



---

# **Gemalto Mifare 1K Datasheet**

---

# Contents

---

<b>1. Overview .....</b>	<b>3</b>
1.1 User convenience and speed .....	3
1.2 Security .....	3
1.3 Anticollision .....	3
<b>2. Gemalto Mifare Features .....</b>	<b>4</b>
2.1 Compatibility with norms .....	4
2.2 Electrical .....	4
2.3 Durability .....	5
2.4 Security .....	5
<b>3. Memory organization &amp; access .....</b>	<b>6</b>
3.1 The memory organization .....	6
3.2 Mifare Memory Commands.....	7

# 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 enters 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 guarantees 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 FEATURES

---

The following list provides a summary of the technical information about the Gemalto Mifare 1K.

### 2.1 Compatibility with norms

---

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

### 2.2 Electrical

---

<b>Chip</b>	NXP & Infineon for Mifare 1K
<b>Memory (EEPROM)</b>	1Kbyte for Mifare 1K
<b>Usable EEPROM for data</b>	752 bytes for Mifare 1K
<b>Basic Functionality</b>	Contactless card operated remotely from a dedicated reader using RF transmission
<b>Operating frequency</b>	13,56 MHz
<b>Modulation from reader to card</b>	Amplitude modulation – ASK 100% (ISO 14443/2 type A)
<b>Modulation from card to reader</b>	Load modulation (847,5 KHz, ASK ISO 14443 Type A)
<b>Communication speed</b>	106 k baud (ISO 14443/2 type A)
<b>Operating range</b>	Up to 10 cm (depending on the reader and the antenna design)
<b>Number of reads</b>	Unlimited
<b>Number of writes</b>	100 000
<b>Data retention</b>	10 years

## 2.3 Durability

---

### **Mechanical stress**

250 bending cycles on each side, 500 torsion cycles on each side as specified in ISO10373 without losing 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 1K : each of the 16 sectors of the card has two 48-bit 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

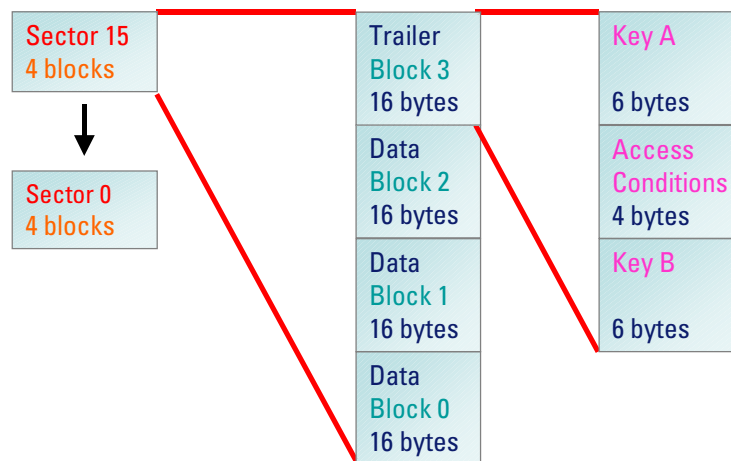
## 3. MEMORY ORGANIZATION & ACCESS

### 3.1 The memory organization

The Gemalto Mifare 1K has 8192 bits EEPROM which is organized in 16 sectors with 4 blocks each. Each block is made of 16 bytes.

The following diagram shows the Gemalto Mifare 1K memory structure.

### Gemalto Mifare 1K – Memory mapping



$$16 \text{ sectors} * 4 \text{ blocks} * 16 \text{ bytes} * 8 \text{ bits} = 8 \text{ Kbits}$$

Each **sector** contains 16 bytes **blocks**

- 3 blocks of data configurable
  - Either as Read/Write Blocks for storing general data
  - Or as Value Blocks e.g. electronic purse applications.
- The **Sector Trailer** contains the individual secret Authentication Key A and optional Key B as well as the block accesses conditions of the respective sector.
  - 6 byte Authentication Key A : this key can never be read.
  - Optional 6 byte Authentication Key B : this key can either be read after an authentication or never be read dependant on the setting of the Access bits.
  - Access Bits to define the access conditions for the specified blocks for every sector individually. The Sector trailer and the data blocks are controlled independently.

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

## 3.2 Mifare Memory Commands

---

<b>Request</b>	Prompts cards within the antenna field to return a card type identifier number.
<b>Anticollision</b>	Chooses one card out of those that are in the antenna field and return its serial number.
<b>Select</b>	Selects the card that the processing commands are sent to using its serial number.
<b>Authenticate</b>	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.
<b>Read</b>	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.
<b>Write</b>	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.
<b>Increment</b>	Increments the contents of a block and stores the result in the data register
<b>Decrement</b>	Decrements the contents of a block and stores the result in the data register.
<b>Restore</b>	Read the contents of a block into the data register.
<b>Transfer</b>	Writes the contents of the data register to a block