

Электронные идентификаторы

eToken PRO (Java).

Новое поколение USB-ключей и смарт-карт – решение компании Aladdin в сфере аутентификации и информационной безопасности, построенное на базе Java-карты, что значительно увеличивает функциональные возможности eToken и расширяет сферу его применения. eToken PRO (Java) обладает всей функциональностью eToken PRO и программно полностью с ним совместим.

Дополнительно eToken o (Java) имеет увеличенный объем памяти для защищённого хранения пользовательских данных (72 КБ) и предоставляет возможность расширения функционала за счет загрузки дополнительных приложений (апплетов). eToken PRO (Java) аппаратно реализует генерацию ключей ЭЦП и формирование ЭЦП по стандарту ГОСТ Р 34.10-2001. Для работы USB-ключей eToken PRO (Java) в ОС Windows Vista установка драйверов не требуется (драйвера входят в состав операционной системы).

Возможные модификации:

- по форм-фактору исполнения: USB-ключ, смарт-карта;
- сертифицированная версия (ФСБ России) – на этапе сертификационных испытаний;
- по наличию встроенной радио-метки;
- нанесение рельефного логотипа на корпус USB-ключа, печать на поверхности смарт-карты, нанесение логотипа на корпус USB-ключа методом тампопечати;
- по цвету корпуса для USB-ключа.

Аппаратный ключ строгой аутентификации eToken PRO.

USB-ключи и смарт-карты eToken PRO выполнены на базе микросхемы смарт-карты и предназначен для аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП).

Возможные модификации:

- по форм-фактору исполнения: USB-ключ, смарт-карта;
- по объёму памяти смарт-карты: 32, 64 КБ;
- сертифицированная версия (ФСТЭК России);
- по наличию встроенной радио-метки;
- нанесение рельефного логотипа на корпус USB-ключа, печать на поверхности смарт-карты, нанесение логотипа на корпус USB-ключа методом тампопечати;
- по цвету корпуса для USB-ключа.

Аппаратный ключ строгой аутентификации eToken ГОСТ.

Персональное средство формирования ЭЦП с неизвлекаемым закрытым ключом. eToken ГОСТ предназначен разработчикам систем дистанционного банковского обслуживания, электронных торгов, сдачи налоговой отчетности для встраивания в клиентскую часть, а также разработчикам СКЗИ для обеспечения надёжной защиты закрытых ключей и аппаратной реализации ЭЦП. Для встраивания eToken ГОСТ в приложения собственной разработки следует использовать комплект разработчика eToken ГОСТ - eToken ГОСТ SDK.

Идентификаторы iButton (Dallas).

Семейство микроэлектронных устройств, разработанных фирмой Dallas Semiconductor, USA (в настоящее время выпускаемых фирмой Maxim). Каждое такое устройство заключено в стальной герметичный цилиндрический корпус и имеет уникальный номер (ID), записываемый в процессе изготовления. Все устройства iButton помещаются в стальной цилиндрический корпус MicroCap, выполнены по жестким стандартам и выдерживают серьезные механические и температурные нагрузки.

Обмен данными с iButton производится через интерфейс 1-Wire. Информация в этом интерфейсе передается по единственному проводнику. Питание iButton получают из этого же проводника, заряжая внутренний конденсатор в моменты, когда на шине нет обмена данными. Ско-

рость обмена достаточна для обеспечения передачи данных в момент касания контактного устройства. Для подключения iButton к компьютеру компанией Aladdin выпускаются считыватели (адаптеры), преобразующие сигналы стандартных портов компьютера (RS232, USB) в сигналы 1-Wire. Брелок для ключей позволяют надежно закрепить "таблетку" iButton.

Электронный идентификатор Rutoken.

Компактное устройство в виде USB-брелка, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных. Заменяет любые парольные системы защиты, ведь теперь не нужно запоминать множество логинов и сложных паролей, все они надежно хранятся в памяти токена. Все что должен сделать пользователь - подключить токен к USB-порту и набрать PIN-код. Таким образом, осуществляется двухфакторная аутентификация, когда доступ к информации можно получить, только обладая уникальным предметом (токеном) и зная некоторую уникальную комбинацию символов (PIN-код). Выступает удачной альтернативой другим аппаратным носителям ключевой информации: смарт-картам, i-button, не говоря уже о дискетах. Аналог смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель), данные надежно хранятся в энергонезависимой памяти токена объемом до 128 Кб, прочный корпус Rutoken устойчив к внешним воздействиям.

Идентификаторы Rutoken ЭЦП.

Аппаратная реализация российского стандарта электронной цифровой подписи и проверенный конструктив идентификаторов Rutoken. Новый USB-токен предназначен для использования в качестве интеллектуального ключевого носителя в российских системах РКІ, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной цифровой подписи.

Электронный идентификатор Rutoken ЭЦП спроектирован на основе современных российских и международных стандартов в области информационной безопасности. Это позволяет легко, без дополнительных усилий, встраивать его поддержку в существующие информационные системы. Общий объем памяти для данных и криптографических ключей — 64 Кбайт.

Позволяет осуществлять механизм электронной цифровой подписи так, чтобы закрытый (секретный) ключ подписи никогда не покидал пределы токена. Таким образом, исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.

Идентификаторы Rutoken Flash.

Комбинированное аппаратное решение, объединяющее в едином корпусе два разных по назначению устройства: Rutoken и обычный Flash-диск объемом 2Гб (USB Flash drive).

Впервые подобное устройство исполнено в таком лаконичном виде. До настоящего времени представленные на рынке решения имели внушительные размеры, тем самым создавая значительные неудобства для пользователей.

С помощью Rutoken Flash можно не только обеспечить безопасное хранение паролей, цифровых сертификатов, ключей шифрования и ЭЦП, но также использовать открытую Flash память для резервного копирования данных, хранения дистрибутивов ПО, автоматического запуска приложений при подключении, загрузки «чистой» операционной системы (ОС MS Windows, Linux) и т.д.

Rutoken для Windows.

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

Продукт могут использовать любые организации и предприятия, информационная структура которых построена на базе сетей Microsoft Windows. Для развертывания и последующей эксплуатации решения Rutoken для Windows не требуется привлечения сторонних специалистов и приобретения дополнительного оборудования и программного обеспечения третьих фирм. Все не-

обходимые настройки сети может выполнить штатный системный администратор предприятия, следуя подробным инструкциям, содержащимся в Руководстве по внедрению Rutoken для Windows.

Rutoken для Linux.

В операционных системах GNU/Linux, xBSD, Solaris, MacOS X и др. работа Рутокен ЭЦП обеспечивается программным обеспечением проектов opensc-project.org и M.U.S.C.L.E..

Программное обеспечение OpenSC вместе с OpenSSL представляет утилиты администрирования и библиотеки прикладного программирования, в том числе реализацию стандарта PKCS#11. OpenCT представляет собой интерфейс низкого уровня (уровня считывателя).

Проект M.U.S.C.L.E. — это открытая реализация программного интерфейса PC/SC (WinSCard) в *nix системах (известна как `pcsc-lite`). Рутокен ЭЦП работает с ним через `ccid`-драйвер. Библиотека `opensc-pkcs11` входит в состав ПО OpenSC и предоставляет возможность использования криптографических алгоритмов ГОСТ28147-89, ГОСТ3411-94 и ГОСТ3410-2001 в Рутокен ЭЦП, согласно draft-версии стандарта PKCS#11 V 2.30.

Rutoken для Mac OS X.

Решение включает драйвер Rutoken для кроссплатформенного проекта M.U.S.C.L.E. (`pcsc-lite`) и набор утилит из проекта OpenSC.

Функционально представляет собой почти полную копию решения Rutoken для Linux. Все программное обеспечение распространяется в виде исходных текстов, что позволяет применить его на любой платформе (PowerPC и Intel).

Возможности: Авторизация пользователей в сетях и на рабочих станциях; Вход по предъявлению токена; Подключение к серверу по предъявлению токена; Безопасность электронной переписки; Электронная цифровая подпись почтовых сообщений; Шифрование почтовых сообщений; Надежное хранение и безопасное использование сертификатов, паролей и так далее; Применение Rutoken в качестве защищенного хранилища любой персональной информации о пользователе.

Rutoken для КриптоПро.

Поддерживают широкий спектр приложений, разработанных компанией Крипто-Про. В программном обеспечении КриптоПро Rutoken используется для безопасного хранения цифровых сертификатов и закрытых ключей ЭЦП и шифрования.

Применение российских идентификаторов дает возможность пользователям КриптоПро надежно обезопасить ключевую информацию от несанкционированного использования. Покидая рабочее место и забрав токен с собой, пользователь может быть уверен, что в его отсутствие никто не отошлет подписанный документ от его имени. Даже в случае кражи устройства злоумышленник не сможет воспользоваться ключевой информацией, т.к. память идентификаторов Рутокен шифруется по алгоритму ГОСТ 28147-89 и для доступа к ней требуется знание PIN-кода пользователя. В решении КриптоПро Рутокен CSP используется аппаратная реализация российских алгоритмов ЭЦП.

Система КриптоТри.

Комплексное решение для организации рабочих мест защищенного документооборота: шифрования и электронной цифровой подписи документов, управления цифровыми сертификатами, аутентификации и т.д. Программный продукт КриптоТри имеет свидетельство о государственной регистрации в Роспатенте.

Продукт предназначен для обеспечения технической составляющей при построении защищенных юридически значимых систем (электронный документооборот, Интернет-приложения, электронные архивы, CRM и ERP-системы и др.). На рабочем месте пользователя устанавливаются криптопровайдер КриптоПро CSP, реализующий сертифицированные криптоалгоритмы, и клиентское приложение КриптоАРМ для выполнения операций шифрования и электронной подписи. Ключи и цифровые сертификаты хранятся на электронном идентификаторе Рутокен для усиления защиты секретных данных.

КриптоТри будет интересен организациям, развертывающим систему PKI, а также пользующимся услугами сторонних Удостоверяющих центров. Продукт КриптоТри позволяет сократить расходы на создание рабочих мест в PKI и уменьшить время выполнения пользователями криптоопераций, обеспечить простоту и удобство настройки. КриптоТри поддерживает работу с различными элементами PKI. Это работа с цифровыми сертификатами и запросами, а также с Доверенными Службами Штamped Времени (TSA) и Актуальных Статусов (OCSP).

Идентификаторы Rutoken RF.

Usb-токен со встроенной радиочастотной (RFID) меткой. Предназначен для доступа пользователей к информационным ресурсам компьютера и для физического доступа в здания и помещения. Rutoken RF объединяет возможности, предоставляемые usb-токенами, смарт-картами и бесконтактными электронными пропусками.

Rutoken RF незаменим в комплексных системах безопасности. Бесконтактный пропуск для выхода из помещения и средство доступа в компьютерную сеть объединены в одном брелке. Система безопасности может быть сконфигурирована так, что сотрудник просто физически не сможет оставить доступ к конфиденциальной информации. Для выхода из помещения необходимо предъявить Rutoken RF, а при отключении идентификатора от USB-порта компьютера пользовательская сессия автоматически блокируется.

Выпускаются четыре линейки Rutoken RF различающиеся интегрированной радиочастотной меткой: Rutoken RF (EM) - поддержка стандарта EM-Marine; Rutoken RF (MF) - поддержка стандарта Mifare; Rutoken RF (HID) - поддержка стандарта HID; Rutoken RF (IND) - поддержка стандарта Indala. В каждой линейке существуют три модели Rutoken RF, отличающиеся объемом памяти: 32, 64 и 128 Кбайт.

еToken с радио-меткой RFID.

Используется для интеграции с системами контроля и управления доступом в помещения (СКУД), в бесконтактных "электронных проходных", системах учёта рабочего времени персонала и т.д. Система информационной безопасности может быть настроена так, что сотрудник не сможет покинуть помещение, оставив свой еToken подключенным к компьютеру. Для прохода в другие помещения необходимо предъявить еToken со встроенной в него радио-меткой RFID, а при отключении еToken компьютер автоматически блокируется. В настоящее время RFID-метки могут быть имплантированы в смарт-карты еToken PRO, USB-ключи еToken PRO, еToken NG-OTP и еToken NG-FLASH.

Комбинированные карты со встроенной радио-меткой (RFID)

Смарт-карты и карты с памятью могут быть дополнены практически любой пассивной RFID-меткой, используемой в бесконтактных "электронных проходных".

Это позволит повысить уровень безопасности и удобства - карта не может быть оставлена подключенной к компьютеру или передана другому лицу, т.к. без нее нельзя покинуть помещение.

Аппаратный ключ строгой аутентификации еToken PASS.

Автономный генератор одноразовых паролей, не требующий для своей работы подключения к компьютеру. еToken PASS имеет кнопку для генерации одноразовых паролей и ЖК-дисплей для их отображения.

Возможные модификации - нанесение логотипа на корпус устройства методом тампопечати.

Комбинированный USB-ключ еToken NG-OTP.

Сочетает функционал смарт-карты и генератора одноразовых паролей. еToken NG-OTP имеет встроенный аппаратный генератор одноразовых паролей, ЖК-дисплей для их отображения и кнопку для их генерации.

Возможные модификации:

- по объёму памяти смарт-карты: 32, 64 КБ;
- сертифицированная версия (ФСТЭК России);

- по наличию встроенной радио-метки;
- по цвету корпуса для USB-ключа.

Комбинированный USB-ключ eToken NG-FLASH.

Сочетает функционал смарт-карты с возможностью хранения больших объёмов пользовательских данных во встроенном модуле flash-памяти. eToken NG-FLASH также обеспечивает возможность загрузки операционной системы компьютера и запуска пользовательских приложений из flash-памяти.

Возможные модификации:

- по объёму встроенного модуля flash-памяти: 512 МБ; 1, 2 и 4 ГБ;
- сертифицированная версия (ФСТЭК России);
- по наличию встроенной радио-метки;
- по цвету корпуса для USB-ключа.

Идентификаторы Rutoken Magistra.

Современная операционная система для смарт-карт и проверенный временем конструктив Рутокен. Операционная система «Магистра» использует криптографический модуль, сертифицированный ФСБ России (сертификат №СФ/114-1009 от 14 мая 2007 года).

Возможности Rutoken ЭЦП позволяют осуществлять механизм электронной цифровой подписи так, чтобы закрытый (секретный) ключ подписи никогда не покидал пределы токена. Таким образом, исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.