YubiKey FIPS
Technical specifications

FIPS 140-2 validated strong security key for enterprise solutions

Industry leading FIPS 140-2 validated hardware authenticator, which is reliable and easy to deploy. The YubiKey FIPS series ensures strong security and defense against phishing and account takeovers. It enables enterprises and government agencies to meet the highest authenticator assurance level of requirements.
## Technical specifications

### Interface

| USB | USB 2.0 type A (USB 3.0 compatible) |

### Applications

| **OTP (One-time password)** | The OTP applet contains two programmable slots, each can hold one of the following credentials:  
- Yubico OTP  
- HMAC-SHA1 Challenge-Response  
- Static Password  
- OATH-HOTP  

USB Interface: OTP |
| **U2F (Universal 2\textsuperscript{nd} factor)** | The U2F application can hold an unlimited number of U2F credentials and is FIDO certified.  

USB Interface: FIDO |
| **OATH** | The YubiKey FIPS series can hold up to 32 OATH credentials and supports both OATH-TOTP (time based) and OATH-HOTP (counter based). Accessing this sub-module requires Yubico Authenticator.  

USB Interface: CCID |
| **PIV (Smart Card)** | This application provides a PIV compatible smart card. On Windows, the smart card functionality can be enhanced with the YubiKey Smart Card Minidriver.  

**Default Values:**  
- PIN: 123456  
- PUK: 12345678  
- Management Key: 01020304050607080102030405060708

**Supported Algorithms:**  
- RSA 2048  
- ECC P256  
- ECC P384  

**Slot Information:**  
- Slot 9a: Authentication  
- Slot 9b: Management Key  
- Slot 9c: Digital Signature  
- Slot 9d: Key Management  
- Slot 9e: Card Authentication  
- Slot f9: Attestation  
- Slots 82-95: Retired Key Management  

USB Interface: CCID |
OpenPGP

This application implements version 2.0 of the OpenPGP Smart Card specification which can be used with GnuPG. For key sizes over 2048 bits, GnuPG version 2.0 or higher is required.

Supported Algorithms:
- RSA 2048
- RSA 3072
- RSA 4096

USB Interface: CCID

Physical Specifications

<table>
<thead>
<tr>
<th>Connector</th>
<th>USB-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions</td>
<td>18mm x 45mm x 3.3mm</td>
</tr>
<tr>
<td>Weight</td>
<td>3g</td>
</tr>
</tbody>
</table>

Temperatures

| Operational range | 0 °C to 40 °C (32 °F to 104 °F) |
| Storage range    | -20 °C to 85 °C (-4 °F to 185 °F) |

Cryptographic algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Max. keysize</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 2048</td>
<td>2048 bits</td>
</tr>
<tr>
<td>RSA 3072</td>
<td>3072 bits</td>
</tr>
<tr>
<td>RSA 4096</td>
<td>4096 bits</td>
</tr>
<tr>
<td>ECC p256</td>
<td>256 bits</td>
</tr>
<tr>
<td>ECC p384</td>
<td>384 bits</td>
</tr>
<tr>
<td>SHA1</td>
<td>160 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