

Рутокен ЭЦП и Рутокен PINPad для защиты платежей



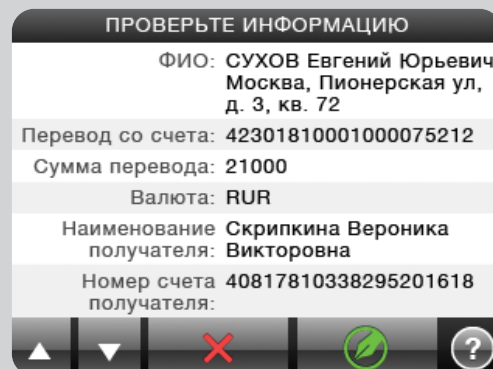
Клиентское программное обеспечение систем дистанционного банковского обслуживания (ДБО) зачастую работает в небезопасной среде. Вредоносное ПО на компьютерах пользователей представляет серьезную угрозу сохранности денежных средств. Использование Рутокен PINPad и Рутокен ЭЦП в системах ДБО позволяет эффективно противостоять всем известным угрозам безопасности таких систем. Рутокен PINPad – это решение, способное защитить пользователей от проблем, связанных с применением злоумышленниками удаленного управления компьютером и подменой платежной информации вредоносным программным обеспечением.

Кража ключевой информации пользователя с носителя или из оперативной памяти компьютера невозможна при использовании в системе ДБО средства криптографической защиты информации (СКЗИ) Рутокен ЭЦП, так как ключи подписи никогда не покидают защищенной памяти токена. Все криптографические операции в Рутокен ЭЦП выполняются на аппаратном уровне в соответствии с требованиями российского законодательства, что подтверждено сертификатом ФСБ РФ №СФ/124-1674 от 11 мая 2011 года.

Более совершенные типы атак на системы ДБО, связанные с несанкционированным доступом к криптографическим функциям токена, с использованием удаленного управления или технологии USB-over-IP, как и подмена платежной информации в момент отправки сообщения на подпись, бессильны в системах ДБО, использующих Рутокен PINPad. В данном случае при осуществлении транзакций клиент получает возможность визуального контроля платежной информации, отправляемой в банк. Ввод PIN-кода и подтверждение выполнения платежа производится на сенсорном дисплее устройства Рутокен PINPad, что гарантирует невозможность выполнения несанкционированных действий.

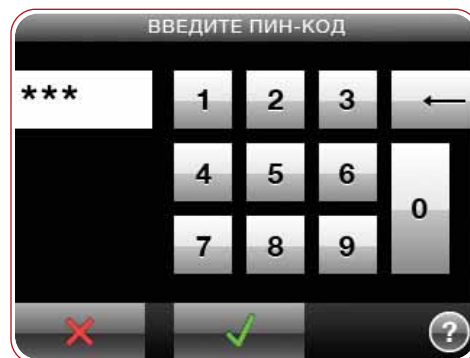
Контроль платежной информации

Для отображения платежной информации на экране Рутокен PINPad данные должны быть специальным образом отформатированы. Для удобства пользователя теги форматирования позволяют выводить на экран не всю информацию платежного поручения, а только значимые поля. Описание формата поставляется в SDK Рутокен PINPad.



Основные возможности Рутокен PINPad

- Доверенный ввод PIN-кода для доступа к криптографическим возможностям USB-токена.
- Просмотр содержания подписываемых документов в доверенной среде. Индивидуальное форматирование и возможность пролистывания больших документов.
- Кеширование PIN-кода внутри PINPad для удобства пользователей. Код вводится один раз при аутентификации, далее при подписи серии платежных документов не нужно вводить его повторно. Пользователь просматривает каждый из документов и нажимает кнопку «Подписать».



Типовой сценарий использования

Рутокен PINPad позволяет осуществлять строгую аутентификацию пользователей для доступа к системе ДБО на базе ЭЦП, а также обеспечивает визуальный контроль подписываемой информации.

Аутентификация в системе ДБО

Для аутентификации может использоваться протокол ISO Public-Key Two-Pass Unilateral Authentication Protocol. Протокол построен на асимметричной криптографии, использует всего две транзакции (пересылки данных) и предназначен для односторонней аутентификации. В процессе аутентификации у пользователя запрашивается PIN-код для доступа к Рутокен ЭЦП, который необходимо набрать на сенсорном экране Рутокен PINPad.

Контроль информации и подпись платежного поручения

Защита от подмены платежной информации осуществляется путем визуального контроля платежного документа на экране устройства и подтверждения корректности информации путем нажатия кнопки «Подписать». Безопасность этого решения основана на том, что клиент-банк отправляет на подпись не хеш платежного поручения, а сам документ в специальном формате. Рутокен PINPad отображает полученную информацию, запрашивает подтверждение у пользователя, и только получив согласие пользователя, отправляет документ в Рутокен ЭЦП для вычисления хеш-функции и подписи документа. Такой подход гарантирует невозможность использования Рутокен ЭЦП для осуществления несанкционированного платежа.

Ключевым преимуществом Рутокен PINPad является то, что для поддержки этого устройства в системах клиент-банк, использующих ЭЦП, не требуется серьезной доработки существующей инфраструктуры. По сути, необходимы лишь небольшие изменения, связанные с форматированием платежных поручений и механизмом подписи.

Широкие продажи устройства **начнутся в декабре 2011 года.**

SDK Рутокен PINPad и полнофункциональные инженерные образцы будут доступны для банков и технологических партнеров в октябре 2011 года. Запросы на образцы для тестирования и встраивания можно отправлять по адресу info@rutoken.ru.