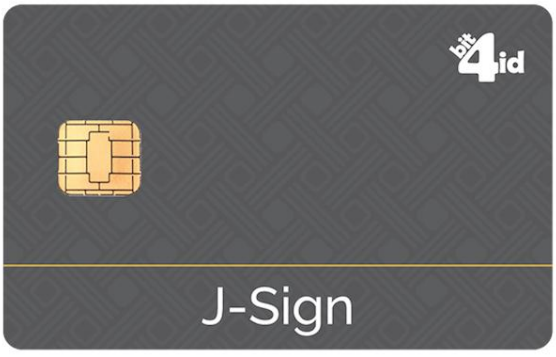
Jsign

Smart card Crittografica per la firma digitale a validità legale

Campi di applicazione

- *Firma digitale a validita legale*
- *Carta di identità elettronica*
- *Tessera Sanitaria*
- *Smart Card Log-On*
- *Controllo degli accessi logici e fisici*
- *Corporate ID*
- *Portafoglio elettronico*

SMART CARD CRITTOGRAFICA PER LA FIRMA DIGITALE



La smart card Jsign è un dispositivo crittografico avanzato aderente agli standard ISO7816-1/2/3/4/8/9 e SSCD Common Criteria EAL4+ (CWA14169). È stata realizzata per aumentare le performance in termini di sicurezza e utilizzo delle chiavi RSA per le operazioni su infrastrutture PKI, che risultane essere essenziali in applicaioni che richiedono l'impiego di smart card PKI come la firma digitale e l'autenticazione forte.

Grazie al middleware sviluppato da Bit4id, al CSP, PKCS#11 ed al TokenD, la smart card crittografica Jsign uò essere facilmente utilizzata su piattaforme ed applicazioni Windows, Mac OS X e Linux.

È in grado di generare chiavi RSA a 2048 bit elaborare algoritmi SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512, AES (fino a 256 bit) per la crittografia simmetrica.

La Jsign può includere diverse interfacce contactless RFID con relativi chip come MIFARE, 125Khz, ed eventualmente anche la banda magnetica.

CARATTERISTICHE PRINCIPALI

Hardware

- *Memoria EEPROM da 80 Kbytes*
- *Compatibile ai protocolli ISO 7816-3 T=0 and T=1*
- *ISO/IEC 14443 Type B interfaccia contactless con UART RF fino a 848 Kbps*
- *Range di alimentazione: da 3V a 5V*
- *Cicli minimi di lettura/scrittura in EEPROM 500K*

Piattaforma SW

- *Java Card™ v.3.0.4 - Classic Edition*
- *GlobalPlatform® v.2.1.1*
- *Cancellazione oggetti (garbage collection) con memory reclamation*
- *API di sicurezza aggiuntiva per:*
    - *Storage sicuro (integrity-protected arrays)*
    - *Generazione casuale di numeri primi*

Certificazioni

- *Common Criteria EAL6+ certificazione hardware: Security IC Platform Protection Profile (BSI-PP-0035), July 15, 2007*
- *Common Criteria EAL5+ per la piattaforma software: JC Protection Profile - Closed Configuration (ANSSI PP 2010-07), Version 3.0, December 2012)*
- *Common Criteria EAL4+ per la piattaforma applicativa: Protection Profile CWA 14169 - Annex C - Secure Signature Creation Device Type 3, version: 1.05, March 2002 (BSI-PP- 0006-2002 EAL 4+)*

SPECIFICHE TECNICHE

Caratteristiche di sicurezza

- *Schermo attivo (Active Shield)*
- *Unità per la protezione della memoria (Memory Protection Unit - MPU)*
- *Numero seriale univoco per ciascun chip*
- *Criptoprocessore NESCRYPT per la cifratura per le infrastrutture a chiave pubblica (RSA, ECC, ECDSA)*
- *Hardware security enhanced DES accelerator*
- *AIS-31 class P2 compatibile con la generazione dei numeri casuali (TRNG)*
- *Algoritmi di hashing: SHA1, SHA-224, SHA-256, SHA-384 e SHA-512*
- *Algoritmi di cifratura e decifratura : DES/3DES ECB e CBC (fino a 192 bits), AES (fino a 256 bits), RSA (fino a 2048 bits)*
- *Generazione chiavi: RSA (fino a 2048 bits) e EC (fino a 521 bits)*
- *Firma digitale : ECDSA (EC su GF(p) fino a 521 bits), RSA-PSS, RSA PKCS#1*
- *Key agreement schemes: Diffie-Hellmann, ECDH*

- *Algoritmio di controllo (checksum) : ISO 3309 CRC-16, CRC- 32*
- *Contromisure per la protezione dagli attacchi side-channel: Differential power analysis (DPA) e differential fault analysis (DFA)*