

EXACARD



DUAL ALGORITHM CRYPTOGRAPHIC CARD

Exacard is the next generation cryptographic card developed by Idoneum Electronic Identity. This card is designed for use in advanced electronic signatures or PKI, putting all its emphasis on safety, both for itself and for the other systems with which it coexists. It is the ideal tool on which to base the hardware security of any identification system.

Covers all aspects of the latest generation technology. From dual or hybrid technology for dual-use, with contact or radio-frequency, through the most advanced systems of inviolability and coming to an innovative system, unique in the world, of dual public key algorithm.

Unlike other systems, the software environment that comes with the card has been developed by the same team, looking for robust functionality of the system that makes it more friendly and safe.

DOUBLE TECHNOLOGY

Current technology allows cards to communicate either by radio-frequency identification (RFID) or by direct contact of the chip. Calmell group has over 15 years leading RFID technology and thus able to offer both hybrid and dual technology. This innovative technology allows many applications on a single medium, such as identification, public transport, payment, loyalty, access control or others.



DOUBLE ALGORITHM

Another of the main features that reflect the degree of innovation of this card is the ability to

work with either of the two algorithms considered safe (RSA and Elliptic Curves). Thus, if the security of one algorithm is compromised the card still maintains its security. The card issuer can choose which of the two algorithms prefer to use, or can choose both algorithms combined.

ROBUSTNESS & MIDDLEWARE

Any cryptographic card is designed to be used extensively in a personal computer. The vision that the user has of the card is the software that comes with the card and any defect or malfunction of the software can be seen as a defect of the card. For this reason Idoneum Electronic Identity has made an integration effort to jointly develop the middleware (software between the PC and card) and the operating system of the card. This symbiosis between software and hardware provides a robust system that makes the user has a high level of security in a software error-free and easy to use.

HARDWARE

- Chip NXP Secure SmartMX P5CC081
- ROM: 264 KB
- RAM: 7,5 KB
- EEPROM: 80 KB
- Contact Interface ISO/IEC 7816 (T=0 y T=1)
- Contactless Interface ISO/IEC 14443-A
- Internal operation frequency: 30 MHz

CRIPTOGRAPHY

- Asymmetric Criptography:
 - RSA up to 4.096 bits.
 - ECDSA (Elliptic Curves) up to 521 bits.
 - Key generation for RSA and ECC.
- Symmetric Criptography: DES, 3DES and AES (up to 256 bits).
- Hash SHA-1, SHA-224 and SHA-256.

SECURITY

- Cryptographic Coprocessor Crypto FameXE
- Dynamic Memory Encryption
- Sensors control for voltage, frequency, light and temperature
- Chip shield
- Hardware random number generator according to FIPS 140-2 and AIS31
- Secured communication with cryptographic secure channel
- Implementation of countermeasures to SPA, DPA, EMA, DFA attacks

OPERATING SYSTEM

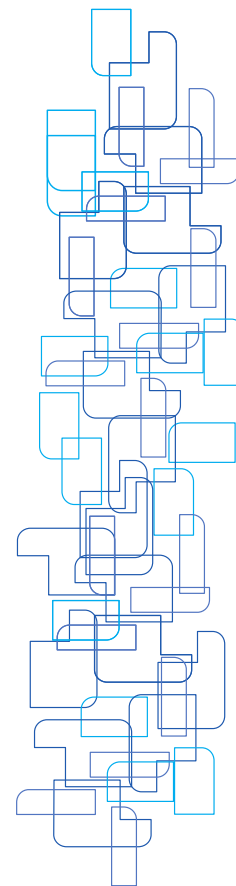
- High-security key generation in card
- Secure authentication systems
- Asymmetric cryptography secure channel according to specification EN 14890
- Flexible authentication and authorization architecture for commands and files
- Antitearing
- Commands according to standard ISO7816-1/2/3/4/8/9.
- Mifare Classic 1K / 4K emulation
- Control of memory integrity and confidentiality
- Electronic purse or counter application

STANDARDS

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

MIDDLEWARE

- CSP for Microsoft apps
- PKCS#11 for:
 - Windows, Linux, Mac Os X
- Client library for integration in embedded environments



Applications	Contact	Contactless	Dual
Document signature	YES	NO	YES
Document Encryption	YES	NO	YES
Secure logon	YES	NO	YES
Physical access control	-	YES	YES
Public transport	-	YES	YES
Electronic purse	YES	-	YES
Loyalty card	-	YES	YES
Citizen card	-	-	YES

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