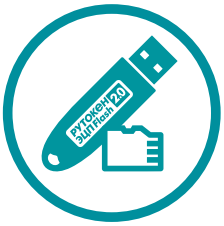
Рутокен ЭЦП 2.0 Flash



Рутокен ЭЦП 2.0 Flash — уникальное устройство, сочетающее в себе всю функциональность сертифицированного средства криптографической защиты информации Рутокен ЭЦП 2.0 с интегрированной управляемой Flash-памятью. Электронный идентификатор предназначен для строгой двухфакторной аутентификации, электронной подписи и шифрования данных на неизвлекаемых ключах.

Основные характеристики Рутокен ЭЦП 2.0 Flash

- Интегрированная управляемая Flash-память для хранения данных объемом от 4 до 64 ГБ.
- Возможность разбиения памяти на разделы, доступ к которым разграничивается с помощью PIN-кодов.
- Возможность создания скрытых и CD-ROM разделов.
- Аппаратная реализация новых стандартов электронной подписи и хеширования ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и VKO ГОСТ 34.10-2012 (RFC 7836).
- Объем защищенной памяти для ключей и сертификатов — 128 КБ.
- Скорость симметричного шифрования до 320 КБ/с и хеширования до 230 КБ/с.
- Поддержка операционных систем Microsoft Windows, GNU/Linux, Apple macOS/OS X.

Уникальные свойства Рутокен ЭЦП 2.0 Flash

Безопасность

Рутокен ЭЦП 2.0 Flash базируется на электронном идентификаторе Рутокен ЭЦП 2.0. Управление разделами Flash-памяти производится при помощи защищенного контроллера Рутокен ЭЦП 2.0 и основано на его внутренних политиках безопасности. Каждый раздел может быть защищен своим собственным PIN-кодом. Верификация PIN-кодов для доступа к разделам производится встроенными алгоритмами.

Удобство

Сочетание двух типов устройств в одном корпусе позволяет пользователю не заботиться о физическом разделении информации. Пользовательские данные, необходимое для работы программное обеспечение, персональная информация и криптографические ключи всегда будут находиться в одном месте, удобном и безопасном.

Унификация

Электронный идентификатор Рутокен ЭЦП 2.0 Flash используется в любых информационных системах, рассчитанных на применение Рутокен ЭЦП 2.0.

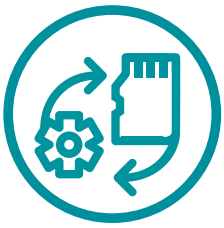
Быстродействие

Рутокен ЭЦП 2.0 Flash обладает непревзойденными скоростными характеристиками, позволяющими «на лету» шифровать, расшифровывать, хешировать и подписывать большие объемы данных. Объем EEPROM-памяти для сертификатов и ключей увеличен до 128 КБ, а быстрый 32-разрядный процессор позволяет достичь скорости симметричного шифрования до 320 КБ/с и хеширования до 230 КБ/с. Высокая скорость шифрования и хеширования расширяет возможности применения электронного идентификатора.

Поддержка новых криптографических стандартов

В устройстве аппаратно реализованы одновременно новые криптографические стандарты электронной подписи и хеширования ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и старые ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, а также симметричное шифрование по ГОСТ 28147-89. Это делает возможным использование Рутокен ЭЦП 2.0 Flash как интеллектуального ключевого носителя и средства ЭП в существующих и перспективных инфраструктурах открытых ключей (PKI) и системах юридически значимого электронного документооборота.

Управляемая Flash-память



Важной особенностью электронного идентификатора Рутокен ЭЦП 2.0 Flash является наличие управляемой Flash-памяти. Доступ и управление доступом к Flash-памяти осуществляется непосредственно через микропроцессор токена без использования каких-либо дополнительных электронных компонентов (хабов, контроллеров и т.п.).
Для каждого раздела Flash-диска определяются индивидуальные права доступа на чтение и запись, которые могут быть изменены «на лету» прямо во время работы устройства. Предусмотрена возможность создания скрытых и CD-ROM разделов. Встроенную Flash-память можно использовать для надежного хранения конфиденциальной информации, дистрибутивов программного обеспечения, автоматического запуска приложений при подключении токена и доверенной загрузки операционной системы.

Сертификация

Согласно выписке из заключения ФСБ России №149/3/2/1-2257 от 12.12.16, Рутокен ЭЦП 2.0 Flash реализует алгоритмы ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 28147-89 и удовлетворяет требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, КС2, а также требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2001г. №796, установленным для класса КС1, КС2.

Применение Рутокен ЭЦП 2.0 Flash

Установка ПО «в один клик»

Для обеспечения работы с электронными торговыми площадками и государственными информационными ресурсами, как правило, требуется установка специального программного обеспечения, такого как криптопровайдер, ActiveX-компоненты и другие дополнительные компоненты операционной системы. Также зачастую есть необходимость в настройке браузера, регистрации сертификата и других административных действиях.
На Flash-памяти электронного идентификатора Рутокен ЭЦП 2.0 Flash может быть размещен неизменяемый CD-ROM раздел с комплектом программного обеспечения и установщиком с технологией автозапуска. Это предоставляет возможность настройки рабочего места «в один клик». При первом подключении устройства к компьютеру нужно всего лишь нажать кнопку «установить» во всплывающем окне, все остальное происходит автоматически.

Устройство доверенной загрузки

Электронный идентификатор Рутокен ЭЦП 2.0 Flash может быть использован в качестве загрузочного устройства типа live-CD, совмещенного с электронным идентификатором и хранящим персональную ключевую информацию. На разделе, эмулирующем CD-ROM, размещается неизменяемый образ операционной системы. Важными отличиями от традиционных носителей являются интегрированность с электронным идентификатором Рутокен ЭЦП 2.0, возможность временного получения прав на запись на read-only разделах для обновления ПО, а также создание специальных разделов для хранения конфигураций, лицензий и т.п.