



ENTRUST

Аппаратные модули безопасности nShield Edge

Сертифицированные портативные устройства, предоставляющие криптографические ключи для настольных приложений

ОБЗОР

Аппаратные модули безопасности nShield Edge (HSM) — это полнофункциональные, сертифицированные по стандарту FIPS USB-устройства, обеспечивающие шифрование, создание и защиту ключей, а также удобство и экономичность.

- Максимальная экономия. nShield Edge — самый бюджетный HSM в семействе nShield
- Поддержка широкого спектра приложений, включая центры сертификации, подписание кода и многое другое
- Высокий уровень безопасности. HSM nShield Edge сертифицированы до уровня 3 по стандарту FIPS 140-2.

Разработаны для сред с небольшим объемом операций

Подходят для автономных сред создания ключей и разработки, обеспечивая при этом поддержку множества алгоритмов различных API. Идеально подходят для развертываний с использованием собственных ключей (BYOK), требующих создания криптографических ключей с гарантией уровня стандарта FIPS 140-2 перед их безопасным экспортом в облако.

Портативные

Небольшая легкая конструкция с удобным USB-интерфейсом, поддерживает множество платформ, включая ноутбуки и другие портативные устройства.

Экономичные и масштабируемые

nShield Edge — самые экономичные HSM в семействе nShield. Это HSM начального уровня с возможностью масштабирования среды по мере роста ваших потребностей. Уникальная архитектура Security World от Entrust позволяет сочетать модели HSM nShield и создавать комбинированную структуру, тем самым обеспечивая гибкую масштабируемость, совместное использование ключей, плавное переключение при отказе и балансировку нагрузок.



БОЛЕЕ ПОДРОБНАЯ ИНФОРМАЦИЯ РАЗМЕЩЕНА ПО ССЫЛКЕ [ENTRUST.COM/RU/HSM](https://www.entrust.com/ru/hsm)



Аппаратные модули безопасности nShield Edge

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Поддерживаемые криптографические алгоритмы (включая полную реализацию пакета NIST Suite B)	Поддерживаемые ОС	Интерфейсы прикладного программирования (API)	Подключение к хосту	Соответствие требованиям безопасности
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64 Red Hat Enterprise Linux AS/ES 6 x64, x86 и 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64, 15.1 x64 Oracle Enterprise Linux 6.10 x64, 7.6 x64 	<ul style="list-style-type: none"> PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI и CNG, nCore, веб-службы (требуется пакет Web Services Option Pack) 	<ul style="list-style-type: none"> USB-порт (совместимый с 1.x, 2.x) 	<ul style="list-style-type: none"> Сертификат FIPS 140-2 уровня 2 и уровня 3

Соответствие стандартам безопасности и экологичности	Управление и мониторинг	Физические характеристики	Производительность
<ul style="list-style-type: none"> UL, CE, FCC, RCM и ICES RoHS2 (Канада), WEEE 	<ul style="list-style-type: none"> Защищенное ведение журнала аудита 	<ul style="list-style-type: none"> Портативный настольный модуль со встроенным устройством чтения смарт-карт Размеры с подставкой 120 x 118 x 27 мм (4,7 x 4,6 x 1 дюйм) Вес: 340 г (0,8 фунта) Входное напряжение: 5 В постоянного тока, питание от хост-устройства через USB-порт Потребляемая мощность: 700 мВт 	<ul style="list-style-type: none"> Производительность подписания для ключей длины, рекомендованной NIST: RSA для 2048 бит: 2 операции в секунду RSA для 4096 бит: 0,2 операции в секунду

ДОСТУПНЫЕ МОДЕЛИ И ИХ ПРОИЗВОДИТЕЛЬНОСТЬ

- nShield Edge доступен в вариантах, соответствующих FIPS уровня 2 и уровня 3
- Также доступна версия для разработчиков без соответствия стандарту FIPS

Подробнее

Более подробная информация об аппаратных модулях безопасности nShield от Entrust размещена по ссылке [entrust.com/HSM](https://www.entrust.com/HSM). Подробнее о решениях Entrust в области цифровой безопасности для выполнения задач идентификации, обеспечения доступа, информационного взаимодействия и использования данных можно узнать на сайте [entrust.com](https://www.entrust.com)



Более подробная информация размещена по ссылке

[entrust.com/HSM](https://www.entrust.com/HSM)



ENTRUST