2008-05

my-d™ proximity 2

SLE 66RxxS

Intelligent EEPROM with Contactless Interface compliant to ISO/IEC 14443 Type A

Short Product Information

Chipcard & Security ICs

Never stop thinking

Important:	For further information please contact: Infineon Technologies AG in Munich, Germany, Chip Card & Security ICs, Fax +49 (0)89 / 234-955 9372 E-Mail: security.chipcard.ics@infineon.com

Edition 2008-05-13

Published by
Infineon Technologies AG
81726 Munich, Germany

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation, warranties of non-infringement of intellectual property rights of any third party.

Information

For further information on technology, delivery terms and conditions and prices, please contact the nearest Infineon Technologies Office (**www.infineon.com**).

Warnings

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

Infineon Technologies components may be used in life-support devices or systems only 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.

my-d™ proximity 2
Intelligent EEPROM with Contactless Interface compliant to ISO/IEC 14443 Type A

Revision History: 2008-05-13

Previous Version:

Page	Subjects (major changes since last revision)
	initial version

Trademarks of Infineon Technologies AG

my-d™.

Features

Intelligent EEPROM with Contactless Interface compliant to ISO/IEC 14443 Type A

Contactless Interface

- Physical interface and Anticollision compliant to ISO/IEC 14443-3 Type A
- Contactless transmission of data and supply energy
- Carrier frequency: 13.56 MHz
- Data rate up to 848 kbit/s from PICC to PCD, 106 kbit/s from PCD to PICC
- Read / write distance up to 10 cm depending on reader antenna configuration

EEPROM

- Up to 5120 bytes in total (R32 version)
  - organized in up to 512 pages (page size 10 byte) located in up to 16 sectors (1 plain and 15 secure sectors)
  - configurable number of sectors (1 to 15) & sector size
  - configurable Key Area with up to 14 key pairs
  - up to 509 pages of user memory (user page size 8 byte)
- Unique IDentification number (UID)
- EEPROM programming time per page < 4 ms
- EEPROM endurance > 100.000 erase/write cycles[1)]
- Data retention > 10 years[1)]
- Access protection of EEPROM by transport key on chip delivery
- EEPROM Error Correction Unit

Security Features

- Challenge and response security algorithm
  - 2-way mutual authentication with 64-bit key
  - 2 keys per sector enable hierarchical key management
  - multi-level security structure possible
  - individual access rights for each key within a sector of each page
  - only one sector can be accessed at a time
  - 32 bit message authentication code (MAC) verifies data integrity
- Transport key on chip delivery

Value Counters: up to 65536 (value range from 0 to 2^{16}-1)

- Each page in the User Area is configurable as a Value Counter
- Support of Anti-Tearing

Electrical characteristics

- ESD protection minimum 2 kV
- Ambient temperature -25°C ... +70°C (for the chip)

1) Values are temperature dependent

1 Ordering and packaging information

Table 1-1 Ordering information

Type	Package	Total Memory	Security	Pages	Ordering code
SLE 66R04S C	Die (wafer)	512 bytes	Yes	64	on request
SLE 66R04S NB	NiAu Bumped				on request
SLE 66R04S MCC2	P-MCC2-2-1				on request
SLE 66R04S MCC8	P-MCC8-2-3				on request
SLE 66R16S C	Die (wafer)	2048 bytes		256	on request
SLE 66R16S NB	NiAu Bumped				on request
SLE 66R16S MCC2	P-MCC2-2-1				on request
SLE 66R16S MCC8	P-MCC8-2-3				on request
SLE 66R32S C	Die (wafer)	4096 bytes		512	on request
SLE 66R32S NB	NiAu Bumped				on request
SLE 66R32S MCC2	P-MCC2-2-1				on request
SLE 66R32S MCC8	P-MCC8-2-3				on request

For more ordering information (wafer thickness and height of NiAu-Bump) please contact your local Infineon sales office.

1.1 Pin description

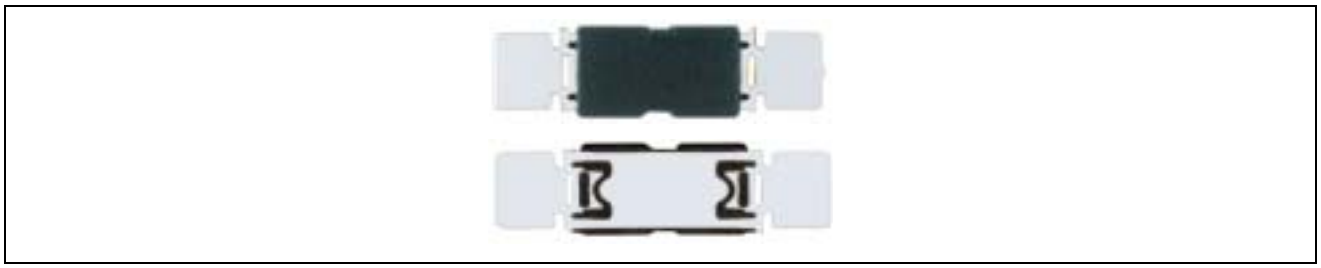

Figure 1-1 Pin configuration Module Contactless Card - MCC2 (top / bottom view)

Figure 1-2 Pin configuration Module Contactless Card - MCC8 (top / bottom view)

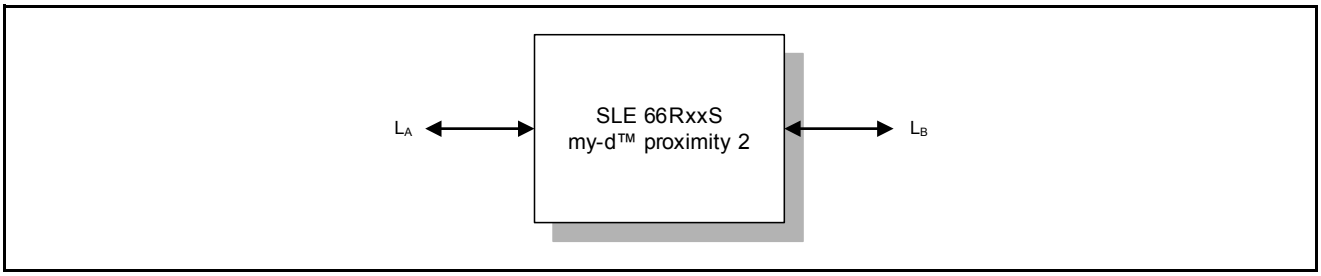

Figure 1-3 Pad configuration die

Table 1-2 Pin description and function

Symbol	Function
L_A	Antenna connection
L_B	Antenna connection

2 my-d™ product family

The my-d™ products are designed to meet increased demands for basic security and design flexibility. The family of contactless memory my-d™ supplies the user with different memory sizes and incorporates security features to enable considerable flexibility in the application design.

The functional architecture, meaning the memory organisation and authentication of my-d™ products is the same for both, my-d™ proximity (ISO/IEC 14443) and my-d™ vicinity (ISO/IEC 18000-3 mode 1 or ISO/IEC 15693). This eases the system design and allows simple adaptation between applications.

All my-d™ products are available in plain mode with open memory access and in secure mode with memory access controlled by authentication procedures.

Flexible controls within the my-d™ ICs start with plain mode operation and individual page locking; for more complex applications various settings in secure mode can be set for multi user / multi application configurations.

In secure mode a cryptographic algorithm based on a 64-bit key is available. Mutual authentication, message authentication codes (MAC) and customized access conditions protect the memory against unauthorized access. Configurable value counters featuring anti-tearing functionality are suitable for value token applications, such as limited use transportation tickets.

Architectural interoperability of all my-d™ products enables an easy migration from simple to more demanding applications.

In addition, the my-d™ light (ISO/IEC 18000-3 mode 1 or ISO/IEC 15693) is part of the my-d™ family. Its optimized command set and memory expands the range of applications to cost sensitive segments.

3 SLE 66RxxS my-d™ proximity 2

The my-d™ proximity 2 products are products based on the ISO/IEC 14443-3 Type A standard for contactless proximity cards. The my-d™ proximity 2 family additionally features my-d™ commands and my-d™ cryptographic algorithm. The products are targeting personal identification, access and event ticketing as well as amusement and entertainment. They are fulfilling the requirements of state of the art contactless memory ICs with respect to compatibility to the ISO/IEC 14443-3 standard part 1-3, operating range and command as well as feature set. The my-d™ proximity 2 focuses on flexible memory and sector configuration.

3.1 Circuit Description

The my-d™ proximity 2 is made up of an EEPROM memory unit, an analog interface for contactless energy and data transmission and a control unit.

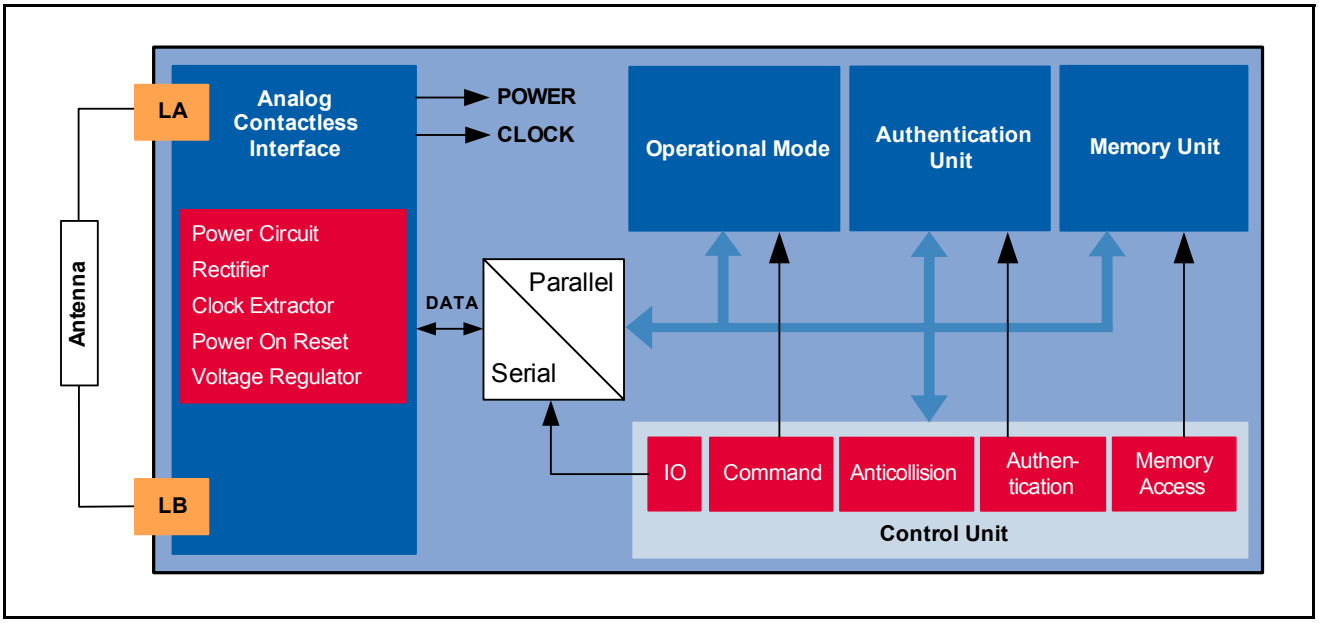

Figure 3-1 Block diagram of the my-d™ proximity 2

- Analog Contactless Interface:
  The Analog Contactless Interface comprises the voltage rectifier, voltage regulator and system clock to supply the IC with appropriate power. Additionally the data stream is modulated and demodulated.
- Operational mode
  The access to the memory depends on the actual mode of the my-d™ proximity 2. The memory is accessed according to plain or secure mode after the PICC is selected.
- Authentication Unit (optional use)
  The Authentication Unit generates random numbers, calculates and verifies the message authentication codes (MAC).
- Memory Unit
  The Memory Unit consists of up to 4096 bytes organised in up to 512 pages each of 8 user and 2 administration bytes.

- Control Unit
  The Control Unit decodes and executes all commands. Additionally the control unit is responsible for the correct anticollision flow.

3.2 Memory Principle

The my-d™ proximity 2 chip features security, flexible memory and sector configuration. It can be configured in up to 16 sectors, where each sector may be build up by a different numbers of pages. The memory is organized in 4 areas:

- User Area
- Key Area
- Service Area
- Administration Area

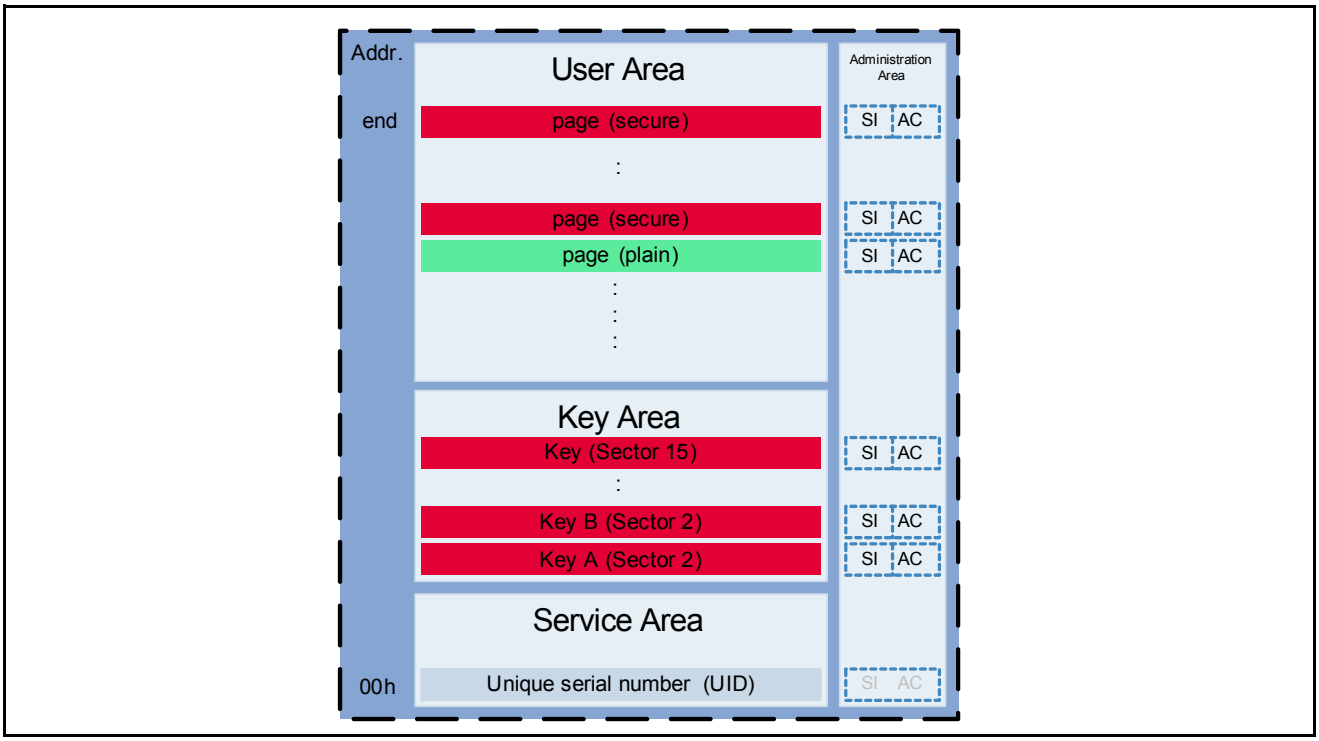

Figure 3-2 my-d™ Memory Organization

The User Area stores user data in flexible numbers of sectors, from 0 to 15, with configurable number of pages (from 1 up to 512 pages), where sector 0 is the plain sector and sector 1 is reserved for authentication counters.

The Key Area stores the key pairs allocated to each secure sector. Two keys per sector with different access rights are available to enable a hierarchical key management.

The Service Area stores manufacturer data, configuration data as well as the authentication counter. This information is programmed at manufacture of the chip and cannot be changed.

The Administration Area stores 2 bytes of information about page administration.

3.3 System Overview

The system consists of a host system, one or more my-d™ proximity 2 cards and an ISO/IEC 14443-3 compatible contactless reader with an antenna. Operation on protected areas of a my-d™ proximity 2 in secure mode require mutual authentication between the label and the reader. To achieve high system security the my-d™ security algorithm has to be integrated into the reader. A license can be obtained from Infineon Technologies for integration of the algorithm into the reader. Optionally, a Security Access Modules (SAM) contains the algorithm for performing the mutual authentication and data integrity check.

To access plain pages on a SLE 66RxxS, the algorithm is not required on the reader.

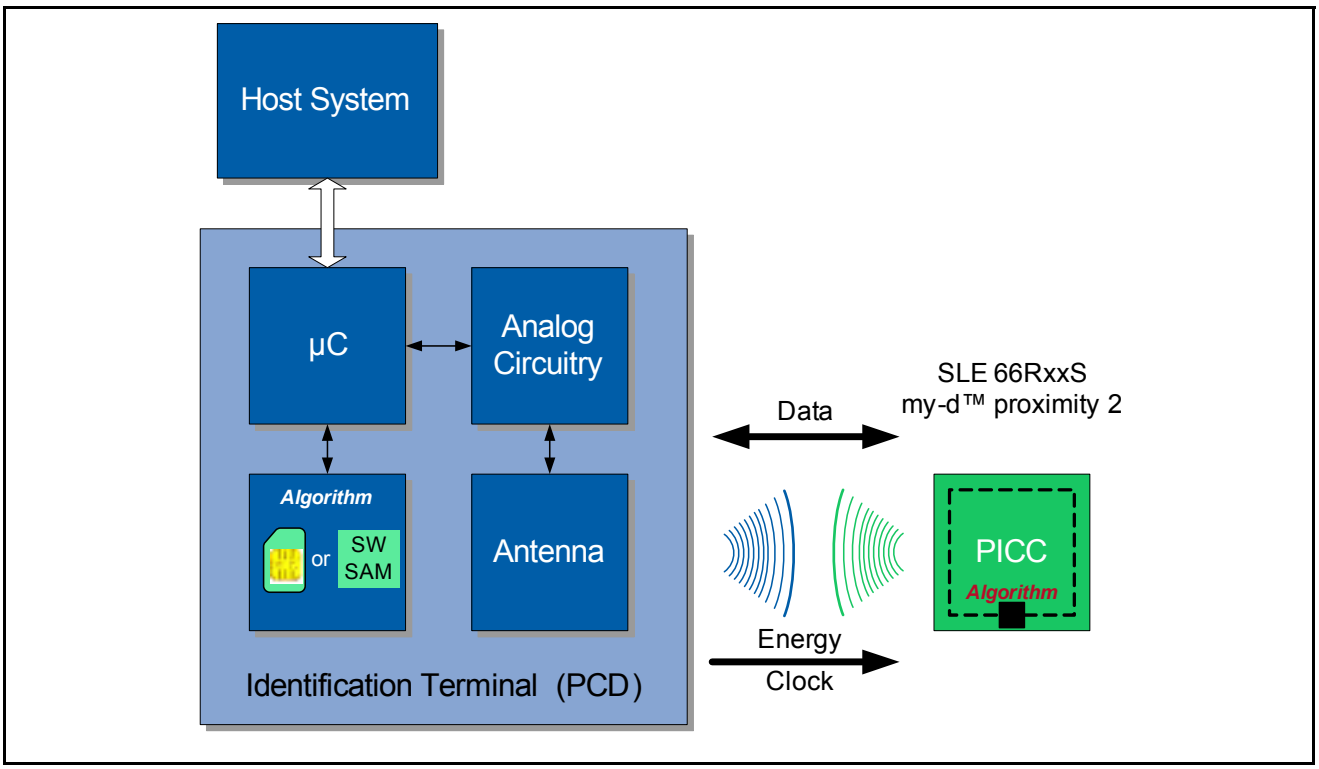

Figure 3-3 Secure my-d™ proximity 2 RFID system

3.4 Product Versions

To identify the different types of my-d™ proximity 2 contactless memories special chip type information is coded into the manufacturer page (page 02_h, byte 0). The table below briefly describes the values of this byte for the different chip versions.

Table 3-1 Chip Information for different product variants

Sales Code	Chip Information Byte
SLE 66R04S	$10xx\_x010_b$
SLE 66R16S	$10xx\_x100_b$
SLE 66R32S	$10xx\_x101_b$

3.5 Supported Standards

- ISO/IEC 14443-3 Type A (Parts 1, 2 and 3)
  tested according to ISO/IEC10373-6 (PICC Test & Validation)

3.6 Command set

The my-d™ proximity 2 chip is compliant to the ISO/IEC 14443-3 standard. A set of standard ISO commands is implemented to operate the chip. Additional to the ISO/IEC 14443 commands, a my-d™ specific command set is implemented. This facilitates the access to the on-chip integrated memory. To execute commands on plain memory pages, no authentication is required.

3.7 Multi-Application Functionality

The my-d™ proximity 2 secure mode provides the possibility to use one large sector or up to 15 smaller ones of flexible size.

Optionally, one sector can be addressed without authentication reading e.g. additional label and user information.

The my-d™ proximity 2 closes the gap between the diverging requirements for low cost memory and secure, value token applications. Its unique value counter functionality eases the implementation of value blocks and limited use.

The hierarchical approach of a key pair enables customized applications comprising different memory access.

3.8 Security features

The serial number is unique for each label and cannot be changed. Access to the protected memory of the label is protected by using mutual authentication.

For all operations to the protected memory the authentication unit calculates and validates the message authentication codes (MAC) to verify the data integrity. Additionally a key pair and individually configurable access conditions secure the access to the protected memory.

www.infineon.com/rfid

Published by Infineon Technologies AG