Chip Card & Security ICs

my-d® vicinity

SRF 55V10S

Intelligent 10 Kbit EEPROM
with Contactless Interface compliant to ISO/IEC 15693
and ISO/IEC 18000-3 mode 1
and Security Logic

Secure Mode Operation

Short Product Information July 2007

SRF 55V10S Short Product Information		Ref.: SRF55V10S_ShortProductInfo_2007-06.doc
Revision History:	**Current Version 2007-07-02**	
Previous Releases:	2002-07-30	
Page	Subjects (changes since last revision)	
	Editorial changes	

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

Published by Infineon Technologies AG, CC Applications Group
D-81726 München

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 10 Kbit EEPROM with Contactless Interface (ISO/IEC 15693 and ISO/IEC 18000-3 mode 1) and Security Logic

Features

Contactless Interface

- Physical Interface and Anticollision compliant to ISO/IEC 15693 and ISO/IEC 18000-3 mode 1
  - contactless transmission of data and supply energy
  - carrier frequency: 13.56 MHz
  - data rate up to 26 kbit/s
  - anticollision with identification of up to 30 tags/sec
  - read / write distance up to 150 cm depending on reader antenna configuration

10 Kbit EEPROM

- ISO mode – block organization of memory
  - up to 248 blocks of user memory (block size 4 bytes) applicable for plain memory only
- Custom mode – page organization of memory
  - up to 128 pages of user memory (page size 8 bytes for data storage and 2 bytes for administrative purposes in addition)
  - configurable number of sectors (1 to 15) and sector size (1 to 128 pages)
  - configurable Key Area with up to 14 key pairs and configurable User Area
- Unique chip identification number (UID)
- EEPROM programming time per block/page < 4 ms
- EEPROM endurance > 100,000 erase/write cycles[1)]
- Data retention > 10 years[1)]

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

Security Features

- State-of-the-art 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

Electrical characteristics

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

1) Values are temperature dependent

Development Tool

– my-d® Evaluation Kit including my-d® Manager Software

1 Ordering and Packaging information

Table 1: Ordering Information

Type	Package[1)]	Memory		Pages	Ordering Code
		User	Admin.		
SRF 55V10S C	Sawn wafer	1024 bytes	256 bytes	128	SP000009268
SRF 55V10S NB	NiAu bump wafer				SP000310866
SRF 55V10S MFCC1	S-MFCC1-2-1 [2)]				SP000010036
SRF 55V10S MCC2	P-MCC2-2-1				SP000009366

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

Pin Description

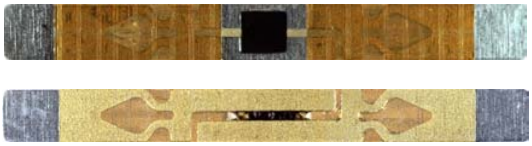

Figure 1: Pin Configuration Module Contactless Card – MFCC1 (top / bottom view)

Figure 2: Pin Configuration Module Contactless Card – MCC2 (top view)

1) Available as a Module Flip Chip Contactless (MFCC1), Module Contactless Card (MCC) for embedding in plastic cards, as NiAu-bump version (NB) or as a die on sawn / unsawn wafer for customer packaging
2) FCoS™ Flip Chip on Substrate

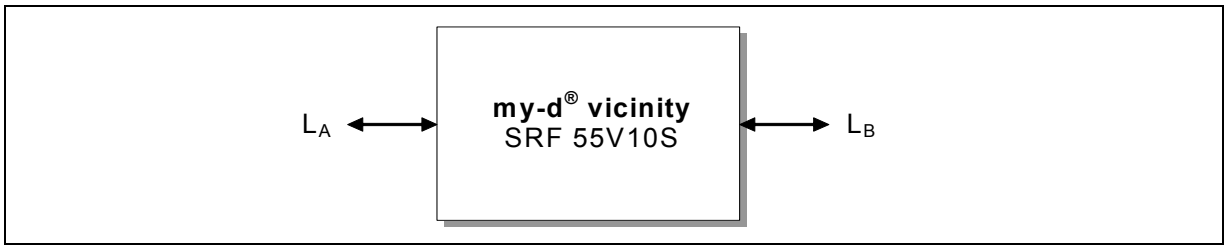

Figure 3: Pad Configuration Die

Table 2 Pin Definitions and Functions

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 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 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 SRF 55V10S my-d® vicinity secure

my-d® vicinity secure focuses on flexible memory and sector configuration at longer read/write distances.

All my-d® vicinity products comply with ISO/IEC 18000-3 mode 1 or ISO/IEC 15693 standards for contactless vicinity smart cards. The power supply and data are transferred to the my-d® products via an antenna. The my-d® vicinity is designed to communicate within the operating distance of up to 1.5m depending on appropriate reader antenna configurations.

3.1 Circuit Description

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

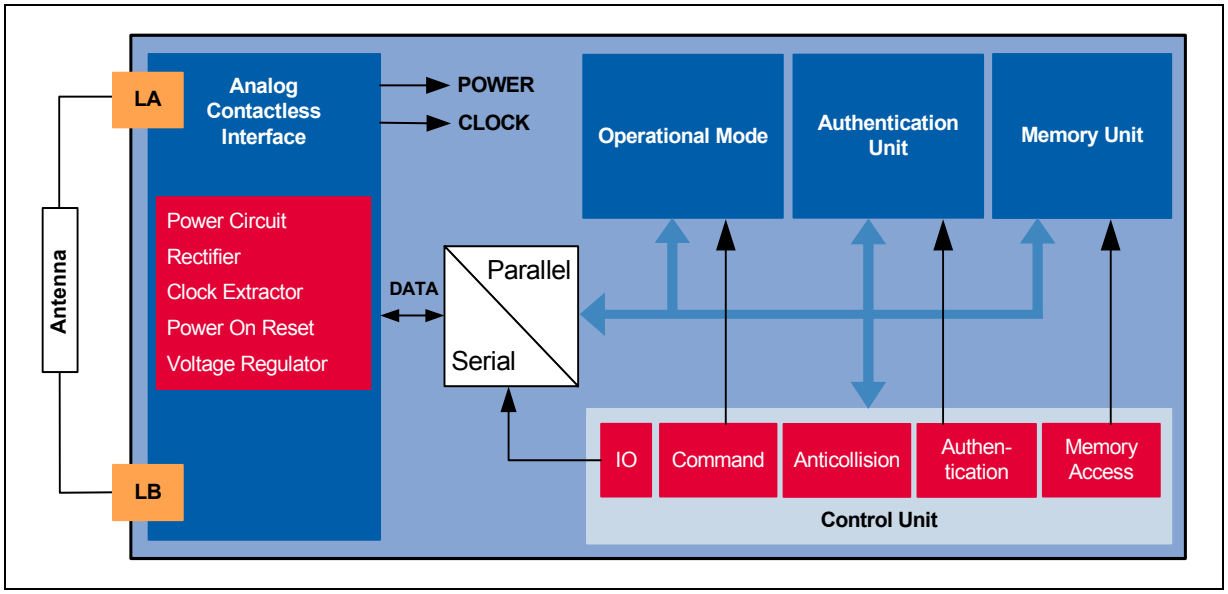

Figure 4: Block diagram of the my-d® vicinity secure

- **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® vicinity. The memory is accessed according to plain or secure mode after the VICC 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 1280 bytes organised in 128 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 and authentication flow.

3.2 Memory Principle

The my-d® vicinity secure features secure memory access.

The User / Key Memory with its flexible organisation permits up to 14 independent secure sectors of a variable size each protected with a 64 bit key pair. Only after a successful authentication a single sector is accessible. In addition, one freely programmable plain sector is available for general purpose use.

The service area contains the UID and manufacturer data. The service area cannot be changed.

The administration area comprises the access conditions and sector information.

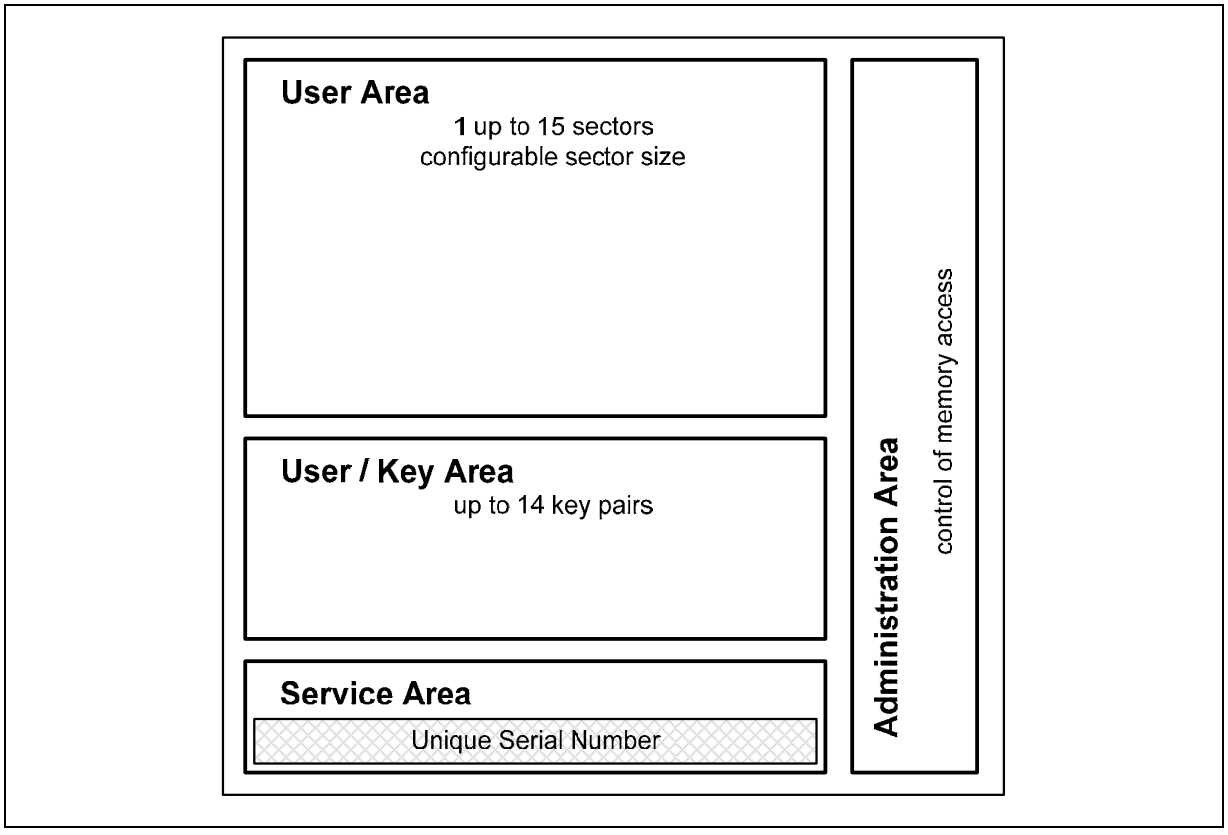

Figure 5: Memory principle of my-d® SRF 55V10S

3.3 System Overview

The system consists of a contactless label and a contactless reader together with an antenna. Operations on protected areas of my-d® vicinity 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. Optionally, a Security Access Modules (SAM) contains the algorithm for performing the mutual authentication and data integrity check.

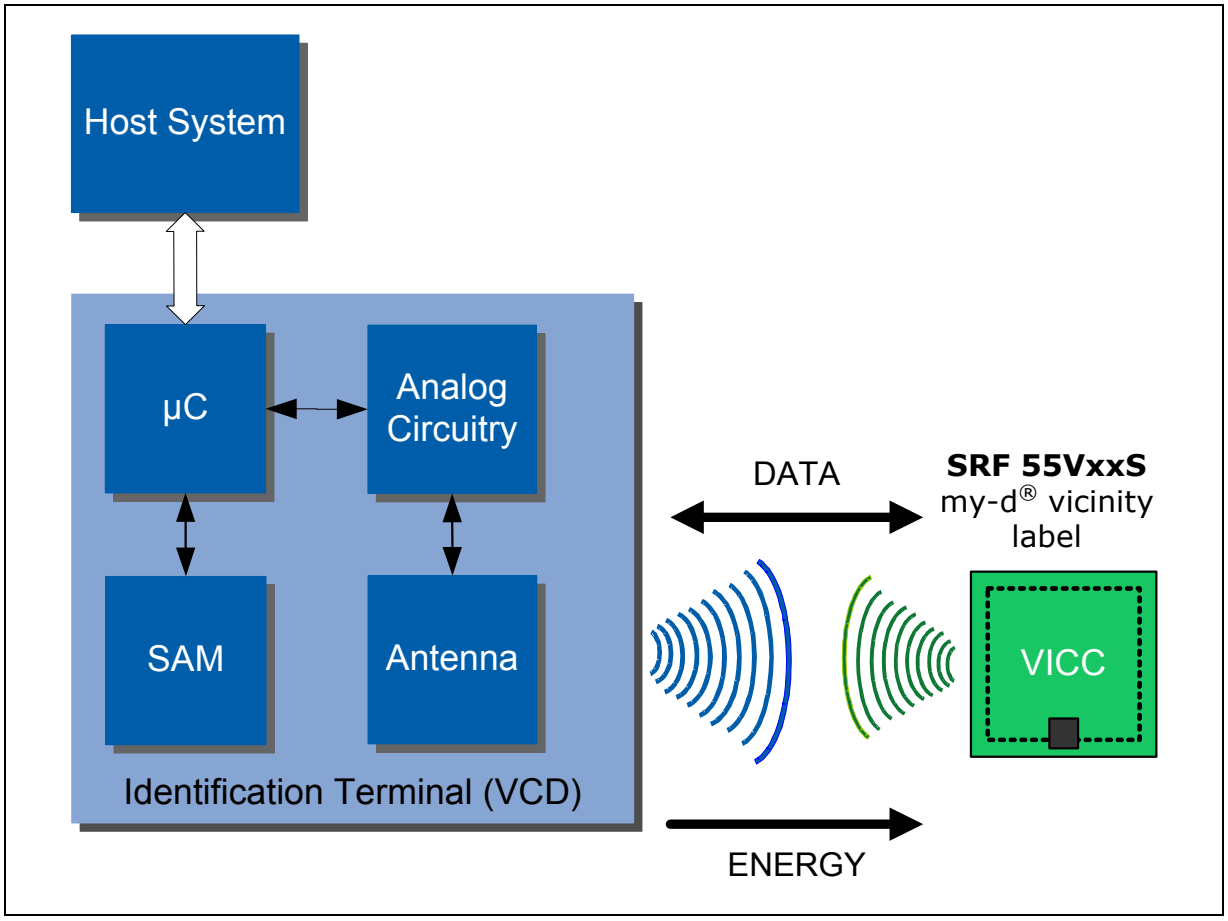

Figure 6: Contactless System Example my-d® vicinity Secure

- VICC – Vicinity Card according to ISO/IEC 18000-3 mode 1 or ISO/IEC 15693
- optional SAM – Security Access Module with contacts according to ISO/IEC 7816

Contactless Energy and Data Transfer

The read / write distance is up to 1.5 m depending on an appropriate reader antenna configuration. The label antenna consists of a simple coil with few turns. Contactless labels are passive. The RF communication interface exchanges data with data rates of up to 26 kbit/s.
An intelligent anticollision function enables operation of more than one label in the field simultaneously. The anticollision algorithm selects each label individually and ensures that the

execution of a transaction with a selected label is performed correctly without data corruption resulting from other labels.

Multi-Application Functionality

The my-d® vicinity 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® vicinity 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.

System Security

In the system design, substantial emphasis has been placed on security against fraud.
The serial number is unique for each label and cannot be changed. Access to the protected memory of the label is only granted after a 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