YubiHSM 2

Технічні характеристики

Кращий економний апаратний модуль безпеки для серверів

YubiHSM 2 — це апаратний модуль, що забезпечує неперевершений захист від фішингу та атак шкідливого ПЗ для кореневих ключів центрів сертифікації на серверах. Економний і доступний — він може бути з легкістю застосований на будь-якому підприємництві. Цей модуль забезпечує високий рівень безпеки для організацій, які працюють із сервісом сертифікації Microsoft Active Directory, надаючи надійний підхід до генерації , зберігання і розподілу цифрових ключів. Його ергономічний “nano” форм-фактор вміщується всередині USB порту, що позбавляє від потреби у додатковому, об’ємистому обладнанні та дозволяє зручно проводити перенесення та резервне копіювання ключів в режимі офлайн.

yubico
Trust the Net.

Технічні характеристики

Інтерфейс	
USB	(USB типу A) 1.x Full Speed (12Mbit/s) периферійній інтерфейс.

Можливості	
Криптографічні інтерфейси (API)	• Microsoft CNG (KSP) • PKCS#11 (Windows, Linux, macOS) • Рідні бібліотеки YubiHSM Core (C, python)
Криптографічні можливості	**Хешування (використовується разом з HMAC та асиметричними підписами)** • SHA-1, SHA-256, SHA-384, SHA-512 **RSA** • 2048, 3072, та 4096-бітні ключі • Підпис за допомогою PKCS#1v1.5 та PSS • Дешифрування за допомогою PKCS#1v1.5 та OAEP **Еліптична Криптографія (ECC)** • Криві: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 • Підпис: ECDSA (всі крім curve25519), EdDSA (тільки curve25519) • Дешифрування: ECDH (всі крім curve25519) **Пакування ключів** • Імпорт та експорт за допомогою NIST AES-CCM Wrap при 128, 196, та 256 бітах **Випадкові числа** • Вбудований в чіп генератор справжніх випадкових чисел (TRNG) із зерном NIST SP 800-90 AES 256 CTR_DRBG **Атестація** • Згенеровані на пристрою асиметричні ключові пари можуть проходити перевірку за допомогою заводського сертифікованого ключа та сертифікату, або за допомогою Вашого особистого ключа, імпортованого до модулю безпеки
Швидкодія	Швидкодія залежить від цільового застосування. У прикладі приведена метрика YubiHSM 2, незастосованого у інших процесах: • **RSA-2048-PKCS1-SHA256: ~139ms серед**. • RSA-3072-PKCS1-SHA384: ~504ms серед. • RSA-4096-PKCS1-SHA512: ~852ms серед. • **ECDSA-P256-SHA256: ~73ms серед.** • ECDSA-P384-SHA384: ~120ms серед. • ECDSA-P521-SHA512: ~210ms серед. • EdDSA-25519-32Bytes: ~105ms серед. • EdDSA-25519-64Bytes: ~121ms серед. • EdDSA-25519-128Bytes: ~137ms серед. • EdDSA-25519-256Bytes: ~168ms серед. • EdDSA-25519-512Bytes: ~229ms серед. • EdDSA-25519-1024Bytes: ~353ms серед. • AES-(128|192|256)-CCM-Wrap: ~10ms серед. • HMAC-SHA-(1|256): ~4ms серед. • HMAC-SHA-(384|512): ~243ms серед.

Об’єм сховища	• Всі дані зберігаються у вигляді об’єктів. 256 слотів для об’єктів, всього макс. 128KB (base 10) • Зберігає до 127 rsa2048, 93 rsa3072, 68 rsa4096 або 255 будь-яких кривих еліптичного типу, з урахуванням присутності одного ключа автентифікації • Типи об’єктів: Ключі автентифікації (використовуються для встановлення сесій); асиметричні приватні ключі; об’єкти двійкових даних, напр. x509 серт.; ключі пакування; ключі HMAC
Адміністративне Керування	• Взаємна авторизація і захищений канал між додатком та апаратним модулем безпеки • M із N розпакування і відновлення ключа через YubiHSM Setup Tool

Загальні характеристики	
Інтерфейс	USB-A
Габаритні розміри (Ш*Д*В)	12мм x 13мм x 3.1мм
Вага	1 г
Споживання струму	20 мА серед., 30 мА макс.
Забезпечення дотримання екологічних норм	• FCC • CE • WEEE • ROHS

Температурні характеристики	
Робочий режим	Від 0 °C до 40 °C
Зберігання	Від -20 °C до 85 °C

Криптографічні протоколи	
RSA	Макс. довжина ключа: 4096 біт
SHA	Макс. довжина ключа: 512 біт
ECC	Макс. довжина ключа: 512 біт
AES	Макс. довжина ключа: 256 біт

Виникли питання?

Об’єднані Арабські Емірати – Головний офіс

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

Tel. +971 (04) 7017 260

Email: info@thekernel.com