DATA SECURITY

FINGERPRINT USB TOKEN (PLAIN)

> OVERVIEW

Based on Public Key Infrastructure technology, the Fingerprint USB Token can be used instantly upon insertion and does not require the installation of any software. It is especially applicable for security authentication of Internet systems, and is ideal for performing tasks like system log-in, information encryption, and generation of digital signatures etc., The token can more effectively guarantee the security of private keys and certificates.

> FEATURES

> I Main Components

- Microprocessor: 32-bit specific cryptographic chip
- Fingerprint Sensors: Swipe semiconductor sensors
- Communication Interface: USB2.0

> II Key Algorithms

- Public Key Algorithm: 1024, 2048-bit RSA algorithm
- Hashing Algorithm: SHA-1, MD5
- Speed of Digital Signature: 32times/second
- Uses unique dynamic templates integrated technology to improve fingerprint one-time passing rate

> III Operation Systems

- Windows 98/ 2000/2003/XP, Vista, Win 7, Linux, etc.

> IV Application Specifications

- Maximum Operating Power: <150mA @ 5V
- ESD Protection: >15 kV
- Length of Connecting Line: 30cm
- Operating Temperature: -25℃ to +70℃
- Operating Humidity: 20% to 95%
- Data Lifespan: >10 years
- Device Lifespan: 1,000,000 uses

> SPECIFICATIONS

- Matching Mode: 1:1, 1: N
- FRR: <0.01%
- FAR: <0.00003%
- Enrollment Speed: 1 second/finger
- Verification Speed: 1:1, <10 milliseconds
  1: N (N<100), <1 second
- Template Size: ≤256 bytes/finger
- Fingerprint Storage Space: 100 fingerprints, expandable
- Storage Space: 64KB, expandable

APPLICATIONS

It is mainly used in e-business, e-government, e.g. online banking, host computer lock, documents encryption, Internet security authentication, etc.