

# Tokens de PKI

Autenticación, cifrado y firmas digitales

## Hardware de tokens de PKI

### Token USB PKI ePass2003



### Descripción

El Feitian ePass2003 es un token certificado de nivel 3 FIPS 140-2 que proporciona un almacenamiento seguro de información personal, certificados digitales y claves privadas para la autenticación, encriptado y firmas digitales. Este token USB PKI, estándar en la industria, ha recibido multitud de reconocimientos internacionales.

### Características

- Conectividad USB
- Generación de claves a bordo
- Firma y verificación digital a bordo
- Cifrado y descifrado de datos a bordo
- Soporte con inicio de sesión en Windows
- PKCS#15
- Almacenamiento de certificado X.509 v3
- Compatible con OpenSC

### Tarjeta inteligente de PKI



### Descripción

Almacenamiento seguro de información de identidad personal, certificados digitales y claves privadas en una tarjeta de tamaño ID-1. Admite un cifrado/ descifrado y firmas digitales a bordo. Compatible con NFC para aplicaciones sin contacto. Se puede utilizar con cualquiera de nuestros lectores de tarjetas inteligentes.

### Características

- Operación NFC sin contacto (ISO/IEC 14443)
- Generación de par de claves RSA a bordo
- Firma y verificación digital a bordo
- Cifrado y descifrado de datos a bordo
- Soporte con inicio de sesión en Windows
- PKCS#15
- Almacenamiento de certificado X.509 v3
- Compatible con OpenSC

## API y protocolos compatibles

- Microsoft CAPI, CNG
- Generic Identity Device Specification (GIDS)
- PKCS#11 v2.40
- Minidriver de tarjeta inteligente de Microsoft
- PC/SC, CCID
- SSL v3
- IPSec/IKE

## API y protocolos compatibles

- Microsoft CAPI, CNG
- Generic Identity Device Specification (GIDS)
- PKCS#11 v2.40
- Minidriver de tarjeta inteligente de Microsoft
- PC/SC, CCID
- SSL v3
- IPSec/IKE

## Algoritmos

- RSA 1024/2048 bit (RSAES-OEAP, RSASSA-PSS)
- ECDSA 192/256 bit (opcional)
- DES/3DES
- AES 128/192/256 bit
- SHA-1, SHA-2, MD5

## Algoritmos

- RSA 1024/2048 bit
- ECDSA 192/256 bit (opcional)
- DES/3DES
- AES 128/192/256 bit
- SHA-1, SHA-2, MD5

## Detalles

- Cumple la norma ISO-7816
- Memoria: 64 KB
- Retención de datos durante más de 10 años
- Temperatura de funcionamiento: 0 °C ~ 50 °C
- Temperatura de almacenamiento: -20 °C ~ 60 °C
- Humedad: 0 ~ 100 % RH

## Detalles

- Java Card 2.2.2
  - Global Platform 2.1.1
  - Cumple la norma ISO-7816
  - Cumple con la norma ISO/IEC 14443
  - Chip: Infineon SLE77CLFX2400PM
  - Tensión de funcionamiento: 3 v/5 v
  - Memoria: 68 KB
  - Más de 500.000 reescrituras de memoria
  - Retención de datos durante más de 10 años
-

## Compatibilidad con SO

- PC/portátil con Windows
- macOS
- Linux

## Compatibilidad con SO

La tarjeta inteligente PKI admite los siguientes sistemas operativos y requiere un lector compatible

- PC/portátil con Windows
  - macOS
  - Linux
  - iPhone
  - iPad
  - Tableta con Windows
  - Android (sin contacto [NFC], o mediante un lector compatible)
- 

## Certificaciones

- CC EAL 5+ (nivel de chip)
- Cumple con las normas CE, FCC, RoHS
- Con certificado FIPS 140-2 nivel 3
- Con certificado ICP-Brasil

## Certificaciones

- CC EAL 5+ (nivel de chip)
  - Cumple con las normas CE, FCC, RoHS
-