**FortiToken™ 300**

Available in: Cloud

**Versatile Secure Digital Certificate Storage and Usage**

FortiToken 300 is a Smart Card USB token that is a USB-interfaced device offering a variety of security capabilities including certificate-based public key infrastructure (PKI) authentication, digital signing, encrypting/decrypting files such as emails and documents, VPN client authentication, and more.

In digital certificate-based PKI applications, private keys play an important role in asymmetric cryptography. The FortiToken 300 is a high-security PKI based token that ensures private keys are generated, stored and used internally in a secure chip, meaning the keys are never at risk of being stolen. The FortiToken 300 token is FIPS 140-2 validated and fully certified to ensure this level of protection meets the highest standards. The FortiToken 300 token is a USB-interfaced device that requires no drivers (i.e., driverless) for most operating system (OS) including Windows, macOS, and Linux. It is natively recognized by the OS, making it easy to use with no plugins necessary. Cryptographic Applications can be authenticated with the FortiToken 300 token based on Microsoft Cryptographic Application Programming Interface (CAPI)* and Public-Key Cryptography Standards (PKCS) #11**.

### Highlights
- Driverless USB device
- High-performance smart card chip
- FIPS 140-2 Level 3 Certified
- Windows, Linux, and MacOS supported
- MS-CAPI and PKCS#11 APIs supported
- Onboard random number generator
- Onboard RSA, AES, DES/3DES, SHA-1, SHA-256 algorithms approved by NIST FIPS CAVP
- Economical PKI Smart Card
- Perpetual license
- Tamper-evident hardware USB Token
- Easy integration with PKI infrastructure

*CAPI: Cryptographic Application Programming Interface.
**PKCS#11: Public-Key Cryptography Standards #11 v2.20, Cryptographic Token Interface Standard.
SPECIFICATIONS

FORTITOKEN 300

**Supported Operating System**
32-bit and 64-bit Windows, Linux and MacOS

**Middleware**
Windows middleware for Windows CSP
Direct-called library for PKCS#11 under Windows, Linux, and MAC

**Standards**
X.509 v3 Certificate Storage, SSL v3, IP/Sec, ISO-7816-1-4 8 9 12, CCID

**Cryptographic Algorithms**
- RSA 2048 bit
- ECDSA P-256 w/ SHA-256
- AES 128/192/256 bit
- SHA-1, SHA-256, SHA-384, SHA-512

**Cryptographic Functions**
- Onboard key pair generation
- Onboard digital signature and verification
- Onboard data encryption and decryption

**Cryptographic APIs**
- Microsoft Crypto API (CAPI)
- Cryptography API: Next Generation (CNG)
- PKCS#11
- PC/SC

**Processor**
32-bit smart card chip

**Memory Space**
64 KB (EEPROM)

**Endurance**
At least 500,000 write/erase cycles

**Data Retention**
More than 10 years

**Connectivity**
USB 2.0 full speed, Connector type A

**Interface**
ISO 7816
CCID

**Power Consumption**
Less than 250 MW

**Operating Temperature**
0–70°C (32–158°F)

**Storage Temperature**
-20–85°C (-4–185°F)

**Humidity**
0–100% without condensation

**Certifications**
- FIPS 140-2 Level 3, CE, FCC, UKCA, ICES

PLATFORM SCALABILITY

FortiToken scalability for specific platforms can be found in the Fortinet Product Matrix located at http://www.fortinet.com/sites/default/files/productdatasheets/Fortinet_Product_Matrix.pdf

ORDER INFORMATION

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiToken 300</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTK-300-5</td>
<td>5 USB tokens for PKI certificate and client software. Perpetual license.</td>
</tr>
<tr>
<td></td>
<td>FTK-300-10</td>
<td>10 USB tokens for PKI certificate and client software. Perpetual license.</td>
</tr>
<tr>
<td></td>
<td>FTK-300-20</td>
<td>20 USB tokens for PKI certificate and client software. Perpetual license.</td>
</tr>
<tr>
<td></td>
<td>FTK-300-50</td>
<td>50 USB tokens for PKI certificate and client software. Perpetual license.</td>
</tr>
<tr>
<td></td>
<td>FTK-300-200</td>
<td>200 USB tokens for PKI certificate and client software. Perpetual license.</td>
</tr>
</tbody>
</table>

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Claims of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).