ViPNet HSM

Высокопроизводительная программно-аппаратная криптографическая платформа

Удобство использования электронных сервисов в любом месте и любое время приводит к их распространению и росту популярности. Для обеспечения безопасности таких сервисов требуются мощные и надежные криптографические средства. ViPNet Hardware Security Module (ViPNet HSM) — решение для защиты электронных сервисов.

ViPNet HSM — высокопроизводительная и высоконадежная платформа, выполняющая криптооперации по запросам различных сервисов. ViPNet HSM может располагаться в любом окружении, так как все операции выполняются во внутренней защищенной среде: хранимые ключи невозможно извлечь, данные пользователей — изменить.

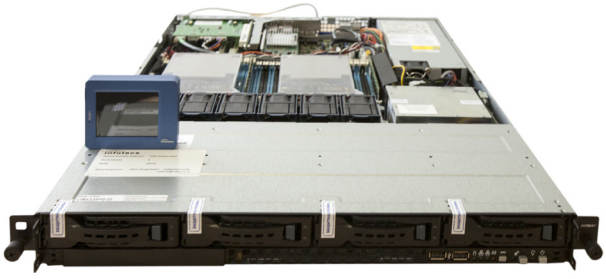
ViPNet HSM обеспечивает поддержание полного жизненного цикла криптоключей, реализацию операций ЭП и шифрования (ГОСТ 28147-89, ГОСТ Р 34.10-2001/2012). ViPNet HSM может использоваться в сценариях управления TLS-соединениями, работы удостоверяющих центров, эмиссии банковских карт и обработки платежных операций.

Преимущества

- Надежная защита от физического НСД к хранимым данным с помощью датчика вскрытия корпуса и изменения физических параметров платформы (температура, питание).
- Криптостойкий механизм выработки ключей с использованием встроенного физического датчика случайных чисел.
- Гарантия неизменности настроек платформы за счет применения ролевой модели разграничения прав администраторов (кворум) и разделения секрета по схеме Шамира.
- Производительность до 35 тысяч операций подписи в секунду.
- Широкие возможности применения посредством интеграции ПО для обработки запросов различных сторонних сервисов.

Сертификация по классу КВ

ViPNet HSM проверяется на соответствие требованиям к СКЗИ и требованиям к средствам ЭП по классу КВ. Завершение сертификационных испытаний планируется в 1 квартале 2016 года.



Особенности

- Запись значимых для безопасности событий в системный журнал.
- Веб-интерфейс для удаленного администрирования по защищенному каналу и сенсорный экран для локальной настройки.
- Интерфейс PKCS#11 для работы с прикладными сервисами.
- Поддержка работы с прикладными сервисами, управляемыми ОС Windows и Linux.

infotecs

Применение ViPNet HSM

Платежные системы: обеспечение безопасности финансовых операций в национальной и международных системах платежных карт, включая MasterCard и Visa.

- Обработка банковских транзакций* в режиме совместимости с протоколами отечественной и международных платежных систем.
- Поддержка эмиссии банковских карт, выработка и печать ПИН-кодов.
- Реализация функций центра сертификации платежных систем.
- Поддержка международного стандарта операций по банковским картам EMV, в том числе со встроенными отечественными криптоалгоритмами.
- Работа с основными отечественными и международными платежными приложениями терминального оборудования (M/Chip, VSDC).

Удостоверяющий центр: увеличение сроков действия ключей электронной подписи и корневых сертификатов, снижение рисков компрометации ключей.

- Создание и хранение ключей администраторов удостоверяющих центров в изолированной доверенной среде ViPNet HSM.
- Формирование и проверка электронной подписи по ГОСТ Р 34.10-2001/2012, хэширование данных по ГОСТ Р 34.11-94/2012.
- Совместное использование с серверами меток времени (TSP) и серверами проверки статуса сертификатов (OCSP).

Облачный сервис ЭП: снижение расходов на развертывание инфраструктуры открытых ключей (PKI).

- Надежное хранение ключей пользователей электронного документооборота в ViPNet HSM.
- Защищенный доступ пользователей к ключам и операции электронной подписи.

TLS-шлюз: повышение быстродействия и защита данных при работе с веб-серверами.

- Установление и поддержание TLS-соединений между пользователями и веб-сервером с помощью оптимизированных программно-аппаратных средств ViPNet HSM.
- Защищенный обмен данными между пользователем и веб-сервером в Интернете.
- Простота интеграции ViPNet HSM в инфраструктуру веб-сервера.

* Заключение по результатам совместного тестирования с модулем авторизации системы WAY4 компании OpenWay ожидается в 1 квартале 2016 года.

ОАО «ИнфоТеКС»
127287, Москва, Старый Петровско-Разумовский проезд, 1/23, стр. 1
Телефон: +7 495 737-6192, 8 800 250-0-260 (бесплатный звонок по России)
Факс: +7 495 737-7278
Email: soft@infotecs.ru, hotline@infotecs.ru
Web: www.infotecs.ru

10030-01 102 01 RUS