ePass PKI USB Token

A stable and secure PKI product

OVERVIEW

ePass PKI USB Token is the world's foremost cryptographic identity verification module. ePass by FEITIAN provides a host of indispensable protective measures for digital communication and transaction through Public Key Infrastructure (PKI) data encryption technology. The token's unique private key functions as an individual's online ID card and brings a new level of accountability and nonrepudiation to the internet. ePass is a smart-card chip based token with a convenient USB insert rendering the device operable with almost all computers without the need for a reader. As a two factor authentication solution ePass can secure local and remote desktop and network log-on. 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.

Flexible and Ready to Deploy

ePass PKI USB Token has been adopted and used successfully in a wide range of different industries from small/medium and large enterprise, government and finance. The production capabilities to fulfill such a dynamic clientele allow FEITIAN to tailor each order to fit the needs of a particular customer; orders can be customized with a specific logo and/or colour scheme to suit the project at hand.

Bigger is Better: Economy of Scale

Through close cooperation with some of the largest worldwide financial institutions FEITIAN Technologies maintains the stable production of millions of token keys each year enabling the capacity to quickly and efficiently satisfy orders from hundreds to hundreds of thousands. This economy of scale enables a cost effective pricing structure that is unequaled by other manufacturers. With millions of keys in circulation ePass PKI USB Token has been consistently improved and refined to the highest degree of quality and stability.

International Standards Compliant Construction

The construction of principal security requirements featured on the ePass PKI USB Token have 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+. ePass 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

ePass PKI USB Token comes loaded with Microsoft MiniDriver standard protocol which allows the device to run smoothly on Windows operating systems with no need for additional middleware investments. The end user need only to insert the key into the host computer and the device driver will be automatically installed through the Windows Update function. The MiniDriver design works with Windows built-in Microsoft Base Smart Card Provider to offer native support for all Microsoft CAPI and up-to-date CNG solutions, such as Windows Smart Card Log-on and RDP Log-on. Certified by PCSC-Lite/LibCCID group the device can provide built-in support for Linux or MAC operating systems and/or applications. ePass PKI USB Token works with FEITIAN private PKCS#11 library or OpenSC PKCS#11 library for integration into popular web browsers such as Firefox as well as various email clients.

BENEFITS

- **Trusted two-factor authentication on ePass safeguards powerful onboard features.**

Two-factor authentication is based on something you have: your hardware key; and something you know: your personal identification number (PIN). Together these two facets of protection ensure that ePass is not subject to unauthorized utilization. Two-factor authentication protects the integrity of valuable certificate based PKI technology like individual credentials, passwords, and the private key. Authentication is established by the proper execution of a unique PIN code upon token log-on and is necessary to perform higher level device functions.

- **Digital signature affixes a virtual watermark to online communications and transactions.**

Validating the veracity of online communications is a vital component in the effective working process of any organization. When attached to a virtual document a digital signature proves non-repudiation or good faith execution by the owner of the PKI key. ePass performs advanced certificate-based signing of data, emails and transactions. If information is modified even by so much as a single character after the signature has been enacted, the credibility will be lost. Secure signing features include global security protocols of triple data encryption standard (3DES) and advanced encryption standard (AES).

- **Self-contained cryptographic processing provides the stable execution of functions impervious to outside manipulation.**

ePass PKI USB Token by FEITIAN offers complete onboard key generation and cryptographic processing all self-contained in the secure environment of the hardware key. With significant user memory the key can store and maintain multiple certificates, keys, passwords, data and application programs so there is no need to purchase multiple devices.

- **Integrate and deploy advanced smart card chip based technology in a user friendly format**

ePass PKI USB Token is based on a smart card chip, that interacts with the host computer through its sleek USB Token, providing powerful smart card technology without the need for additional hardware purchase such as a compliant card reader. The compact key design and convenient USB interface make ePass PKI USB Token easier to use and easier to maintain than multiple component card systems or one-time PIN keys. The key is engineered to support a wide range of portable systems and desktop applications included and enabled through cryptographic API support that encompasses PKCS #11, Microsoft CAPI, Microsoft and Apple PC/SC.

- **Personalize your security solution with unique customization: your security/your way**

FEITIAN recognizes the significance of the work, trust, and reputation that went into building your brand and that is why ePass PKI USB Token can easily be customized with unique logo printing as well as distinctive colour and branding schemes. Software OEM customization services are also available for large or special projects.

FEATURES

- Built-in high-performance secure smart card chip
  - Smart card chip certified by Common Criteria EAL 5+
  - On board RSA, AES, DES/3DES, SHA-1, SHA-256 algorithms approved by NIST FIPS CAVP
  - Hardware random number generator
  - 64KB EEPROM memory to store private keys, multiple certificates and sensitive data
- FEITIAN Card Operating System with proprietary IP
  - Design according to FIPS 140-2 level 3 standard, FIPS 140-2 level 2 certified
  - Secure messaging ensures confidentiality between the device and the application
  - Support X.509 v3 standard certificate. Support storing multiple certificate on one device
  - Onboard RSA2048 key pair generation, signature and encryption
  - 64 bit universal unique hardware serial number
- Temper evident hardware USB Token
  - USB full speed device
  - Compliant with ISO 7816 1-4 8 9 12, PC/SC and CCID device
  - Water resistant with glue injection (under evaluation)
  - Flexible hardware customization options such as logo, colour and casing
- Reliable middleware supports multiple operating systems
  - Supports Windows, Linux and Mac OS
  - Compliant with Windows mini driver standard, work with Microsoft Base Smart Card CSP, supports Microsoft smart card enrollment for windows smart card user and smart card logon
  - Support PKCS #11 standard API, Microsoft CryptoAPI and Microsoft CryptoAPI : Next Generation (CNG)
  - Work with PKCS#11 & CSP compliant software like Netscape, Mozilla, Internet Explorer and Outlook
- Easy integration with various PKI applications

- Ideal device to carry digital certificates and works with all certificate related applications
- Highly security ensured device for computer and network sign-on
- Easy-to-use web authentication, Plug & Play under Windows systems
- Support document, email and transaction signature and encryption

SPECIFICATION

Product Specification

Supported Operating System	32bit and 64bit Windows XP SP3, Server2003 , Vista, Server2008, Seven 32bit and 64bit Linux MAC OS X
Middleware	Microsoft Windows MiniDriver 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) Microsoft Smart Card MiniDriver PKCS#11 PC/SC
Processor	16 bit smart card chip (Common Criteria EAL 5+ certified)
Memory Space	64KB (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 250mW
Operating Temperature	0°C ~ 70°C (32°F ~ 158°F)
Storage Temperature	-20°C ~ 85°C (-4°F ~ 185°F)

Humidity	0% ~ 100% without condensation
Water Resistance	IPX8 with glue injection (under evaluation)

Feature varies according to product model

Casing Specification

Dimension	53.3mm x 16.5mm x 8.5mm
Weight	4.5 (without glue injection)
Colour	Blue
Material	PC (Polycarbonate)
Label	Inside front side socket Size: 20mm x 6mm 
Serial Number	Ink printed at back side of the case or laser printed on USB connector
Customization	Alternative casing colour (blue, brown, green, grey, purple, red) Glue injection to improve physical resistance * Label logo * ** Require minimum purchase volume*

Certification & Compliance

- FIPS 140-2 Level 2 Certified
- Common Criteria EAL 5+ (chip level)
- Microsoft WHQL
- Linux PCSC-Lite/LibCCID
- RoHS
- Check Point
- Entrust Ready
- USB
- CE
- FCC