PKI Tokens

Authentication, Encryption and Digital Signatures

Hardware PKI Tokens

PKI tokens are hardware devices that store digital certificates and private keys securely. When you need to encrypt, decrypt or sign something, the token does this internally in a secure chip meaning the keys are never at risk of being stolen.

We supply the following PKI tokens:

			
	USB PKI Token (ePass2003)	**USB PKI Token (Mini)**	**PKI Smart Card**
Description	The ePass2003 is a FIPS 140-2 Level 3 certified token providing secure storage of personal identity information, digital certificates and private keys for authentication, encryption and digital signatures. This industry-standard USB PKI token is highly regarded internationally.	Secure storage of personal identity information, digital certificates and private keys in a tiny keychain-sized USB key. Supports on-board encryption/decryption and digital signatures. Driverless on Windows, Mac and Linux.	Secure storage of personal identity information, digital certificates and private keys in a ID-1 sized card. Supports on-board encryption/decryption and digital signatures. NFC-enabled for contactless applications. Can be used with any of our smart card readers.
Features	• USB connectivity • Onboard key generation • Onboard digital signing and verification • Onboard data encryption and decryption • PKCS#15 • PKCS#11 V2.2 with OEAP/PSS support • X.509 v3 Certificate Storage • OpenSC compatible	• Driverless • USB connectivity • Onboard key generation • Onboard digital signing and verification • Onboard data encryption and decryption • PKCS#15 • X.509 v3 Certificate Storage • OpenSC compatible	• Contactless NFC operation (ISO/IEC 14443) • Onboard RSA key-pair generation • Onboard digital signing and verification • Onboard data encryption and decryption • PKCS#15 • Supports Microsoft CAPI and PKCS#11 • X.509 v3 Certificate Storage • OpenSC compatible • Chip: Infineon SLE77CLFX2400PM
Algorithms	• RSA 1024/2048 bit (RSAES-OEAP, RSASSA-PSS) • ECDSA 192/256 bit (Optional) • DES/3DES • AES 128/192/256 bit • SHA-1, SHA-2, MD5	• RSA 1024/2048 bit • ECDSA 192/256 bit (Optional) • DES/3DES • AES 128/192/256 bit • SHA-1, SHA-2, MD5	• RSA 1024/2048 bit • ECDSA 192/256 bit (Optional) • DES/3DES • AES 128/192/256 bit • SHA-1, SHA-2, MD5
Supported APIs & Protocols	• Microsoft CAPI, CNG • PKCS#11 V2.20 • Microsoft Smart Card Minidriver • PC/SC, CCID • SSL v3 • IPSec/IKE	• Microsoft CAPI, CNG • PKCS#11 V2.20 • Microsoft Smart Card Minidriver • PC/SC, CCID • SSL v3 • IPSec/IKE	• Microsoft CAPI, CNG • PKCS#11 V2.20 • Microsoft Smart Card Minidriver • PC/SC, CCID • SSL v3 • IPSec/IKE

Specification	• ISO-7816 compliant • Memory: 64 KB • 10 year+ data retention • Operating temperature: 0 °C ~ 50 °C • Storage temperature: -20 °C ~ 60 °C • Humidity: 0 ~ 100 % RH	• 32-bit ARM-based Smart Card Chip (CC EAL 6+) • Java Card 2.2.2 • Global Platform 2.1.1 • ISO-7816 compliant • Memory: 31 KB • 500,000+ write/erase cycles • 10 year+ data retention	• Java Card 2.2.2 • Global Platform 2.1.1 • ISO-7816 compliant • ISO/IEC 14443 compliant • Operating voltage: 3 v/5 v • Memory: 68 KB • 500,000+ memory rewrites • 10 year+ data retention
OS Compatibility	• Windows PC/Laptop • macOS • Linux	• Windows PC/Laptop • macOS • Linux	The PKI Smart Card supports the following operating systems and requires a compatible reader • Windows PC/Laptop • macOS • Linux • iPhone • iPad • Windows tablet • Android (contactless (NFC), or via compatible reader)
Certifications	• CC EAL 5+ (chip level) • CE, FCC, RoHS compliant • FIPS 140-2 Level 3 Certified • ICP-Brasil Certified	• CE, FCC, RoHS compliant	• CC EAL 5+ (chip level) • CE, FCC, RoHS compliant

PKI SDK

Our PKI Software Development Kit includes everything you need to integrate PKI into your software. The SDK include libraries, detailed sample code and documentation for C, C++ and Java.