

2FA PKI USB Token



2FA PKI USB Token

Overview

2FA PKI USB Token is a market leading cryptographic identity verification module. This small, easy to carry token provides a host of indispensable protective measures for digital communication and transaction through Public Key Infrastructure (PKI) data encryption technology. The 2FA PKI USB token contains a smart-card chip in a USB token form factor. The convenient USB function renders the device operable with almost all computers without the need for a reader. As a two factor advanced authentication solution, the 2FA PKI USB token can secure local and remote desktops and VPN network logon. Key cryptography and the digital signing of emails, documents, and transactions are performed onboard in the secure token framework which is impervious to after-market modification and manipulation.

International Standards Compliant Construction

The construction of principal security components featured on the 2FA PKI USB Token has been carefully tested against the rigorous standards of international third-party experts. The Common Criteria for Information Technology Security Evaluation (CC) has awarded the status of EAL 5+. The 2FA PKI USB Token has received the Federal Information Processing Standard (FIPS) 140-2 level 2, a public standard developed by the United States federal government to distinguish both hardware and software components of cryptographic computer systems, assuring physical tamper-evidence and role-based authentication.

Equipped with Actionable User Interface Features

The 2FA PKI USB Token comes loaded with Microsoft mini-driver standard protocol, which allows the device to run smoothly on Windows operating systems. The end user inserts the key into the host computer and the device driver will be automatically installed through the Windows Update function.

Specifications

Supported Operating Systems	32 bit and 64 bit Windows XP SP3, Server 2003, Vista, Server 2008, Win 7 34 bit and 64 bit, Linux, and Mac OS X
Middleware	Microsoft Windows Mini-driver Windows middleware for Windows CSP
Standards	X.509 v3 Certificate Storage, SSL v3, IPsec, ISO 7816 1-4 8 9 12, CCID
Cryptographic Functions	Onboard key pair generation Onboard digital signature and verification Onboard data encryption and decryption
Cryptographic API's	Microsoft Crypto API (CAPI), Cryptography API: Next Generation (CNG) Microsoft Smart Card mini-driver, PKCS#11, PC/SC
Endurance	At least 500,000 write/erase cycles
Connectivity	USB 2.0 full speed
Humidity	condensation

Benefits

Replace insecure and unstable fixed username/password systems with 2FA's PKI USB Token.

- CJIS compliant two-factor advanced authentication
- Simplified issuance and lifecycle management when used with 2FA ONE Server and Microsoft Certificate Services
- Windows logon to Active Directory
- Works with 2FA ONE Shared Workstation and Secured Applications (SSO)
- Digitally sign and encrypt email and other transactions
- Seamless integration with NetMotion Mobility XE and other VPN technology

Features

- Built-in high-performance secure smart card chip
 - o Smart card chip certified by Common Criteria EAL 5+
 - o Hardware random number generator
 - o 64 KB EEPROM memory to store private keys, multiple certificates, and sensitive data
- Tamper evident hardware USB token
 - o USB full speed device
 - o Compliant with ISO 7816 1-4 8 9 12, PC/SC and CCID devices
- Easy integration with various PKI applications
 - o Easy-to-use web authentication, Plug & Play under Windows systems
 - o Support documentation, email and transaction signature and encryption

Case Specifications



Dimension	53.3mm x 16.5mm x 8.5mm
Weight	4.5
Color	Blue
Serial Number	Ink printed at back side of the case or laser printed on USB connector

Customization	Casing color* (*Requires minimum purchase)
----------------------	---

Certification & Compliance

- FIPS 140-2 Level 2 (under evaluation)
- Common Criteria EAL 5+ (chip level)
- Microsoft WHQL
- USB
- CE
- FCC

10713 N. FM 620, Suite 201
Austin, TX 78726
512.918.3200
Sales@2FA.com