

МОНОБЛОК 2U ДЛЯ УСТАНОВКИ В СТОЙКУ 19"



ПРЕИМУЩЕСТВА

Высокая производительность

Совместимость с основными вендорами ПО

Технические преимущества

- Защита ключей (в «железе» в защищённой зоне)
- Двойной контроль (необходимы два администратора безопасности для подтверждения операций)
- Разделение полномочий
- Надёжный генератор случайных чисел
- Разделение ключей по назначению

Защита бренда посредством защиты приложений

- Защита конфиденциальных данных (ключей шифрования, ПИН-кодов и т.п.)
- Конфиденциальные данные и их обработка проходит в границах МБ
- Защита от внешнего и внутреннего нарушителя

Выполнение требований регуляторов и платёжных систем

- Соответствие требованиям МПС и НПСК
- Соответствие требованиям международных стандартов (PCI DSS, PCI PIN)

Наличие соответствующих сертификатов и реализация необходимых стандартов, предоставляет надёжный фундамент для аттестации/сертификации всей системы

ХАРАКТЕРИСТИКИ

Интерфейс, протокол с HOST системой	2x1 GbE, UDP, TCP/IP для МБ СПК Base (SPB HSM PS base)
Производительность	1000 tps для МБ СПК Base (SPB HSM PS base)
Лицензии	Core, Legacy, Загрузка LMK с внешних носителей
Международные криптографические алгоритмы и механизмы	<p>Криптографические алгоритмы: DES/3DES – NIST FIPS 46-3 SP 800-67 и ISO 10116, AES – NIST FIPS 197, RSA – RFC 3447 NIST FIPS 186-4, SHA-1 – RFC 3174 и NIST FIPS 180-4, SHA-224, SHA-384, SHA-256, SHA-512 – ISO/IEC 10118-2 и NIST 180-4, MAC – ISO 9797 и NIST FIPS 198-1, HMAC – ISO/IEC 9797-2</p> <p>Поддерживаемые механизмы: Global Platform v.2.2.1, EMV CPS 1.1, EMV3 1.1, EMV 4.1, EMV 4.3 (ARQC/ARPC/AAC), IND, Union Pay (ARQC/ARPC), CVP/iCVP/CVP2 CVC/CVV/CVC3, PVV, MST, MasterCard CAP, CAVV, PIN Block (ISO 9564-1) – в том числе ISO-0, ISO-3, ISO-4, IBM 3624, ANSI X9-24 (DUKPT)</p>
Российские криптографические алгоритмы (РКА)	Блочный шифр «Кузнечик» ГОСТ Р 34.12-2015 в режимах ГОСТ Р 34.13-2015, хэш функция ГОСТ Р 34.11-2012
Совместимость с банковским ПО	ОБ-Инвестиция, БПС Инновационные решения, Компас Плюс
Электропитание	220 В, резервированное питание, два источника
Физическая безопасность	Конструкция, обеспечивающая защиту от НДС, использование различных систем обнаружения НДС и датчиков вскрытия – механические микропереключатели, акселерометр, датчик света/датчик объёма
Методы генерации и защиты локальных мастер ключей	Совместное использование ФДСЧ и ПДСЧ для генерации, хранение в зашифрованном виде на РКА во внутренней памяти криптоблока гарантированное стирание при обнаружении попытки НДС. При генерации используется вариантный метод и метод keyblock
Поддерживаемые форматы ключевых контейнеров для экспорта	ASC X9 TR-31-2018 (в том числе TR-31-ТК26 MAGMA/KUZNECHIK), Thales Variant Scheme (ANSI X9.17), PKCS #1 v1.5, PKCS #1 v2.2
Резервирование локальных мастер ключей	В виде компонент на смарт-картах непосредственно из криптоблока с применением алгоритмических мер защиты от ПЭМИН
Защита от ПЭМИН	Соответствует классу KB для СКЗИ, обеспечивается рядом конструктивных, схмотехнических и алгоритмических мер
Сертификат ФСБ	№СФ/124-4566 от 10.05.23

