Security & Chip Card ICs

my-d products for contactless systems
my-d vicinity

SRF 55V02S

Intelligent 2–KBit EEPROM
with Contactless Interface complying to ISO/IEC 15693
and Security Logic

Secure Mode Operation

Short Product Information

July 2002

Downloaded from Arrow.com.

SRF 55V02S Short Product Information	Ref.: SPI_SRF55V02S_0702.doc
Revision History: Current Version 2002-07-30	
Previous Releases: 2001-08-15	
Page	Subjects (changes since last revision)
	Editorial changes

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 53, D-81541 München
© Infineon Technologies AG 2002
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.

Downloaded from Arrow.com.

Intelligent 2–KBit EEPROM with Contactless Interface complying to ISO/IEC 15693 and Security Logic

my-d vicinity – Secure Mode Operation

Features

- **2-KBit EEPROM**
  - Organised in 32 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 up to 128 pages)
  - Service Area 4 pages
  - Configurable Key Area with up to 14 key pairs
  - Configurable User Area
  - Unique chip identification number
- **Smart Electronic Article Surveillance (EAS)**
  - Easy Integration in existing infrastructure
  - On/Off EAS switch feature
- **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 (optional use)**
  - 2-way (mutual) authentication with 64-bit secret key between reader and label
  - 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 (optional use)**
- **Physical Interface and Anticollision complying to ISO/IEC 15693**
  - Carrier frequency: 13.56 MHz
  - up to 26 kbit/s data rate transfer
  - Anticollision method complying with ISO/IEC 15693 with identification of up to 30 tags/sec
  - Contactless transmission of data and supply energy
  - Coupling distance from 0 to 120 cm (typical, dependent on antenna)
- **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 4 kV**
- **Ambient temperature –25 … +85°C for chip and MCC, –25 … +70°C for Inlay**

[1)] Values are temperature dependent

Downloaded from Arrow.com.

Document References

- Confidential Data Sheet
- Qualification report chip

- Chip delivery specification for wafer with chip-layout (die size, orientation, …)

- Module specification containing description of package, product logistic etc.
- Qualification report module

- Inlay specification containing description of package, product logistic etc.
- Qualification report inlay

Development Tool Overview

- my-d vicinity evaluation and demonstration kit

1 Ordering and Packaging information

Table 1 Ordering Information

Type	Package[1)]	Memory		Pages	Ordering Code
		User	Admin.		
SRF 55V02S C	Die	256 bytes	64 bytes	32	Q67100H4895
SRF 55V02S MCC8	P-MCC8-2-1				on request
SRF 55V02S Y1.0	Inlay 45 x 45 mm^2				Q67100H4910
SRF 55V02S Y2.0	Inlay 45 x 76 mm^2				Q67100H4911

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

Downloaded from Arrow.com.

Pin Description

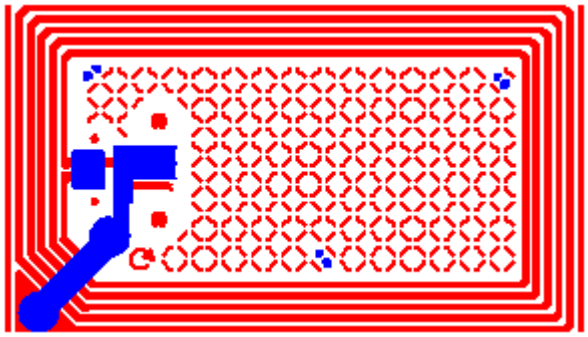

Figure 1 Pin Configuration Label Inlay (top view)

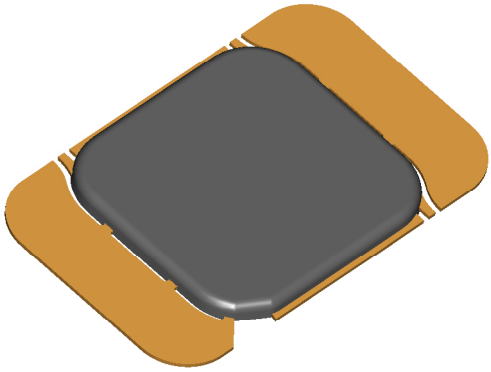

Figure 2 Pin Configuration Module Contactless Card (top view)

Figure 3 Pad Configuration Die

Table 2 Pin Definitions and Functions

Symbol	Function
L_A	Antenna connection
L_B	Antenna connection

Downloaded from Arrow.com.

2 my-d products for contactless systems

my-d products for contactless systems are designed to meet the increased security and flexibility demand of the market. This family of contactless memories supports the different interface and memory size needs as well as various security requirements for variable applications.

The product series functional architecture (e.g. memory organisation, authentication) is the same for both proximity (ISO/IEC 14443) and vicinity (ISO/IEC 15693). This eases the system design and allows simple adaptation of applications from my-d proximity to my-d vicinity or vice versa.

Applications are supported very flexible by setting the appropriate mode for the my-d product, starting with plain mode with a page locking mechanism up to various settings in secure mode for multi user / multi application configurations with tearing protected counters. In secure mode a strong cryptographic algorithm with 64 bit key length is additionally available for security mechanisms like mutual authentication and message authentication codes.

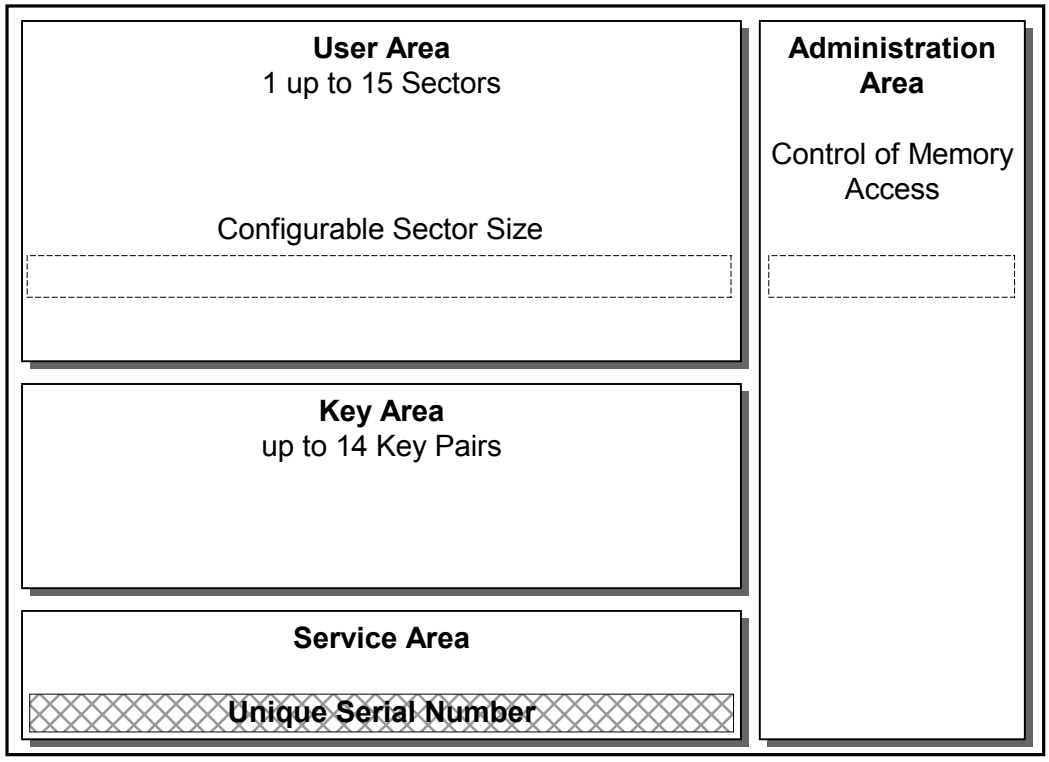

Figure 4 Memory principle of my-d products

These powerful features make the contactless security memory product series my-d ready to cope with even high-end requirements. Architectural compatibility of all my-d products allow an easy migration path from simple to powerful demanding applications.

Downloaded from Arrow.com.

3 my-d vicinity products

my-d vicinity focuses on flexible memory and sector configuration with higher read/write distances. This family of contactless memory chips supplies the user with different memory sizes and optionally offers the use of security features meeting the requirements of variable applications. As special feature the EAS (Electronic Article Surveillance) mode is built in to achieve higher and more robust performance in the demanding EAS application.

my-d vicinity products are available in two memory sizes as well as in plain mode and in secure mode:

- my-d vicinity plain mode with plain memory allowing unlimited access (SRF 55VxxP). Thus the memory is organised in one sector.
- my-d vicinity secure mode allowing to configure counters and to secure memory access by authentication measures (SRF 55VxxS). Thus the memory may be organised in up to 16 sectors with at least one sector in plain mode.
- 2,5 KBit memory sizes 32 pages with 10 Bytes (8 byte user data)
- 10 KBit memory sizes 128 pages with 10 Bytes (8 byte user data)
- In security mode advanced functions are available. Please refer to the relevant data book for details.

All my-d vicinity products comply to the standard ISO/IEC 15693 for contactless vicinity smart cards. The power supply and data are transferred to my-d products via an antenna. my-d vicinity is designed to communicate up to a typical operating distance of 120 cm with a contactless reader in an appropriate gate configuration.

Downloaded from Arrow.com.

3.1 Circuit Description

my-d vicinity consists of a EEPROM memory unit, an analog interface for contactless energy and data transmission, a control and a crypto unit.

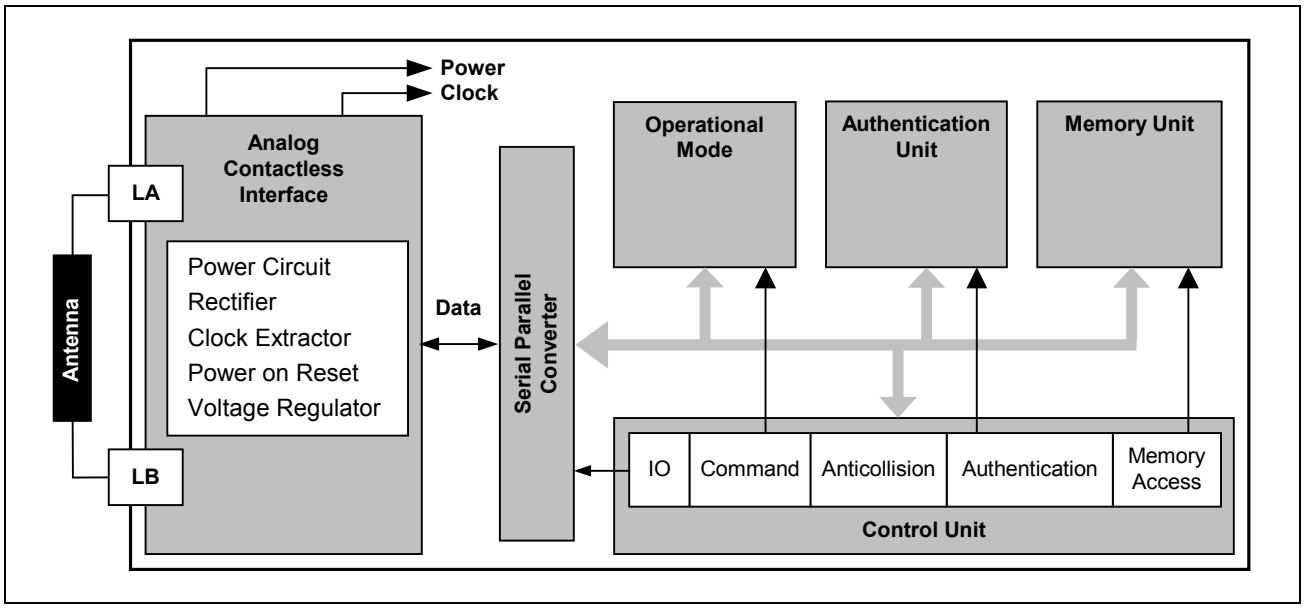

Figure 5 Block diagram of my-d vicinity

- **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 my-d vicinity; the memory is accessed according to plain or protected mode when the VICC is selected.
- **Authentication Unit (optional use)**
  Generates random numbers, checks and calculates message authentication code (MAC).
- **Memory Unit**
  320 bytes organised in 32 pages with 8 + 2 bytes each.
- **Control Unit**
  - Decoding and execution of the **commands**
  - **Anticollision** method complying to ISO/IEC 15693. It allows the recognition of several labels 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

Downloaded from Arrow.com.

3.2 System Overview

The system consists of a contactless label on one hand and a contactless reader together with an antenna on the other. Operations on protected areas of my-d vicinity in secure mode require a mutual authentication with the reader. To achieve a high system security a Security Access Module (SAM) holds the algorithm for performing the mutual authentication and integrity check of all data exchange.

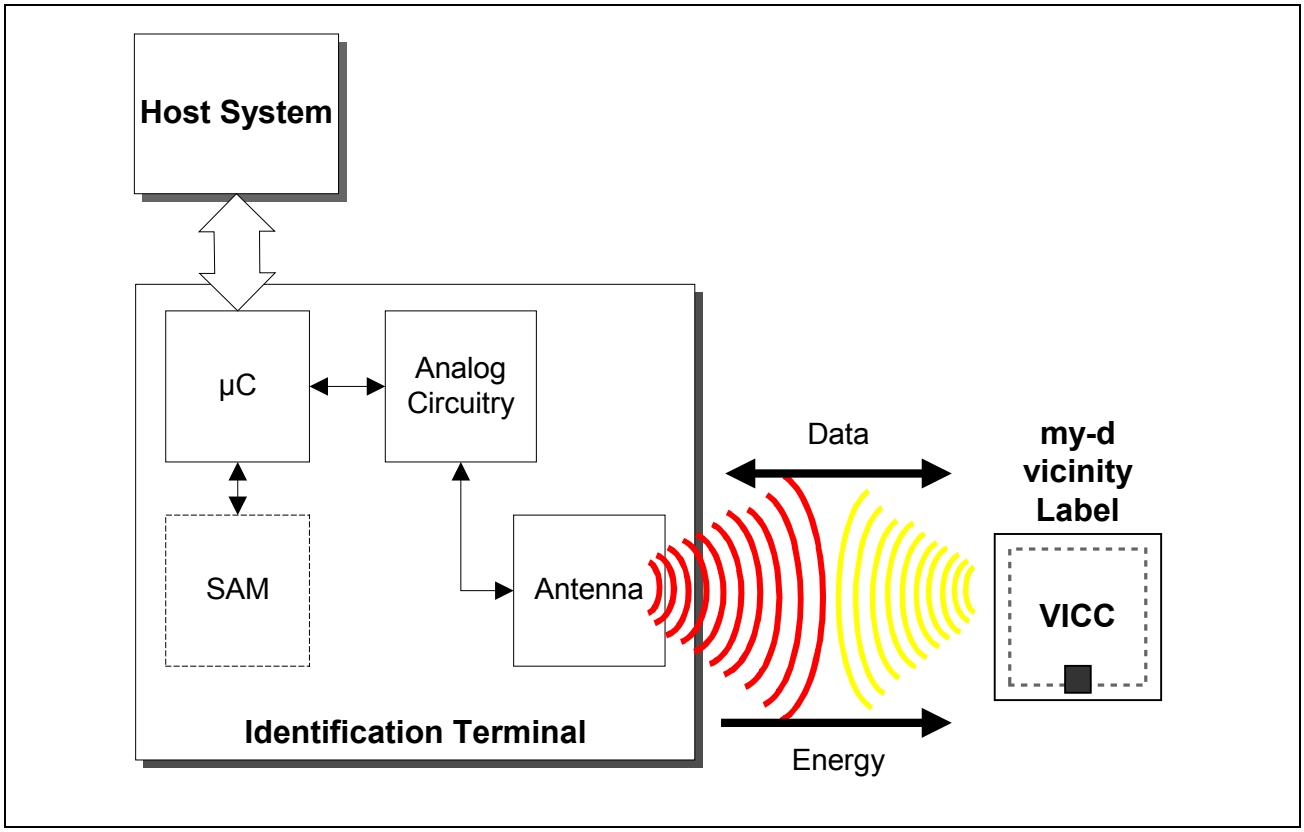

Figure 6 Contactless System Example

- VICC – Vicinity Card according to ISO/IEC 15693
- optional SAM – Security Access Module with contacts according to ISO/IEC 7816

Contactless Energy and Data Transfer

The operating distance between label and reader antenna is typically up to 120 cm in an appropriate gate configuration. The label antenna consists of a simple coil with a few turns. Contactless labels are passive. The RF communication interface allows to exchange data with 26 kbit/s. This high data transmission rate permits short transaction times.
An intelligent anticollision function allows to operate 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.

Downloaded from Arrow.com.

Multi-Application Functionality

my-d vicinity 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 label and issuer information.
Thus, my-d vicinity 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.

System Security

In the system design, special emphasis has been placed on security against fraud.
The serial number is unique for each label and can not be changed. Access to the protected memory of the label 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.

Downloaded from Arrow.com.