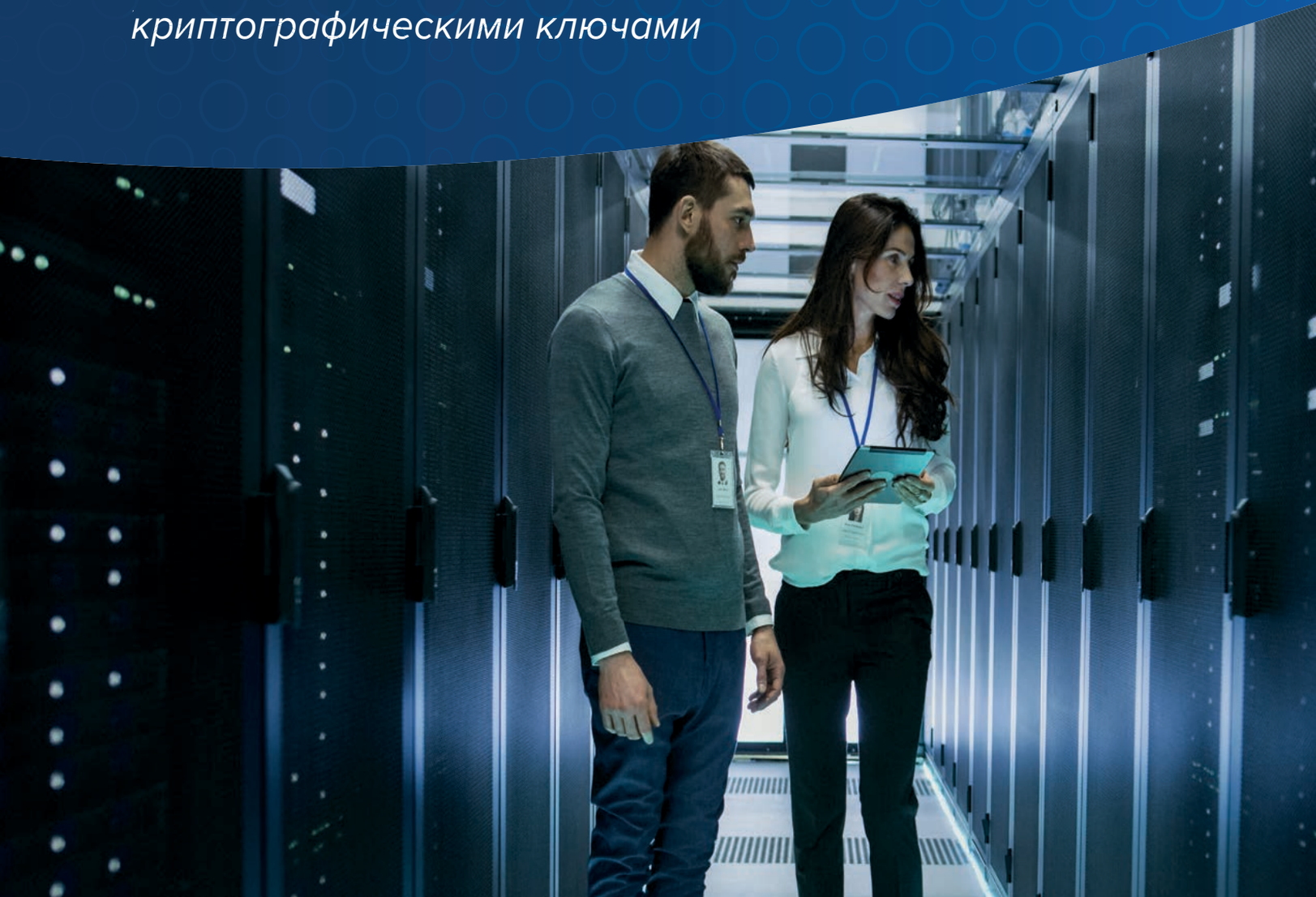
www.ncipher.com

nShield Edge

- nShield Edge - наиболее экономически эффективный модуль в линейке nShield
- Поддерживает разнообразные сценарии применения, включая центры сертификации, подписание кода
- Обеспечивает высокий уровень безопасности. nShield Edge имеет сертификат FIPS 140-2 Level 3

nShield Edge HSM

Сертифицированные USB-устройства для работы с криптографическими ключами



nShield Edge HSMs

Обзор возможностей

nShield Edge - это полнофункциональные модули с сертификатом FIPS , подключаемые при помощи USB. Они осуществляют шифрование, генерацию ключей и их хранение, при этом модули экономичные и удобные.

РАЗРАБОТАНЫ ДЛЯ СРЕД С НЕБОЛЬШИМ КОЛИЧЕСТВОМ ТРАНЗАКЦИЙ

Подходит для генерации ключей офлайн, сред разработки, поддерживает API.

ПОРТАТИВНЫЙ

Небольшой и легкий модуль с удобным USB интерфейсом поддерживает целый ряд платформ, работает с ноутбуками и другими портативными устройствами.

ВЫГОДНЫЙ И МАСШТАБИРУЕМЫЙ

Самый экономичный HSM в семействе nShield, nShield Edge станет отправной точкой для внедрения HSM, предоставляя вам возможность масштабировать вашу среду по мере роста ваших потребностей. Уникальная архитектура Security World позволяет комбинировать модели nShield HSM для создания смешанной среды, обеспечивающей гибкую масштабируемость, совместное использование ключей, плавную отработку отказа и балансировку нагрузки.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Поддерживаемые криптографические алгоритмы

- **Асимметричный алгоритм:** RSA, Diffie-Hellman, ECMQV, DSA, El- Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- **Симметричный алгоритм:** 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, Triple DES
- Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 бит), HAS-160, RIPEMD160
- Реализованы алгоритмы Suite B с полностью лицензированной ECC, включая Brainpool и пользовательские кривые

Поддерживаемые операционные системы

- Microsoft Windows 7 x64, 10 x64, Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, x86 and 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Enterprise Linux 6.8 x64, 7.1 x64

Интерфейсы API

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI и CNG, nCore, nShield Web Services Crypto API

Совместимость и возможности модернизации

- USB port (1.x, 2.x)

Соответствие стандартам безопасности

- FIPS 140-2 Level 2 и Level 3, NIST SP 800-131A

Безопасность и соблюдение стандартов безопасности

- UL, CE, FCC, C-TICK, и Canada ICES RoHS2, WEEE

Управление и мониторинг

- Удаленный автоматический оператор / многопользовательский контроль доступа
- Аудит безопасности
- Диагностика системного журнала
- Мониторинг производительности Windows
- Агент SNMP

Физические характеристики

- Портативное настольное устройство со встроенным считывателем смарт-карт
- Размеры с открытой подставкой 120 x 118 x 27 мм (4.7 x 4.6 x 1 дюймов)
- Вес: 340 г
- Входное напряжение: 5 В пост.тока, питание USB
- Потребляемая мощность: 700 мВт

Производительность

- Производительность подписи для рекомендуемых длин ключей NIST:
- 2048 бит RSA: 2 транзакции в секунду
- 4096 бит RSA: 0.2 транзакции в секунду

ДОСТУПНЫЕ МОДЕЛИ

- nShield Edge доступен в вариантах FIPS Level 2 и Level 3
- Также доступна версия для разработчиков, non-FIPS

ПОДРОБНЕЕ

Если вы хотите узнать, как nCipher Security обеспечивает целостность и контроль критически важной информации и приложений для вашего бизнеса, посетите сайт **ncipher.com**

Искать: nCipherSecurity: