

DATA SHEET

mifare[®]

Standard Card IC

MF1 IC S50

Functional Specification

Product Specification

November 1999

Revision 5.0

Philips
Semiconductors



PHILIPS

CONTENTS

1 FEATURES..... 4

1.1 MIFARE® RF Interface (ISO/IEC 14443 A)..... 4

1.2 EEPROM..... 4

1.3 Security..... 4

2 GENERAL DESCRIPTION..... 5

2.1 Contactless Energy and Data Transfer..... 5

2.2 Anticollision..... 5

2.3 User Convenience..... 5

2.4 Security..... 5

2.5 Multi-application Functionality..... 5

2.6 Delivery Options..... 6

3 FUNCTIONAL DESCRIPTION..... 6

3.1 Block Description..... 6

3.2 Communication Principle..... 7

3.2.1 REQUEST STANDARD / ALL..... 7

3.2.2 ANTICOLLISION LOOP..... 7

3.2.3 SELECT CARD..... 7

3.2.4 3 PASS AUTHENTICATION..... 7

3.2.5 MEMORY OPERATIONS..... 8

3.3 Data Integrity..... 8

3.4 Security..... 8

3.4.1 THREE PASS AUTHENTICATION SEQUENCE..... 8

3.5 RF Interface..... 8

3.6 Memory Organisation..... 9

3.6.1 MANUFACTURER BLOCK..... 10

3.6.2 DATA BLOCKS..... 10

3.6.3 SECTOR TRAILER (BLOCK 3)..... 11

3.7 Memory Access..... 12

3.7.1 ACCESS CONDITIONS..... 13

3.7.2 ACCESS CONDITIONS FOR THE SECTOR TRAILER..... 14

3.7.3 ACCESS CONDITIONS FOR DATA BLOCKS..... 15

4 DEFINITIONS..... 16

5 LIFE SUPPORT APPLICATIONS..... 16

Functional Specification

Standard Card IC MF1 IC S50

6 REVISION HISTORY 17

MIFARE® is a registered trademark of Philips Electronics N.V.

1 FEATURES

1.1 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)

1.2 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

1.3 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

2 GENERAL DESCRIPTION

Philips has developed the MIFARE[®] MF1 IC S50 to be used in contactless smart cards according to ISO/IEC 14443A. The communication layer (MIFARE[®] RF Interface) complies to parts 2 and 3 of the ISO/IEC 14443A standard. The security layer sports the field-proven CRYPTO1 stream cipher for secure data exchange of the MIFARE[®] Classic family.

2.1 Contactless Energy and Data Transfer

In the MIFARE[®] system, the MF1 IC S50 is connected to a coil with a few turns and then embedded in plastic to form the passive contactless smart card. No battery is needed. When the card is positioned in the proximity of the Read Write Device (RWD) antenna, the high speed RF communication interface allows to transmit data with 106 kBit/s.

2.2 Anticollision

An intelligent anticollision function allows to operate more than one card in the field simultaneously. The anticollision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without data corruption resulting from other cards in the field.

2.3 User Convenience

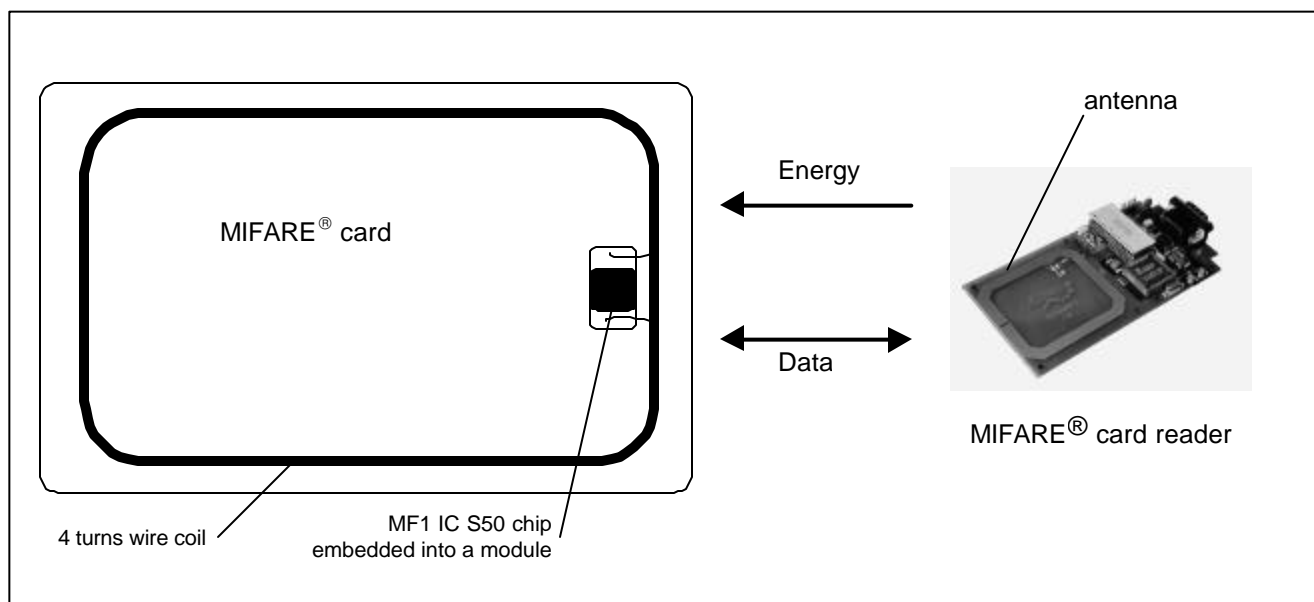
The MIFARE[®] system is designed for optimal user convenience. The high data transmission rate for example allows complete ticketing transactions to be handled in less than 100 ms. Thus, the MIFARE[®] card user is not forced to stop at the RWD antenna leading to a high throughput at gates and reduced boarding times onto busses. The MIFARE[®] card may also remain in the wallet during the transaction, even if there are coins in it.

2.4 Security

Special emphasis has been placed on security against fraud. Mutual challenge and response authentication, data ciphering and message authentication checks protect the system from any kind of tampering and thus make it attractive for ticketing applications. Serial numbers, which can not be altered, guarantee the uniqueness of each card.

2.5 Multi-application Functionality

The MIFARE[®] system offers real multi-application functionality comparable to the features of a processor card. Two different keys for each sector support systems using key hierarchies.



Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.