

moka



TARJETA JAVACARD

La tarjeta Moka Card de Idoneum Electronic Identity es, en realidad, una familia de tarjetas Java Card con diferentes opciones y prestaciones. Existen dentro de la familia distintas versiones en función de las necesidades del cliente y de las prestaciones dadas por los distintos fabricantes de silicio.

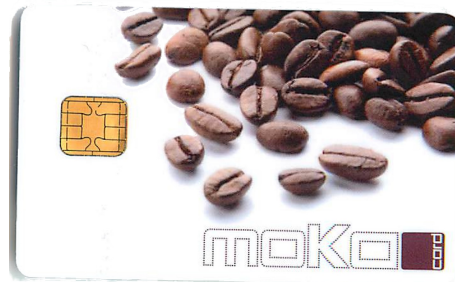
Entre otros, pueden cumplir con niveles de seguridad contrastados por varias certificaciones de seguridad como Common Criteria EAL 5+ o como por la certificación para módulos criptográficos FIPS 140-2.

Su naturaleza multiaplicación cumple con el estándar GlobalPlatform permitiendo la carga de diversas aplicaciones (applets) en memoria, ya sean propietarias o adquiridas a terceros. Son ideales para control de acceso, tarjeta ID empleado o tarjeta ciudadano, entre otras muchas aplicaciones.

WRITE ONCE – RUN ANYWHERE

El eslogan, “write once – run anywhere”, que abandera Java, destaca la independencia en cuanto al hardware que necesita para su ejecución.

Las tarjetas Moka Card tienen como máscara diferentes sistemas operativos intérpretes de Java. Permite la ejecución de cualquier applet desarrollado según la especificación para tarjetas Java.



SEGURIDAD

La tarjeta Moka card cumple con la especificación Java Card 2.2.2 proporcionando soporte para funcionalidades y algoritmos criptográficos que pueden ser tanto simétricos (3DES, AES) como asimétricos (RSA, ECC). Asimismo, también proporciona mecanismos para la verificación de integridad de datos mediante la generación de hash.

VERSATILIDAD

La tarjeta Moka Card es una plataforma multiaplicación que permite la carga de varias aplicaciones de forma simultánea en la memoria de la propia tarjeta.

Existen opciones desde los 40KB hasta los 256 KB de EEPROM, que proporcionan la flexibilidad de poder tener en la misma tarjeta diversas aplicaciones de diferentes funcionalidades convirtiendo las Moka Card en un todo-en-uno.

GARANTÍA

Los productos de Idoneum siempre ofrecen los más altos niveles de calidad y fiabilidad.

Esta tarjeta proporciona unas prestaciones de seguridad probadas mediante distintas certificaciones internacionales de seguridad como Common Criteria EAL5+ o FIPS 140-2 en función de la versión.



ESPECIFICACIÓN GLOBALPLATFORM

- Gestión CVM (Global PIN) implementado: todos los APDU descritos y las interfaces de la API están operativos
- Soporte para protocolo de canales seguros (SCP01 y SCP02)

ESPECIFICACIÓN JAVACARD

- Garbage Collection implementado con una reclamación total de la memoria
- Soporte para APDU Extended Length

ESPECIFICACIÓN TARJETA

- Chip microprocesado con opción de capacidad criptográfica.
- EEPROM: desde 40 KB hasta 256 KB
- Interfaz contacto ISO/IEC 7816 (T=0 y T=1)

Opcionales:

- Interfaz contactless ISO/IEC 14443 (T=CL)
- Interfaz MIFARE 1k

CERTIFICACIONES DE SEGURIDAD

- Common Criteria EAL 5+ (según versión)
- FIPS 140-2 (según versión)

FUNCIONALIDADES Y ALGORITMOS CRITOGRÁFICOS

- Simétricas (según versión):
 - 3DES con claves de 112 y 168 bits para des-/cifrado (CBC y ECB) y generación y verificación MAC (Retail-MAC y CBC-MAC)
 - AES (Advanced Encryption Standard) con claves de tamaño de 128, 192 y 256 bits para des-/cifrado (CBC y ECB)
- Asimétricas (según versión):
 - RSA con claves de 1280 hasta 2048 bits para generación de claves, des-/cifrado, y generación y verificación de firmas
 - ECC sobre GF(p) para claves de 192 y 320 bits
- Algoritmo hash SHA-1, SHA-224 y SHA-256
- Generación de números aleatorios según clase K3 de AIS 20

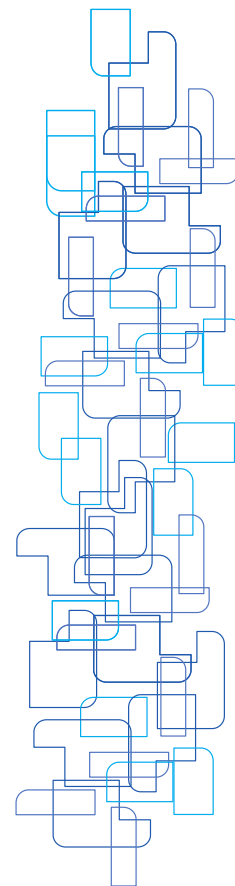


TABLA SELECCIÓN VERSIONES

	Criptografía	Memoria	Certificaciones
Moka Card CR1-40	RSA	40KB	CC / FIPS
Moka Card CR1-80	RSA	80KB	CC / FIPS
Moka Card CR2-40	RSA, ECC	40KB	CC / FIPS
Moka Card CR2-80	RSA, ECC	80KB	CC / FIPS
Moka Card PR-64	NO	64KB	-
Moka Card PR-128	NO	128KB	-
Moka card PR-256	NO	256KB	-



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