PKI Authentication Token

FIPS 140-2 Level 3 Certified

Data encryption

Authenticity and integrity checking

User authentication

Email protection

Windows smartcard logon

Remote VPN access

Major Features & Benefits

- **Offers multiple application security Authentication support**
  pToken CryptoID supports standard smart card applications like Windows smart card logon, VPN, Bit Locker etc.

- **Smart Card Based**
  Utilizes 32-bit smart card technology enabling smart card-based authentication and strong authentication.

- **On-Board Encryption processing**
  Encryption and decryption processes take place on-board the pToken device, minimizing the risk of performing the process locally on the host computer.

- **Non-Repudiation Digital Signing**
  Offers non-repudiation digital signing and storing of transactions and documents through PKI technology; ensuring the authenticity of electronic transactions in finance and retail industries.

- **Multiple Algorithms Employed**
  Makes use of several industry-approved encryption algorithms including:
  - Symmetric Algorithm: DES, 3DES, AES168, AES192, AES256
  - Asymmetric Algorithm: RSA1024/2048
  - Digest Algorithm: MD5, SHA1, SHA256, SHA384, SHA512

- **Secure File System**
  Secure file system for storage of digital credentials and files using the three-level permission system.

- **Unique Global Hardware ID**
  Employs both a unique global hardware ID and user-defined 32-bit software ID for device own identification.

- **Three Level Permission System**
  Hardware serial number will be read when token plug in. Token is in super user mode after super password verified.

- **Token is in usage mode after password verified**
  Implements a three-level high security permission system: Administrator, User and Guest.

- **Encrypted Credentials**
  Credentials are encrypted and stored on the device and cannot be exported.

- **Cryptography Standards Compliant**
  - Microsoft CryptoAPI and CNG X509 v3 certificate storage
  - SSL V3, IPSEC/KEC, PC/SC, CCID
  - PKCS# 11 V2.20
  - Microsoft SmartCard Mini Driver

- **Custom API Support for numerous applications**

- **Multiple Platform Compatibility**
  Support across various OS platform including XP, Server 2003, Vista and 7,8,10, Mac OS X, and Linux

Technical Parameters

Power supply	USB Port
Working Voltage	5V (USB Chargeable)
Working current	50mA
Working temperature	0 – 70℃
Storing temperature	-20 – 85℃
Casing Material	Metal
Communication	USB CCID
Interface Standard	USB 2.0 High speed support; compliant with 3.0
Processor	32-bit Smartcard chip
Memory	128KB EEPROM
Number of Read/Write Cycles	At least 100,000 write/erase cycles
Data Retention	At least 10 Years
Power Consumption	Less than 100mW
Cryptography Standards Compliant	Microsoft Smart Card Mini Driver
	Microsoft CryptoAPI and CNG
	PKCS# 11 V2.20
	X509 v3 certificate storage
	SSL V3, IPSEC/KEC, PC/SC, CCID

Supporting OS

pToken CryptoID follows international cross-platform standards thus suitable for multiple operating systems. Supported Operating System include the following:
- Windows XP, 2003, Vista, 7 , 8 , 10 (both 32 and 64-bit)
- Windows SERVER 2003/2012/2015 and more
- Linux 2.6 and more
- Mac OS X 10 and above

Meanwhile, multiple secure algorithms and middleware are also supported.

pToken CryptoID offers Microsoft Mini Driver, Microsoft Crypto API and PKCS#11 interface; supports multiple certificates and key pairs. All applications compatible with these standard interfaces can be integrated with and hence secured.

COS Features

- ISO 7816 Standard
- Support for DES, 3DES, AES128/192/256, SHA1/SHA256/SHA384/SHA512, RSA(1024/2048)
- Support multiple applications, multiple containers and multiple certificates;
- Support for X.509 v3 certificate storing and certificate importing.

Software and Middleware

- In-built CD-ROM – designed for users to store custom middleware.
- Support for pToken API libraries, pToken PKI middleware (for PKCS#11 v2.2 and MS-CAPI applications) and self-defined interfaces.