



HSM PS plus

payment systems

СПБ

ГРУППА КОМПАНИЙ

Модуль безопасности для систем платёжных карт

Отечественная разработка

Программно-аппаратный комплекс в исполнении 1U и в единой конструкции, обеспечивающий уровень физической и логической защиты.



подробнее



Интерфейсы

2 HOST x 1GbE

2 RM x 1 GbE

ПРИМЕНЕНИЕ

в Бэкенд системах банков и платёжных системах для защиты персональных данных держателей карт, в следующих в процессах и механизмах систем платёжных карт:

- инициализация платёжных карт при их производстве,
- эмиссия платёжных карт,
- авторизация платёжных транзакций,
- эквайринг,
- 3D-Secure,
- генерация, смена, резервирование, экспорт ключей,
- поддержка работы НСПК в качестве ОПКЦ.

ПРЕИМУЩЕСТВА

- Высокая производительность — до 25 000 tps (на AES key block).
- Компактное исполнение — моноблок 1U для стойки 19" с обдувом Front-to-Back.
- Доступны четыре интерфейса с резервированием: 2 HOST и 2 Удаленное управление, подключение к которым теперь возможно с задней панели.
- Подключение сменных оптических SFP модулей.
- Дисплей на передней панели.
- Поддержка команд с использованием криптографии на эллиптических кривых (ECC): ECDSA, ECDH-ES.
- Поддержка команд экспорта/импорта ключей в формате ASC X9 TR 34-2019.
- Расширенный мониторинг и диагностика по SNMP v3.
- Улучшенный интерфейс настройки сетевых параметров с визуализацией состояния сетевых интерфейсов.
- Поддержка российских криптоалгоритмов в соответствии с ГОСТ.

ХАРАКТЕРИСТИКИ

HOST-интерфейсы	2 x 1 GbE, TCP/IP, UDP	сменные SFP-модули, LC, SMF: 1310 нм, MMF: 850 нм
Remote control-интерфейсы	2 x 1 GbE, TLS 1.3	сменные SFP-модули, LC, SMF: 1310 нм, MMF: 850 нм
Local management-интерфейс (передняя панель)	1 GbE, RJ-45	
Производительность	до 25 000 CPS/TPS	
Мониторинг	SNMPv3	
Форм-фактор	19" моноблок 1U, обдув Front-to-Back	
Электропитание	220 В, два блока питания с резервированием	
Основные криптографические алгоритмы и механизмы	Криптографические алгоритмы: DES/3DES – NIST FIPS 46-3/SP 800-67 и ISO/IEC 10116; AES – NIST FIPS 197; RSA – RFC 3447 и NIST FIPS 186-4; SHA-1 – RFC 3174 и NIST FIPS 180-4; SHA-384, SHA-256, SHA 512 – ISO/IEC 10118-2 и NIST 180-4; MAC – ISO 9797-1; HMAC – ISO/IEC 9797-2 и NIST FIPS 198-1; ECDSA – ANSI X9.62; ECDSA-DH, ECKA – NIST SP 800-56A, NIST SP 800-56C Поддерживаемые механизмы: SCP-02, SCP-03, в том числе Global Platform v.2.2.1; EMV CPS 1.1; EMV 3.1.1, EMV 4.1, EMV 4.3 (ARQC/ARPC/AAC), IDN, Union Pay (ARQC/ARPC) CVP/iCVP/CVP2; CVC/CVV/CVC3; PVV, IBM 3624; MST; MasterCard CAP; CAVV; PIN Block (ISO 9564-1): ISO-0 (Format 0), ISO-1 (Format 1), ISO-3 (Format 3), ISO 4 (Format 4); ANSI X9-24 (DUKPT) ISO 15946-1, EMV v4.4 B2.2.4 (ECC Key Generation)	
Поддерживаемые форматы ключевых контейнеров для экспорта	ASC X9 TR 31-2018, ASC X9 TR 34-2019, Thales Variant Scheme (ANSI X9.17), PKCS #1 v1.5, PKCS #1 v2.2, ECC ANSI X9.62	
Российские криптографические алгоритмы (PKA)	Блочный шифр «Кузнечик» ГОСТ Р 34.12-2015 в режимах ГОСТ Р 34.13 2015, хэш функция ГОСТ Р 34.11-2012	
Физическая безопасность	Конструкция, обеспечивающая защиту от НСД, использование различных систем обнаружения НСД и датчиков вскрытия — механические микропереключатели, датчик света/датчик объёма	
Класс СКЗИ	класс KB	

ПРОИЗВОДИТЕЛЬ

CBS



СИСТЕМЫ ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

ООО «Системы
практической
безопасности»
+7 (812) 468-15-61
info@systempb.ru
www.systempb.ru
www.skzi.ru

ДИСТРИБЬЮТОР

ГРУППА
КОМПАНИЙ
«СПБ»

СПЕЦИНТ



ООО «СПЕЦИНТ»

+7 (495) 727-28-25
ask@specint.ru
www.specint.ru