User Manual

1.0. Introduction

In the Online transaction system process, the malicious software can complete its illegal electronic transaction behavior successfully through intercepting and tampering transaction data between the user and server, like Phishing Attack, Trojan Horse Attack.

It is time for WatchKey ProX USB Token .

WatchKey ProX USB Token is a USB - based PKI, two - factor authentication token device which is portable, easy - to - use and cost - efficient for on - line authentication, signature, encryption and online transactions. The USB interface eliminates the need to install card readers at the client side. The WatchKey ProX USB Token is among the securest and lightest cryptographic USB tokens in the word. The built - in TIMECOS chip (100K bytes FLASH) complies with the most stringent international standards, like ISO 7816-4, FIPS140 - 2 compatible and possesses the most reliable encrypting capabilities like AES, 3DES, RSA and ECDSA.

The chip embedded in the WatchKey ProX USB Token is a highly secure data container. The user's private and public keys are generated on the chip the first time a user request a certificate. The private key is stored on the chip and can never be exported, making the WatchKey ProX USB Token one of the most secure data containers in the world.

A true "plug and play" solution, WatchKey ProX USB Token Anywhere eliminates the need for pre - installation of desktop client software, enabling online service providers and organizations to offer customers, partners and employees secure remote access to online services and business portals with the added benefit of digital signing capabilities. With WatchKey ProX USB Token Anywhere, users can access web - based applications, corporate networks and carry out online transactions easily, conveniently and - most of all, securely - from just about anywhere. WatchKey ProX USB Token Anywhere is ideal for corporate and Internet security needs, enabling organizations to expand their range of online business services while providing end - users with full roaming capabilities. For consumers, the convenience of a robust yet simple "plug and - play" solution is unbeatable. WatchKey ProX USB Token Anywhere is a certificate - based strong authentication solution that combines the security of PKI with the simplicity and convenience of traditional OTP products.

2.0. Benefits

- **Simple:** Plug and play simplicity for users, with no end - point software installation

- **Strong Security:** Certificate - based authentication with onboard smartcard
- **Interactive:** LED light displays power and communication status
- **Conveniently:** small and portable, easy to use.
- **Application Rich:** Ideal for expanding online services and offering simple and secure access to partners, customers and mobile workers from any location

3.0. Typical Applications

- Online Banking
- E - government
- Identification authentication on network
- Secure e - commerce and secure remote access
- Public Key Infrastructure based Application
- PKCS#11 & CSP & KeyChain - compliant software applications
- Customized applications

4.0. Features

4.1. Cryptographic Smart Card

- TIMECOS
- Employ 32 - bit microprocessor security chip design capable of making USB communications**.**
- FIPS140 - 2(US Federal Information Processing Standards) compatible.
- Highly secured, supports 1024 - bit, 2048 - bit RSA and P-192/P-256 ECDSA asymmetrical encryption algorithm, and generates RSA/ECDSA key pairs inside card.
- Supports with the ability to produce 1024 - bit/2048 - bit RSA and P-192/P-256 ECDSA signature, verify, encryption, decryption.
- Provides multiple Security Algorithms: AES, 3DES, MAC, SHA - 1, SHA - 256 , SHA-384, SHA-512.
- Supports 100KB FLASH;
- Complies to USB1.1 standard and USB 2.0 full speed

4.2. Software/Middleware

- Support X.509V3 certificate format;
- Supports ISO7816 part4 file structures: transparent, linear fixed, linear variable, cyclic;
- Supports CCID and USB Mass Storage protocol;
- Supports Microsoft CAPI2.0, PKCS#11 v2.11, PKCS#1,7,8,10 and12, PKCS#15;

- Supports Windows 2000 / XP / Vista / 2003 / 7 / 8 / 8.1, Mac OS X;
- Supports Internet Explorer 6 and above, Mozilla Firefox, Safari;

5.0. Specifications

Supported operating systems	Windows 2000 / XP / Vista / 2003 / 7 / 8 / 8.1, Mac OS X
Supported browsers	Internet Explorer 6.0+; Firefox 3.0+ ; Safari
API & standards support	PKCS#11 v2.01, Microsoft CSP, CCID, X.509 v3 certificate SSL v3, TLS1.0/1.1/1.2
Memory Size	100K
On board security algorithms	RSA 1024-bit and 2048-bit, ECDSA P-192/P-256, 3DES (Triple DES), MAC , AES SHA-1, SHA-256, SHA-384, SHA-512
Security certifications	smart card chip: FIPS 140-2
ISO specification support	Support for ISO 7816-4 specifications
Operating temperature	0° C to 70° C (32° F to 158° F)
Storage temperature	-40° C to 85° C (-40° F to 185° F)
Humidity rating	0-100% without condensation
Connector	USB type A; supports USB 1.1 and 2.0 (full speed and high speed)
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000
Weight and Size	Approx. 7g. Approx. 52.1mm * 16.8mm * 7.9mm

6.0. FCC STATEMENT

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.