Gemalto Mifare 4K Datasheet

Contents

1. OVERVIEW

The Gemalto Mifare is a contactless multi-application smart card that is designed for use as a payment card for public transport ticketing systems. It has been developed with a peculiar emphasis on user convenience, fast transaction speed, exceptional reliability for frequent usage, security against fraud and cost effectiveness.

1.1 User convenience and speed

The card and reader start to transmit data as soon as the card enter the reader RF antenna field, thus enabling the card holder to carry out transactions quickly and conveniently, through an intentional action.

The RF communication interface transfers data between the Gemalto Mifare card and reader at a baud rate of 106k baud. This high data transfer rate enables ticketing transactions to be handled in 0,1 to 0,5 second. Therefore, transactions can be carried out without cardholders having to stop in front of the reader or remove the Gemalto Mifare card from their wallets.

1.2 Security

Mutual challenge and response authentication, data ciphering, and message authentication protect the whole system from the fraud. These checks are implemented in a fraction of the overall transaction time. Furthermore, each Gemalto Mifare has a unique hard-written serial number which guaranties that each card can be individually selected.

1.3 Anticollision

If two cards enter a field antenna at the same time, which is most likely to happen in many applications, a fast anticollision algorithm automatically triggers to prevent cross transactions. The reader can select one single card in the field, thus preventing transaction data corruption as a result of other cards being present or entering the RF field reader. Even if a cardholder has more than one Gemalto Mifare card in his wallet, the reader can select the appropriate card related to the application by implementing the anticollision mechanism, and carry out the transaction.

2. GEMALTO MIFARE 4K FEATURES

The following list provides a summary of the technical information about the Gemalto Mifare 4K.

2.1 Compatibility with norms

ISO 14443-1/2/3	Defines a proximity card used for identification that used the credit card form factor (ISO 7810-ID-1)	✓ Yes compliant
ISO 14443-4	High level protocol (T=CL)	✓ No : Mifare Protocol
ISO 9798-2	Security techniques – 3-pass authentication mechanism	✓ Yes compliant
ISO 7810	Format for identification card (ID-1)	✓ Yes compliant
ISO 7813	Additional characteristics of ID-1 plastic banking cards (thickness for example)	✓ Yes compliant
ISO 7816	ID-1 identification with an embedded chip and contact surfaces	✓ Yes compliant
ISO 10373	Protocol test methods for proximity cards	✓ Yes compliant

2.2 Electrical

Chip	NXP for Mifare 4K.
Memory (EEPROM)	4Kbytes for Mifare 4K
Usable EEPROM for data	3440 bytes for Mifare 4K
Basic Functionality	Contactless card operated remotely from a dedicated reader using RF transmission
Operating frequency	13,56 MHz
Modulation from reader to card	Amplitude modulation – ASK 100% (ISO 14443/2 type A)
Modulation from card to reader	Load modulation (847,5 KHz, ASK ISO 14443 Type A)
Communication speed	106 k baud (ISO 14443/2 type A)
Operating range	Up to 10 cm (depending on the reader and the antenna design)
Number of reads	Unlimited
Number of writes	100 000
Data retention	10 years

2.3 Durability

Mechanical stress	250 bending cycles on each side, 500 torsion cycles on each side as specified in ISO10373 without loosing functionality and aesthetic aspects.

2.4 Security

- Mutual 3- pass authentication (ISO/IEC DIS 9789-2).

Encryption based on a Mifare cipher algorithm including random generator, serial number and 48bit keys.
The encryption provides :

  - Card/Reader mutual authentication,
  - Anti-replay mechanism,
  - Encrypted transmission providing confidentiality of transmitted data.

- RF Channel data encryption with replay attack protection.

- Memory structured into sectors with each sector protected by its own key set enabling the use of multiple applications with key hierarchy.
  - Mifare 4K : each of the 40 sectors has 2 -48 bits diversified keys.

- Anti-cloning

Each chip has a unique card serial number (4 bytes) to ensure the uniqueness of each device.

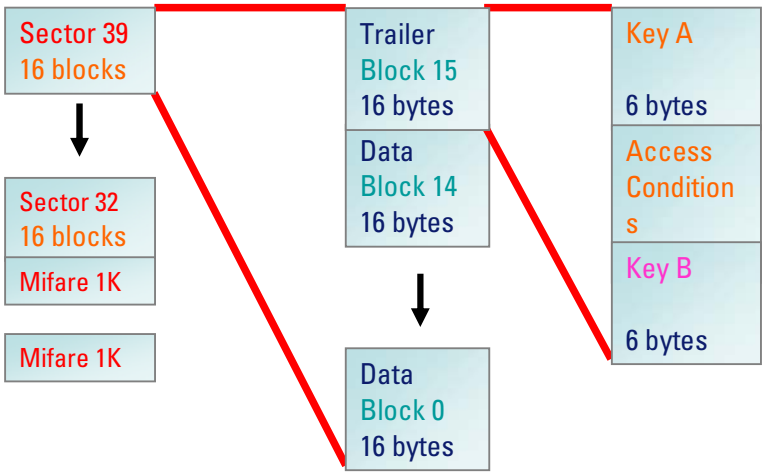
- Anti-collision

- Access protection to EEPROM by transport key on chip delivery

3. MEMORY ORGANIZATION & ACCESS

The Gemalto Mifare 4K has 3440 bits EEPROM which is organized into 40 sectors of 16 blocks each. Each block is made of 16 bytes.
The following diagram shows the Gemalto Mifare 4K memory structure.

Gemalto Mifare 4K – Memory mapping



8 sectors * 16 blocks * 16 bytes * 8 bits
+ 2 Mifare 1K = 32 Kbits

The first data block of the first sector is the manufacturer block. It is a read-only block that contains the manufacturer serial number.

Each sector has a sector trailer that holds :

- The secret keys A and B (optional) of the sector
- The access conditions for all the blocks of that sector.

The access conditions for the data area and the sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector. The access bits control the rights of memory access using the secret keys A and B.

4. MIFARE MEMORY COMMANDS

Request	Prompts cards within the antenna field to return a card type identifier number.
Anticollision	Chooses one card out of those that are in the antenna field and return its serial number.
Select	Selects the card that the processing commands are sent to using its serial number.
Authenticate	Selects a key that is stored in the reader, and challenges it against the corresponding key in the sector to be accessed in the selected card. If the challenge is successful, access is granted to the sector holding the challenged key for the functions defined by the access conditions.
Read	Reads one memory block. This command can only be executed if the appropriate key for granting read access (as defined by the target sector access condition) has been successfully challenged using the authenticate command.
Write	Writes one memory block of data. This command can only be executed if the appropriate key for granting write access (as defined by the target sector access condition) has been successfully challenged using the authenticate command.
Increment	Increments the contents of a block and stores the result in the data register
Decrement	Decrements the contents of a block and stores the result in the data register.
Restore	Read the contents of a block into the data register.
Transfer	Writes the contents of the data register to a block