Product Description

The YubiHSM 2 FIPS is a game changing hardware solution for protecting Certificate Authority root keys from being copied by attackers, malware, and malicious insiders. It offers superior cost effective security and easy deployment making it accessible for every organization. It offers a higher level of security for cryptographic digital key generation, storage, and management, for organizations running Microsoft Active Directory Certificate Services.

The YubiHSM 2 features are accessible by integrating with an open source and comprehensive software development toolkit (SDK) for a wide range of open source and commercial applications. The most common use case is hardware-based digital signature generation and verification. In additional emerging use cases such as securing cryptocurrency exchanges and IoT gateways are just a few examples of how the world's smallest HSM can secure modern infrastructures.

YubiHSM 2 secures cryptographic keys through their entire lifecycle from secure key generation, attestation, secure key storage, secure key distribution, secure key backup all the way to secure key destruction if needed. Screen reader support enabled.

Benefits

- Cost-effective HSM solution
- Easy deployment
- Secure key storage and operations

Use Cases

Enhance Protection for Cryptographic Keys

YubiHSM 2 offers a compelling option for secure generation, storage and management of keys. Key protection is done in the secure on-chip hardware isolated from operations on the server. Most common use cases involve protecting of the certificate authorities (CAs) private key. YubiHSM 2 capabilities include: generate, write, sign, decrypt, hash and wrapping keys.

Rapidly integrate with Hardware-based Strong Security

YubiHSM 2 can be used as a comprehensive cryptographic toolbox for low-volume operations in conjunction with a huge set of open source and commercial applications spanning many different products and services. Most common use case involve on-chip hardware based processing for signature generation and verification. The YubiHSM 2 supports the PKCS#11 industry standard.

Secure Microsoft Active Directory Certificate Services

YubiHSM 2 can provide hardware backed keys for your Microsoft-based PKI implementation. Deploying YubiHSM 2 to your Microsoft Active Directory Certificate services not only protects the CA root keys but also protects all signing and verification services using the private key.

- Secure key storage and operations
- FIPS 140-2 validated (Level 3)
- Extensive cryptographic capabilities: RSA, ECC, ECDSA (ed25519), SHA-2, AES

- Secure session between HSM and application
- Role-based access controls for key management and key usage
- 16 concurrent connections
- Optionally network shareable
- Remote management
- Unique “Nano” form factor, low-power usage
- M of N wrap key Backup and Restore
- Interfaces via YubiHSM KSP, PKCS#11, and native libraries
- Tamper evident Audit Logging

Secure Cryptocurrency Exchanges

With the explosive growth of the cryptocurrency market also comes a high volume of assets that need protection to mitigate against emerging security risks. The YubiHSM 2 allows organizations to strongly secure cryptographic keys and keep sensitive financial information safe.

Protect Internet of Things (IoT) Environments

The Internet-of-Things (IoT) is a rapidly emerging area where systems often operate in hostile environments. That makes securing cryptographics keys even more important as organizations need to protect sensitive information. Cryptographic keys are used in numerous IoT applications, with insufficient security in place. Developers building IoT applications can rapidly enable support for the YubiHSM 2 to protect cryptographic keys and keep critical IoT environments from falling victim to hostile takeovers.

Feature Details

Secure key storage and operations

Create, import, and store keys, then perform all crypto operations in the HSM hardware to prevent theft of keys while at rest or in use. This protects against both logical attacks against the server, such as zero-day exploits or malware, and physical theft of a server or its hard drive.

Extensive cryptographic capabilities

YubiHSM 2 supports hashing, key wrapping, asymmetric signing and decryption operations including advanced signing using ed25519. Attestation is also supported for asymmetric key pairs generated on-device.

Secure session between HSM and application

The integrity and privacy of commands and data in transit between the HSM and applications are protected using a mutually authenticated, integrity and confidentiality protected tunnel.

Role-based access controls for key management and key usage

All cryptographic keys and other objects in the HSM belong to one or more security domains. Access rights are assigned for each authentication key at creation time which allow a specific set of cryptographic or management operations to be performed per security domain. Admins assign rights to authentication keys based on its use case, such as a event monitoring app that needs the ability to read all audit logs in the HSM, or a Registration Authority that needs to issue (sign) end user digital certificates, or a domain security admin who needs to create and delete crypto keys.

16 concurrent connections

Multiple applications can establish sessions with a YubiHSM to perform cryptographic operations. Sessions can be automatically terminated after inactivity or be long-lived to improve performance by eliminating session creation time.

Network Shareable

To increase the flexibility of deployments, the YubiHSM 2 can be made available for use over the network by applications on other servers. This can be especially advantageous on a physical server that is hosting multiple virtual machines.

Remote Management

Easily manage multiple deployed YubiHSMs remotely for the entire enterprise – eliminate on-call staff complexity and travel expense.

Unique “Nano” form factor, low-power usage

The Yubico “Nano” form factor allows the HSM to be inserted completely inside a USB-A port so it’s completely concealed – no external parts that protrude out of the server back or front chassis. It uses minimal power, max of 30mA, for cost-savings on your power budget.

M of N wrap key Backup and Restore

Backing up and deploying cryptographic keys on multiple HSMs is a critical component of an enterprise security architecture, but it’s a risk to allow a single individual to have that ability. The YubiHSM supports setting M of N rules on the wrap key used to export keys for backup or transport, so that multiple administrators are required to import and decrypt a key to make it usable on additional HSMs. For example in an enterprise, the Active Directory root CA private key might be key wrapped for 7 administrators (N=7) and at least 4 of them (M=4) are required to import and unwrap (decrypt) the key in the new HSM.

Interfaces via YubiHSM KSP, PKCS#11, and native libraries

Crypto enabled applications can leverage the YubiHSM via Yubico’s Key Storage Provider (KSP) for Microsoft’s CNG or industry-standard PKCS#11. Native libraries are also available on Windows, Linux and macOS to enable more direct interaction with the device’s capabilities.

Tamper evident Audit Logging

The YubiHSM internally stores a log of all management and crypto operation events that occur in the device and that log can be exported for monitoring and reporting. Each event (row) in the log is hash chained with the previous row and signed so that it's possible to determine if any events are modified or deleted.

Direct USB Support

The YubiHSM 2 can talk directly to the USB layer without the need for an intermediate HTTP mechanism. This delivers an improved experience for the developers who are developing solutions for virtualized environments.

FIPS 140-2

The YubiKey HSM 2 FIPS is FIPS 140-2 validated (Level 3) and meets the highest authenticator assurance level 3 (AAL3) of NIST SP800-63B guidance.

Specifications

Operating System Support

Windows, Linux, macOS

Linux	CentOS 7 Debian 8 Debian 9 Debian 10 Fedora 28 Fedora 30 Fedora 31 Ubuntu 1404 Ubuntu 1604 Ubuntu 1804 Ubuntu 1810 Ubuntu 1904 Ubuntu 1910
Windows	Windows 10 Windows Server 2012 Windows Server 2016 Windows Server 2019
macOS	10.12 Sierra 10.13 High Sierra 10.14 Mojave

Cryptographic interfaces (APIs)

- Microsoft CNG (KSP)
- PKCS#11 (Windows, Linux, macOS)
- Native YubiHSM Core Libraries (C, python)

Cryptographic capabilities

Hashing (used with HMAC and asymmetric signatures)

- SHA-1, SHA-256, SHA-384, SHA-512

RSA

- 2048, 3072, and 4096 bit keys
- Signing using PKCS#1v1.5 and PSS
- Decryption using PKCS#1v1.5 and OAEP

Elliptic Curve Cryptography (ECC)

- Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519
- Signing: ECDSA (all except curve25519), EdDSA (curve25519 only)
- Decryption: ECDH (all except curve25519)

Key wrap

- Import and export using NIST AES-CCM Wrap at 128, 196, and 256 bits

Random numbers

- On-chip True Random Number Generator (TRNG) used to seed NIST SP 800-90 AES 256 CTR_DRBG

Attestation

- Asymmetric key pairs generated on-device may be attested using a factory certified attestation key and certificate, or using your own key and certificate imported into the HSM

Performance

Performance varies depending on usage. The accompanying Software Development Kit includes performance tools that can be used for additional measurements. Example metrics from an otherwise unoccupied YubiHSM 2

- **RSA-2048-PKCS1-SHA256: ~139ms avg**
- RSA-3072-PKCS1-SHA384: ~504ms avg
- RSA-4096-PKCS1-SHA512: ~852ms avg
- **ECDSA-P256-SHA256: ~73ms avg**
- ECDSA-P384-SHA384: ~120ms avg
- ECDSA-P521-SHA512: ~210ms avg
- EdDSA-25519-32Bytes: ~105ms avg
- EdDSA-25519-64Bytes: ~121ms avg
- EdDSA-25519-128Bytes: ~137ms avg
- EdDSA-25519-256Bytes: ~168ms avg
- EdDSA-25519-512Bytes: ~229ms avg
- EdDSA-25519-1024Bytes: ~353ms avg
- AES-(128|192|256)-CCM-Wrap: ~10ms avg
- HMAC-SHA-(1|256): ~4ms avg
- HMAC-SHA-(384|512): ~243ms avg

Storage capacity

- All data stored as objects. 256 object slots, 128KB (base 10) max total
- Stores up to 127 rsa2048, 93 rsa3072, 68 rsa4096 or 255 of any elliptic curve type, assuming only one authentication key is present
- Object types: Authentication keys (used to establish sessions); asymmetric private keys; opaque binary data objects, e.g. x509 certs; wrap keys; HMAC keys

Management

- Mutual authentication and secure channel between applications and HSM
- M of N unwrap key restore via YubiHSM Setup Tool

Software Development Kit

A Software Development Kit for YubiHSM 2 is available for download on Yubico.com and includes:

- YubiHSM Core Library (libyubihsm) for C, Python
- YubiHSM Shell (Configuration CLI)
- PKCS#11 Module
- YubiKey Key Storage Provider (KSP) for use with Microsoft
- YubiHSM Connector
- YubiHSM Setup Tool
- Documentation and code examples

Physical characteristics

- Form factor: ‘nano’ designed for confined spaces such as internal USB ports in servers
- Dimensions: 12mm x 13mm x 3.1mm
- Weight: 1 gram
- Current requirements 20mA avg, 30mA max
- USB-A plug connector

Safety and environmental compliance

- FCC
- CE
- WEEE
- ROHS

Host interface

- Universal Serial Bus (USB) 1.x Full Speed (12Mbit/s) Peripheral with bulk interface.