123056, Россия, г. Москва
ул. Красина, д.3, компания Актив
тел./факс: (095) 105-77-90

1. Что такое ruToken

ruToken относится к классу устройств, называемых электронными идентификаторами. Он представляет собой малогабаритное устройство в виде брелока с интерфейсом USB и может быть использован во всех приложениях, где ранее использовались пароли, смарт-карты и другие идентификаторы.

ruToken обладает всеми свойствами смарт-карт: он обеспечивает **надежность, простоту, безопасность** процесса **идентификации**.

Однако, в отличие от смарт-карт, токен обладает несомненным преимуществом: он не требует применения считывателей, что делает его гораздо более удобным в использовании. Порты USB в настоящее время имеются даже у персональных компьютеров начального уровня, поэтому токены могут использоваться самым широким кругом пользователей в самых различных условиях.

Поскольку архитектура токена основана на микропроцессоре, способном производить криптографические преобразования, в зависимости от задачи, ruToken может служить не только пассивным, но и активным средством идентификации.

2. Зачем был разработан ruToken

Уже несколько лет на российском рынке представлены электронные идентификаторы зарубежных производителей. Однако далеко не все они адаптированы к российской специфике применения средств защиты информации. Поэтому нами было принято решение разработать и запустить в производство российский электронный идентификатор - устройство, предназначенное специально для российского рынка.

С нашей точки зрения это устройство должно было обладать следующими важнейшими характеристиками:

- **Оно должно поддерживать промышленные стандарты (ISO 7816, PC/SC, PKCS #11, MS CryptoAPI)**
- **В нем должен быть аппаратно реализован российский алгоритм шифрования (ГОСТ 28147-89)**
- **Оно должно быть недорогим**
- **Пользователи должны иметь возможность получать техническую поддержку непосредственно от разработчиков**

Поддержка промышленных стандартов позволит легко встраивать ruToken в широко используемое программное обеспечение и готовые приложения. Кроме того, разработчикам оригинального программного обеспечения не придется изучать новые интерфейсы прикладного программирования - они могут использовать стандартные общепринятые интерфейсы и применять ruToken в качестве альтернативы иным средствам аутентификации.

Использование российского алгоритма шифрования позволит применять идентификаторы ruToken в системах информационной безопасности в соответствии с российским законодательством.

123056, Россия, г. Москва
ул. Красина, д.3, компания Актив
тел./факс: (095) 105-77-90

Невысокая стоимость сделает возможным использование ruToken широким кругом пользователей, а также его внедрение даже в малобюджетных проектах.

Оперативная техническая поддержка от разработчиков обеспечит максимально возможную обратную связь: она позволит быстро реагировать на сигналы пользователей и при необходимости, по возможности, реализовывать их пожелания.

Все это позволяет нам рассчитывать на то, что ruToken займет достойное место на российском рынке безопасности.

3. Кто разработал ruToken

ruToken явился детищем сотрудничества двух известных российских предприятий: Компании Актив и фирмы Анкад.

Компания Актив

Компания Актив существует уже более 10 лет. Большую часть этого времени наша компания специализируется на разработке и производстве программно-аппаратных средств защиты программного обеспечения. Основная продукция компании - электронные ключи семейства Guardant, хорошо зарекомендовавшие себя не только среди отечественных разработчиков, но и среди зарубежных клиентов.

На сегодняшний день Актив является самым крупным производителем электронных ключей в России и имеет хорошо налаженную технологию, позволяющую производить электронные изделия в достаточных количествах и с высоким качеством.

Весь цикл производства электронных ключей Guardant, от разработки до упаковки, осуществляется в России, поэтому Актив может оперативно реагировать на пожелания своих клиентов.

Также мы обладаем квалифицированной службой технической поддержки, что позволяет разрешать вопросы наших клиентов в минимальные сроки.

Фирма Анкад

Фирма Анкад работает на рынке средств защиты информации длительное время. Основным профилем компании является защита компьютерной информации методами криптографии и электронной цифровой подписи в соответствии с государственными стандартами России.

Фирма активно работает в сфере программных и аппаратных средств криптографической защиты информации (это известные шифраторы серии КРИПТОН), ЭЦП, систем контроля и разграничения доступа, занимается смарт-карт технологиями и средствами защиты телефонных переговоров.

Анкад владеет обладает самым широким набором лицензий ФАПСИ, ФСБ и Гостехкомиссии.

Обе компании объединили свои возможности: Актив занялся разработкой и производством аппаратной части идентификатора, а также продвижением на рынок марки ruToken, а Анкад взял на себя разработку криптографической части проекта.

123056, Россия, г. Москва
ул. Красина, д.3, компания Актив
тел./факс: (095) 105-77-90

4. Что умеет ruToken

В первую очередь, ruToken предназначен для **безопасного хранения идентификационной информации** для аутентификации пользователей в приложениях, где необходимо разграничивать доступ к конфиденциальной информации. Он может использоваться как очень надежная альтернатива парольной защите при регистрации в Active Directory, при доступе к локальным рабочим станциям, базам данных, веб-серверам, виртуальным частным сетям, и другим информационным системам.

Как минимум, ruToken позволяет хранить "сильные" пароли, обычно весьма трудные для запоминания, и выдавать их по предъявлении PIN-кода пользователя, что уже значительно увеличивает уровень безопасности. То есть ruToken может использоваться как защищенный контейнер для паролей.

Кроме паролей, ruToken может хранить и другую информацию, например ключи шифрования и цифровые сертификаты.

Во-вторых, ruToken может использоваться для безопасной передачи идентификационной информации, например, при ее передаче через открытые каналы связи. Эта возможность может быть необходима при доступе к удаленным ресурсам через защищенные соединения.

В-третьих, ruToken способен быть **самостоятельным средством шифрования** информации. В нем реализован алгоритм симметричного шифрования ГОСТ 28147-89 в режимах простой замены, гаммирования и гаммирования с обратной связью. Это является важнейшим отличием от идентификаторов зарубежного производства. Ключи шифрования могут быть сгенерированы самим токеном или импортированы из внешних файлов. В первом случае ключ шифрования никогда не покидает памяти токена и, следовательно, не может быть скомпрометирован.

Все перечисленное в комплексе с соответствующими программными и аппаратными средствами делает возможным применение токена в задачах защиты персональной и корпоративной конфиденциальной информации, разделения доступа к защищенным ресурсам, в системах электронной торговли, банковских приложениях и любых других задачах, где требуется надежная аутентификация и криптографическая защита информации.

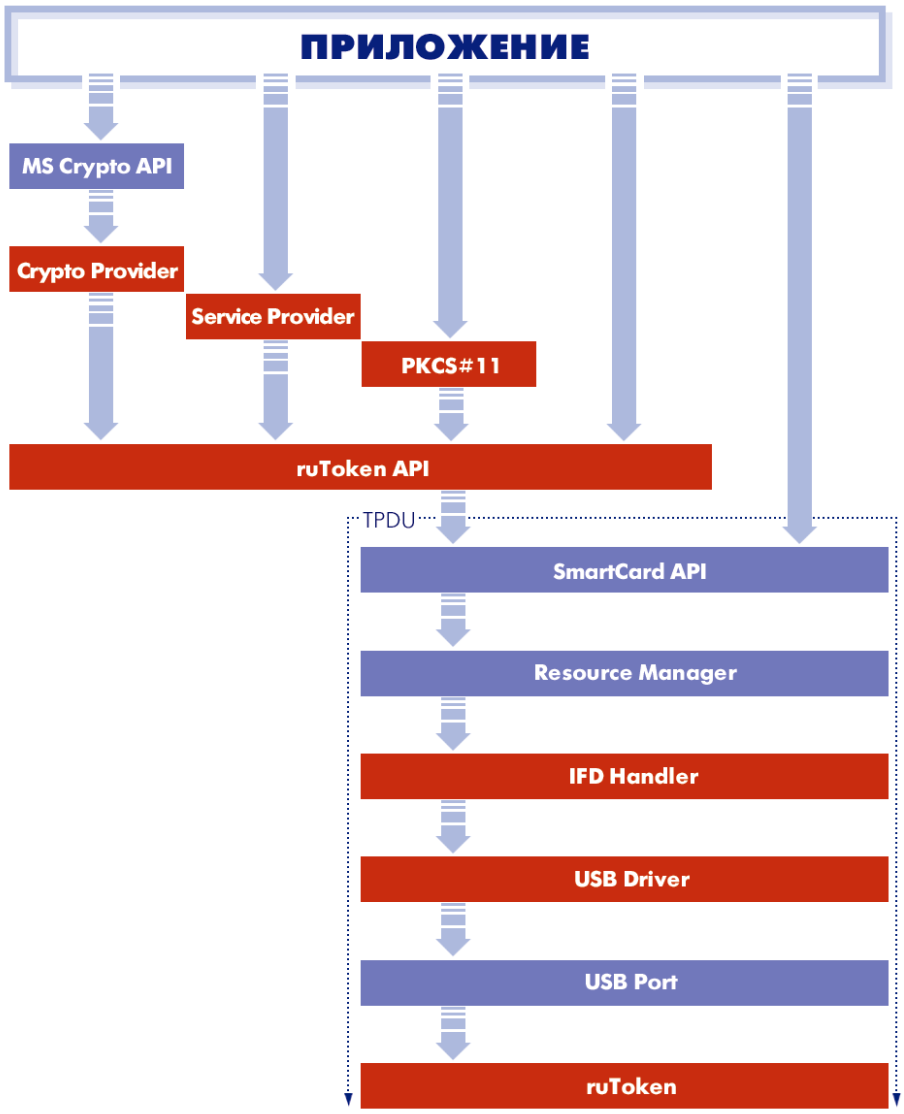
123056, Россия, г. Москва
ул. Красина, д.3, компания Актив
тел./факс: (095) 105-77-90

5. Архитектура и технические характеристики ruToken

Теперь давайте кратко рассмотрим архитектуру и технические характеристики ruToken.

Архитектура ruToken

Архитектура токена схематически показана на рисунке, где синим цветом обозначены стандартные компоненты, входящие в состав Windows, а красным - разработанные компанией Актив.



Нижний уровень представлен непосредственно токеном, USB драйвером и IFD хэндлером. Все эти компоненты обеспечивают представление ruToken в качестве смарт-карты,

подключенной к считывателю, что позволяет использовать стандартный интерфейс Windows для работы со смарт-картами - Resource Manager.

Компоненты более высоких уровней обращаются к токену уже через Smart Card API - также стандартный интерфейс Windows.

На более высоких уровнях находятся реализации промышленных стандартов для работы со смарт-картами:

- Библиотека PKCS #11, реализующая работу с криптографическими функциями токена по стандарту, разработанному компанией RSA.
- Сервис-провайдер смарт-карты (Integrated Circuit Card Service Provider, ICCSP), обеспечивающий реализацию доступа к некриптографическим функциям токена в соответствии со стандартом PC/SC
- Криптографический сервис-провайдер, обеспечивающий доступ к криптографическим функциям токена, в том числе и посредством стандартного высокоуровневого интерфейса MS Crypto API.

Технические характеристики ruToken

- Поддерживаемые ОС: Windows 98/Me/2000/XP
- Поддержка ISO/IEC 7816, PC/SC, ГОСТ 28147-89, PKCS #11 (v. 2.10+) Microsoft Crypto API и Microsoft Smartcard API
- Встроенная файловая система. Объекты данных для security-ориентированных операций.
- PIN-коды Пользователя и Администратора
- возможность интеграции ruToken в любые smartcard-ориентированные программные продукты (e-mail, internet, платежные системы и т.п.)
- Защищенное хранение ключей асимметричного шифрования и цифровых сертификатов
- Возможность использования ruToken для асимметричного шифрования данных и для работы с цифровыми сертификатами из любых smartcard-приложений, поддерживающих стандарт PC/SC
- Протестирована работа с e-mail-клиентами: Microsoft Outlook, Microsoft Outlook Express и с центрами сертификации: Microsoft и Verisign
- WinLogon и PKI Logon

6. Программное обеспечение ruToken

- **Сервисная библиотека классов C++**, предназначенная для облегчения разработки приложений, использующих ruToken. Является надстройкой над SmartCard API и предоставляет классы, облегчающие работу с ruToken на уровне APDU
- **Утилита программирования ruToken:**
    - Создание объектов файловой системы ruToken: папок, файлов, ключей шифрования и т.п.
    - Назначение прав доступа к объектам файловой системы

  - Редактирование символьного имени токена
  - Манипулирование объектами файловой системы: получение сведений, просмотр, редактирование, удаление и т.п.
  - Шифрование внешних данных по алгоритму ГОСТ 28147-89
- **Утилита администрирования ruToken:**
  - Получение сведений о выбранном токене
  - Инициализация памяти ruToken
  - Изменение PIN-кодов Пользователя и Администратора
  - Разблокирование PIN_кода Пользователя
- **Подробные примеры работы с ruToken в исходных текстах.**
- **Набор инсталляторов отдельных компонентов ПО ruToken для удобного переноса ПО на компьютеры конечных пользователей**

7. Цены и политика продаж

В настоящее время продукт ориентирован в первую очередь на разработчиков прикладных систем и систем безопасности.

Цена ruToken с объемом памяти 8К составляет около 20 долларов.

8. Контактная информация

Компания Актив

E-mail:

Общие вопросы: rutoken@rutoken.ru

Тех. поддержка: hotline@rutoken.ru

Отдел продаж: sales@rutoken.ru

Телефон и факс:

(095) 105-77-90 (многоканальный)

Адрес:

123056, Россия,

г. Москва, ул. Красина, 3

Web-сайт:

www.rutoken.ru