Security & Chip Card ICs

SLE 55R04

Intelligent 770–Byte EEPROM
with Contactless Interface complying to ISO/IEC 14443 Type A
and Security Logic

Short Product Information

January 2001

SLE 55R04 Short Product Information	Ref.: SPI_SLE55R04_0101.doc
Revision History: Current Version 2001-01-31	
Previous Releases:	
Page	Subjects (changes since last revision)

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Security & Chip Card ICs,
Tel +49 - (0)89 / 234-80000
Fax +49 - (0)89 / 234-81000
E-Mail: security.chipcard.ics@infineon.com

Published by Infineon Technologies AG, CC Applications Group
St.-Martin-Strasse 76, D-81541 München
© Infineon Technologies AG 2001
All Rights Reserved.

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realise that we may have missed a few things. If you find any information that is missing or appears in error, please use the contact section above to inform us. We appreciate your assistance in making this a better document.

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives world-wide (see address list).

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Intelligent 770–Byte EEPROM with Contactless Interface complying to ISO/IEC 14443 Type A and Security Logic

Features

- **770 bytes EEPROM**
  - Organised in 77 pages located in up to 16 sectors
  - Each page organised in 8 bytes for data storage + 2 bytes for administrative purposes
  - Configurable number of sectors (1 to 15) & sector size (1 to up to 77 pages)
  - Service Area 4 pages
  - Configurable Key Area with up to 14 key pairs
  - Configurable User Area
  - Unique chip identification number
  - Access conditions unchangeable in user mode
- **Value Counters: up to 65536 units** (with a value range from 0 to 2^{16}-1)
  - Each page in User Area configurable as a Counter
  - Support of Anti-Tearing
- **High Security Authentication Unit**
  - 2-way authentication with 64-bit secret key between reader and card
  - 2 keys for each sector allow hierarchical key management
  - Multi-level security structure possible
  - Individual access rights for each key within a sector for each page
  - Only one sector can be opened at a time
  - Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication)
- **Access protection of EEPROM by transport keys on chip delivery**
- **Physical Interface and Anticollision complying to ISO/IEC 14443 Type A**
  - Carrier frequency: 13.56 MHz
  - 106 kbit/s data rate transfer
  - Bit oriented anticollision method complying with ISO/IEC 14443
  - Contactless transmission of data and supply energy
  - Coupling distance from 0 to 10 cm (typ.)
- **EEPROM updating (erase and program) time maximum 4 ms per page**
- **EEPROM endurance minimum 10^5 write/erase cycles**[1)]
- **Data retention for minimum of 10 years**[1)]
- **ESD protection typical 4kV**
- **Ambient temperature –25 … +85°C**

[1)] Values are temperature dependent

Ordering and Packaging information

Table 1 Ordering Information

Type	Package[1)]	Memory		Pages	Ordering Code
		User	Admin.		
SLE 55R04C	Die	616 bytes	154 bytes	77	on request
SLE 55R04LM	MCC2-2-1	616 bytes	154 bytes	77	on request

Pin Description

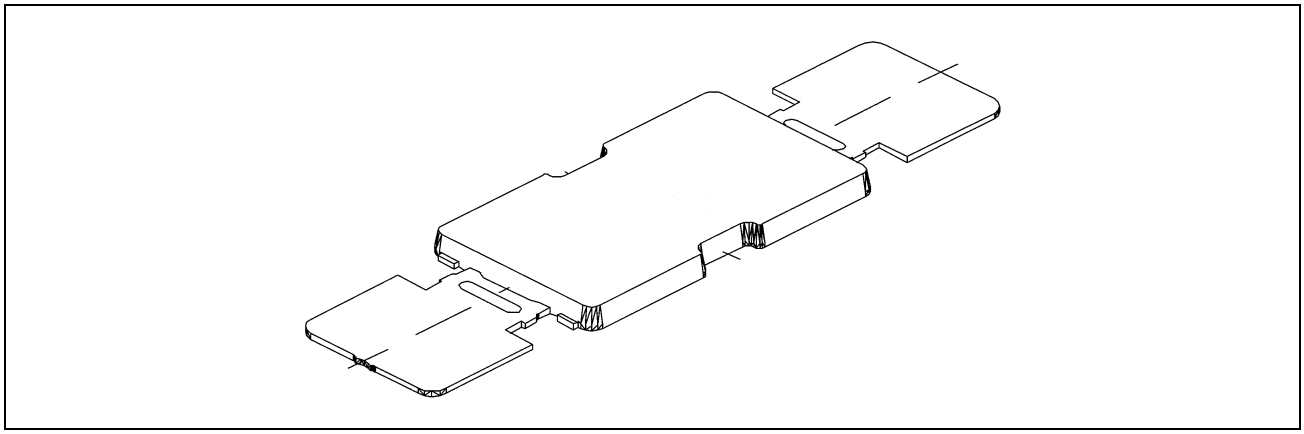

Figure 1 Pin Configuration Module Contactless Card (top view)

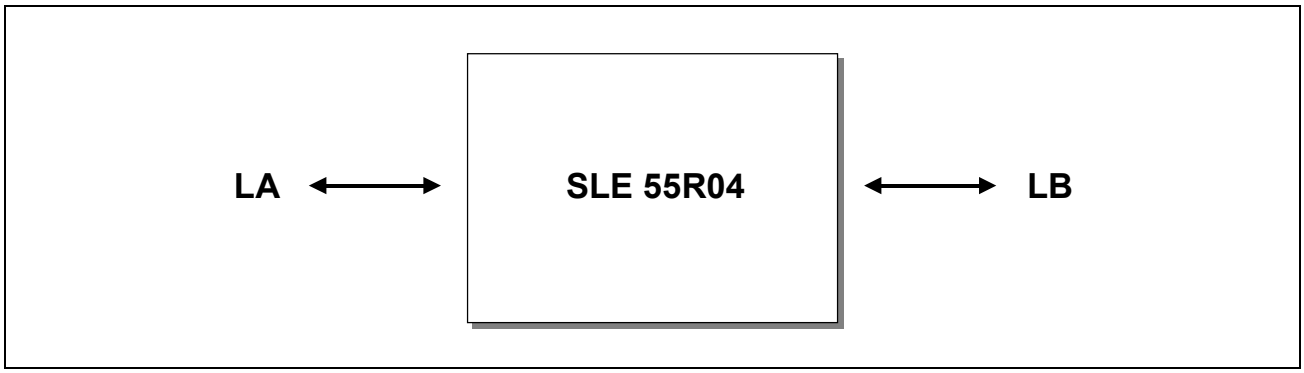

Figure 2 Pad Configuration Die

Table 2 Pin Definitions and Functions

Symbol	Function
LA	Antenna connection
LB	Antenna connection

[1)] Available as a Module Contactless Card (MCC) for embedding in plastic cards or as a die (C) for customer packaging

1 General Description

SLE 55Rxx-family of contactless memory chips focuses on high security and flexible memory and sector configuration. This family of memory chips supplies the user with different memory sizes meeting the requirements of variable applications.

SLE 55R04 complies to ISO/IEC 14443 part 2 and part 3 Type-A (modulation ASK 100%) for contactless proximity smart cards. The power supply and data are transferred to SLE 55R04 via an antenna. SLE 55R04 is designed to communicate with a contactless card reader up to a typical operating distance of 10 cm.

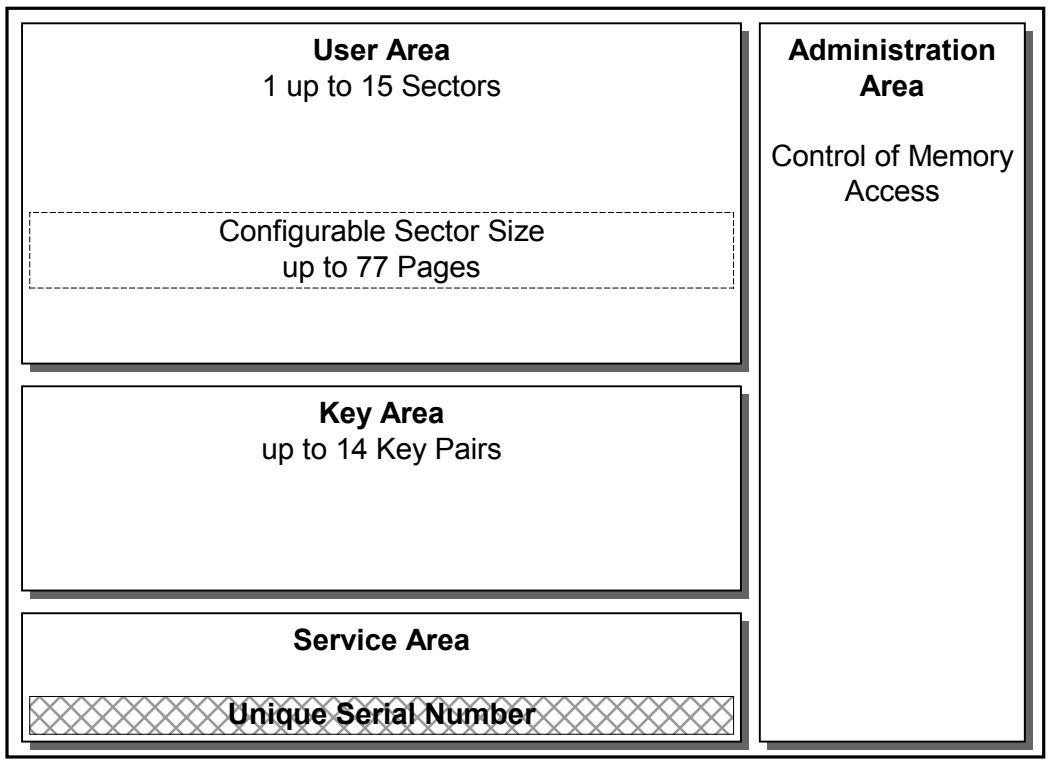

Figure 3 Memory principle of SLE 55R04

1.1 Circuit Description

SLE 55R04 consists of a EEPROM memory unit, an analog interface for contactless energy and data transmission, a control and a crypto unit.

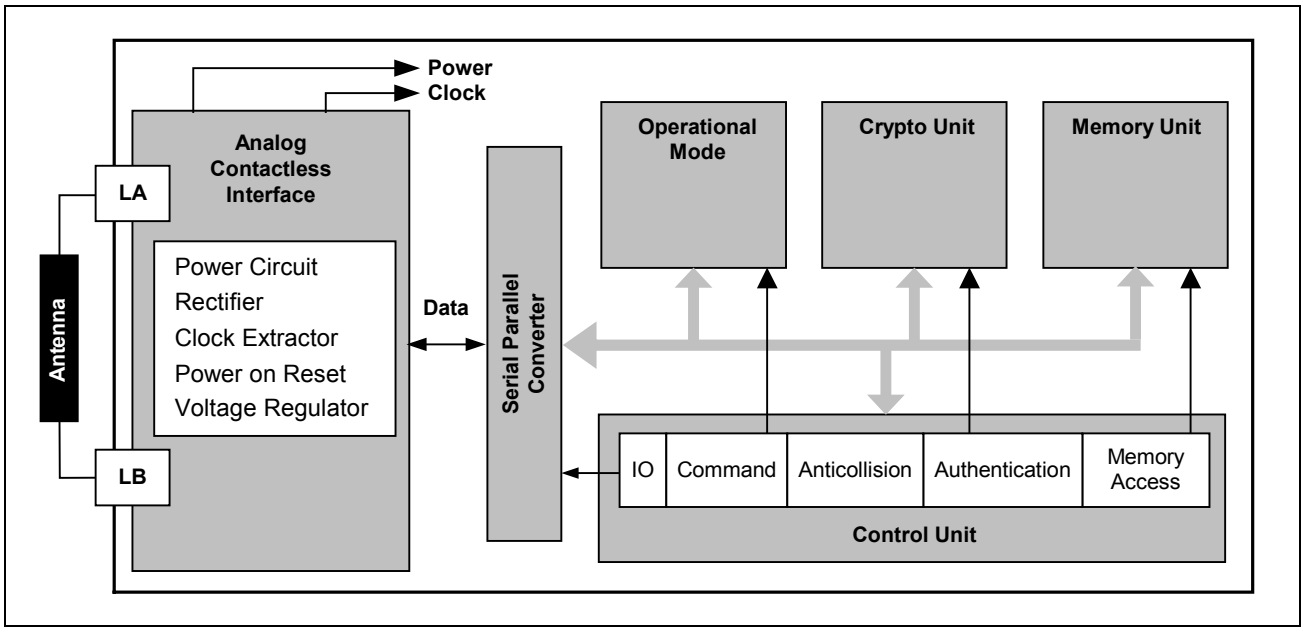

Figure 4 Block diagram of SLE 55R04

- Analog Contactless Interface consists of:
  - Rectifier
  - Voltage Regulator
  - Power on Reset
  - Modulator / Demodulator
  - Clock Extractor
- Operational mode
  The access to the memory depends on the actual mode of SLE 55R04; the memory is accessed according to plain or protected mode when the PICC is selected.
- Crypto Unit
  Generates random numbers, checks and calculates message authentication code (MAC).
- Memory Unit
  770 bytes organised in 77 pages with 8 + 2 bytes each.
- Control Unit
  - Decoding and execution of the **commands**
  - Bit oriented **anticollision** method with 4 or 7 byte long serial numbers (complying to ISO/IEC 14443-3 – cascade level 1 and 2 are supported). It allows the recognition of several cards in the field which may be selected and operated in sequence.
  - Access to key-protected sectors is only permitted after **authentication** with an appropriate key. Only one sector is opened within a session. One sector is optionally configurable without key protection and authentication.
  - **Memory access** to the pages according to the individual access conditions programmed for every page and every key

1.2 System Overview

The system consists of a contactless card on one hand and a contactless card reader together with an antenna on the other. Operations on protected areas of SLE 55R04 requires a security access module at the reader or system side to perform a high system security. The security access module (SAM) holds the algorithm for the fast and secure calculation of the authentication and the integrity check of the transferred and received data.

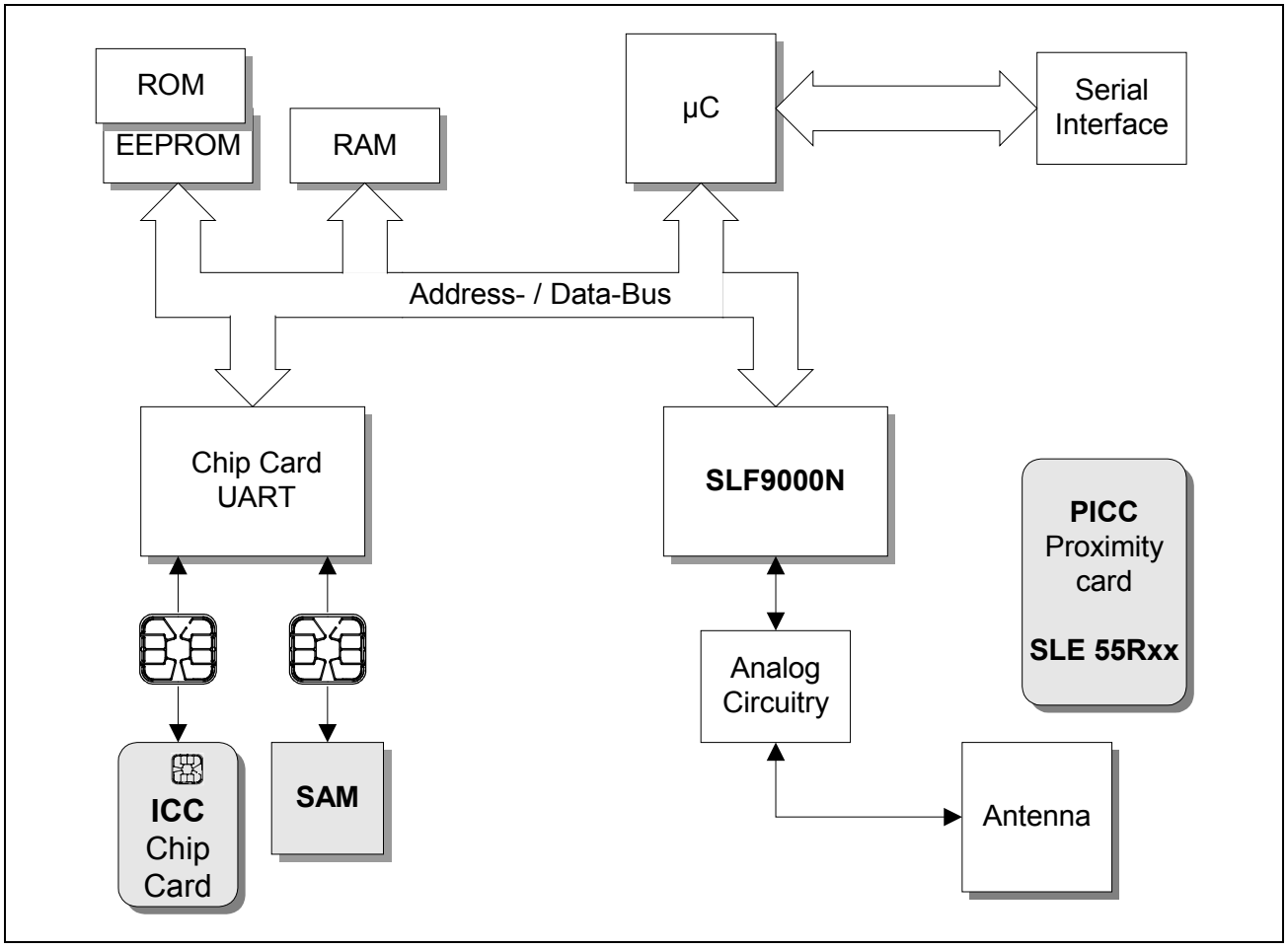

Figure 5 Contactless System Example

- Chip card UART – Interface between Address- / Data-Bus of µ-processor system and reader contacts
- SLF 9000 – Interface between Address- / Data-Bus of µ-processor system and contactless interface
- ICC – Integrated Circuit(s) Card with Contacts according to ISO/IEC 7816
- PICC – Proximity Card according to ISO/IEC 14443
- SAM – Security Access Module with contacts according to ISO/IEC 7816

Contactless Energy and Data Transfer

The operating distance between card and reader antenna is typically up to 10 cm. The card antenna consists of a simple coil with a few turns embedded in plastic. Contactless cards are passive. The high speed RF communication interface allows to exchange data with 106 kbit/s. This high data transmission rate permits short transaction times.
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.

Multi-Application Functionality

SLE 55R04 provides the possibility to use one large sector or several smaller ones with different sizes.
Optionally, one sector can be opened without authentication to read e.g. additional card and issuer information.
Thus, SLE 55R04 meets the need of low cost memory applications like public transport as well as the more extensive needs of payment systems, which is also supported by the counter 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.
The serial number is unique for each card and can not be changed. Access to the protected memory of the card is only possible after a mutual authentication (challenge/response) which is a function of the unique serial number, random number and key to be used. Authentication is only possible with a security access module, SAM, that holds the algorithm.
Therefore, for all operations on the protected memory, the SAM calculates and checks by a message authentication code (MAC) the integrity of the transferred data. Thus, operations on the protected memory are key protected, and restricted by page-configurable access conditions.