

ePass2000_FT12

Hardware Description

1. Advantages of ePass2000_FT12

ePass2000_FT12 integrates first-class manufactured smartcard chip. It is the ideal device to protect the sensitive data. Its advantages include:

- **Excellent Performance**

8-bit RISC stably working in 6 MHz clock frequency makes the smartcard's performance achieve perfect.

- **High Security**

Integrated hardware-based RSA algorithm, ePass2000_FT12 is more secure than applications that only employ software-implemented RSA. Because the sensitive data is stored in the secure storage zone of ePass2000_FT12 hardware, unauthorized people is unable to access the data. The data signature and encryption operation are performed inside ePass2000_FT12. The private key is also stored inside ePass2000_FT12 since its generation. These could effectively prevent hacker program attacks. In addition, the algorithms used by ePass2000_FT12 are publicly acknowledged by the industry, widely open, and proven. The first-class chip encapsulation technique provides further security for data inside the chip.

- **Easy to Use**

Using ePass2000_FT12 does not require any additional devices. Users only need to plug ePass2000_FT12 into the USB port of desktop computers, laptop computers, keyboards or displays. Users do not need to shut down the computer or stop any running programs. After finishing the use, users could disconnect ePass2000_FT12 directly.

- **Low Cost**

ePass2000_FT12 could save more cost than any other hardware-based security systems, because it does not require any additional devices. This makes ePass2000_FT12 especially suitable for widely deployed applications. ePass2000_FT12 could provide all the functionalities of smartcard card devices with its special advantage that no smartcard reader is required.

- **Portability**

ePass2000_FT12 is small and light, which makes it perfectly portable. Small casing shell is manufactured by all-in-one once-forming technique. It is hard and durable with waterproof feature. Users could carry ePass2000_FT12 conveniently on their key rings.

- **Compatibility**

ePass2000_FT12 supports two types of most popular standard interfaces: PKCS#11 and Microsoft CryptoAPI. Any application that is compliant with these two interfaces could be integrated with ePass2000_FT12 directly. Moreover, ePass2000_FT12's compatibility has been optimized for many third-party software products. Additionally, ePass2000_FT12 integrates mass secure storage memory. It could store multiple certificates, private keys and other data. That means, multiple PKI applications could share one ePass2000_FT12 device.

- **High Reliability**

ePass2000_FT12 is manufactured with strict standard technique. It supports at least a hundred thousand times of erasing and writing. Data stored in ePass2000_FT12 could be retained for at least 10 years under room temperature. This effectively ensures that the sensitive data is stored securely and stably.

2. ePass2000_FT12 Hardware Features

- **High-performance processor**

ePass2000_FT12 integrates 8-bit RISC high-level secure SOC processor, presenting high performance, high-level security, low power dissipation and low cost features.

- **Hardware implemented encryption algorithms**

The advanced smartcard technique of ePass2000_FT12 provides the following hardware-based encryption algorithms:

- 1) 512-bits, 1024-bits RSA dissymmetrical encryption algorithm and related signature, verification functionalities;
- 2) Symmetrical cryptographic algorithms: DES and 3DES;
- 3) Digest function: SHA-1 and MD5.

These key encryption algorithms are implemented inside the hardware. This ensures the security of the keys pairs in encryption calculation.

- **Hardware-based RSA key-pair generator**

The ePass2000_FT12's RSA key pairs are generated inside the hardware instantly. The grand prime numbers used to generate the key pairs are also provided by the hardware random number generator.

- **Hardware-based random number generator**

The ePass2000_FT12 integrates the hardware random number generator. This generator could be used for generating the RSA key pairs, random access message identification code and so on.

- **Multi-level accessing privilege**

The ePass2000_FT12's file system supports up to 16 security levels. Users could define single or multiple key administration levels. More complicated security level and relations could be defined by users according to their application's requirements.

- **On-chip secure memory area**

The ePass2000_FT12's data storage RAM, firmware storage ROM and computing components are integrated within a single chip. This assures the secure storage of the data.

3. ePass2000_FT12 Specifications

Supported Operating Systems	Windows 98SE/ME/2000/XP/Server 2003, Linux, Mac OS X
Certifications and Standards	CSP/PKCS#11, supports X.509 v3 standard format certificate, SSL v3,IPSec/IKE and compatibility with ISO7816
Qualification	Compliant with CE and FCC standards
Processor	8-bit smartcard chip
Memory Size	32KB
On-Board Security Algorithms	RSA, DES, 3DES, MD5, and SHA-1
Chip Security Level	Secured and Encrypted Data Storage
Power	<250mW
Operating Temperature	0°C to 70°C
Storage Temperature	- 20°C to 85°C
Humidity Rating	0% to 100% without condensation
Interface Type	Standard USB 1.1 devices, support for USB 2.0 interface, Type A connector
Dimension	50x17x7mm (A1+ Casing)
Weight	6g
Casing Material	PC (polycarbonate)
Data Retention	At least 10 years
Erasing Times	At least 100,000 times