



ViPNet HSM

Высокопроизводительная программно-аппаратная криптографическая платформа

infotecs

www.infotecs.ru

Основа обеспечения безопасности электронных сервисов – мощные и надежные криптографические средства. В качестве криптографического ядра системы защиты может быть использован Программно-аппаратный комплекс ViPNet HSM (Hardware Security Module).

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

ViPNet может использоваться в сценариях работы платежных систем, удостоверяющих центров, систем электронного документооборота, АСУ ТП, систем, построенных на технологии блокчейн.

ViPNet HSM обеспечивает поддержание полного жизненного цикла криптоключей, реализацию операций ЭП, шифрования и имитозащиты (ГОСТ 28147-89, ГОСТ Р 34.10-2001/2012, 34.11-94/2012).



- Производительность до 35 тысяч операций подписи в секунду.
- Широкие возможности применения посредством интеграции для обработки запросов различных сторонних сервисов.



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.



ПРЕИМУЩЕСТВА

- Криптостойкий механизм выработки ключей с использованием встроенного физического датчика случайных чисел.
- Надежная защита от физического НСД к хранимым данным с помощью датчика вскрытия корпуса и изменения физических параметров платформы (температура, питание).
- Гарантия неизменности настроек платформы за счет применения ролевой модели разграничения прав администраторов (кворум) и разделения секрета по схеме Шамира.



СЕРТИФИКАЦИЯ

Получен сертификат ФСБ России о соответствии ViPNet HSM требованиям к СКЗИ и средствам ЭП по классу KB (KB2).



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).

** По результатам совместного тестирования с модулем авторизации системы WAY4 компании OpenWay и ПО TranzWare online компании Compass Plus*

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.

БЛОКЧЕЙН:

Доверенная платформа для различных применений распределенного реестра.

- Аппаратный кошелек и/или шлюз между реальным счетом и криптовалютым.
- Поддержка функционала высокопроизводительного узла (ноды) блокчейн-сети, например, валидатора в протоколах достижения консенсуса.
- Интерфейс между реальным и цифровым миром.
- Реализация криптографических блокчейн-примитивов: механизмов кольцевых электронных подписей и протоколов доказательства с нулевым разглашением.