

A background image of a businessman in a suit holding several large, metallic, interlocking gears. The scene is dimly lit, with a focus on the gears and the man's hands. The overall tone is professional and technical.

ViPNet HSM как доверенная криптографическая платформа

Бадмаева Римма, ОАО «ИнфоТеКс»

Что такое ViPNet HSM?



- Программно-аппаратный модуль (HSM – Hardware Secure Module)
- Выполнение криптографических операций по запросам различных сервисов («большой токен»)
- Высокопроизводительная и высоконадежная платформа
- Повышенные меры безопасности
- СКЗИ и средство ЭП класса КВ (получение сертификата в 2016 году)

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

ViPNet HSM: повышенные меры безопасности



- Имеет встроенный физический датчик случайных чисел (ФДСЧ), реализованный по требованиям для СКЗИ класса КВ
- 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

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

ViPNet HSM PS:

сервис для банковских электронных систем платежных карт

The logo for infotecs, featuring the word "infotecs" in white lowercase letters on a blue rectangular background.The logo for СИБ (SIB), consisting of the Cyrillic letters "СИБ" in a bold, blue, serif font.

- обработка банковских транзакций электронных платёжных систем в режиме совместимости с протоколами Visa и Mastercard, МИР
- поддержка необходимых режимов для эмиссии (генерация секретных величин и электрическая персонализация) карт с магнитной полосой и чиповых карт стандарта EMV и платёжных карт «МИР»
- 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
- хранение информации, подлежащей защите в рамках работы систем электронных платежей, на отечественных криптографических алгоритмах
- 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

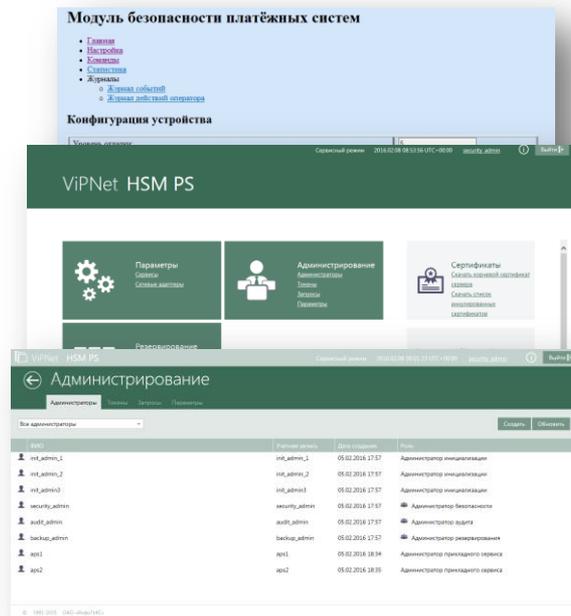
ViPNet HSM PS:

сервис для банковских электронных систем платежных карт

infotecs®



- Реализованы криптоалгоритмы DES, TripleDES, AES, RSA и т.д.
- Раздельное лицензирование функциональности:
 - Процессинг
 - Режим Удостоверяющего центра
 - Поддержка 3D-Secure
 - Печать ПИН-конвертов
 - Предперсонализация карт
 - Персонализация карт
- В режиме проверки PIN PVV/CVV - 4 000 транзакций в секунду
- Дополнительная WEB-консоль для управления платежными сервисами
- Получено заключение от компании OpenWay, подтверждающее совместимость с модулем авторизации WAY4



The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the middle ground, there are several high-voltage power line towers with multiple cross-arms. The sun is low on the horizon, creating a strong glow and casting long shadows. The overall scene represents renewable energy and power infrastructure.

Спасибо за
внимание!