YubiHSM 2

Найбільш компактний та ефективний апаратний модуль безпеки

Найкращий економний апаратний модуль безпеки для серверів

YubiHSM 2 — це апаратний модуль безпеки, що надає чудовий захист від фішингу та атак шкідливого ПЗ для кореневих ключів центрів сертифікації на серверах. Бувши економним і компактним, він може бути легко впроваджений на будь-якому підприємстві. YubiHSM 2 забезпечує високий рівень безпеки для організацій, що працюють із сервісом сертифікації Microsoft Active Directory, надаючи впевнений підхід до генерації, зберігання та розподілу цифрових ключів. Завдяки ергономічному формфактору YubiHSM 2 розміщується всередині USB порту, що позбавляє потреби в додатковому, громіздкому обладнанні, і дозволяє гнучко проводити перенесення та резервне копіювання ключів у режимі офлайн.

Можливості

- Безпечне сховище ключів.
- Розширені криптографічні можливості.
- Захищена сесія між HSM та додатком.
- Керування доступом на основі ролей для використання та розподілу ключів.
- 16 одночасних з'єднань.
- Можливість надання мережевого доступу.
- Віддалене керування.
- Унікальний «Nano» формфактор, низьке енергоспоживання.
- Інкапсуляція ключів за допомогою коду з постійною вагою (M of N), резервне копіювання та відновлення.
- Інтерфейс на основі YubiHSM KSP, PKCS#11 та власних бібліотек.
- Аудит контролю доступу.
- Підтримка роботи з USB безпосередньо.

Технічні характеристики

Інтерфейс	
USB	(USB тип A) 1.x Full Speed (12Mbit/s) периферійний інтерфейс
Можливості	
Криптографічні інтерфейси (API)	▪ Microsoft CNG (KSP) ▪ PKCS#11 (Windows, Linux, macOS) ▪ Власні бібліотеки YubiHSM Core (C, Python)
Криптографічні можливості	Хешування (застосовується з HMAC та асиметричними підписами) ▪ SHA-1, SHA-256, SHA-384, SHA-512 RSA ▪ 2048, 3072, и 4096-бітні ключі ▪ Підпис за допомогою PKCS#1v1.5 та PSS ▪ Дешифрація PKCS#1v1.5 та OAEP Еліптична криптографія (ECC) ▪ Криві: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 ▪ Підпис: ECDSA (усі крім curve25519), EdDSA (тільки curve25519) ▪ Дешифрація: ECDH (усі крім curve25519) Пакування ключів ▪ Імпорт та експорт за допомогою NIST AES-CCM Wrap при 128, 196 та 256 бітах Випадкові числа ▪ Вбудований у чіп генератор реальних випадкових чисел (TRNG) із зерном NIST SP 800-90 AES 256 CTR_DRBG Атестація ▪ Асиметричні ключові пари, що згенеровані на пристрої, можуть проходити перевірку за допомогою заводського сертифікованого ключа атестації та сертифіката, або за допомогою Вашого особистого ключа, імпортованого в модуль безпеки.
Швидкість дії	Швидкість дії залежить від цільового застосування. У прикладі наведено метрику YubiHSM 2, незадіяного в 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-25519-32 Байт ~105ms серед. ▪ EdDSA-25519-64 Байт ~121ms серед. ▪ EdDSA-25519-128 Байт ~137ms серед. ▪ EdDSA-25519-256 Байт ~168ms серед. ▪ EdDSA-25519-512 Байт ~229ms серед. ▪ EdDSA-25519-1024 Байт ~353ms серед. ▪ AES-(128|192|256)-CCM-Wrap ~10ms серед. ▪ HMAC-SHA-(1|256) ~4ms серед. ▪ HMAC-SHA-(384|512) ~243ms серед.
Обсяг сховища	▪ Усі дані зберігаються як об'єктів. 256 слотів для об'єктів, всього макс. 128 KB (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 аутентифікації (використовуються для встановлення сесій); асиметричні приватні ключі; об'єкти двійкових даних, напр. x.509 серт.; ключі пакування; ключі HMAC.
Адміністрування	▪ Взаємна авторизація і захищений канал між додатком та модулем безпеки. ▪ M з N розпакування та відновлення ключа через YubiHSM Setup Tool.

Загальні характеристики	
Інтерфейс	USB-A
Габаритні розміри (Ш×Д×В)	(ш) 12мм x (д) 13мм x (в) 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

Додаткова інформація:

Документація для розробників:
https://developers.yubico.com/YubiHSM2/

Бібліотеки та програмні проєкти:
https://developers.yubico.com/Software_Projects/YubiHSM/

Є запитання?

Україна

вул. Михайла Грушевського, 10, оф. 212
01001, Київ, Україна
Тел. +38 (044) 35 31 999
Ел. почта: info@thekernel.com.ua
Вебсайт: https://thekernel.ua

Об'єднані Арабські Емірати – Головний офіс

Dubai Airport Free Zone 6EA, #209. Dubai – UAE
Tel. +971 (04) 7017 260
Email: info@thekernel.com
Web: https://thekernel.com