MEGAMOS CRYPTO

Read-Write High Security Device - Memory organisation

Description

The MC is a high security Read-Write RFID Transponder. A challenge and re-sponse cryptoalgorithm with 96 bits of user-configurable secretkey contained in EEPROM are implemented in the device.
A freely programmable USER-MEMORY of 30 bits and a unique device identification of 32 bits are characteristic of the Magic. Bits 15 and 14 of word 1 are used as Lock-Bits. At delivery, these two bits have the contents " 10" which is the requirement for writing or erasing the memory. Data transmission to the transceiver is performed by modulating the amplitude of the electro-magnetic field. Receiving data and commands takes place in a similar way.

Features

- On Chip Crypto-Algorithm (Challenge & Response)
- Two Way Authentication
- 96 bits of Secret-Key in EEPROM (unreadable)
- 32 bits of fix Device Identification
- 32 bits of USER-MEMORY (UM) with read access (OTP)
- Secret-Key programmable via CID-Interface
- Lock-Bits to inhibit programmation
- Data transmission performed by Amplitude Modulation
- Bit period = 32 periods of carrier frequency

Memory Organisation

The 160 bits EEPROM are organised in 10 words of 16 bits. Word 0 and 1 contain the USER-MEMORY and the LB1 and LB0 Lock-Bits.
Writing is only possible if LB1 = " 1" and LB0 = " 0" .
Words 2 and 3 contain the ID which can never be altered.
Words 4 through 9 contain the 96 bits of secret-key. These bits influence the crypto-algorithm but cannot be read directly.

	Bit 15	Bit 0
word 9	Crypt Key 95	Crypt Key 80
8	Crypt Key 79	Crypt Key 64
7	Crypt Key 63	Crypt Key 48
6	Crypt Key 47	Crypt Key 32
5	Crypt Key 31	Crypt Key 16
4	Crypt Key 15	Crypt Key 0
3	ID 31	ID 16
2	ID 15	ID 0
1	LB1, LB0, UM 29	UM 16
0	UM 15	UM 0