КриптоПро HSM 2.0

Защищённое хранилище криптографических ключей

Высокопроизводительный программно-аппаратный криптографический модуль, сертифицированный ФСБ России по классу КВ2, предназначенный для безопасного хранения и использования криптографических ключей, применяемых в различных информационных системах.

Назначение

HSM обеспечивает выполнение следующих операций:

- **Формирование и проверка ЭП**
  по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, ECDSA и RSA
- **Вычисление значений хэш-функции**
  по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012, SHA-1, SHA-2
- **Шифрование и расшифрование данных**
  по ГОСТ Р 34.12-2015, ГОСТ 28147-89, AES, DES, 3DES, RC2, RC4
- **Имитозащита данных**
  по ГОСТ 28147-89
- **Операции на эллиптических кривых**
  в т.ч. работа на сверхскоростных скрученных эллиптических кривых Эдвардса

Безопасность

В КриптоПро HSM 2.0 реализованы надежные механизмы защиты ключей:

- Разделение секрета «3 из 5» между администраторами безопасности для активации HSM
- Датчики вскрытия корпуса HSM
- Доверенная операционная система
- Безопасные механизмы аудита и контроля подключений

Безопасное хранилище ключей ЭП

КриптоПро HSM 2.0 может использоваться для безопасного размещения ключей любой системой, поддерживающей выполнение криптографических операций через CryptoAPI и JCA (Java), например:

- Удостоверяющий центр (КриптоПро УЦ)
- Создание ЭП в автоматизированном режиме
- Служба онлайн проверки статусов сертификатов (КриптоПро OCSP Server)
- Служба штампов времени (КриптоПро TSP Server)
- Система облачной электронной подписи (КриптоПро DSS)

Производительность и отказоустойчивость

- Поддержка отказоустойчивых конфигураций и горизонтального масштабирования
- Производительность до 50 000 формирований ЭП в секунду (при пакетной обработке)
- Возможность хранения до 500 000 ключей с возможностью расширения до 20 000 000 и более

Единая биометрическая система (ЕБС)

Класс защиты КВ2 позволяет банкам использовать HSM для выполнения требований по взаимодействию с ЕБС:

- Для ЭП собираемых биометрических ПДн
- Для взаимодействия с ЕБС при аутентификации и авторизации пользователей

Подпись кода

HSM может быть использован для подписи кода распространенных платформ и для безопасного хранения ключей ЭП кода. Ведущие поставщики EV-сертификатов (DigiCert) позволяют использовать HSM в качестве хранилища ключей.

Поддерживаемые технологии подписи:

- Microsoft Authenticode
- Java Code Signing

Поддерживаемые API:

- Microsoft CryptoAPI
- Microsoft CNG
- PKCS#11
- Java Cryptography Architecture (JCA)

Технические характеристики

Напряжение:	220 В, в корпусе установлены два вентилятора охлаждения
Число электрических входов:	2 шт.
Блок питания:	500 Вт, двойной, с горячей заменой
Разъемы электропитания:	C14 (2 шт.)
Энергопотребление:	До 300 Вт
Процессоры:	INTEL XEON E5-2620V3 2.4 GHz (2 шт.)
Сетевая карта:	Allied Telesis, Gigabit Ethernet Fiber Adapter, 1000-Base-SX двойной (1 шт.)
Габариты (в, ш, г):	9 см (2U), 43 см (19”), 52 см
Вес нетто:	12,5 кг
Вес с упаковкой:	17 кг
Размер упаковки:	64x57x21 см

Контакты

@CryptoProAssistantBot info@cryptopro.ru +7 (495) 995-48-20 https://cryptopro.ru