# Программно-аппаратный модуль «ViPNet HSM PS» для обеспечения безопасности платежных систем

**Поташников Александр**

# Применение HSM в платежных системах

**Требования PCI DSS**

- Генерация стойких криптографических ключей
- Безопасное распространение ключей
- Безопасное хранение ключей
- Обеспечение жизненного цикла ключей, смена и удаление
- Шифрование данных держателей карт

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

# APPROVED PTS DEVICES

PIN Transaction Security (PTS) devices are used by a merchant at the point-of-interaction for capturing payment card data and validating approval of its use for a transaction. The Council, via PCI Recognized Laboratories, validates the conformance of PTS devices to the PCI PTS standard and provides a list of approved devices. The Council urges merchants to use approved PTS devices in their payment environments. Some payment brands require the use of approved PTS their acquirer or the payment br about such requirements.

*Please review the legal PTS*

HSM 13

Results: 13

| COMPANY | APPROVAL NUMBER | VERSION | PRODUCT TYPE | EXPIRY DATE |
|---|---|---|---|---|
| **ARX (Algorithmic Research, Ltd.)** | | | | |
| Algorithmic Research PrivateServer | | | | |
| **Hardware #:** Part Number: 4.8, Hardware Version Number: 4.7<br>**Firmware #:** Firmware Version Number: 4.8.2<br>**Applic #:**<br>View Security Policy | 4-70019 | 2.x | HSM | 30 Apr 2022 |
| **Bull S.A.S**<br>http://www.bull.com/payment-security/index.html | | | | |
| Crypt2Pay, Crypt2Protect | | | | |
| **Hardware #:** 005/A<br>**Firmware #:** 8.05-04-I, 8.05-07-I, 8.05-13I (The integral version), 8.05-13D (The CB version)<br>**Applic #:**<br>View Security Policy | | | | |
| **Cryptera A/S**<br>www.cryptera.com | | | | |
| INT1217-54xx | | | | |
| **Hardware #:** INT1217-54xx<br>**Firmware #:** 414-0487 R2x<br>**Applic #:** | | | | |
| **SafeNet Inc.**<br>www.safenet-inc.com | | | | |
| SafeNet Luna EFT 2.0 | | | | |
| **Hardware #:** 808-000059-001<br>**Firmware #:** 6.10.5<br>**Applic #:** 2.0.0<br>View Security Policy | 4-70020 | 2.x | HSM | 30 Apr 2022 |
| Luna EFT 1.3.2 and Luna EFT 1.4.4 and Luna EFT 1.4.7 and Luna EFT 1.4.9 | | | | |
| **Hardware #:** GRK-15-0100<br>**Firmware #:** MAL000001E, MAL 1.1<br>**Applic #:** M090401E, M090900E, M090902E,M090904E<br>View Security Policy | 4-70014 | 1.x | HSM | 30 Apr 2019 |
| **Thales E-Security** | | | | |
| payShield 9000 | | | | |
| **Hardware #:** 1600A466.01.X.X.X.X.X.X, 1600B466.01.X.X.X.X.X.X, 1600A466.04.X.X.X.X.X.X, 1600B466.04.X.X.X.X.X.X, 1600D466.04.X.X.X.X.X.X, 1600A466.05.X.X.X.X.X.X, 1600B466.05.X.X.X.X.X.X, 1600D466.05.X.X.X.X.X.X, 1600A466.06.X.X.X.X.X.X, 1600B466.06.X.X.X.X.X.X, 1600D466.06.X.X.X.X.X.X<br>**Firmware #:** 1317-1900 (Version 1.2a) including Boot Manager, PCI HSM Compliance Mode, Approved Boot Manager Versions: 1.16.12, 1.16.8, 1.18.2, 1346-1905 (Version 2.1c) including Boot Manager, HSM Manager: 4.1.x, 5.x.x, 1346-1907 (Version 2.1d) including Boot Manager, 1346-1914 (Version 2.3c) including Boot Manager, 1346-1917 (Version 2.3f) including Boot Manager, HSM Manager: 4.1x<br>**Applic #:** .<br>View Security Policy | 4-40069 | 1.x | HSM | 30 Apr 2019 |

# Авторизованные лаборатории


https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories

# 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 PCI лаборатории | Отечественные испытательные лаборатории, аккредитованные ФСБ |

# ViPNet HSM

## Основные характеристики

- 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
- Отключаемая панель управления для выполнения наиболее критических операций инициализации и контроля режимов работы
- WEB-консоль удаленного управления под защитой TLS на ГОСТ

# 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

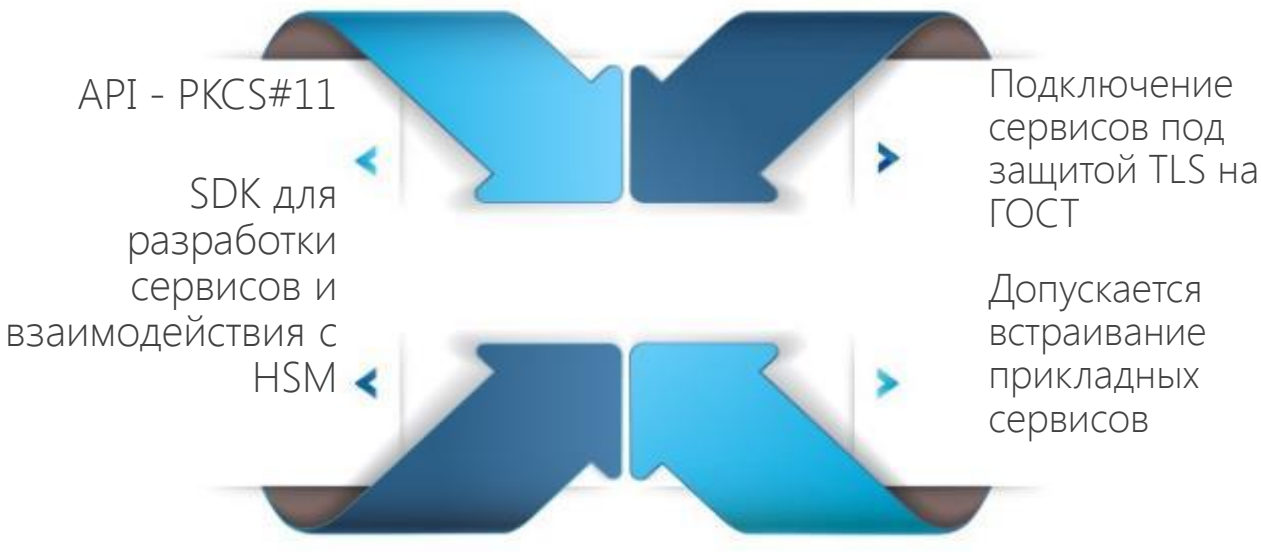
# ViPNet HSM

## 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



# 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**

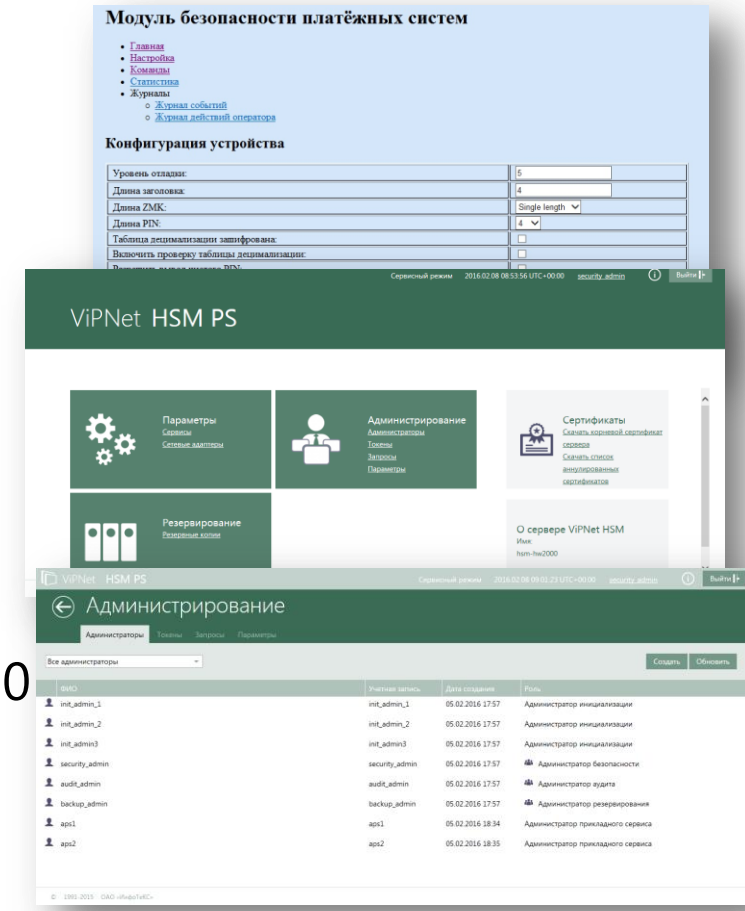

- Поддержка протоколов Visa и Mastercard, China Union Pay, American Express, МИР.
- Система команд и протоколы взаимодействия ViPNet HSM PS соответствуют реализованным в HSM Thales PayShield 9000 при работе в режиме совместимости с международными платёжными системами.
- Имеет дополнительную систему команд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

ТК 26 ГОСТР

# 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**

- Проведено несколько циклов тестирования в режиме Удостоверяющего центра на площадке НСПК, продолжаются работы по уточнению ПМИ и выбору лаборатории.
- Проведено тестирование в режиме «Процессинг» на совместимость с командами HSM Thales на площадке Сбербанка/Сбертеха – совместимость подтверждена, замечания учтены. Ожидается продолжение тестирование в июне 2016г.
- Тестирование в OpenWay (СПб), завершено успешно, установлена совместимость устройства ViPNet HSM PS с модулем авторизации Системы WAY4 по всей поддерживаемой на настоящий момент функциональности. Планируется дополнительное тестирование в режиме персонализации для карты МИР.

# Сертификация

- Завершается сертификация ПАК ViPNet HSM по требованиям к СКЗИ и ЭП класса КВ (криптоплатформа с алгоритмами ГОСТ).
  Заключение №149/3/2/1/901
- 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.
- Согласование модели нарушителя, формирование и утверждение требований к модулям HSM для использования в НСПК. Работы начаты, проводятся совместно с ООО «Крипто-ПРО».
- Проверка соответствия разработанным требованиям, по готовности требований.

infotecs

# Спасибо за внимание!
# Вопросы?

**Поташников Александр**
potashnikov@infotecs.ru