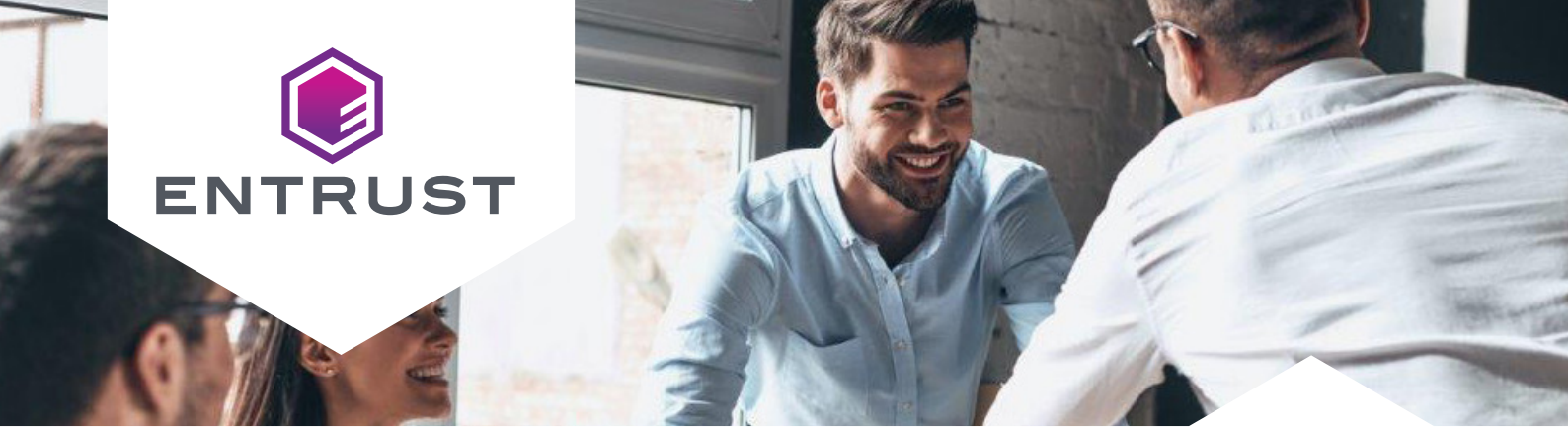


Аппаратные модули безопасности nShield Solo

Сертифицированные карты PCI-Express, предоставляющие криптографические ключи для автономных серверов

ОБЗОР

Аппаратные модули безопасности nShield Solo (HSM) — это сертифицированные по стандарту FIPS низкопрофильные карты PCI-Express, которые предоставляют криптографические ключи приложениям, размещенным на сервере или устройстве. Эти устойчивые к взлому карты выполняют такие функции, как шифрование, цифровая подпись, создание ключей и защита в широком спектре приложений, включая центры сертификации, подписание кода, пользовательское программное обеспечение и многие другие.

В серию nShield Solo включены модули nShield Solo+ и высокопроизводительные модули nShield Solo XC.

Архитектура с высокой степенью гибкости

Уникальная архитектура Security World от nCipher позволяет сочетать модели HSM nShield и создавать комбинированную структуру, тем самым обеспечивая гибкую масштабируемость, плавное переключение при отказе и балансировку нагрузок.

Обработка большего объема данных за меньшее время

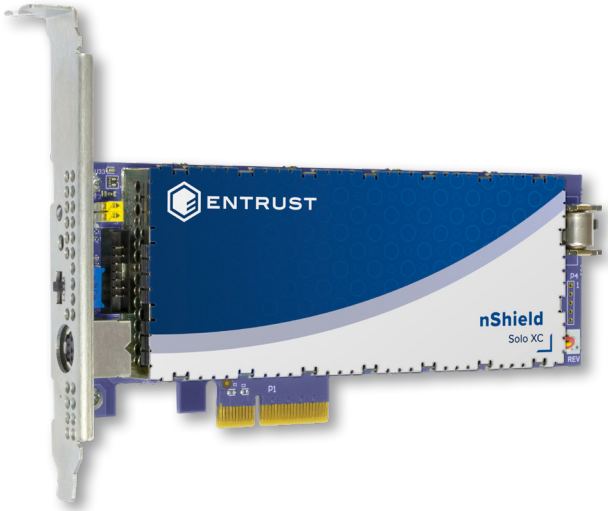
Благодаря поддержке высокой скорости операций аппаратные модули безопасности nShield Solo являются оптимальным решением для производственных предприятий, розничной торговли, Интернета вещей и других сред, где критически важна пропускная способность.

Защитите свои фирменные приложения и данные

Функция CodeSafe обеспечивает безопасную среду для запуска конфиденциальных приложений в пределах nShield.

ОСНОВНЫЕ СВОЙСТВА И ПРЕИМУЩЕСТВА

- Максимизация производительности и доступности за счет высокой скорости криптографических операций и гибкого масштабирования
- Поддержка широкого спектра приложений, включая центры сертификации, подписание кода и многое другое
- nShield CodeSafe защищает приложения в безопасной среде выполнения от nShield
- nShield Remote Administration помогает сократить расходы и количество выездов в центры обработки данных



БОЛЕЕ ПОДРОБНАЯ ИНФОРМАЦИЯ РАЗМЕЩЕНА ПО ССЫЛКЕ ENTRUST.COM/RU/HSM

Аппаратные модули безопасности nShield Solo

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Поддерживаемые криптографические алгоритмы

- Асимметричные алгоритмы: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- Симметричные алгоритмы: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES
- Хэш / дайджест сообщения: MD5, SHA-1, SHA-2 (224, 256, 384, 512 бит), HAS-160, RIPEMD160
- Реализация Full Suite B с полностью лицензированным шифрованием на основе эллиптических кривых (ECC), включая Brainpool и пользовательские кривые

Поддерживаемые платформы

- ОС Windows и Linux, включая дистрибутивы RedHat, SUSE и основных поставщиков облачных услуг, виртуальные машины, контейнерные приложения
- Поддерживаются виртуальные среды Solo XC, включая VMware ESX, Microsoft Hyper-V, Linux KVM и Citrix XenServer

Интерфейсы прикладного программирования (API)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI и CNG, nCore и веб-службы (требуется пакет Web Services Option Pack)

Подключение к хосту

- PCI Express версии 2.0; разъем Solo+: однополосный, разъем Solo XC: четырехполосный

Соответствие требованиям безопасности

- Сертификат FIPS 140-2 уровня 2 и уровня 3
- Solo+: сертификат Common Criteria EAL4+ (AVA_VAN.5)
- Solo+ признано квалифицированным устройством для создания подписей (QSCD)
- Solo XC: сертификаты eIDAS и Common Criteria EAL4 + AVA_ VAN.5 и ALC_ FLR.2 в соответствии с профилем защиты EN 419 221-5, по голландской программе NSCIB
- Solo XC: соответствует BSI AIS 20/31

Соответствие стандартам безопасности и экологичности

- UL, UL/CA, CE, FCC, ICES (Канада), KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Управление и мониторинг

- nShield Remote Administration и nShield Monitor
- Защищенное ведение журнала аудита
- Поддержка диагностики системного журнала и мониторинг производительности Windows
- Агент наблюдения по протоколу SNMP

ДОСТУПНЫЕ МОДЕЛИ И ИХ ПРОИЗВОДИТЕЛЬНОСТЬ

Модели nShield Solo	500+	XC Base	6000+	XC Mid	XC High
Производительность подписания по алгоритму RSA (количество операций в секунду) для ключей длины, рекомендованной NIST					
2048 бит	150	430	3000	3500	8600
4096 бит	80	100	500	850	2025
Производительность подписания по простой кривой при шифровании на основе эллиптических кривых (количество операций в секунду) для ключей длины, рекомендованной NIST					
256 бит	540	680	2400	7515[1]	14 400[1]

Размеры	Вес		Потребление энергии	
	Solo+	Solo XC	Solo+	Solo XC
56,2 × 167,1 × 15,4 мм	230 г	280 г	10 Вт	24 Вт
2,2 × 6,6 × 0,6 дюйма	0,5 фунта	0,62 фунта		

Примечание 1. Для указанной производительности требуется бесплатная активация функции быстрого генерирования случайных чисел по алгоритму ECDSA на основании запроса в службу поддержки nCipher.

Более подробная информация размещена по ссылке
entrust.com/HSM

ENTRUST

Пишите нам:
HSMinfo@entrust.com