

TRUSTED KEY PKI®

PKI Authentication Token



Email Signature and Encryption

Windows Smart Card Logon

Document Digital Signature

Secure Online Transaction

Disk and File Encryption

Remote VPN Access

Trusted Key PKI® is a high security PKI based USB token incorporating the most powerful cryptographic technology and standards available today. It is designed for all Public Key Infrastructure environments and brings two-factor cryptographic authentications to applications where security is critical. FIPS 140-2 validated card operating system on-board key management mechanism enable a higher level of security assurance to wide range of sensitive applications. With combined compatibility of Microsoft Minidriver and OpenSC, the Trusted Key PKI® is compatible with applications running on Windows, Linux and macOS and therefore is the ideal choice for all industries requiring high level protection such as government, enterprise, financial institutions and media companies.

Enterprise

Corporations need not only keep networks secure but also digitally sign documents and emails. Instead of using several devices the Trusted Key PKI® does it all. Trusted Key PKI® works with Microsoft Office for signing documents and also smart card logon and range of VPN vendors such as CheckPoint VPN to ensure your network is safe and secure. With support for both CSP and PKCS#11 interfaces you can be sure that Trusted Key PKI® works with your application.

Publishing and Media

In the world of publishing and media, getting media delivered to customers securely is key in order to safeguard ROI. With support for Windows EFS, PGP and other major file encryption formats media can be distributed quickly and easily online and offline without worrying about copyright theft. The Trusted Key PKI® also supports all major internet browsers such as Firefox, Chrome, Safari and Internet Explorer to ensure your media reaches the widest possible audience.

E-Government

The Trusted Key PKI® is a token of high standards. Compliant with FIPS 140-2, Trusted Key PKI® is perfect for government solutions such as the declaring of taxes and judiciaries. In today's digital age where governments are moving towards a paperless workflow in order to reduce costs, help protect the environment and increase efficiency, the Trusted Key PKI® is the perfect replacement for written signatures.

Finance

In finance trust is king. In order to ensure the finances of millions of customers around the world, using a token that boasts the highest security on the market is key. With RSA 2048-bit, AES 256 and SHA-2 high security algorithms the customer's online transfers can be secured. With support also for SSL connections, the industry standard in secure online connections, there is always a secure connection every time. The Trusted Key PKI® is flexible due to its large memory, which allows the token to store many certificates and therefore be used with multiple accounts and applications.

Specifications

Supported operating systems	Windows 2000/XP/Server 2003/Vista/Server 2008/Server 2008 R2/7/Server 2012/Server 2012 R2/8/8.1/10, Linux, macOS	Cryptographic algorithm	Asymmetric Key: PKCS#1 V2.2 RSA 1024/2048 bit (RSAES-OEAP, RSASSA-PSS) ECDSA 192/256 bit Symmetric Key: DES (Non-FIPS mode)/3DES AES 128/192/256 bit Digest: SHA-1, SHA-256, SHA-384, SHA-512, SHA512/224, SHA-512/256	Physical parameters	Standards: CE, FCC, RoHS Secure MCU: 32 bits Memory Space: 64 KB Data Retention: at least 10 years Certificate Re-write: >100,000 times, data rewrite cycle >100,000 times Connectivity: USB 1.1/2.0 compliant USB Connectors Durability: ≥2,500 plug-unplug cycles Power Consumption: <250 mW Operating: 0°C~60°C Storage: -20°C~70°C Humidity: 0~100% RH
Hardware interface	ISO 7816-1, 2, 3, 4 compliant, CCID				
API standards	PKCS#11 V2.20 Cryptographic Service Provider (CSP) Microsoft Smart Card Minidriver Microsoft CNG, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE				
Certification	FIPS 140-2 Level 3 Certified				