ViPNet HSM
и сценарии его применения

Бадмаева Р.В.

Содержание вебинара

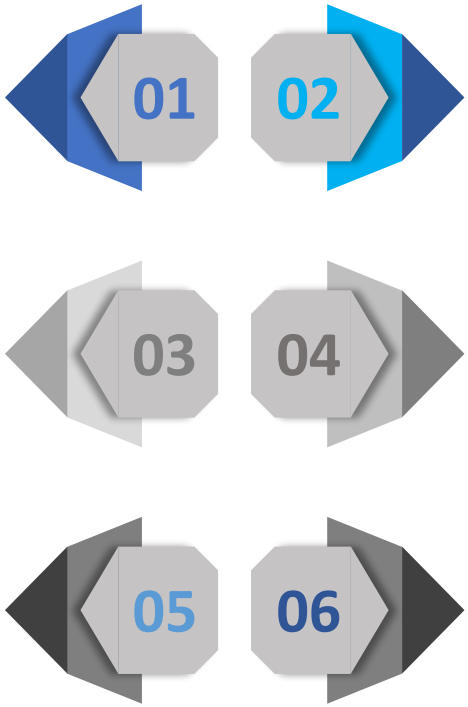
- Что такое ViPNet HSM?
- Сценарии применения ViPNet HSM
- Опыт ИнфоТеКС по разработке новых продуктов с использованием платформы ViPNet HSM:
  - ViPNet HSM PS - новый уровень обеспечения безопасности систем платежных карт;
  - ViPNet PKI Service – сервер подписи в линейке продуктов ViPNet PKI.

Что такое ViPNet HSM?

Программно-аппаратный модуль (HSM – Hardware Secure Module)

Высокопроизводительная платформа

СКЗИ класса КВ



Выполнение криптографических операций по запросам различных сервисов («большой токен»)

Повышенные меры безопасности

Средство ЭП класса КВ2

Что такое ViPNet HSM?

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3071* от "*28*" *февраля* 2017 г.

Действителен до "*31*" *декабря* 2018 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet HSM** (вариант исполнения 1) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС»
сертификационных испытаний образца продукции № 818А-001001.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00127-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **А.М. Ивашко**

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

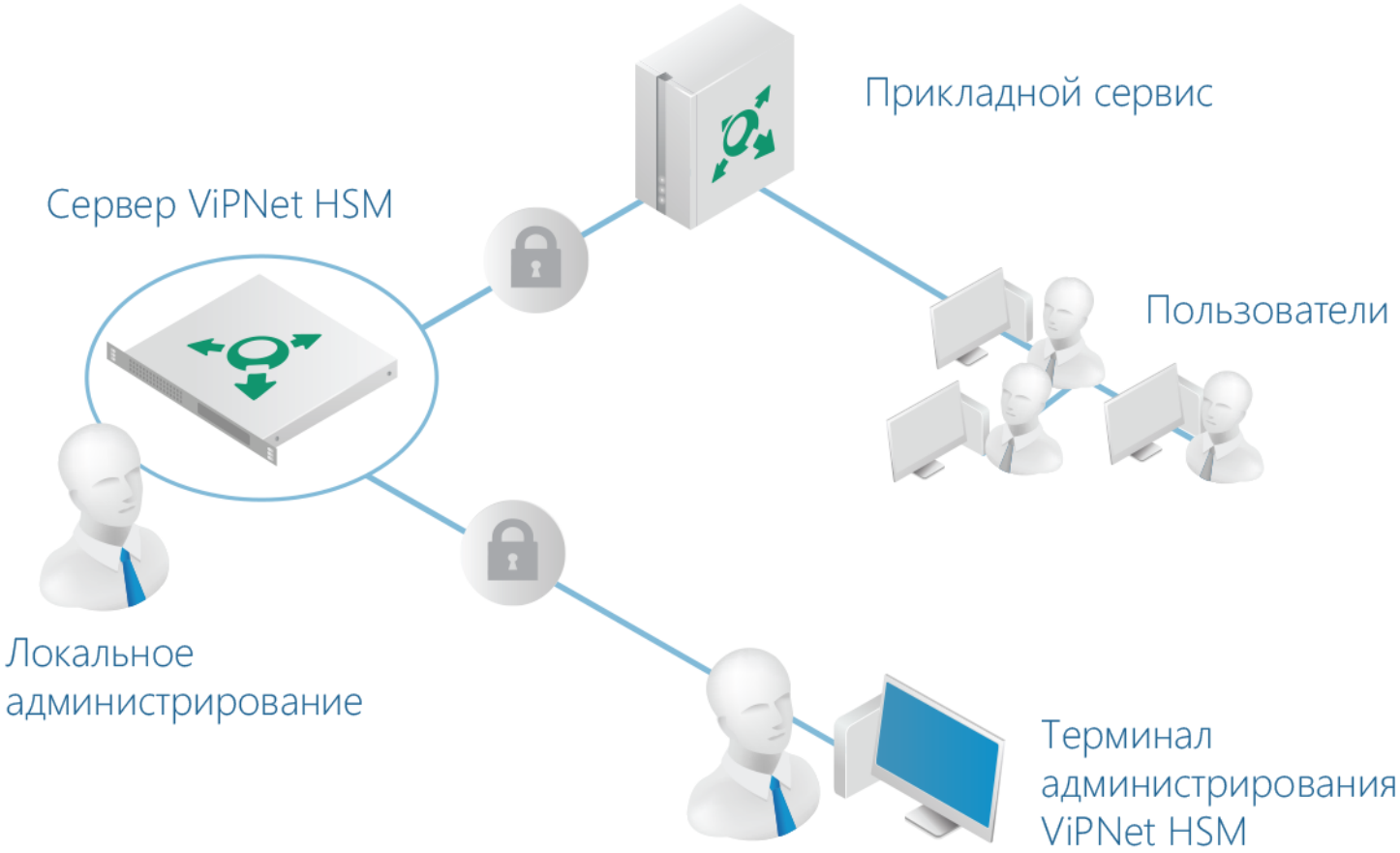
ViPNet HSM: функциональные возможности

- Поддержка криптоалгоритмов:
  ГОСТ 28147-89,
  ГОСТ Р 34.10-2001/2012,
  ГОСТ Р 34.11-94/2012
- Криптографический интерфейс PKCS#11 для использования в прикладных сервисах
- Сценарии применения ViPNet HSM

ViPNet HSM: повышенные меры безопасности

- Имеет встроенный модуль обнаружения вскрытия и контроля основных параметров работы платформы, хранения и гарантированного уничтожения мастер-ключей
- Исполнение со встроенным физическим датчиком случайных чисел (ФДСЧ)
- Разделение «секрета», сбор кворума для выполнения критических операций
- Развитая ролевая модель

ViPNet HSM:
подключение прикладных сервисов



ViPNet HSM:
подключение прикладных сервисов

ViPNet HSM:
сценарии применения

Криптомодули для удостоверяющих центров и серверов систем электронного документооборота

Системы сдачи отчетности и любые другие системы электронных сервисов

Банковские системы электронных платежей

Продукты на базе ViPNet HSM

ViPNet HSM PS

ViPNet PKI Service

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 и печать паролей, ключей и ПИН-конвертов владельцев карт.

СПБ

ViPNet HSM PS

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.
- Имеет дополнительную систему команд с отечественными криптографическими алгоритмами для обеспечения перехода к картам и протоколам с отечественными криптоалгоритмами.

СПБ

ViPNet HSM PS

ViPNet HSM PS: специфика

- Дополнительно реализованы криптоалгоритмы DES, TripleDES, AES, RSA, SHA-1, SHA-256.
- Раздельное лицензирование функциональности.
- В режиме проверки PIN PVV/CVV - 4000 транзакций в секунду.
- Дополнительная WEB-консоль для управления платежными сервисами.

Есть эмулятор в виде VA.

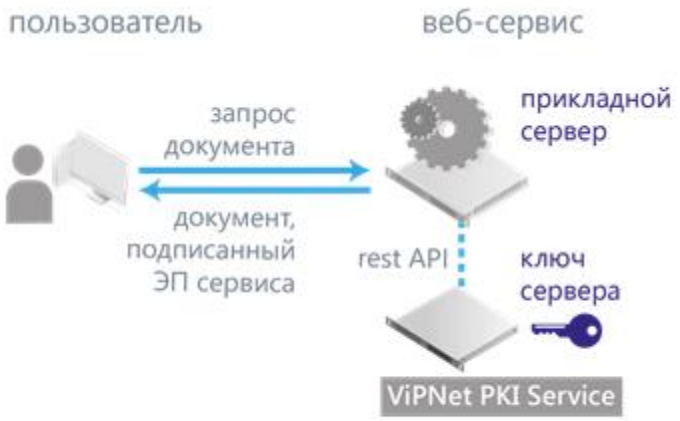
ViPNet HSM PS

ViPNet HSM PS: тестирование

- По итогам тестирования в OpenWay 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 АС Way4/SmartVista, так и для выпуска карт.
- Проведено тестирование в АКБ «Россия», проводится тестирование в Compass Plus

ViPNet PKI Service: функциональные возможности

- Возможность встраивания в информационные системы (наличие REST API).
- Ролевая модель и управление учетными записями пользователей.
- Взаимодействие с компонентами PKI
- Поддержка криптоалгоритмов ГОСТ Р 34.10 2001/2012, ГОСТ Р 34.11 94/2012, ГОСТ 2814789.
- Поддержка форматов подписи: PKCS#7 (CMS), XMLDSig, CAdES-BES.
- Возможность удаленного администрирования через веб-интерфейс

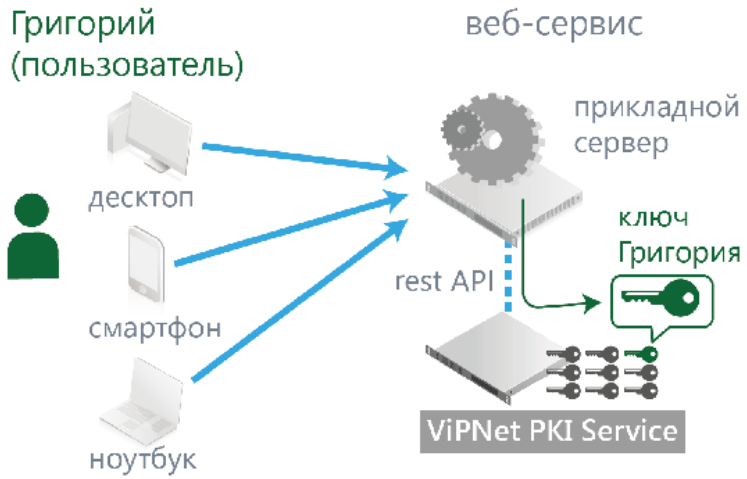


ViPNet PKI Service: функциональные возможности

Для разработчиков: есть эмулятор в виде VA

Лицензирование:
- По количеству пользователей
- По количеству сертификатов

Сертификация:
проводятся сертификационные испытания по требованиям к СКЗИ и средствам ЭП по классу КВ (КВ2)




Спасибо!