DNA Distribution

DNA Distribution - официальный дистрибьютор Thales e-Security в России и СНГ

THALES
Thales e-Security

Thales nShield Solo – аппаратный модуль безопасности (HSM) для отдельно стоящих серверов

nShield Solo – лучшее аппаратное решение для защиты вашей корпоративной информации.

Thales nShiled Solo – аппаратный модуль безопасности для отдельно стоящих серверов. Он обеспечивает снижение нагрузки на сервер и аппаратное ускорение криптографических операций. Модуль реализует физические и логические методы защиты данных и будет эффективен там, где программной защиты информации уже не достаточно.

С nShield Solo значительно проще реализовывать политики безопасности вашей организации и автоматизировать сложные и подверженные рискам административные задачи вашего бизнеса.

Преимущества Thales nShield Solo

- Аппаратная структура модуля исключает слабые стороны, присущие программным средствам защиты информации
- Уникальная архитектура управления ключами сокращает операционные расходы
- Встраиваемая конструкция модуля обеспечивает высокую производительность
- Изоляция критических функций безопасности минимизирует взаимозависимость IT-систем
- Соответствие отраслевому стандарту FIPS 140-2 Level 3 – гарантия того, что nShield Solo станет оптимальным решением для организаций даже с самыми высокими требованиями к системам безопасности информации

DNA Distribution - официальный дистрибьютор Thales e-Security в России и странах СНГ
Тел.:+7(495)228-00-05 Факс:+7(495)228-00-06 E-mail:info@dnadis.ru Website: www.dnadis.ru

Thales nShield Solo

Функциональные возможности

Встроенная клиент-серверная поддержка приложений
Аппаратное хранение и обработки ключей шифрования и приложений
Криптографическая разгрузка и ускорение
Многоуровневая аутентификация и контроль доступа
Строгое разделение обязанностей администраторов и операторов
Безопасная изоляция, резервирование, репликация и восстановление ключей шифрования
Безопасное хранение неограниченного количества ключей шифрования
Кластеризация, балансировка нагрузки и многофакторная аутентификация
Неограниченное логическое/криптографическое разделение ключей приложений

Совместимость с ОС

Windows, Linux, Solaris, IBM AIX, HP-UX

Интерфейсы приложений

PKCK#11, OpenSSL, Java (JCE), Microsoft CAPI, CNG
nCore (низкоуровневый интерфейс Thales для разработчиков)

Совместимость и обновление

Совместим с nShield Connect, nShield Edge и netHSM
Обновление программной составляющей

Интерфейсы подключения

PCI 2.1, 2.2, 2.3, PCI-X совместим
PCIe 1.1, 1.2

Криптографические алгоритмы

Ассиметричные алгоритмы открытых ключей: RSA (1024, 2048, 4096), Diffle-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH
Симметричные алгоритмы: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES
Хэширование: SHA-1, SHA-2 (224, 256, 384, 512бит)
Полноценная реализация лицензированных алгоритмов эллиптической криптографии (ECC), а также поддержка пользовательских алгоритмов ECC

Бесперебойная работа

Твердотельные накопители данных
Наработка на отказ (см. таблицу)

Управление и мониторинг

Удаленный доступ; многопользовательский контроль доступа
Поддержка системного журнала диагностики Syslog
Система контроля производительности
Интерфейс с командной строкой (CLI)/ графический интерфейс пользователя (GUI)
Система контроля, совместимая с SNMPv3

Соответствие стандартам

FIPS 140-2 Level 2 и Level 3, NIST SP 800-131A
Common Criteria EAL4+

Физические характеристики

Габариты: стандартные платы PCI и PCIe с низким профилем; внешний считыватель смарт-карт
Температура: рабочая 10…35C°, хранение -20…70C
Влажность (без конденсации при 35%): рабочая 10…90%, хранение 0…85%

Размеры, вес, максимальное потребление энергии и наработка на отказ

Модель	Размеры (мм)	Вес (г)	Потребление (Вт)	Наработка на отказ
PCI 500	107 x 129 x 15	330	14	193000
PCIe 500, PCIe 6000	56,5 x 167,1 x 15,4	230	10	216600
PCIe 6000+	56,2 x 167,1 x 15,4	230		
PCI 2000, PCI 4000	107 x 175 x 16,5	340	14	125700

Модельный ряд и производительность

Модель	PCI 500	PCIe 500	PCI 2000	PCI 4000	PCIe 6000
RSA 1024бит (RSA)	500	500	2000	4000	6000
RSA 2048бит (RSA)	80	150	300	580	3000
RSA 4096бит (RSA)	15	65	20	40	500

Модельный ряд и производительность

Модель	PCIe 6000+
192 бит (ECC NISTP)	2300
256 бит (ECC NISTP)	2400
512 бит (ECC NISTP)	1300

DNA Distribution - официальный дистрибьютор Thales e-Security в России и странах СНГ
Тел.:+7(495)228-00-05 Факс:+7(495)228-00-06 E-mail:info@dnadis.ru Website: www.dnadis.ru