

Рутокен PINPad

Рутокен PINPad — это полноценное средство криптографической защиты информации, позволяющее визуализировать подписываемый документ в доверенной среде непосредственно перед созданием электронной подписи.



Назначение и преимущества

Рутокен PINPad предназначен для подтверждения платежа (или массовых платежей) и электронной подписи. Представляет собой, по сути, Рутокен ЭЦП, дополненный TouchScreen экраном. Решение обеспечивает двухфакторную аутентификацию — для работы пользователю необходимо наличие устройства и знание PIN-кода. При этом ввод PIN-кода происходит на экране устройства в доверенной среде, что обеспечивает дополнительную защиту от мошенников.

Рутокен PINPad обеспечивает усиленный уровень безопасности и удобен для пользователей при работе с системами дистанционного банковского обслуживания. Платежный документ отображается на экране и в случае подтверждения пользователем корректности информации осуществляется подпись непосредственно на самом устройстве. Данное решение гарантировано защищает от фишинга, атак при помощи средств удаленного управления, подмены содержимого документа при передаче его на подпись (атака Man-in-the-browser). В отличие от аналогичных решений, Рутокен PINPad представляет собой средство криптографической защиты информации (СКЗИ), что не требует использования в системе сторонних вендоров для хранения ключей электронной подписи.

Простота встраивания

Специальное программное обеспечение - мультиплатформенный кроссбраузерный плагин - позволяет легко интегрировать Рутокен PINPad с системами дистанционного банковского обслуживания (ДБО) и электронного документооборота (ЭДО). Для начала работы с устройством Рутокен PINPad нужно лишь подключить его к USB-порту компьютера. Устройство не требует прав администратора или установки драйверов, так как работает через стандартный CCID-драйвер. Благодаря интуитивно-понятному интерфейсу Рутокен PINPad прост и удобен в использовании.

Основные характеристики

Рутокен PINPad может применяться в системах, использующих цифровые сертификаты формата X.509 и инфраструктуру PKI. Устройство и его программное обеспечение позволяют:

- Формировать запросы на сертификат в формате PKCS#10 для неизвлекаемых ключей электронной подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Подписывать и шифровать данные в формате CMS и неформатированные данные с использованием алгоритмов ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012, ГОСТ 28147-89, схемы обмена сессионными ключами VKO GOST R 34.10-2001/VKO GOST R 34.10-2012. Формат CMS поддерживается в полном объеме.
- Хранить и использовать сертификаты открытого ключа ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 в формате X.509.
- Поддержка прикладного уровня: кроссплатформенный браузерный плагин Рутокен и библиотека PKCS#11.

Сценарии применения и функциональные возможности

➤ Полнофункциональное СКЗИ

Устройство Рутокен PINPad, аналогично Рутокен ЭЦП, позволяет подписывать платежи электронной подписью, шифровать платежи, производить строгую аутентификацию исполнителя платежа, проводить контроль целостности платежных данных. При этом подключать дополнительно смарт-карты или токены не нужно, так как Рутокен PINPad является СКЗИ.

➤ Визуализация платежа

В устройстве Рутокен PINPad аппаратно реализована возможность подписывания документов как с визуализацией, так и без визуализации, что позволяет использовать его в том числе для проведения массовых платежей в комфортном режиме для пользователя. Визуализация платежа может производиться избирательно и с учетом анализа XML-тегов подписываемого документа.

➤ Механизм подтверждения платежей

Ввод дополнительного PIN-кода и подтверждение создания электронной подписи платежа производится на сенсорном дисплее устройства Рутокен PINPad. Такой дополнительный PIN-код пользователь должен ввести непосредственно на сенсорном дисплее, а не на клавиатуре компьютера. Такой PIN-код не может быть перехвачен злоумышленником. Весь подписываемый документ загружается в Рутокен PINPad, а ключевые поля подписываемого документа визуализируются на экране непосредственно перед выполнением подписи. Все это гарантирует защиту от атак при помощи средств удаленного управления и от подмены содержимого документа при передаче его на подпись.

➤ Массовые платежи и ввод PIN-кодов

В случае проведения массовых платежей использование Рутокен PINPad не доставит неудобства в силу того, что у пользователя нет необходимости при каждой операции вводить требуемый PIN-код. При подписывании первой платежки на дисплее Рутокен PINPad выводится окно «Введите PIN код». Введенный PIN-код сохраняется в памяти Рутокен PINPad и в дальнейшем уже может не запрашиваться. Однако, при подписывании последующих платежей, вместо запроса ввода рабочего PIN-кода на дисплей будет выдаваться окно «Ok / Отмена». Таким образом, при подписи нескольких платежей пользователь должен будет подтвердить каждую операцию, однако, PIN-код будет браться из кэша устройства.

➤ Ведение журнала операций

Рутокен PINPad ведет защищенный журнал операций, который позволяет системе ДБО проверить, что содержимое подписанного документа было визуализировано на экране зарегистрированного в системе устройства, а сами данные подтверждены пользователем вводом PIN-кода непосредственно на экране Рутокен PINPad. Журнал операций может быть подписан по ГОСТ на специальном ключевом материале, заранее созданным владельцем ДБО. Такой ключевой материал не удалится при форматировании устройства и однозначно идентифицирует используемое устройство. Таким образом, исключается подключение к системе «чужих» устройств, а пользователь выполняет все операции только с зарегистрированного в системе Рутокен PINPad. Использование журнала значительно помогает при расследовании инцидентов информационной безопасности в системах ДБО.

Хотите попробовать?

Для ознакомления по запросу может быть предоставлена полнофункциональная демо-версия решения Рутокен PINPad. Технологическим партнерам предоставляется комплект разработчика (SDK) с подробными примерами для встраивания. Для получения демо-версии обращайтесь по телефону: **+7 (495) 925-77-90** или по электронной почте: info@rutoken.ru