ID-One Cosmo

dispositivo cualificado de creación de firma

Información y contacto

Aplicaciones

- Firma electrónica cualificada
- Smart Card Log-on
- Acceso a redes y VPN
- Control de acceso físico
- Servicios múltiples oncard
- Identificación biométrica
- Tarjeta Sanitaria
- Monedero electrónico

>> 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 tarjeta ID-One Cosmo es la propuesta de Bit4id de dispositivo criptográfico certificado y basado en el paradigma Java Card.

Los 72KBytes de memoria EEPROM del chip permiten almacenar un elevado número de pares de claves y certificados. La tarjeta permite la generación de claves RSA de hasta 2048 bits. ID-One Cosmo cumple con los estándares ISO 7816-3 protocolos T=0 y T=1, así como PPS negotiation, correspondiente a la velocidad de transmisión de 9.600 a 614.400 bauds.

ID-One Cosmo implementa todos los mecanismos de seguridad para las certificaciones Common Criteria. Cumple con las Guías de Seguridad contra ataques DFA (Differential Fault Analysis) y las certificaciones internacionales de seguridad Common Criteria EAL4+ (CWA14169), certificado como “Dispositivo Cualificado de Creación de Firma” (QSCD) y opcionalmente FIPS 140-2 nivel 3.

FIPS VALIDATED 140-2

Common Criteria

Características

Chip
- 72K de memoria EEPROM
- Cumple con especificaciones ISO 7816 partes 1, 2, 3 y 4
- Ciclos de lectura/grabación: 500.000
- Alimentación 1,8 ÷ 5.5V
- Número de serie unívoco

Java Card 2.2.2
- RMI
- Canal lógico
- Garbage Collector
- APDU extendidas
- Sun 2.2.2

Biometría
- Java Card API biométrica para acceder a la cotejo ID3 en memoria ROM

Criptografía
- DES, 3 DES (2 y 3 keys)
- AES 128/192/256bits
- Longitud de claves RSA 1024 y 2048 bits
- Algoritmo DSA GFP de curva elíptica de 160/192/224/256/384/521 bits
- Curvas elípticas Diffie-Helman de 160/192/224/256/384/521 bits
- Algoritmos de hash: SHA-1, SHA-2, SHA-224, SHA-256, SHA-384, SHA-512
- Generador aleatorio compatible con FIPS 186-2

Sistemas operativos:
- Sistemas operativos: Windows, Linux y Mac OS X