

Высокопроизводительная криптографическая платформа ViPNet HSM как основа для построения доверенных автоматизированных систем и сервисов

Поташников Александр

Зам. директора Центра разработок ОАО «ИнфоТекС»

potashnikov@infotecs.ru

Доверенные АС

Типовая архитектура и уровни доверия



HSM доверенные криптографические модули

- Криптографическая стойкость реализуемых алгоритмов и протоколов
- Соответствие требованиям в рамках соответствующей системы сертификации
- Подтверждение корректности и полноты реализации мер защиты со стороны аккредитованной испытательной лаборатории, сертификация
- Гарантии сопровождения, устранения неисправностей и уязвимостей со стороны производителя на всем протяжении жизненного цикла изделия

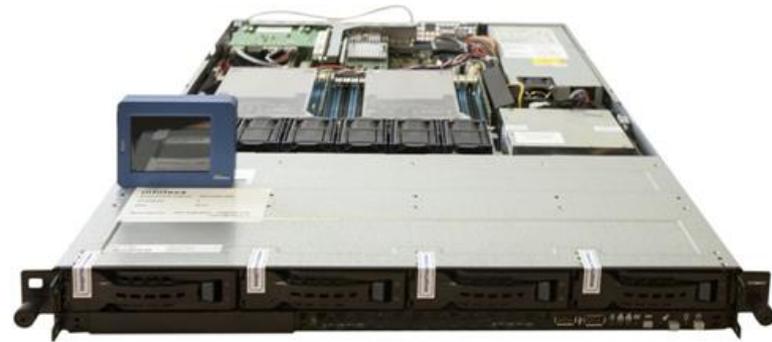
Требования

	Требования МПС	Российское законодательство
Алгоритмы	RSA, 3DES, AES, SHA	ГОСТ 34.10, 34.11, 34.12, 34.13, ГОСТ 28147-89
Требования	FIPS 140-2/PCI HSM	Требования к СКЗИ и ЭП ФСБ
Сертификация	Международные аккредитованные FIPS лаборатории	Отечественные испытательные лаборатории, аккредитованные ФСБ

ViPNet HSM

Высокопроизводительная криптографическая платформа

- Криптоалгоритмы: ГОСТ 28147-89, ГОСТ Р 34.10-2001/2012, ГОСТ Р 34.11-94/2012
- Криптографический интерфейс PKCS#11 для использования в прикладных сервисах
- Подключение сетевых сервисов по Ethernet 10 Гбит/с в многопоточном режиме
- SDK для ОС Windows/Linux для разработки сетевых прикладных сервисов и взаимодействия с HSM
- Отключаемая панель управления для выполнения наиболее критических операций инициализации и контроля режимов работы
- WEB-консоль удаленного управления под защитой TLS на ГОСТ



Безопасность применения достигается:

- реализацией схемы разделения секрета (нет суперпользователя)
- развитой ролевой моделью администраторов безопасности
- двухфакторной аутентификации

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

Сценарии применения

Криптомодули для удостоверяющих центров и серверов систем юридически значимого документооборота (в рамках 63-ФЗ)

Системы аутентификации пользователей

Построение TLS-шлюзов

Системы сдачи отчетности и любые другие системы электронных сервисов для B2B, B2C и B2G

Банковские системы электронных платежей



ViPNet HSM

Специфика архитектуры

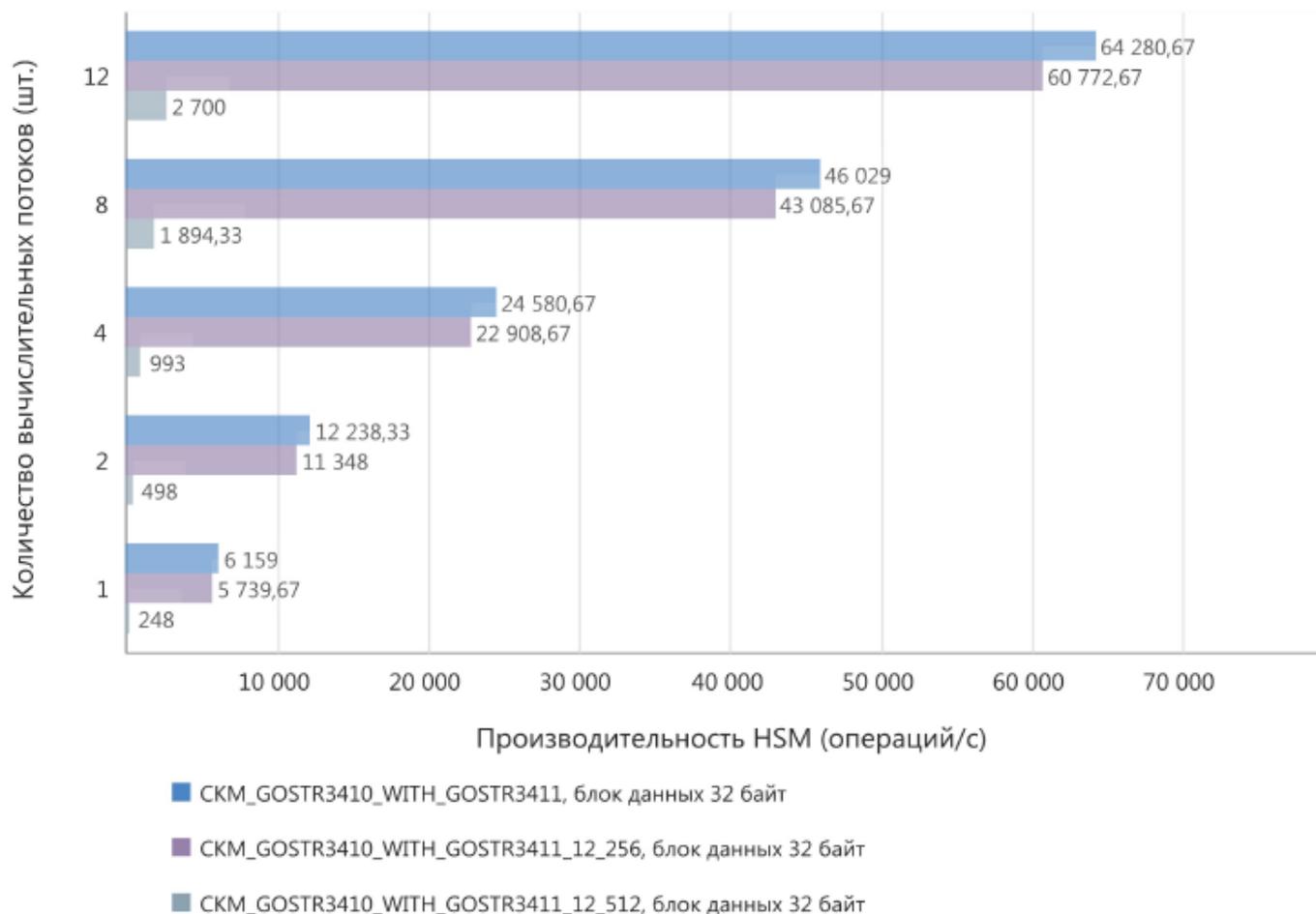
- Построен на базе двухпроцессорного сервера компании Аквариус
- Имеет встроенный физический датчик случайных чисел, реализованный по требованиям ФСБ России для СКЗИ классов КВ/КА
- Имеет встроенный модуль обнаружения вскрытия и контроля основных параметров работы платформы, хранения и гарантированного уничтожения мастер-ключей
- Допускает встраивание прикладных сервисов сторонних разработчиков, написанных на C, C++



ViPNet HSM

Производительность ViPNet HSM при вычислении электронной подписи

ПАК ViPNet HSM 1.0.284016



ViPNet HSM PS

сервисы для банковских электронных систем платежных карт

- 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

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 - 40 000 транзакций в секунду
- Дополнительная WEB-консоль для управления платежными сервисами

The image displays two screenshots of the ViPNet HSM PS web interface. The top screenshot shows the 'Модуль безопасности платёжных систем' (Payment System Security Module) configuration page. It includes a navigation menu with options like 'Главная', 'Настройка', 'Команды', 'Статистика', and 'Журналы'. The 'Конфигурация устройства' (Device Configuration) section contains several input fields: 'Уровень отладки' (Debug level) set to 5, 'Длина заголовка' (Header length) set to 4, 'Длина ZMK' (ZMK length) set to 'Single length', 'Длина PIN' (PIN length) set to 4, 'Таблица легимализации зашифрована' (Encryption table) set to 'on', and 'Высчитать проверку таблицы дешифрования' (Calculate decryption table check) set to 'on'. The bottom screenshot shows the 'Администрирование' (Administration) page, which features a dashboard with tiles for 'Параметры' (Parameters), 'Администрирование' (Administration), 'Резервирование' (Backup), and 'Сертификаты' (Certificates). Below the dashboard is a table listing administrators with columns for ID, Username, Password, Date of creation, and Role.

ID	Имя администратора	Пароль администратора	Дата создания	Роль
1	int_admin_1	int_admin_1	05.02.2016 17:57	Администратор инициализации
2	int_admin_2	int_admin_2	05.02.2016 17:57	Администратор инициализации
3	int_admin3	int_admin3	05.02.2016 17:57	Администратор инициализации
4	security_admin	security_admin	05.02.2016 17:57	Администратор безопасности
5	audit_admin	audit_admin	05.02.2016 17:57	Администратор аудита
6	backup_admin	backup_admin	05.02.2016 17:57	Администратор резервирования
7	api1	api1	05.02.2016 18:34	Администратор прикладного сервиса
8	api2	api2	05.02.2016 18:35	Администратор прикладного сервиса

ViPNet HSM PS

тестирование

- Проведено несколько циклов тестирования в режиме Удостоверяющего центра на площадке НСПК, продолжаются работы по уточнению ПМИ
- Проведено тестирование в режиме «Процессинг» на совместимость с командами HSM Thales на площадке Сбербанка/Сбертех – совместимость подтверждена, есть ряд предложений к развитию
- С ноября 2015 ведется тестирование в OpenWay (СПб), завершение тестирования ожидается в марте 2016

Сертификация

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?

Спасибо за внимание!
Вопросы?



Поташников Александр
potashnikov@infotecs.ru