SIEMENS

ICs for Chip Cards

SLE 55R04

Contactless Secured Memory IC

Intelligent 512-Byte EEPROM with Interface
for Contactless Transmission, Security Logic;
Physical Interface and Anticollision according to ISO 14443

Preliminary Short Product Information 12.98

This document contains preliminary information about a new product under development. Details are subject to change without notice.

Preliminary Short Product Information		
Revision History:	Current Version:	12.98
	Previous Releases:	09.97
Page (in previous version)	Page (in current version)	Subjects (changes since last revision)
2 and 4	3 and 5	Slotted aloha anticollision method replaced by bit anticollision method 8 byte serial number is replaced by 4 or 7 byte serial number (cascaded)
2	3	Optional activation of parity bit is cancelled; parity bit is activated complying to ISO 14443 Type A Editorial Changes: 55 family fully complies to ISO 14443 Type A

Important: Further information is confidential and on request. Please contact:
Siemens Semiconductor Group in Munich, Germany,
Sales and Solutions Center, Security and ChipCard ICs,
Fax +49 89 636-28925

Published by Siemens AG, Bereich Halbleiter, HL CC Applications Group
St.-Martin-Str. 76
D-81617 München

Attention please!

As far as patents or other rights of third parties are concerned, liability is only assumed for components, not for applications, processes and circuits implemented within components or assemblies.

The information describes the type of component and shall not be considered as assured characteristics.
Terms of delivery and rights to change design reserved.
For questions on technology, delivery and prices please contact the Semiconductor Group Offices in Germany or the Siemens Companies and Representatives worldwide (see address list).
Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Siemens Office, Semiconductor Group.
Siemens AG is an approved CECC manufacturer.

Packing

Please use the recycling operators known to you. We can help you - get in touch with your nearest sales office. By agreement we will take packing back, if it is sorted. You must bear the costs of transport.
For packing material that is returned to us unsorted or which are not obliged to accept, we shall have to invoice you for any costs incurred.

Components used in life-support devices or systems must be expressly authorized for such purpose!

Critical components[1] of the Semiconductor Group of Siemens AG, may only be used in life-support devices or systems[2] with the express written approval of the Semiconductor Group of Siemens AG.

[1] A critical component is a component used in a life-support device or system whose failure can reasonably be expected to cause the failure of that life-support device or system, or to affect its safety or effectiveness of that device or system.

[2] Life support devices or systems are intended (a) to be implanted in the human body, or (b) to support and/or maintain and sustain human life. If they fail, it is reasonable to assume that the health of the user may be endangered.

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

Intelligent 512-Byte EEPROM with
Interface for Contactless Transmission and Security Logic;
Physical Interface and Anticollision complying to ISO 14443

Features

Memory

- 608 bytes EEPROM, organized in 76 pages of 8 bytes each
- **User-configurable number of sectors (up to 15)**
- **User-configurable sector size (1 to 70 pages)**
- Erasing and writing of one page in one shot at less than 5 ms
- Minimum of 100.000 write/erase cycles
- Data retention for minimum of ten years

Contactless Interface (complying to ISO 14443 Type A)

- Contactless transmission of data and supply energy (batteryless operation)
- Fast data transfer (up to 106 Kbit/s)
- Carrier frequency: 13.56 MHz
- Modulation: ASK 100%
- Coupling distance from 0 to 10 cm (typ.)
- ***Bit oriented anticollision method complying to ISO 14443***
- ***Several* cards may be operated with one reader simultaneously**

Security

- On chip high security crypto unit
- 2-way authentication with 64 bit key between reader and card
- Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication)
- **2 keys for each sector allow hierarchical key management**
- **Secret keys are only programmable but never readable**
- Access conditions unchangeable in user mode
- **Multi-level security structure possible by key-individual access rights for each page**
- Unique chip identification number for each chip
- Only one sector is to be opened at a time
- Access protection of EEPROM by transport keys on chip delivery

Additional features

- Optional one sector accessible without authentication
- On-chip redundancy and anti-tearing functionality for value data
- value data in a range of 0 to 2^{16} (= 65536 values)

Contactless secured memory chip for proximity coupling smart card systems

The SLE 55R04 is the first member of a new generation of memory chips complying to the ISO 14443 Type-A (modulation ASK 100%) for contactless proximity smart cards.

This family of contactless chips focus on high security, very flexible memory configuration and reduction of the chip size. The SLE 55R04 is the first chip of the 55-family which supplies the user with different memory sizes meeting the requirements of variable applications.

The SLE 55R04 does fully comply to the proposed new ISO 14443 Type-A. After a software upgrade Mifare® systems can also profit from the features of the 55-family.

System description

The system consists of a smart card on the one hand and a card reader together with an antenna on the other hand.

The operating distance between card and reader antenna can vary from 0 cm up to 10 cm. The card's antenna consists of a simple coil with a few turns embedded in plastic. The contactless smart cards are passive and work batteryless. The high speed RF communication interface allows to transmit data with 106 Kbit/s.

The User-Friendly Contactless System

The high data transmission rate permits short transaction times and user-friendly transaction times. For example, a ticketing transaction can be handled in less than 100 ms so that the card user needs not to stop at the reader target (antenna). The card even may remain in the wallet of the user even if there are coins in it.

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.

Multi-Application Functionality

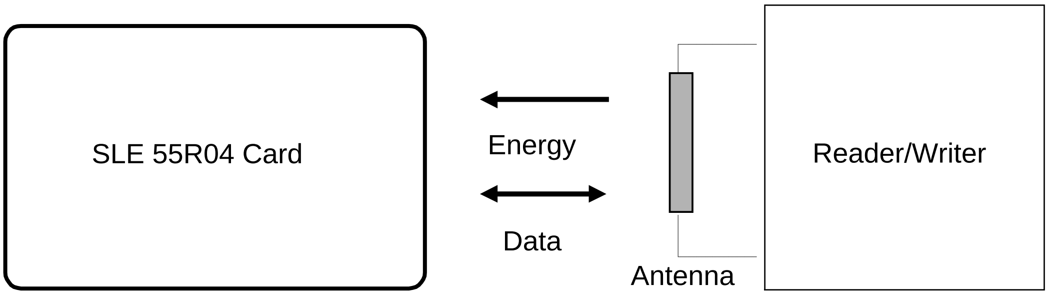
The SLE 55R04 shows its user-friendliness by its unrivaled memory flexibility. It provides the possibility to use one big sector or 2 or more smaller sectors with different sizes each. Optionally one sector is to be opened without authentication to read e.g. additional card and issuer information.

Thus the SLE 55R04 can meet the needs of low memory applications like public transport as well as the more extensive needs of payment systems, which is also supported by the value function

Two different key sets for each memory sector support systems using key hierarchies.

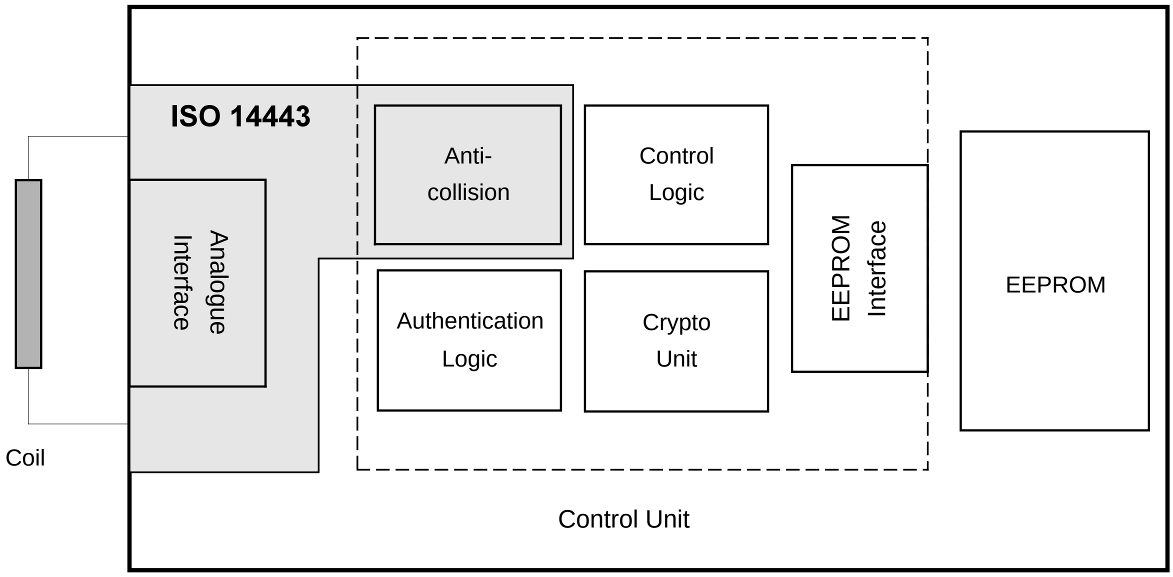
High System Security

In the system design, special emphasis has been placed on security against fraud. An access to the card memory is only possible after a two pass authentication. Memory operations are restricted by page-configurable access conditions. The serial number is unique for each card and can never be changed.



General Circuit Description

The SLE 55R04 contains on a single chip a 608 byte EEPROM, an analogue interface for contactless energy and data transmission and a control unit. The power supply and data are transferred to the SLE 55R04 via an antenna which consists of a coil with a few turns directly connected to the chip. No further external components are necessary. The circuit is designed according to ISO 14443 to communicate with a card reader at an operating distance between 0 cm and 10 cm.



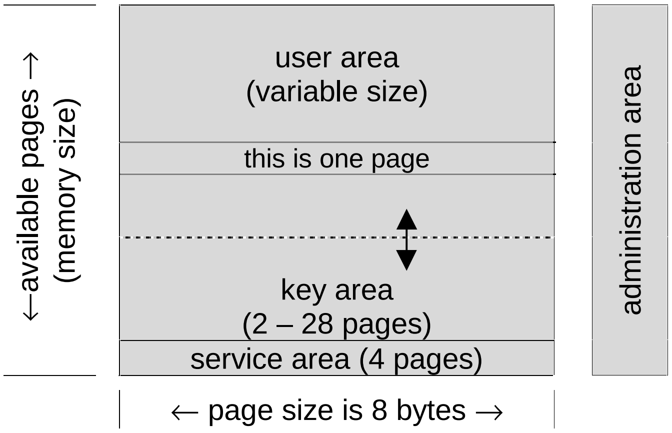
Block diagram SLE 55R04

- Analogue Interface, consisting of
  - Modulator / Demodulator
  - Rectifier
  - Clock Separator
  - Power on Reset
  - Voltage Regulator
- Anticollision
  Internal logic of the SLE 55R04 ensures the recognition of several cards in the field which may be selected and operated simultaneously. This is done by the **bit oriented anticollision method** with 4 or 7 byte serial numbers (complying to ISO 14443 – cascading of serial numbers).
- Authentication Control
  Access to key-protected sectors is only permitted after authentication with an appropriated key. One sector is optionally configurable without key protection and authentication. Only one sector is to be opened within a session.
- Control Logic:
  Each page can only be accessed according to the individual access conditions programmed for every page and every key.
- EEPROM-Interface

- EEPROM: 608 bytes organized in 76 pages with 8 bytes each.
  The size of the available user area results in 512 bytes if 4 sectors are programmed.

  The memory is organized in 4 areas:

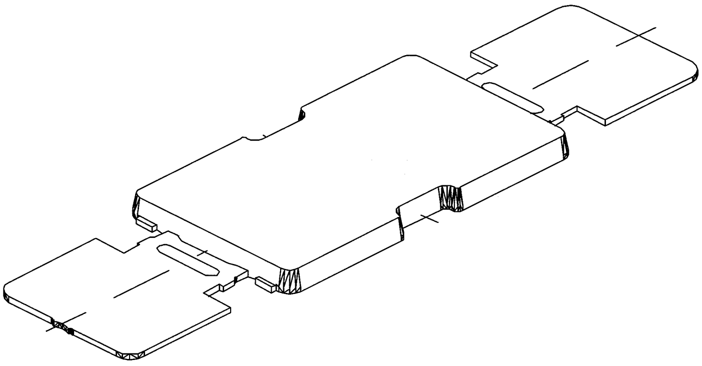
  - user area — variable number of sectors with variable size;
    one sector configurable as accessible without authentication
  - key area — the key-pairs are stored in this area; size is 2 pages per sector
  - service area — this area stores manufacturing and personalization data
  - administration area — sector management and access rights area



Memory structure of SLE 55R04

Packaging Information

The SLE 55R04 will be available as die for customer packaging and in the module MCC2.



Leadframe Module MCC2