YubiHSM 2

Технические характеристики

Лучший экономный аппаратный модуль безопасности для серверов

YubiHSM 2 — это аппаратный модуль безопасности, предоставляющий превосходную защиту от фишинга и атак вредоносного ПО, для корневых ключей центров сертификации на серверах. Будучи экономным и доступным, он может быть с легкостью внедрен на любом предприятии. Данный модуль обеспечивает высокий уровень безопасности для организаций, работающих с сервисом сертификации Microsoft Active Directory, предоставляя уверенный подход к генерации, хранению и распределению цифровых ключей. Его эргономичный «нано» форм-фактор помещается внутри USB порта, что избавляет от потребности в дополнительном, объемистом оборудовании, и позволяет гибко производить перенос и резервное копирование ключей в офлайн режиме.

Технические характеристики

Интерфейс	
USB	(USB тип A) 1.x Full Speed (12Mbit/s) периферийный интерфейс.

Возможности	
Криптографические интерфейсы (API)	• Microsoft CNG (KSP) • PKCS#11 (Windows, Linux, macOS) • Родные библиотеки YubiHSM Core (C, python)
Криптографические возможности	**Хеширование (применяется с HMAC и ассиметричными подписями)** SHA-1, SHA-256, SHA-384, SHA-512 **RSA** • 2048, 3072, и 4096-битные ключи • Подпись с помощью PKCS#1v1.5 и PSS • Дешифрация PKCS#1v1.5 и OAEP **Эллиптическая криптография (ECC)** • Кривые: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 • Подпись: ECDSA (все кроме curve25519), EdDSA (только curve25519) • Дешифрация: ECDH (все кроме curve25519) **Упаковка ключей** • Импорт и экспорт при помощи NIST AES-CCM Wrap при 128, 196, и 256 битах **Случайные числа** • Встроенный в чип генератор реальных случайных чисел (TRNG) с зерном NIST SP 800-90 AES 256 CTR_DRBG **Аттестация** • Сгенерированные на устройстве асимметрические ключевые пары могут проходить проверку при помощи заводского сертифицированного ключа аттестации и сертификата, или при помощи Вашего личного ключа, импортированного в модуль безопасности
Быстродействие	Быстродействие зависит от целевого применения. В примере приведена метрика YubiHSM 2, незадействованного в других процессах: • RSA-2048-PKCS1-SHA256: ~139ms сред. • RSA-3072-PKCS1-SHA384: ~504ms сред. • RSA-4096-PKCS1-SHA512: ~852ms сред. • ECDSA-P256-SHA256: ~73ms сред. • ECDSA-P384-SHA384: ~120ms сред. • ECDSA-P521-SHA512: ~210ms сред. • EdDSA-25519-32 Байт: ~105ms сред. • EdDSA-25519-64 Байт: ~121ms сред. • EdDSA-25519-128 Байт: ~137ms сред. • EdDSA-25519-256 Байт: ~168ms сред. • EdDSA-25519-512 Байт: ~229ms сред. • EdDSA-25519-1024 Байт: ~353ms сред. • AES-(128|192|256)-CCM-Wrap: ~10ms сред. • HMAC-SHA-(1|256): ~4ms сред. • HMAC-SHA-(384|512): ~243ms сред.

Объем хранилища	• Все данные хранятся в виде объектов. 256 слотов для объектов, всего макс. 128KB (base 10) • Хранит до 127 rsa2048, 93 rsa3072, 68 rsa4096 или 255 любых кривых эллиптического типа, с учетом присутствия одного ключа аутентификации • Типы объектов: Ключи аутентификации (используются для установки сессий); асимметрические приватные ключи; объекты двоичных данных, напр. x.509 серт.; ключи упаковки; ключи HMAC
Администрирование	• Взаимная авторизация и защищенный канал между приложением и модулем безопасности • M из N распаковка и восстановление ключа через YubiHSM Setup Tool

Общие характеристики	
Интерфейс	USB-A
Габаритные размеры (Ш*Д*В)	12мм x 13мм x 3.1мм
Вес	1 г
Потребление тока	20 мА сред., 30 мА макс
Обеспечение соблюдения экологических норм	• FCC • CE • WEEE • ROHS

Температурные характеристики	
Рабочий режим	От 0 °C до 40 °C
Хранение	От -20 °C до 85 °C

Криптографические протоколы	
RSA	Макс. длина ключа: 4096 бит
SHA	Макс. длина ключа: 512 бит
ECC	Макс. длина ключа: 512 бит
AES	Макс. длина ключа: 256 бит

Есть вопросы?

Российская Федерация:

121099, Москва, Смоленская площадь, дом 3, офис 49

Тел. +7 (495) 231 82 24

Эл. почта: info@thekernel.ru

Объединённые Арабские Эмираты - Главный офис

Dubai Airport Free Zone 6EA, #209. Dubai – UAE

Tel. +971 (04) 7017 260

Email: info@thekernel.com