

InterPass PKI Token

An interactive PKI product

OVERVIEW

InterPass PKI Token by FEITIAN allows the user to audit and control the entire cryptographic process. InterPass PKI Token is a user interactive PKI device for online banking; offering the most comprehensive standards of transaction verification. With a traditional USB Token a user passes data to the device without explicitly knowing what is actually being processed. InterPass PKI Token is equipped with a large LCD screen which displays details of the secure operations being performed in real time, such as the transfer amount of funds and the transacting bank account numbers. The user retains complete control of the entire process through use of the interactive buttons. Once the information on the screen has been confirmed the transaction is completed by the push of a button, likewise should anything appear amiss the transaction can be cancelled just as easily. By directly involving the user in the PKI authorization process the security of the entire procedure is greatly enhanced.

A Modern Solution for a Modern Problem

FEITIAN engineered InterPass PKI Token in response to the need of online banking institutions to combat increased levels of theft and fraudulent activity. InterPass PKI Token offers unparalleled security by requiring users to expressly confirm their intention to complete a transfer of funds in the exact amount and account locations displayed on the device's onboard LCD screen. Assuming nothing has been modified in transit the user can confirm the integrity of the transaction with the push of a button; alternatively by pressing the designated "cancel" button the entire transaction process is stopped. This measure effectively prevents instances of fraud involving the interception and perversion of data between the user interface and the server known as "Man-in-the-Middle" or "Man-in-the-Browser" attacks; put an immediate stop to unwarranted third party modifications.

Advanced Features Through Advanced Engineering

The essential components of InterPass PKI Token are based on a high performance 32-bit smart card chip. To provide users with the maximum level of convenience, without sacrificing strength, InterPass PKI Token has a fully plug-and-play functional USB Token interface featuring RSA 2048 and SHA-2, the most advanced cryptographic algorithms. With significant available memory space it has the capacity to perform multiple certificate based signatures and transactions, eliminating the need for users to carry and maintain multiple key solutions.

BENEFITS

- **Interactive visual and manual user validation provides full control of the entire cryptographic operation**

Seeing is believing. Exercise total control over your online finances with the ability to visually confirm, or reject, transaction details. Users can audit the full PKI cryptographic process- when a signature operation is required and what data is going to be signed. By monitoring the LCD screen the transaction status is strictly regulated using onboard cancel and confirm buttons.

- **Effectively combat the most advanced online fraud attacks with InterPass**

The level of sophistication involved in modern cyber-attacks is constantly developing. Man-in-the-Middle, Man-in-the-Browser, and advanced Trojan programs have become powerful enough to intercept control over a user's computer to perform fake signatures which are almost indistinguishable from the real thing, with InterPass by FEITIAN the user visually confirms transaction details and can put an immediate stop to unwarranted third party modifications.

- **Enjoy the benefits of a pure "Plug & Play" device.**

InterPass PKI Token features "Plug & Play" middleware auto-installation. Accessing onboard middleware through a full speed USB port which requires no additional hardware or software investment. Smaller than your thumb and weighing less than a coin InterPass PKI Token by FEITIAN is a secure solution to be used anywhere and everywhere you need protection.

- **Based on the most highly advanced cryptographic algorithms**

With internationally recognized security standard 1024 or 2048 bit RSA key-pair generation DES and 3DES cryptography algorithms InterPass PKI Token is engineered to deliver the most cutting edge interactive features and hardware casing technology along with the industry's most trusted underlying program components.

- **Two-factor authentication protects the integrity of device functions from abuse**


Strong two-factor authentication increases security of the token by ensuring that even if the device is lost or stolen the user must produce the unique PIN number affixed to the log on entry screen to be able to access the transaction validating and data encryption features stored within.

FEATURES

- Built-in user interactive buttons to control onboard cryptographic operation
 - Four buttons: two buttons to confirm and cancel the operation, two buttons to scroll up and down the screen
 - Blue LED keyboard light
 - Automatically cancel the operation after timeout
- Built-in high-performance 32 bit secure smart card chip
 - Onboard RSA, DES/3DES, MD5, SHA-1, SHA-256
 - Hardware random number generator
 - 32KB user memory to store private keys, multiple certificates and sensitive data
- FEITIAN Card Operating System with proprietary IP
 - Hardware render the transition details and control user interaction
 - Secure messaging ensures confidentiality between the token 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
- Reliable middleware supports multiple operating systems
 - Supports Windows OS
 - Support PKCS #11 standard API and Microsoft CryptoAPI
 - Work with PKCS#11 & CSP compliant software like Netscape, Mozilla, Internet Explorer and Outlook
- Easy integration with various PKI application
 - 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
 - Support document, email and transaction signature and encryption

SPECIFICATION

Product Specification

Supported Operating System	 32bit and 64bit Windows XP SP3, Server2003 , Vista, Server2008, 7, 8
Middleware	Windows middleware for Windows CSP PKCS#11 library for Windows
Standards	X.509 v3 Certificate Storage, SSL v3, IPSec, ISO 7816 compliant
Cryptographic Algorithms	RSA 512/1024/RSA 2048 bit DES/3DES MD5 SHA-1 / SHA-256
Cryptographic Functions	Onboard key pair generation Onboard digital signature and verification Onboard data encryption and decryption

Cryptographic APIs	PKCS#11 Microsoft Crypto API
Button	Number of button: 4 (confirm/cancel/scroll up/scroll down) Material: Acrylic (PMMA) Endurance: more than 300,000 times
Flash Memory	2MB (default)
Flash Endurance	At least 20,000 write/erase cycles
Processor	32 bit smart card chip
Memory Space	32KB user memory
Endurance	At least 500,000 write/erase cycles (EEPROM)
Data Retention	More than 10 years
Connectivity	USB 1.1, USB2.0 compliant, Connector type A (through USB cable)
Interface	ISO 7816
Power Consumption	Less than 500mW
Operating Temperature	0°C ~ 50°C (32°F ~ 122°F)
Storage Temperature	-20°C ~ 70°C (-4°F ~ 158°F)
Humidity	40% ~ 90% without condensation

Casing Specification



Certification & Compliance

- RoHS
- USB
- CE FCC