Аппаратные модули безопасности nShield Connect

Безопасность приложений напрямую зависит от того, где вы храните свои ключи

ОБЗОР

Комплексные возможности

Аппаратные модули безопасности nShield Connect (HSM) — это сертифицированные по стандартам FIPS 140-2 и Common Criteria EAL4+ (EN 419 221-5) устройства, обеспечивающие использование масштабируемых служб криптографических ключей высокой надежности в сетях клиентов.

- Высокая скорость криптографических операций и гибкое масштабирование
- Интеграция с более чем 150 решениями от ведущих поставщиков приложений
- Среда CodeSafe для защиты логики приложений и логики предметной области в безопасной среде выполнения nShield

Аппаратные модули безопасности nShield Connect — это защищенные от несанкционированного доступа платформы, выполняющие такие функции, как шифрование, цифровая подпись, а также создание и защита ключей для ряда сфер применения, включая:

- Центры сертификации
- Подписание кода
- Программное обеспечение под заказ
- Облачные и контейнерные приложения
- Веб-сервисы
- Блокчейн
- Шифрование баз данных

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

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

Аппаратные модули безопасности nShield Connect

ОСНОВНЫЕ СВОЙСТВА И ПРЕИМУЩЕСТВА

Архитектура с высокой степенью гибкости

Уникальная архитектура Security World 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 Connect являются оптимальным решением для сред, где критически важна пропускная способность, например для производственных предприятий, розничной торговли и Интернета вещей.

ВЫСОКАЯ ЭФФЕКТИВНОСТЬ ДИСТАНЦИОННЫХ ФУНКЦИЙ

Больше не потребуется посещать центры обработки данных

Решение для удаленного администрирования nShield Remote Administration: безопасное дистанционное представление смарт-карт авторизации удаленным HSM для проведения обслуживания, включая обновление встроенного ПО, регистрацию новых HSM и переназначение/реконфигурацию существующих HSM. Имеется отдельный лист технических данных.

Решение для дистанционного изменения конфигурации Remote Configuration: версия Connect XC с последовательной консолью позволяет персоналу центра обработки данных проводить простую установку, удаленно изменять конфигурацию сети и настраивать пользовательский интерфейс.

nShield Monitor: единая панель мониторинга всех ваших аппаратных модулей безопасности nShield, позволяющая оптимизировать операции и увеличивать время безотказной работы. Имеется отдельный лист технических данных.

Защитите свои фирменные приложения

CodeSafe обеспечивает безопасную среду для запуска конфиденциальных приложений в пределах физических границ оборудования nShield в соответствии со стандартом FIPS 140-2. Более подробная информация приведена в листе технических данных CodeSafe.

ДОСТУПНЫЕ МОДЕЛИ И ИХ ПРОИЗВОДИТЕЛЬНОСТЬ

Модели nShield Connect	500+	XC Base	1500+	6000+	XC Mid	XC High
Производительность подписания по алгоритму RSA (количество операций в секунду) для ключей длины, рекомендованной NIST						
2048 бит	150	430	450	3000	3500	8600
4096 бит	80	100	190	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	1260	2400	7515[2]	14 400[2]
Клиентские лицензии						
Включено	3	3	3	3	3	3
Максимальное количество	10	10	20	без ограничений[1]	20	без ограничений[1]

Примечание 1. Требуется клиентская лицензия уровня предприятия.

Примечание 2. Для указанной производительности требуется бесплатная активация функции быстрого генерирования случайных чисел по алгоритму ECDSA на основании запроса в службу поддержки nCipher Support.

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

Аппаратные модули безопасности nShield Connect

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Поддерживаемые криптографические алгоритмы (включая полную реализацию пакета NIST Suite B)	Поддерживаемые платформы	Интерфейсы прикладного программирования (API)	Подключение к хосту	Соответствие требованиям безопасности
• Асимметричные алгоритмы: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (включая кривые NIST, Brainpool и secp256k1), ECDH, Edwards (Ed25519, 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	• ОС Windows и Linux, включая дистрибутивы RedHat, SUSE и основных поставщиков облачных услуг, виртуальные машины, контейнерные приложения	• PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG и веб-службы (требуется пакет Web Services Option Pack)	• Два порта Gigabit Ethernet (два сегмента сети)	• Сертификат FIPS 140-2 уровня 2 и уровня 3 • Сертификат IPv6 и совместимость с USGv6 • Connect 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 • Connect+: сертификат Common Criteria EAL4+ (AVA_VAN.5) • Connect+: признано квалифицированным устройством для создания подписей (QSCD) • Connect XC: соответствует BSI AIS 20/31

Соответствие стандартам безопасности и экологичности	Высокая доступность	Управление и мониторинг	Физические характеристики
• UL, CE, FCC, RCM (Канада) ICES RoHS2, WEEE	• Все твердотельные накопители • Блок вентиляторов, обслуживаемый на месте, два блока питания с возможностью замены без выключения	• nShield Remote Configuration (доступно в моделях Connect XC с последовательной консолью) • nShield Remote Administration (приобретается отдельно) • nShield Monitor (приобретается отдельно) • Защищенное ведение журнала аудита • Поддержка диагностики системного журнала и мониторинг производительности Windows • Агент наблюдения по протоколу SNMP	• Монтаж в стандартной стойке 1U 19 дюймов. Размеры: 43,4 x 430 x 705 мм (1,7 x 16,9 x 27,8 дюйма) • Вес: 11,5 кг (25,4 фунта) • Входное напряжение: 100–240 В переменного тока с автоматическим переключением, 50–60 Гц • Потребляемая мощность: до 2,0 А при напряжении 110 В переменного тока, 60 Гц | 1,0 А при напряжении 220 В переменного тока, 50 Гц • Теплоотдача: от 327,6 до 362,0 БТЕ/ч (при полной нагрузке) • Надежность: средняя наработка на отказ (часов)[3], Connect XC: 107 384 ч, Connect+: 99 284 ч

Примечание 3. Рассчитано при рабочей температуре 25 °C по стандарту Telcordia SR-332 «Процедура прогнозирования надежности электронного оборудования».

Более подробная информация об аппаратных модулях безопасности nShield от Entrust:

HSMinfo@entrust.com
entrust.com/ru/HSM

ОБ ENTRUST CORPORATION

Корпорация Entrust стоит на страже безопасности в сферах идентификационной информации, платежей и защиты данных по всему миру. Сегодня требования к бесперебойной и безопасной работе как никогда высоки и проявляются во всех аспектах жизни: во время зарубежных поездок, совершения покупок, получения доступа к услугам электронного правительства, входа в корпоративную сеть. Entrust предлагает беспрецедентно широкий спектр решений в области цифровой безопасности и выдачи учетных данных, на которых основано любое такое взаимодействие. Нам доверяют самые надежные организации мирового масштаба, и это неудивительно: мы предлагаем поддержку от более чем 2500 сотрудников и глобальную партнерскую сеть, которую уже оценили клиенты в более чем 150 странах.

Более подробная информация размещена по ссылке
entrust.com/HSM

ENTRUST

Пишите нам:
HSMinfo@entrust.com