DATA SHEET

FortiToken™ 300

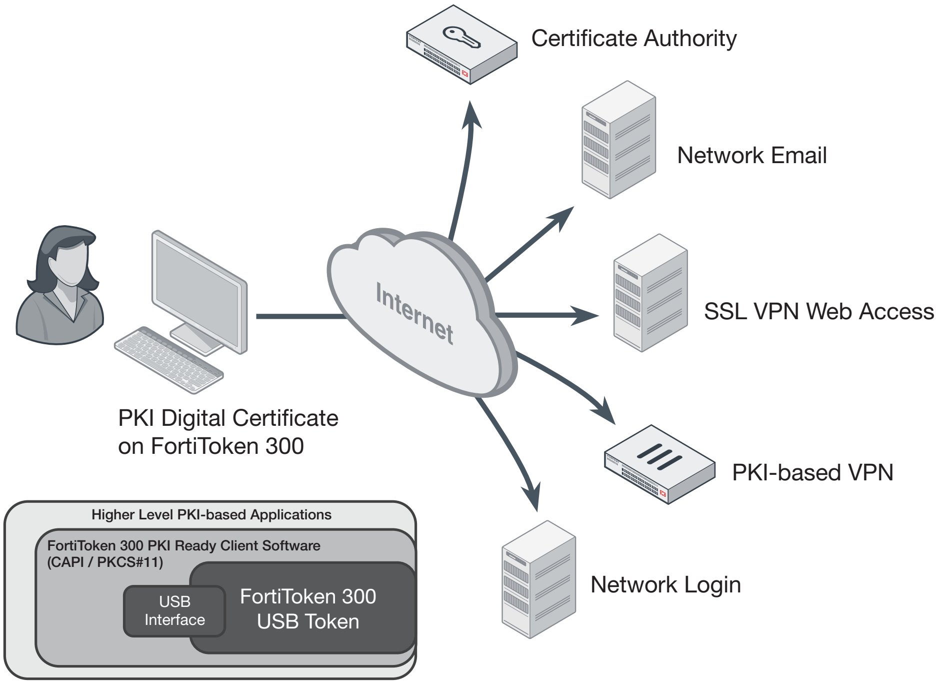
Available in:

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**.


Certificate Authority
Network Email
Internet
SSL VPN Web Access
PKI Digital Certificate on FortiToken 300
PKI-based VPN
Network Login
Higher Level PKI-based Applications
FortiToken 300 PKI Ready Client Software (CAPI / PKCS#11)
USB Interface
FortiToken 300 USB Token

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

Highlights

- Driverless USB device
- High-performance smart card chip
- FIPS140-2 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

SPECIFICATIONS

	FORTITOKEN 300
Supported Operating System	32-bit and 64-bit Windows XP SP3, Server2003, Vista, Server2008, 7, 8, 10, Server2012, 8.1 32-bit and 64-bit Linux MAC OS X
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, IPSec, ISO 7816 1-4 8 9 12, CCID
Cryptographic Algorithms	RSA 512/1024/RSA 2048 bit ECDSA 192/256 bit DES/3DES AES 128/192/256 bit SHA-1 / SHA-256
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	16-bit smart card chip (Common Criteria EAL 5+ certified)
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
Water Resistance	IPX8 with glue injection (under evaluation)

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

Product	SKU	Description
FortiToken 300	FTK-300-5	5 USB tokens for PKI certificate and client software. Perpetual license.
	FTK-300-10	10 USB tokens for PKI certificate and client software. Perpetual license.
	FTK-300-20	20 USB tokens for PKI certificate and client software. Perpetual license.
	FTK-300-50	50 USB tokens for PKI certificate and client software. Perpetual license.
	FTK-300-200	200 USB tokens for PKI certificate and client software. Perpetual license.

www.fortinet.com