

# ePass2000\_FT12 Hardware Description

## 1. Advantages of ePass2000\_FT12

ePass2000\_FT12 integrates first-class manufactured smartcard chip. It is the ideal device to protect user's sensitive data. Its advantages include:

- Superiority performance

Integrating 8-bit RISC, stably working in 6 MHz frequencies makes the smartcard's performance achieve perfect.

- High-level security

Integrated hardware-based RAS algorithm, ePass2000\_FT12 provides more security than simply software-implemented RSA applications. Because the sensitive data are stored in ePass2000\_FT12 hardware secure storage zone, unauthorized personal is unable to access the information. The digital signature and encryption operations are processed in ePass2000\_FT12, and the private key is stored in the ePass2000\_FT12 since it is initially generated. This could effectually prevent hacker program attacking. Another fact is that all of the algorithms used by ePass2000\_FT12 are broadly published, tested by years and widely accepted by the public. The first-class chip encapsulation technique could also provide security factor to data on the chip.

- Easy to use

Using ePass2000\_FT12 does not require any additional devices. User needs simply plug ePass2000\_FT12 into any USB ports of desktop computers, laptop computers, keyboards or displays. User does not need to shut down the computer or closing any running programs. After finished usage, user could pull out the ePass2000\_FT12 directly.

- Low cost

ePass2000\_FT12 could save more costs than any other hardware-based security systems. Because it does not require any additional devices. This makes ePass2000\_FT12 suitable for wide range applied applications. ePass2000\_FT12 could provide all the functions of smartcard card devices with its special advantage that no smartcard reader is required when using those functionalities.

- Portability

The small and exquisite shape, low weight makes ePass2000\_FT12 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 in their key ring.

- Compatibility

ePass2000\_FT12 supports two type of most popular PKI standard interfaces: PKCS#11 and Microsoft CryptoAPI. Any applications compliant with these two interfaces could be integrated with ePass2000\_FT12 directly. Moreover, ePass2000\_FT12 has been compatibility optimized for most third-party software products. Additionally, ePass2000\_FT12 integrates mass secure storage memory. It could store multiple certificates, private keys and other data. It means that multiple PKI applications could share one ePass2000\_FT12 resources.

- High Reliability

ePass2000\_FT12 is manufactured with strict-standard technique. It supports at least a hundred thousand times erasing and writing. Data stored in ePass2000\_FT12 could be retained for at least 10 years under room temperature. This effectively ensures the sensitive data being stored securely and stably.

## 2. Hardware features of ePass2000\_FT12

- 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) 1024-bytes RSA dissymmetrical encryption algorithm and related signature, verification functionalities.
- 2) Symmetrical cryptographic algorithm: DES and 3DES.
- 3) Hashing function: SHA-1 and MD5.

These key encryption algorithms are implemented inside the hardware. This ensures the security for the key pairs generated in encryption.

- Hardware-based RSA key pair generator

The RSA key pair is generated inside the hardware instantly. The maximal prime numbers used to generate the key pair 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 to generate the RSA key pairs, random access message identification code and so on.

- Multi-level access privilege

The ePass2000\_FT12 file system supports up to 16 security levels. User could define single or multiple key administration levels. More complicated security level and relations could be defined by users due to their application's requirements.

- On chip secure memory zone

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

## 3. Specifications of ePass2000\_FT12

Supported Operating Systems	Windows, Linux, Mac OS X
Certifications and Standards	CSP/PKCS#11, supports X.509 v3 standard format certificate, SSL v3, IPSec/IKE , compliant with ISO7816

Qualification	Compliant with CE and FCC standards
Processor	8-bit smartcard chip
Memory Size	32KB
On-Board Security Algorithms	RSA,DES,3DES,SHA-1
Chip Security Level	Secured and Encrypted Data Storage
Power Dissipation	<250mW
Operating Temperature	0° C ~ 70° C
Storage Temperature	- 20° C ~ 85° C
Humidity Rating	0 ~ 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