню контроля отсутствия НДВ. Разрешает использовать электронные идентификаторы Рутокен при работе с информацией, имеющей гриф «Секретно», и в системах, обрабатывающих конфиденциальную информацию.

## Сертификат №1395 ФСТЭК России

Выдан: 30 мая 2007 г. Действителен до: 30 мая 2010 г.

Удостоверяет, что в прикладном программном обеспечении Рутокен нет программных закладок и недеklarированных возможностей. Сертификат по 3-му уровню контроля отсутствия НДВ. Разрешает использовать ПО Rutoken при работе с информацией, имеющей гриф «Секретно», и в системах, обрабатывающих конфиденциальную информацию.





Рутокен — универсальное устройство, предназначенное для решения широкого круга задач: программно-аппаратная аутентификация при подключении к сети; защищенные соединения при доступе к базам данных и web-ресурсам; криптографическая защита информации; разграничение доступа к компьютеру; защита электронной переписки; хранение и использование ЭЦП в системах юридически значимого документооборота.

### Рутокен для КристоПро CSP

Программный продукт, позволяющий пользователям криптографического сервис-провайдера (CSP) компании Кристо-Про обезопасить ключевую информацию от несанкционированного использования. Ключи и сертификаты хранятся в защищенной файловой системе Рутокен. Это бесплатное решение, любой легальный пользователь CSP КристоПро может загрузить его по адресу [www.rutoken.ru/download](http://www.rutoken.ru/download)

### Продукты технологических партнеров

Электронные идентификаторы Рутокен поддерживаются ведущими российскими разработчиками систем информационной безопасности. Полный список наших технологических партнеров и подробные описания их продуктов вы можете найти на сайте [www.rutoken.ru](http://www.rutoken.ru)

## Комплект разработчика Рутокен

Комплект разработчика Рутокен предназначен для разработчиков и системных интеграторов в области информационной безопасности. Содержит все необходимое, чтобы встроить поддержку Рутокен в собственные программные продукты и интегрировать Рутокен в уже существующие приложения. Комплект разработчика включает два электронных идентификатора Рутокен, подробную документацию и набор программного обеспечения.



## Рутокен — совместная разработка компаний «Актив» и «Анкад»

**Компания «Актив»** — разработчик и производитель программно-аппаратных средств информационной безопасности. Основная продукция — электронные ключи Guardant® ([www.guardant.ru](http://www.guardant.ru)) и идентификаторы Рутокен® ([www.rutoken.ru](http://www.rutoken.ru)). Компания является самым крупным производителем подобных устройств в России.

**Фирма «Анкад»** основана в 1991г. и специализируется на разработке, производстве, поставках и обслуживании аппаратных и программных средств информационной безопасности. Сферы деятельности: криптографическая защита информации, защита информации от несанкционированного доступа, технологии смарт-карт, электронная цифровая подпись, защита Интернет-коммуникаций, заказное проектирование. Фирма «Анкад» действует на основании лицензий ФСБ, ФСТЭК и МО.