YubiHSM 2
Technical specifications

Best cost-effective hardware security module for servers

YubiHSM 2 is a hardware module providing superior protection from phishing and malware attacks for CA root keys on servers. Cost-effective and accessible, it makes deployment easy for every enterprise. The module provides a greater level of security for organizations running Microsoft Active Directory Certificate Services, offering a compelling approach for generation, storage and management of digital keys. Its convenient “nano” form-factor fits inside a USB port, which eliminates the need for additional, space-consuming hardware and offers a flexible way for offline key backup and transfer.
## Technical specifications

### Interface

| USB | (USB-A) 1.x Full Speed (12Mbit/s) Peripheral with bulk interface. |

### Features

#### 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, secp521r1, 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. 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-P512-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

Physical Specifications

<table>
<thead>
<tr>
<th>Connector</th>
<th>USB-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions</td>
<td>12мм x 13мм x 3.1мм</td>
</tr>
<tr>
<td>Weight</td>
<td>1 г</td>
</tr>
<tr>
<td>Current requirements</td>
<td>20mA avg, 30mA max</td>
</tr>
</tbody>
</table>

Safety and environmental compliance

- FCC
- CE
- WEEE
- ROHS

Temperatures

<table>
<thead>
<tr>
<th>Operational range</th>
<th>0 °C to 40 °C (32 °F to 104 °F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage range</td>
<td>-20 °C to 85 °C (-4 °F to 185 °F)</td>
</tr>
</tbody>
</table>

Cryptographic algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Max. keysize</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>4096 bits</td>
</tr>
<tr>
<td>SHA</td>
<td>512 bits</td>
</tr>
<tr>
<td>ECC</td>
<td>512 bits</td>
</tr>
<tr>
<td>AES</td>
<td>256 bits</td>
</tr>
</tbody>
</table>

Contact us

**UAE - Headquarters**

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

Tel. +971 (04) 7017 260

Email: [info@thekernel.com](mailto:info@thekernel.com)