

EXACARD



TARJETA CRIPTOGRÁFICA DE DOBLE ALGORITMO

Exa Card es la tarjeta criptográfica de última generación desarrollada por Idoneum Electronic Identity. Esta tarjeta está diseñada para su uso en sistemas avanzados de firma electrónica o PKI, poniendo todo su énfasis en la seguridad, tanto de sí misma como del resto de sistemas con los que convive. Es la herramienta ideal en que basar la seguridad hardware de cualquier sistema de identificación.

Contempla todos los aspectos tecnológicos de más avanzada generación. Desde la tecnología dual o híbrida para su doble uso con contacto o a través de radiofrecuencia, pasando por los más avanzados sistemas de inviolabilidad y llegando a un innovador sistema, único en el mundo, de doble algoritmo de clave pública.

A diferencia de otros sistemas, el entorno software que se facilita con la tarjeta se ha desarrollado en conjunto con la misma buscando una funcionalidad robusta del sistema que lo hace más amigable y seguro.

DOBLE TECNOLOGÍA

La tecnología actual permite que las tarjetas puedan utilizarse comunicando bien por radiofrecuencia (RFID) o bien por contacto directo del chip. El grupo Calmell lleva más de 15 años liderando la tecnología de RFID y, de este modo, poder ofrecer tecnología tanto híbrida como dual. Esta innovadora tecnología permite infinidad de aplicaciones en un solo soporte, como la identificación, el transporte público, el pago, la fidelización, el control de acceso o cualquier otro.



DOBLE ALGORITMO

Otra de las características principales que reflejan el grado de innovación de esta tarjeta es la posibilidad de trabajar con cualquiera de los dos algoritmos considerados seguros (RSA

y Curvas Elípticas). De este modo, frente a la rotura de cualquiera de los dos algoritmos se mantiene la seguridad en el uso de la tarjeta. De esta manera, el emisor de la misma puede escoger cuál de los dos algoritmos prefiere utilizar y, hasta incluso, puede llegar a optar por la utilización de ambos de forma combinada.

ROBUSTEZ Y MIDDLEWARE

Cualquier tarjeta criptográfica está orientada a su utilización de forma amplia en un ordenador personal. Por esto, lo que el usuario ve de la tarjeta es el software de la misma y cualquier defecto o disfunción del software puede verse como un defecto de la tarjeta. Por este motivo desde Idoneum Electronic Identity se ha hecho un esfuerzo de integración para desarrollar de forma conjunta el middleware (software entre el PC y la tarjeta) y el sistema operativo de la tarjeta. Esta simbiosis entre software y hardware proporciona una robustez al sistema que hace que el usuario disponga de un altísimo nivel de seguridad en un entorno software sin errores y fácil de usar.

HARDWARE

- Chip NXP Secure SmartMX P5CC081
- ROM: 264 KB
- RAM: 7,5 KB
- EEPROM: 80 KB
- Interfaz contacto ISO/IEC 7816 (T=0 y T=1)
- Interfaz contactless ISO/IEC 14443-A
- Frecuencia interna operación 30 MHz

CRIPTOGRAFÍA

- Criptografía asimétrica:
 - RSA hasta 4.096 bits.
 - ECDSA (Curvas Elípticas) hasta 521 bits.
 - Generación claves RSA y ECC.
- Criptografía simétrica: DES, 3DES y AES (hasta 256 bits).
- Hash SHA-1, SHA-224 y SHA-256.

SEGURIDAD

- Coprocesador criptográfico Crypto FameXE
- Cifrado dinámico de memoria
- Sensores de control de tensión, frecuencia, lumínicos y temperatura.
- Blindaje del chip.
- Generador de números aleatorios hardware según FIPS 140-2 y AIS31.
- Comunicación securizada con canal seguro criptográfico.
- Implementación de contramedidas para ataques SPA, DPA, EMA, DFA.

SISTEMA OPERATIVO

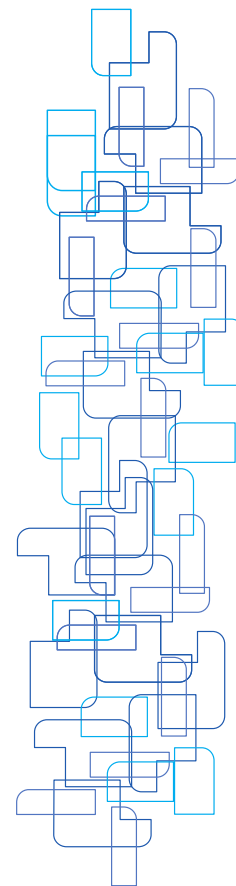
- Generación de claves en tarjeta con alta seguridad.
- Sistemas de autenticación segura.
- Canal seguro criptográfico asimétrico según especificación EN 14890.
- Arquitectura de autenticación y autorización flexible de comandos y ficheros.
- Control de integridad del sistema de ficheros (antitearing).
- Comandos según ISO7816-1/2/3/4/8/9.
- Emulación Mifare Classic 1K / 4K
- Control de integridad y confidencialidad de memoria.
- Aplicación de monedero o contador

ESTÁNDARES

- ISO/IEC 7816-1/2/3/4/6/8/9/15
- ISO/IEC 14443-A
- Common Criteria EAL4+ PP CWA 14169 (aplicación criptográfica)
- Common Criteria EAL5+ PP BSI-PP-0002 (chip)
- EN 14890
- PKCS#1, PKCS#11, PKCS#15.

MIDDLEWARE

- CSP de Microsoft
- PKCS#11 multiplataforma:
 - Windows, Linux, Mac Os X
- Librería cliente para integración en entornos incrustados.



Aplicaciones	Contact	Contactless	Dual
Firma de documentos	SI	NO	SI
Cifrado de documentos	SI	NO	SI
Logon seguro	SI	NO	SI
Control de acceso físico	-	SI	SI
Transporte público	-	SI	SI
Monedero	SI	-	SI
Tarjeta fidelización	-	SI	SI
Tarjeta ciudadano	-	-	SI

Idoneum Electronic Identity - Calmell Group
Polígono Industrial Pla d'en Coll C/ Fresser, 12 C
Montcada i Reixac (Barcelona) Tel. 93 564 14 00 - Fax 93 564 58 22