J-Sign

dispositivo seguro de creación de firma

Información y contacto

Opcionales

- Acceso al chip criptográfico mediante contacto y proximidad
- Mifare
- 125Khz
- Banda magnética Lo-Co y Hi-Co
- Impresión offset, serigrafía, digital

>> the smart difference

comercial@bit4id.com

Bit4id tiene como misión el desarrollo y la difusión de tecnologías para la gestión de la identidad digital de forma simple, rápida e intuitiva.

La información y las características técnicas mostradas no suponen ninguna obligación por parte de Bit4id, y podrán sufrir cambios sin previo aviso. Todas las otras marcas están registradas o depositadas y de propiedad de sus respectivas compañías.

Common Criteria

www.bit4id.com

Características Hardware

- Microcontrolador seguro ST23 con CPU core de 8/16-bit
- Memoria EEPROM de 80KB
- ISO 7816-3 con protocolos de longitud extendida T=0 y T=1
- ISO/IEC 14443 sin contacto tipo B con RF UART hasta 848 Kbps
- Rango de alimentación de 3V y 5V
- 500.000 ciclos de lectura/escritura de EEPROM
- Protección mayor a 6kV (HBM) en descargas electroestáticas (ESD)

Características de la Plataforma

- Java Card™ v.3.0.4 - Classic Edition
- GlobalPlatform® v.2.1.1
- Borrado de objetos con memory reclamation
- API segura para almacenamiento seguro (arrays íntegros protegidos) y generación aleatoria de números primos

Características de Seguridad

- Escudo activo
- Unidad de protección de memoria (MPU)
- Número de serie unívoco
- Criptoprocesador mejorado NESCRYPT para criptografía de clave pública (RSA, ECC, ECDSA)
- Seguridad hardware mejorada de acelerador DES
- Generación aleatoria de números (TRNG) AIS-31 clase P2
- Firma electrónica/digital: ECDSA (EC sobre GF(p) hasta 521 bits), RSA-PSS, RSA PKCS#1
- Algoritmos de hash SHA1, SHA-224, SHA-256, SHA-384 y SHA-512
- Algoritmos de cifrado/descifrado DES/3DES ECB y CBC (hasta 192 bits), AES (hasta 256 bits), RSA (hasta 2048 bits)
- Algoritmos RSA de generación de pares de claves (hasta 2048 bits) y EC (hasta 521 bits)
- Esquema de acuerdo de claves Diffie-Hellmann, ECDH
- Algoritmo de checksum ISO 3309 CRC-16, CRC- 32
- Contramedidas contra los ataques de canal lateral mediante análisis de grado de poder (DPA) y análisis de grado de fallo (DFA)

Certificaciones

- Common Criteria EAL6+ certificación del hardware: Security IC Platform Protection Profile (BSI-PP-0035)
- Common Criteria EAL5+ de la plataforma Software: JC Protection Profile - Closed Configuration (ANSSI PP 2010-07), Version 3.0
- Common Criteria EAL4+ certificación de aplicación de firma: Protection Profile CWA 14169 - Annex C -Secure Signature Creation Device Type 3, (BSI-PP- 0006-2002 EAL 4+)

Sistemas operativos

- Sistemas operativos: Windows, Linux, MAC OS X

bit4id