

ePass3000 Hardware Description

1. Advantages of ePass3000

ePass3000 integrates first-class manufactured smartcard chip. It is the ideal device to protect user's sensitive data. Its advantages include:

- Superiority performance

Integrating 32-bit RISC, stably working in 100 MHz frequencies makes the smartcard's performance achieve perfect.

- High-level security

Integrated hardware-based RSA algorithm, ePass3000 provides more security than simply software-implemented RSA applications. Because the sensitive data are stored in ePass3000 hardware secure storage zone, unauthorized person is unable to access the information. The digital signature and encryption operations are processed in ePass3000, and the private key is stored in the ePass3000 since it is initially generated. This could effectually prevent hacker program attacking. Another fact is that all of the algorithms used by ePass3000 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 ePass3000 does not require any additional device. User needs simply plug ePass3000 into any USB port of desktop computers, laptop computers, keyboards or displays. User does not need to shut down the computer or close any running program. After finished usage, user could pull out the ePass3000 directly.

- Low cost

ePass3000 could save more costs than any other hardware-based security systems. Because it does not require any additional device. This makes ePass3000 suitable for wide range applied applications. ePass3000 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 make ePass3000 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 ePass3000 conveniently in their key ring.

- Compatibility

ePass3000 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 ePass3000 directly. Moreover, ePass3000 has been compatibility optimized for most third-party software products. Additionally, ePass3000 integrates mass secure storage memory. It could store multiple certificates, private keys and other data. It means that multiple PKI applications could share one ePass3000 resources.

- High Reliability

ePass3000 is manufactured with strict-standard technique. It supports at least a hundred thousand times erasing and writing. Data stored in ePass3000 could be retained for at least 100 years under room temperature. This effectively ensures the sensitive data being stored securely and stably.

2. Hardware features of ePass3000

- High-performance processor

ePass3000 integrates 32-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 ePass3000 provides the following hardware-based encryption algorithms

- 1) 512, 1024, 2048-bytes RSA dissymmetrical encryption algorithm and related signature, verification functionalities.
- 2) Symmetrical cryptographic algorithm: DES and 3DES.
- 3) Hashing function: SHA-1.

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 ePass3000 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 ePass3000 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 ePass3000

Supported Operating Systems	Windows 98SE/ME/2000/XP/2003/Vista, Linux, Mac OS X
Certifications and Standards	CSP/PKCS#11 v2.11, supports X.509 v3 standard format certificate, SSL v3, IPSec/IKE , compliant with ISO7816
Qualification	Compliant with CE and FCC standards
Processor	32-bit smartcard chip
Memory Size	64KB
On-Board Security	RSA,DES,3DES,SHA-1

Algorithms	
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 100 years
Erasing Times	At least 100,000