TARJETA TOUCH & SIGN 2048

Introducción

La tarjeta Touch&Sign 2048 ha sido diseñada para infraestructuras de clave pública (PKI) para la firma electrónica.

Ofrece RSA, con claves de hasta 2048 bits como algoritmo de clave pública, SHA-1 y SHA-256 para el hashing y AES-128 para el cifrado simétrico. El sistema operativo de la tarjeta cumple con las especificaciones PC/SC y tiene una interfaz Microsoft CryptoAPI (CSP) y PKCS#11.

La tarjeta criptográfica Touch&Sign2048 está certificada como Dispositivo Seguro de Creación de Firma (Common Criteria PP EAL4+ CWA14169) y es utilizada para la firma electrónica reconocida (Qualified Digital Signature), autenticación e identificación lógica y física. Permite una integración simple en Windows, Mac OS X y Linux.

Características y especificaciones técnicas

- Certificación del Chip: CC EAL5+ PP 9806, BSI-PP-002-2001
- Certificación SO: CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3)
- Estándar ISO 7816 1-4,8,9, I/O speed up to 31 cycle/etu
- Protocolo de Comunicación: T=0, T=1, (Opcional contactless)
- Memoria EEPROM 66KB
- Algoritmos criptográficos AES-128, DES, 3DES, RSA
- Algoritmos de Hash SHA-1 y SHA-256
- Longitud de claves RSA 1024 y 2048 bits
- Generador aleatorio AIS-31 y FIPS 140-2
- Nivel de transacciones de APDU individual y múltiple
- Secure Messaging
- Comandos opcionales de monedero electrónico
- Netlink HPC y PDC
- Ciclos de lectura/grabación 500.000
- Alimentación 1.8 ÷ 5.5V
- Número de serie unívoco

- Sistemas operativos Windows 2000, XP (32 y 64), Vista (32 y 64), 7 (32 y 64), Server 2003 (32 y 64), Server 2008 (R2) (32 y 64), Mac OS X 10.5, 10.6 y 10.7 y Linux distribuciones generalistas basadas en Debian y Red HatLinux

Especificaciones de Universal Middleware

- Compatibilidad con Windows XP, Vista, 7, 2003 Server y 2008 Server en versiones de 32 y 64 bits (donde se aplique). o Compatibilidad PKCS#11 y CSP
- Compatibilidad con Mac OS X 10.5, 10.6 y 10.7 o Compatibilidad PKCS#11 y tokenD
- Compatibilidad con Linux, distribuciones generalistas basadas en Debian y en Red Hat o Compatibilidad PKCS#11

Certificaciones del chip

El chip con capacidad criptográfica Touch&Sign2048 dispone de las siguientes certificaciones:

- Certificación del Chip: CC EAL5+ PP 9806, BSI-PP-002-2001
- Certificación SO: CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3)