



Вопросы применения
отечественных СКЗИ в банковской
отрасли

Александр Поташников

**Зам. директора Центра Разработок ОАО
«ИнфоТеКС»**

potashnikov@infotecs.ru

Применение СКЗИ



- Платежные системы, процессинг и эмиссия карт

- Дистанционное банковское обслуживание, аутентификация пользователей



- Документооборот, электронная подпись

- Дополнительные услуги, требующие применения квалифицированной электронной подписи пользователей



ViPNet HSM

Функциональные возможности

- Электронная подпись данных
- Проверка электронной подписи
- Генерация ключей (симметричных, асимметричных)
- Шифрование, имитозащита (выработка контрольных сумм)
- Надежное хранение секретных ключей и данных пользователей

ViPNet HSM

Повышенные меры защиты



Имеет встроенный модуль обнаружения вскрытия и контроля основных параметров работы платформы, хранения и гарантированного уничтожения мастер-ключей

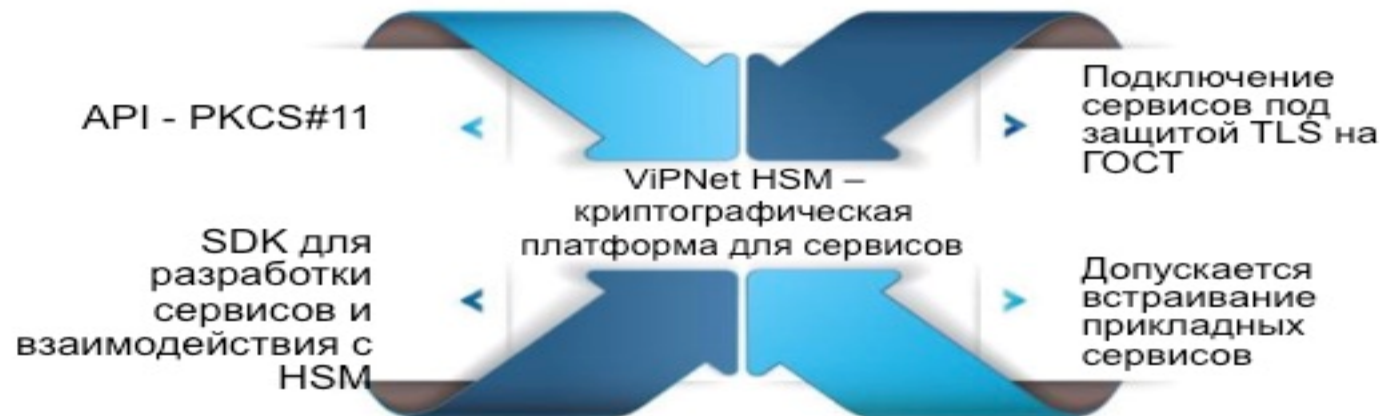
Разделение «секрета», сбор кворума для выполнения критических операций

Развитая ролевая модель

Физический датчик случайных чисел

ViPNet HSM

Подключение прикладных сервисов



Платформа ViPNet HSM



ViPNet HSM PS

Функциональные возможности

- Обработка банковских транзакций электронных платёжных систем.
- Поддержка необходимых режимов для эмиссии карт (генерация секретных величин и электрическая персонализация) .
- Поддержка криптографических режимов, необходимых для обеспечения межбанковского взаимодействия.
- Генерация ключей для обеспечения работы терминальной сети
- Генерация и печать паролей, ключей и ПИН-конвертов владельцев карт.

ViPNet HSM PS

Протоколы и совместимость

- Поддержка протоколов Visa и Mastercard, China Union Pay, American Express, МИР.
- Система команд и протоколы взаимодействия ViPNet HSM PS соответствуют реализованным в HSM Thales PayShield 9000 при работе в режиме совместимости с международными платёжными системами.
- Имеет дополнительную систему команд с отечественными криптографическими алгоритмами для обеспечения перехода к картам и протоколам с отечественными криптоалгоритмами.



ViPNet HSM PS

Специфика

- Дополнительно реализованы криптоалгоритмы DES, TripleDES, AES, RSA, SHA-1, SHA-256.
- Раздельное лицензирование функциональности:
 - Процессинг
 - Режим Удостоверяющего центра
 - Поддержка 3D-Secure
 - Печать ПИН-конвертов
 - Предперсонализация карт
 - Персонализация карт
- В режиме проверки PIN PVV/CVV - 4000 транзакций в секунду.
- Дополнительная WEB-консоль для управления платежными сервисами.



ViPNet HSM PS

Тестирование

- По итогам тестирования в OpenWay в 2016г. ViPNet HSM PS включен в перечень рекомендованных устройств, поддерживаемых коммуникационными серверами NetServer и Transaction Switch Системы WAY4
- В НСПК разработана ПМИ на HSM для головного удостоверяющего центра НСПК, выбрана лаборатория для проведения функционального тестирования.
- Завершен второй цикл тестирования на площадке Сбербанка/Сбертеха – подтверждена техническая возможность использования изделия как для online операций в AC Way4/SmartVista, так и для выпуска карт.
- Проведено тестирование в АКБ «Россия»
- Стартовал цикл тестирования в компании Compass Plus на совместимость с TranzWare Online.

ViPNet PKI Service

- Выполнение криптографических функций (создание и проверка ЭП, генерация ключей ЭП, шифрование/расшифрование данных, хэширование, формирование имитовставки).
- Возможность встраивания в информационные системы (наличие REST API).
- Ролевая модель и управление учетными записями пользователей.
- Взаимодействие с компонентами PKI: с УЦ (pkcs#10), TSP (RFC 3161), OCSP (RFC 2560), CDP.
- Поддержка криптоалгоритмов ГОСТ Р 34.10- 2001/2012, ГОСТ Р 34.11 94/2012, ГОСТ 28147-89.
- Поддержка форматов подписи: PKCS#7 (CMS), XMLDSig, CAdES-BES.
- Возможность удаленного администрирования через веб-интерфейс



ViPNet HSM SIM Service

Предназначен для создания абонентских профилей, содержащих наборы уникальных атрибутов для записи на SIM-карты*: IMSI, ICCID, PIN1, PIN2, PUK1, PUK2, ключ аутентификации абонента (KI), ADM-ключи, OTA-ключи (KIC, KID, KIK).



ПАК позволяет создавать абонентские профили, в двух форматах:

- Для записи на SIM карту
- Для загрузки в программно-аппаратные комплексы домашнего регистратора местонахождения (HLR) и центра аутентификации абонентов (AuC).

Поддержка конкретных моделей SIM-карт и оборудования реализуется на заказ.

Сертификация планировалось в 2016

Завершается сертификация
ПАК ViPNet HSM по
требованиям к СКЗИ и ЭП
класса KB2
(криптоплатформа с
алгоритмами ГОСТ)

Согласовано ТЗ на ПАК ViPNet HSM PS
на проведение тематических
исследований по оценке влияния
платежного сервиса и дополнительного
криптоядра с импортными
криптоалгоритмами на СКЗИ ПАК
ViPNet HSM – работы начнутся по факту
получения заключения на ПАК ViPNet
HSM

FIPS 140-2 и PCI HSM?

Сертификация



Аккредитованные лаборатории

Official PCI Security Stan... X
 ← → C Назадный | https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories

Vendors are encouraged to contact a PCI-recognized laboratory directly in regards to the above services, and any fees associated with them. However, the laboratories cannot offer any advice on POI design. Please contact any of the PCI-recognized laboratories listed below to obtain information and documentation on scheduling test dates and test fees:

Beijing Unionpay Card Technology Co., Ltd. (Bank Card Test Center)

9th Building No.26 West Waihuan Road,
 Fengtai Science Park, 100070 Beijing
 China
 Mr. Andy Liu
 Phone: +86 10 58055955
 Email: liu.sp@bctest.com
 Website: www.bctest.com/index_en.aspx

BrightSight B.V.

Deifttechpark 1 2628 XJ
 Deift, The Netherlands
 Rob van Marrewijk, Shu Gao (China)
 Phone: +31 15 269 2522, +31 15 269 2568
 Fax: +31 15 269 2555
 Email: terminal@brightsight.com
 Email: marrewijk@brightsight.com
 Website: www.brightsight.com

EWA-Canada Limited

1223 Michael Street, Suite 200
 Ottawa, Ontario K1J 7T2
 Canada
 Mr. Erin Connor or Ms. Dawn Adams
 Phone: +1 613.230.6067 Extension 1214 (Erin) or 1249
 Fax: +1 613.230.4933
 Email: pcilab@ewa-canada.com

T-Systems International GmbH

Mr. Robert Hammelrath
 Bonner Talweg 100
 53113 Bonn
 Germany
 E-Mail: robert.hammelrath@t-systems.com
 Website: http://www.t-systems.com/ict-security
 Tel: +49 (0)228 181-49910
 FAX: +49 (0)228 811-49992

UL Verification Services

(formerly RFI Global Services)
 Basingstoke, United Kingdom Pavilion A, Ashwood Park
 Ashwood Way
 Basingstoke, Hampshire RG23 8BG
 Ms. Julie Miller
 Phone: +44 (0) 1256 312081
 Fax: +44 (0) 1256 312001
 Email: Julie.Miller@ul.com
 Website: www.ul.com

UL Transaction Security

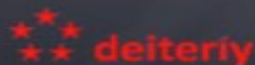
Level 7 / 277 William Street
 Melbourne, Australia
 Victoria 3000

UL Transaction Security

Guangzhou, China
 (additional lab location)

PCI PTS/HSM аккредитация лаборатории

- Подписать с Советом PCI SSC документы: NDA и Соглашение об отсутствии конфликтов интересов.
- Получить от Совета PCI SSC документы, включая перечень требований к лаборатории и ее оборудованию.
- Подтвердить наличие оборудования и выполнение иных требований.
- Выполнить пробную сертификацию одного устройства.
- Пройти он-сайт аудит лаборатории.



Спасибо за внимание!
Вопросы?



Александр Поташников
potashnikov@infotecs.ru