

MIFARE® CONTACTLESS CARD TECHNOLOGY

GENERAL

The MIFARE contactless smart card and MIFARE card reader/writer were developed to handle payment transactions for public transportation systems. Although contact smart cards could also do the job, contactless readers are faster and easier to use, and there is virtually no maintenance on the readers, or wear and tear on the cards.

MIFARE technology is owned by Philips Electronics. They do not make cards or readers, but they make and sell the card and reader chips on the open market. A reader chip is not required to read the card's fixed random ID number, but it IS required to access any data stored on the card. Philips has also licensed manufacture of the card chip technology to Infineon.

Similarities between MIFARE and Proximity:

- Both are passive cards (no battery)
- Both consists of a chip and a coil antenna
- Both are available in ISO card packages, fobs, discs
- Both use RF energy to power the chip and send and receive data

FEATURES

MIFARE® RF Interface (ISO/IEC 14443 A)

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: Up to 100mm (depending on antenna geometry)
- Operating frequency: 13.56 MHz
- Fast data transfer: 106 kbit/s
- High data integrity: 16 Bit CRC, parity, bit coding, bit counting
- True anticollision
- Typical ticketing transaction: < 100 ms (including backup management)

EEPROM

- 1 Kbyte, organized in 16 sectors with 4 blocks of 16 bytes each (one block consists of 16 byte)
- User definable access conditions for each memory block
- Data retention of 10 years.
- Write endurance 100.000 cycles

Security

- Mutual three pass authentication (ISO/IEC DIS9798-2)
- Data encryption on RF-channel with replay attack protection
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy
- Unique serial number for each device
- Transport key protects access to EEPROM on chip delivery

Differences between MIFARE and traditional Proximity:

MIFARE

1 - 4 inch read range
Uses a frequency of 13.56 MHz
64 bytes – 64 Kbytes storage
Holds 16 separate applications
Open standard
ISO/IEC 14443

PROXIMITY

3 - 30 inch range
Uses 125 kHz
8 to 256 bytes of storage
Holds one application
Proprietary standard
ISO/IEC 7810

HOW MIFARE IS USED

In fare collection systems, a MIFARE transit card is issued to a passenger, who goes to an automated terminal and uses a credit card or cash to load value on to the card. The value is stored in an “electronic purse” on the card, from which the appropriate fare is subtracted every time the passenger boards a bus or train. When the stored value is used up, the passenger goes to the automated terminal and reloads the electronic purse.

Philips recommends the MIFARE cards for automatic fare collection, toll roads, airline ticketing, loyalty schemes, park and ride, prepaid metering, and phone, banking, city, ID and university cards.

Although MIFARE cards have security features, such as encrypted RF transmission, mutual authentication, and security keys, most banks do not feel that MIFARE has enough power or capability to process the type of encryption required for banking and credit card transactions.

The MIFARE card has up to 16 separate sectors, which can be configured as purses or for general data storage. The first sector is typically used as a directory for the rest of the card, leaving 15 segments available for data or purses.

Up to 15 different applications can be stored on a MIFARE card, and these applications will be separate and secure from one another by using unique keys

(passwords) for each sector. The only requirement is that the various application providers must cooperate in the programming of the MIFARE Applications Directory (MAD), and that the keys to this directory must be available to all application providers.

Each sector has two keys, called the A and B keys, allowing different access privileges to that sector. These key pairs can be designated as read and read/write, or decrement and increment/decrement. For example, this would allow turnstile readers with the A key to only deduct value from a card sector, while ticket booth readers with the B key could either add or subtract value.

The MIFARE card also has a 32-bit unique random number, which is permanently encoded into each chip by the chip manufacturer (Philips or Infineon). This is sometimes called the Card Serial Number (CSN) or Universal Identifier (UID), and can be read by any MIFARE reader without knowing any of the secure keys used to protect the rest of the card.

MIFARE FOR ACCESS CONTROL

While its short read range makes it less than ideal for access control, MIFARE is becoming specified more frequently for access control applications due to its potential to store multiple applications on one card.

At a large facility, the MIFARE card could serve as an access card, cafeteria debit card, an ID card, a parking fee card, a library or equipment checkout card, or a vending machine debit card. It could even store biometric templates to be verified by biometric readers.

Some customers may already have MIFARE cards in use for other applications, and would like to use their existing cards for access control applications. These customers would only need to acquire readers formatted with the relevant read/write permissions (A/B key data) Access Control data into an unused card sector or specified sector. Alternately, all or part of the 32-bit random CSN can be converted to Wiegand format and used for access control (although most access panels cannot handle random numbers ranging up to 4 billion).

Customers may want to purchase MIFARE cards and readers for access control because of MIFARE's future potential.

Dual technology cards, containing both 125 kHz Proximity and 13.56 MHz MIFARE chips and antennas are also available. This card provides the longer read range of proximity when used with 125 kHz readers, plus the added flexibility of MIFARE.

MIFARE is very common in Europe and Asia, but it is also being specified for access control in the US by agencies such as the US Navy.

MIFARE ACCESS CONTROL CARD PROGRAMMING

Although MIFARE cards and readers are available from many different suppliers worldwide, not all are able to provide readers and cards specifically configured for access control OEMs requiring formatted Wiegand output. Generally, for compatibility and/or integration with other systems, suppliers should be able to have the capability of programming OEM data into one of the sectors on the MIFARE cards, and be able to provide cards programmed with any facility code, format, and numbering sequence currently available in 125 kHz proximity cards.

Some suppliers will also supply a MIFARE Card Programmer, which can program relevant formatted OEM Wiegand data into any available sector on an existing card. This requires knowledge of the “write” keys for the existing card population.

Consideration must also be given to the reader output when reading the CSN. The reader should read/output the full number, not just part of it. Cutting off part of a large random number (called *truncating*) creates a risk of number duplication (called *aliasing*). This could also happen when using data stored in sectors.

Here is an example of aliasing caused by truncating: suppose you had three different cards – 111234, 211234, 661234. Now suppose that in the reader software, you truncate the number (make it smaller) by cutting off the two highest digits, producing – 1234, 1234, 1234. Obviously, three different cardholders with unique cards will now be seen by the system as the same person.

TECHNICAL DETAILS

Card Memory Structure

Each of the 16 Sectors on the MIFARE card consists of four 16-byte blocks numbered 0-3, containing the following:

- Block 0 – Data*
- Block 1 – Data
- Block 2 - Data
- Block 3 – Sector Trailer

In Sector 0, Block 0 contains the card manufacturer code and 32-bit ID – as programmed by the IC manufacturer - it can not contain any user data and cannot be modified. This data can be read without MIFARE Keys. In all other sectors, Block 0 may be programmed with user data.

Blocks 0 – 2 of any given sector contain whatever user data is encoded into them. Depending on how the data is formatted, a block may be data, or it may be stored value.

Block 3, the Sector Trailer contains keys and access conditions for all four blocks including itself.

There is only one key pair for the sector, but there can be unique access conditions for those keys in each block:

Security Key A
Access Conditions
For Block 0
For Block 1
For Block 2
For Block 3

Security Key B

Having two keys per sector enables the system manager to structure the encoding of cards so that different people (using different readers) have different privileges with respect to the data. For example, in a card with stored data, a reader with Key A would be able to read Block 1, whereas a reader with Key B would be able to read and write to Block 1. Or a reader with Key A could be denied access to Block 1, whereas a reader with Key B could read the data. Or, in a system with stored value, a reader with Key A could increment a value in Block 1, whereas a reader with Key B could only decrement that same value.

Access Conditions

Access conditions for a given segment can be unique for each block 0 – 3. Access conditions for each of the four blocks in a segment are expressed as a 3-bit binary number (000 – 111), which allows 8 different possible ways to configure the access of each Key Pair to each block.

Access conditions for the sector trailer can allow or prevent one or both keys and/or the access condition table from being read or changed.

Access conditions for the data blocks can allow or prevent data from being read, written, incremented or decremented by using one or both keys.

These access conditions are shown in the tables below (from the Philips IC specification):

Depending on the access bits for the sector trailer (block 3) the read/write access to the keys and the access bits is specified as 'never', 'key A', 'key B' or key A|B' (key A or key B).

Access conditions for the Sector trailer (Y-3)

Access bits			Access condition for						Remark
			KEY A		Access Bits		KEY B		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A B	never	never	key B	
1	1	0	never	never	key A B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A B	key B	never	key B	
1	0	1	never	never	key A B	key B	never	never	
1	1	1	never	never	key A B	never	never	never	

Note: the grey marked lines are access conditions where key B is readable and may be used for data.

Access conditions for the Data blocks (Y – 0 to 2)

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A B ₁	key A B ₁	key A B ₁	key A B ₁	transport configuration
0	1	0	key A B ₁	never	never	never	read/write block
1	0	0	key A B ₁	key B ₁	never	never	read/write block
1	1	0	key A B ₁	key B ₁	key B ₁	key A B ₁	value block
0	0	1	key A B ₁	never	never	key A B ₁	value block
0	1	1	key B ₁	key B ₁	never	never	read/write block
1	0	1	key B ₁	never	never	never	read/write block
1	1	1	never	never	never	never	read/write block

¹ If Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in previous table). **Consequences:** If the RWD tries to authenticate any block of a sector with key B using grey marked access conditions, the card will refuse any subsequent memory access after authentication.

Value and Data Blocks

Depending on how it is encoded by the factory or the integrator, a data block can be either a read/write block, containing 16 bytes of general data, or it can be a value block containing 4 bytes of value data. Only value blocks can be incremented decremented, transferred or restored.

Value Blocks consist of

- 4 bytes of address information
- 4 bytes of value data
- 4 bytes of the complement of the value data
- 4 bytes of value data repeated

The value is stored three times in a value block to allow error detection and correction capability. A sector could contain any combination of value or data blocks in blocks 0-2.

MIFARE KEYS

MIFARE Keys are basically numeric passwords used to control access to information stored on the MIFARE contactless card (using the Philips MF1 IC S50 chip or

equivalent). A MIFARE Key is a 6- byte (or 48-bit) data field, typically expressed as 12 Hex characters. The key can be any number from 000000000000 – FFFFFFFF.

MIFARE Keys are associated in pairs, with one referred to as the A Key and the other as the B Key.

Each sector on the MIFARE card (0-15) has a key pair, which means that there are 16 key pairs on a MIFARE Card. Each key pair controls access to data in the sector in which it is located.

References:

<http://www.semiconductors.philips.com/markets/identification/datasheets/#mifare>

M001051

M028630

M043531

M073110

M075031

<http://www.smartcardalliance.org>

Contactless Technology for Secure Physical Access: Technology and Standards Choices

Government Smartcard Handbook