

Устройство Рутокен PINPad

Цена: 0 р.



Рутокен PINPad - первое сертифицированное ФСБ решение класса TrustScreen, позволяющее визуализировать подписываемый документ в доверенной среде непосредственно перед вычислением электронной подписи. Документ отображается на экране, и при подтверждении пользователем корректности информации подпись происходит непосредственно на устройстве. Рутокен PINPad гарантированно защищает от поддельных сайтов (фишинга), атак при помощи средств удаленного управления, подмены содержимого документа при передаче на подпись (атака Man-in-the-browser).

Рутокен PINPad — это устройство, предоставляющее доверенную среду для выполнения наиболее критичных операций, требующих визуального контроля пользователем. Вынесение подобных операций из среды рабочей станции позволяет успешно противостоять вредоносному ПО (вирусы, трояны, руткиты и т.п.), которое может находиться на компьютере пользователя и заниматься копированием ключей или модификацией документов, подписываемых электронной подписью.

Устройство Рутокен PINPad обеспечивает защищенную двухфакторную аутентификацию: для работы пользователю необходимо как физическое наличие устройства, так и знание PIN-кода. При этом ввод PIN-кода происходит на экране устройства в доверенной среде, что обеспечивает дополнительную защиту от мошенничества.

Комплектация:

- Устройство
- Упаковка



Технические данные:

Сенсорный экран	<p>Полноцветный сенсорный LCD экран с разрешением 320x240 пикселей. Возможность просмотра больших документов. Визуализация подписываемых документов с возможностью отказа от подписи.</p>
Криптографические возможности	<p>Поддержка алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001: генерация ключевых пар с проверкой качества, импорт ключевых пар, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет. Поддержка алгоритмов ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи. Поддержка алгоритма ГОСТ 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ). Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012, расшифрование по схеме EC El-Gamal. Генерация последовательности случайных чисел требуемой длины. Выработка запросов на сертификаты для неизвлекаемых ключей подписи ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 в формате PKCS#10 с возможностью визуализации и подтверждения на устройстве. Поддержка сообщений SMS, подписанных и зашифрованных с использованием криптоалгоритмов ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и ГОСТ 28147-89.</p>
Аппаратные криптографические операции	<p>Скорость шифрования ГОСТ 28147-89: до 48 Кбайт/сек. Скорость хеширования ГОСТ Р 34.11-2012: до 21 Кбайт/сек. Скорость хеширования ГОСТ Р 34.11-94: до 24 Кбайт/сек. Электронная подпись ГОСТ Р 34.10-2012 (512 бит): 0,29 подп./сек. Электронная подпись ГОСТ Р 34.10-2012 (256 бит): 0,95 подп./сек. Электронная подпись ГОСТ Р 34.10-2001: 0,97 подп./сек.</p>



Специальные возможности	Возможность создания специальной неудаляемой ключевой пары устройства. Ведение неубывающего счетчика операций ЭП. Доверенное считывание значения неубывающего счетчика, подтвержденное электронной подписью. Журналирование операций электронной подписи, фиксация критических параметров ЭП и окружения. Доверенное получение журнала операций, подтвержденное электронной подписью.
Возможности аутентификации владельца	Два фактора аутентификации: наличие у пользователя устройства и знание PIN-кода. Аппаратный ввод PIN-кода (на экране устройства в доверенной среде). Настраиваемый минимальный размер PIN-кода. Ограничение числа попыток ввода PIN-кода.
Файловая система	Встроенная файловая структура по ISO/IEC 7816-4. Число файловых объектов внутри папки – до 255 включительно. Использование File Allocation Table (FAT) для оптимального размещения файловых объектов в памяти. Уровень вложенности папок ограничен объемом свободной памяти для файловой системы. Хранение закрытых и симметричных ключей без возможности их экспорта из устройства. Использование Security Environment для удобной настройки параметров криптографических операций. Использование файлов Rutoken Special File (RSF-файлов) для хранения ключевой информации: ключей шифрования, сертификатов и т.п. Использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов.
Интерфейсы	Протокол обмена по ISO 7816-12. Поддержка USB CCID: работа без установки драйверов устройства в современных версиях ОС. Поддержка PC/SC. PKCS#11 (включая российский профиль). Интерфейс кроссплатформенного кроссбраузерного плагина Рутокен. Интерфейс OpenSSL.



Соответствие стандартам	<p>ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94, ГОСТ 28147-89.</p> <p>Наборы параметров для этих алгоритмов соответствуют RFC 4357.</p> <p>Выработка ключа согласования по схемам VKO GOST 34.10-2001 (RFC 4357) и VKO GOST 34.10-2012.</p> <p>Поддерживаемые форматы защищенных сообщений соответствуют RFC 3851 и 3852, использование российских алгоритмов в этих форматах соответствует RFC 4490.</p> <p>Сертификаты и списки отзывов реализованы в соответствии с RFC 3280.</p> <p>Упаковка открытых ключей алгоритмов ГОСТ реализована в соответствии с RFC 4491.</p> <p>Работа с PINPad-type-устройством реализована в соответствии со стандартом PKCS#11 v. 2.20.</p>
-------------------------	--