DATA SHEET

mifare®

Standard 4 kByte Card IC

MF1 IC S70

Functional Specification

Product Specification

October 2002

Revision 3.1

PUBLIC

Philips Semiconductors

PHILIPS

CONTENTS

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

- 4 Kbyte, organised in 32 sectors with 4 blocks and 8 sectors with 16 blocks (one block consists of 16 bytes)
- 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 key set 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 S70 to be used in contactless smart cards according to ISO/IEC 14443 A. The communication layer complies to parts 2 and 3 of the ISO/IEC 14443 A standard. The security layer supports 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 S70 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 Proximity Coupling Device (PCD) 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

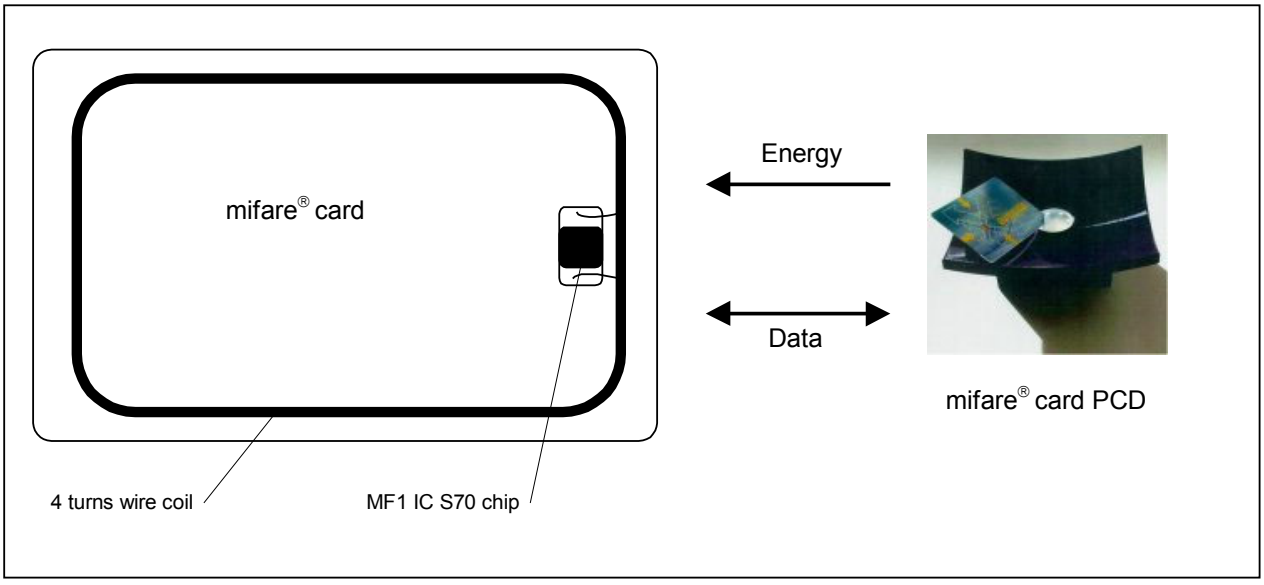
The mifare® system is designed for optimal user convenience. The high data transmission rate for example allows complete ticketing transactions to be handled in less than 100ms. Thus, the mifare® card user is not forced to stop at PCD antenna leading to a high throughput at gates and reduced boarding 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 electronic purse 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.



2.6 Delivery Options

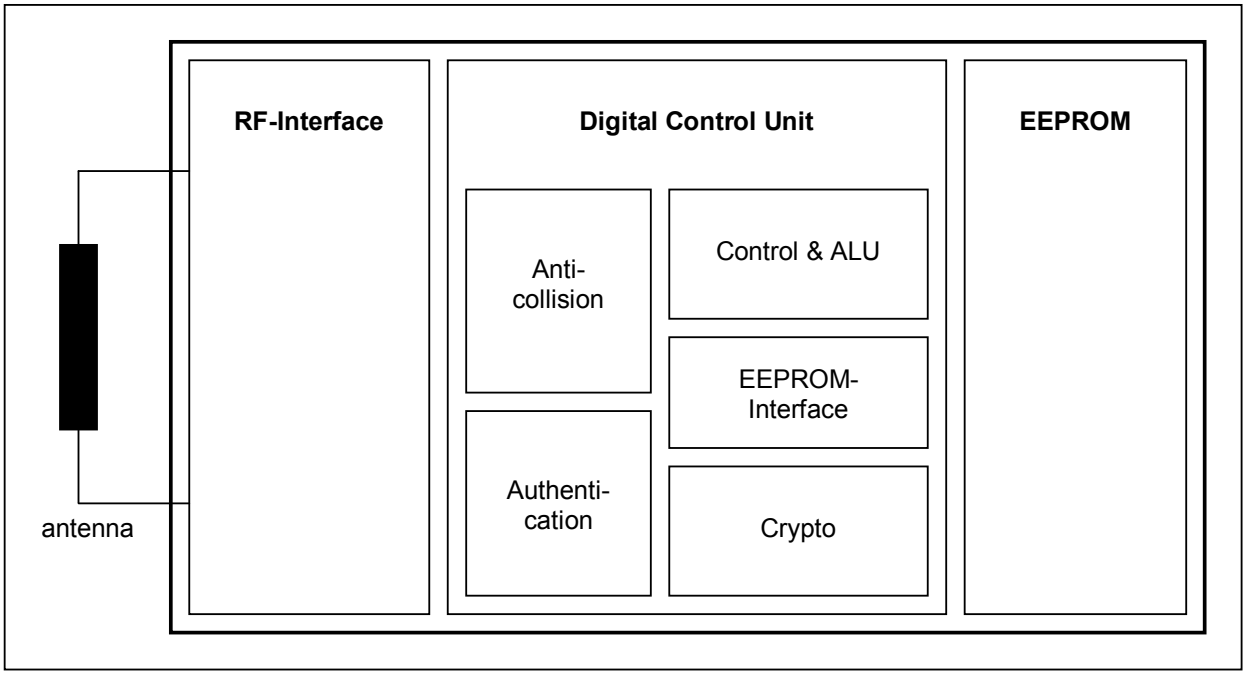
- Die on wafer: MF1ICS70W/V5D
- Bumped die on wafer: MF1ICS70W/V4D
- Chip Card Module: MF1MOA2S70/D

3 FUNCTIONAL DESCRIPTION

3.1 Block Description

The MF1 IC S70 chip consists of the 4 Kbytes EEPROM, the RF-Interface and the Digital Control Unit. Energy and data are transferred via an antenna, which consists of a coil with a few turns directly connected to the MF1 IC S70. No further external components are necessary. (For details on antenna design please refer to the document *mifare® (Card) Coil Design Guide*.)

- RF-Interface:
  – Modulator/Demodulator
  – Rectifier
  – Clock Regenerator
  – Power On Reset
  – Voltage Regulator
- Anticollision: Several cards in the field may be selected and operated in sequence
- Authentication: Preceding any memory operation the authentication procedure ensures that access to a block is only possible via the two keys specified for each block
- Control & Arithmetic Logic Unit: Values are stored in a special redundant format and can be incremented and decremented
- EEPROM-Interface
- Crypto unit: The field-proven CRYPTO1 stream cipher of the mifare® classic family ensures a secure data exchange
- EEPROM: 4 Kbytes are organised in 32 sectors with 4 blocks each and 8 sectors with 16 blocks each. One block contains 16 bytes. The last block of each sector is called “sector trailer”, which contains two secret keys and programmable access conditions for each sector.



DOCKET ALARM

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.