yubico

Secure, low cost hardware protection for cryptographic keys

Secure your sensitive data and critical applications by storing, protecting and managing cryptographic keys with the YubiHSM 2, a dedicated hardware security module (HSM) that offers superior protection against key theft and misuse. A FIPS 140-2 validated version (Level 3) is also available via the YubiHSM 2 FIPS. With the same feature set as the YubiHSM 2, the YubiHSM 2 FIPS can meet the requirements of government agencies, and organizations in financial services, healthcare, energy, and any other area where the FIPS security standard is a requirement.

With Yubico's HSM offerings, you get uncompromised cryptographic hardware security for your applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.

Technical Specifications

Cryptographic Interfaces

- PKCS#11 API version 2.40
- Microsoft CNG via the Yubico Key Storage
- Provider (KSP), both 32 and 64-bit DLLs
- Full access to device capabilities through Yubico's YubiHSM Core Libraries (C, Python)

RSA

- 2048, 3072, and 4096 bit keys
- Signing: PKCS#1 v1.5 and PSS
- Decryption: PKCS#1 V1.5 and OAEP

Elliptic Curve Cryptography (ECC)

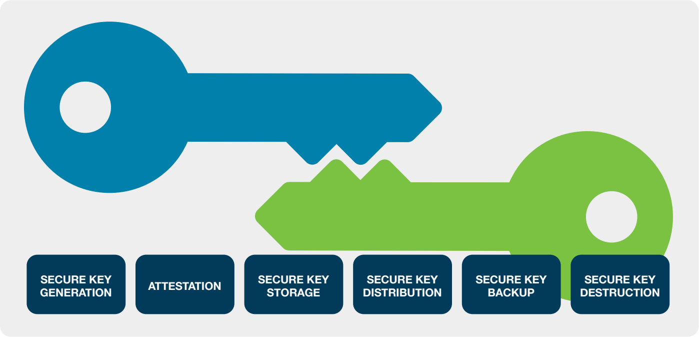
- Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, Ed25519
- Signing: ECDSA (all except Ed25519), EdDSA (Ed25519 only)
- Derivation: ECDH (all except Ed25519)

Hashing functions

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

Key wrap

- Import and export using NIST-approved AES CCM



Securing the Cryptographic Key Lifecycle

Performance

Performance varies depending on usage (the accompanying Software Development Kit includes performance tools that can calculate additional measurements). Example metrics from an otherwise unoccupied YubiHSM 2:

- RSA-2048-PKCS1-SHA256: ~139ms
- RSA-3072-PKCS1-SHA384: ~504ms
- RSA-4096-PKCS1-SHA512: ~852ms
- ECDSA-P224-SHA1: ~64ms
- ECDSA-P256-SHA256: ~73ms
- ECDSA-P384-SHA384: ~120ms
- ECDSA-P521-SHA512: ~210ms
- EdDSA-25519-32Bytes: ~105ms
- EdDSA-25519-64Bytes: ~121ms
- EdDSA-25519-128Bytes: ~137ms
- EdDSA-25519-256Bytes: ~168ms
- EdDSA-25519-512Bytes: ~229ms
- EdDSA-25519-1024Bytes: ~353ms
- AES-(128|192|256)-CCM-Wrap: ~10ms
- HMAC-SHA-(1|256): ~4ms
- HMAC-SHA-(384|512): ~243ms

Random numbers

- On-chip True Random Number Generator (TRNG) used to seed NIST SP 800-90A Rev.1 AES-256 CTR_DRBG

Attestation

- Asymmetric key pairs generated on-device may be attested using a device-specific Yubico attestation key and certificate or using imported custom keys and certificates

Storage capacity

- 126KB
- 256 object slots
- Object types:

  – Authentication keys

  – Asymmetric private keys

  – Opaque binary data objects

  – Wrap keys

  – HMAC keys
- The potential to store up to 127 rsa2048 or 93 rsa3072 or 68 rsa4096 or 255 of any elliptic curve type

Management

- Mutual authentication and secure channel between applications and the YubiHSM 2
- M of N unwrap key restore via the YubiHSM Setup Tool

Physical Characteristics

Weight & Dimensions

- Weight: 0.035274 oz (1g)
- Dimensions: 0.47” x 0.51” x 0.12” (12mm x 13mm x 3.1mm)

Host interface

- USB-A connector
- Universal Serial Bus (USB) 2.0

Power Consumption

- Less than 150mW
- Input voltage: 5V

Reliability

- Can withstand 500,000 read/write cycles
- Mean Time Between Failure (MTBF) is greater than 100 years in most commonly used environments, but may vary in harsher environments
- Comes with a standard 1-year warranty

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088