

Yubico YubiHSM 2.4

Mit dem YubiHSM können Unternehmen jeder Größe die Sicherheit kryptografischer Schlüssel während des gesamten Lebenszyklus sicher zu verwalten. Tutto per i vostri progetti di bricolage.

Artikelnummer 5060408461976

Gewicht 0.1kg



Produktbeschreibung

Yubico YubiHSM 2.4

Das Yubico YubiHSM 2.4 ist ein kompaktes Hardware-Sicherheitsmodul (HSM) im Nano-Format zur sicheren Verwaltung kryptografischer Schlüssel. Es wurde speziell für Unternehmen in sicherheitskritischen und regulierten Branchen entwickelt, darunter das Finanzwesen, die Industrie und der Gesundheitssektor. Die Hardware ermöglicht die sichere Erzeugung, Speicherung, Nutzung und gegebenenfalls Vernichtung kryptografischer Schlüssel im gesamten Lebenszyklus. Das Modul unterstützt ein breites Spektrum kryptografischer Algorithmen und Funktionen, darunter RSA, ECC, AES sowie verschiedene Hash-Verfahren und erfüllt gängige Anforderungen an Sicherheit und Integrität in professionellen IT-Infrastrukturen.

Durch die Verwendung des YubiHSM 2.4 werden CA-Schlüssel, digitale Signaturen und sensible Daten vor unberechtigtem Zugriff geschützt. Typische Anwendungsbereiche sind die Absicherung von Active Directory Certificate Services, Signatur- und Verifizierungsdienste sowie kritische Infrastrukturen wie IoT-Systeme oder Kryptobörsen. Das offene SDK ermöglicht die Integration in bestehende Plattformen und Anwendungen. Das Gerät arbeitet stromsparend über einen USB-A-Anschluss und ist durch seine Größe diskret einsetzbar.

Das YubiHSM 2.4 schützt kryptografische Schlüssel durch isolierte Verarbeitung im Gerät selbst, wodurch ein Zugriff durch Malware oder Server-Angriffe verhindert wird. Durch rollenbasierte Zugriffskontrollen und die Möglichkeit zur Netzwerkfreigabe sowie Fernverwaltung eignet sich das Gerät für Unternehmen mit verteilter IT-Infrastruktur. Die neue Version 2.4 bietet zusätzlich asymmetrische Backupfunktionen, Unterstützung für Bring Your Own Key-Konzepte in Multi-Cloud-Umgebungen sowie eine aktualisierte Kryptografie-Bibliothek. Mithilfe der nativen Schnittstellen (YubiHSM Core Libraries), Microsoft CNG (KSP) und PKCS#11 lassen sich verschiedene Anwendungen direkt anbinden.

Das YubiHSM 2.4 ist ein spezialisiertes Gerät zur Absicherung kryptografischer Prozesse. Es kann eingesetzt werden, um Zertifikatsdienste abzusichern, digitale Signaturen zu erzeugen oder kryptografische Schlüssel sicher zu speichern. Funktionen wie Schlüsselerzeugung, -import, -signierung, -entschlüsselung, Hashing und Key-Wrapping erfolgen vollständig hardwarebasiert im Gerät. Die Kommunikation zwischen Modul und Anwendungen erfolgt über gesicherte Kanäle, wobei gleichzeitig eine Protokollierung aller Ereignisse mit Prüfsummen (Audit Logging) erfolgt. Der Nano-Formfaktor ermöglicht eine unauffällige Integration in bestehende Systeme, und dank geringer Stromaufnahme ist ein dauerhafter Betrieb auch in energieoptimierten Umgebungen möglich. Die Fernverwaltung erlaubt es, mehrere Geräte

zentral zu administrieren.

Für wen eignet sich dieses Modell

- Unternehmen: Schutz von CA-Schlüsseln, Datenbanken oder digitalen Signaturen
- Unternehmen: Compliance-konforme Verschlüsselung in kritischen Infrastrukturen

Wesentliche Vorteile

- Kosteneffizientes HSM mit einfacher Bereitstellung
- Sichere Schlüsselspeicherung und Operationen im isolierten Hardware Chip
- Offenes SDK 2.0 und Bibliotheken für schnelle Integration
- Hohe Sicherheit bei geringem Platzbedarf
- Schutz vor Schlüsselverlust durch Hardware-gestützte Speicherung
- Reduziert Risiko durch Admin-Fehler oder Malware-Angriffe
- Skalierbarkeit durch flexible Integration via offenes SDK

Neue Funktionen in Version 2.4

- Backups mit asymmetrischer Kryptografie für sichere Datensicherung auch über das Internet
- Bring Your Own Key Unterstützung für Multi Cloud Umgebungen
- Aktualisierte Kryptografie Bibliothek für RSA und ECC identisch zur YubiKey 5.7 Generation

Typische Anwendungsfälle

- Absicherung von Certificate Authority Root Keys und Microsoft Active Directory Certificate Services
- Hardwarebasierte Signaturerzeugung und Verifikation
- Absicherung von Kryptowährungsbörsen
- Schutz von IoT Gateways und Geräten in rauen Umgebungen

Leistung, Kapazität und Management

- Beispielmetriken im Leerlauf, RSA 2048 Signatur etwa 139 ms, RSA 3072 etwa 504 ms, RSA 4096 etwa 852 ms
- ECDSA P256 etwa 73 ms, P384 etwa 120 ms, P521 etwa 210 ms
- Ed25519 Signatur etwa 105 bis 353 ms abhängig von Datenlänge
- AES CCM Wrap etwa 10 ms, HMAC SHA 1 oder 256 etwa 4 ms
- Speicher, 256 Objekt Slots, insgesamt 128 KB, Beispiel, bis zu 127 RSA 2048 oder 255 ECC Schlüssel
- Objekttypen, Authentisierungsschlüssel, asymmetrische Private Keys, Opaque Daten etwa X509 Zertifikate, Wrap Keys, HMAC Keys
- Software Development Kit Inhalte, Core Library C und Python, YubiHSM Shell CLI, PKCS 11 Modul, KSP, Connector, Setup Tool, Dokumentation und Beispiele

Schnittstellen und Integration

- APIs und Libraries, YubiHSM KSP für Microsoft CNG, PKCS#11, native YubiHSM Core Libraries C und Python
- Direkter USB Zugriff ohne zwischengeschaltetes HTTP
- Optionale Netzwerkfreigabe für den Einsatz über mehrere Server
- Fernverwaltung für zentral administrierte Rollouts

Sicherheitsfunktionen und Verwaltung

- Gesicherte Sitzung zwischen Anwendung und HSM mit gegenseitiger Authentisierung sowie Integritäts und Vertraulichkeitsschutz
- Rollenbasierte Zugriffskontrolle über Security Domains und Rechte je Authentisierungsschlüssel
- Tamper evident Audit Logging mit Hash Chain zur Manipulationserkennung
- M of N Wrap Key Backup und Restore für kontrollierte Schlüsselübertragung an mehrere HSMs
- Bis zu 16 gleichzeitige Sitzungen
- Nano Formfaktor vollständig im USB A Port versenkbar, niedrige Leistungsaufnahme bis 30 mA

Kryptografische Fähigkeiten

- Operationen, Erzeugen, Importieren, Speichern, Signieren, Entschlüsseln, Hashen, Key Wrapping
- Hashing, SHA 1, SHA 256, SHA 384, SHA 512
- RSA 2048, 3072, 4096 mit PKCS 1 v1.5 und PSS für Signatur, PKCS 1 v1.5 und OAEP für Entschlüsselung
- ECC Kurven secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519
- ECDSA Signaturen, EdDSA auf curve25519, ECDH für Entschlüsselung außer curve25519
- Key Wrap, NIST AES CCM mit 128, 196, 256 Bit
- Attestation für auf dem Gerät erzeugte asymmetrische Schlüsselpaare
- Zufallszahlen, On Chip TRNG zur Seed Generierung für NIST SP 800 90 AES 256 CTR DRBG

Merkmale im Überblick

- Schnittstellen: USB (Typ-A, via Standard-Port)
- Formfaktor: Nano (kleinstes HSM der Welt, direkt anschließbar)
- Unterstützte Standards: PKCS#11, Microsoft CNG (KSP), YubiHSM Core Libraries (C, Python)
- RSA: 2048, 3072, 4096 Bit; ECC: Ed25519, secp256r1, secp384r1 u. a.
- AES: 128, 192, 256 Bit (inkl. CCM für Key-Wrap)
- Hash-Funktionen: SHA-1, SHA-256, SHA-384, SHA-512
- Import-/Exportfunktionen für Schlüsselmaterial mit NIST-zertifizierter Verschlüsselung

Kompatibilität

- Plattformen: Windows, Linux, macOS (via API/SDK)
- Private Dienste: Nicht vorgesehen
- Unternehmensdienste: Unterstützung für CAs, HSM-gesicherte Anwendungen, Signaturdienste
- [Zur vollständigen Kompatibilitätsliste](#)

Technische Daten

- Firmware, 2.4
- USB Versorgung, 20 mA durchschnittlich, 30 mA maximal
- Host Interface, USB 1.x Full Speed 12 Mbit pro Sekunde mit Bulk Interface
- Datenübertragungsrate, 12 Mbit pro Sekunde
- Abmessungen, 12 mm x 13 mm x 3.1 mm
- Gewicht, 1 g
- Gehäuse Schutz, IP68
- Betriebstemperatur, 0 bis 40 Grad Celsius
- Lagerungstemperatur, minus 20 bis 85 Grad Celsius
- Konformität, FCC, CE, WEEE, RoHS

Lieferumfang

- YubiHSM 2.4 Gerät (Nano-Hardwaremodul)

Serien und Alternativen

- **YubiHSM 2 FIPS** für Regierungsbehörden / stark regulierte Märkte mit FIPS 140-2 Validierung
- **YubiKey 5 Serie** für Benutzer-Authentifizierung mit Multi-Protokoll-Support
- **Security Key Serie** für einfache FIDO2/U2F Authentifizierung

Links

- [Offizielle Produktseite](#)
- [Works with YubiKey Katalog](#)

Weitere Links

- [Yubico Setup](#)
- [Yubico Keys: Grundeinführung](#)
- [Login Security und Anwendungen](#)
- [Sichere Authentifizierung mit YubiKey](#)

Produkteigenschaften

Zolltarifnummer	84718000
Gewicht Brutto (in kg)	0.100
Farbe	schwarz
Herkunftsland	Schweden
Anschlüsse	USB 2.0 Stecker / Typ A
VPE	1
Hersteller	YUBICO
Artikelnummer	5060408461976
EAN	5060408461976
Hersteller Produktnummer	5060408461976
Serie	YubiHSM 2 Series

Weitere Bilder

