my-d™ vicinity secure

Extended datasheet

Intelligent EEPROM with contactless interface compliant to ISO/IEC 15693 secure mode operation

Devices

- SRF 55V02S
- SRF 55V02S HC
- SRF 55V10S
- SRF 55V10S HC

Key features

Contactless interface

- Physical interface and anticollision compliant to ISO/IEC 15693
  - Contactless transmission of data and supply energy
  - Data rate up to 26.69 kbit/s
  - Operation frequency: 13.56 MHz
  - Anticollision logic: Several cards may be operated in the field simultaneously with identification of up to 30 Tags per second
- Read and write distance up to 70 cm and more (influenced by external circuitry that is reader-antenna configuration)

EEPROM

- Up to 10 kbit EEPROM memory
- Custom mode-page organization of memory, accessible with ISO custom commands
  - Up to 128 pages of user memory (page size 8 bytes for data storage and 2 bytes for administration purposes)
- 4 pages Service Area
- Configurable number of sectors (1 to 15)
- Configurable sector size (1 to 28, or 1 to 124 pages respectively)
- Configurable key area (up to 14 key pairs)
- Unique identification (UID) number
- EEPROM programming time per page < 4 ms
- Endurance minimum 100,000 erase/write cycles[1)]
- Data retention for minimum of 10 years[1)]

Value counters: Up to 65536 units (with a value range from 0 to 2^{16} -1)

- Each page in the User Area configurable as a value counter
- Support of anti-tearing

Security features

- 2-way authentication with a 64-bit secret key between the reader and card
- 2 keys for each sector allow hierarchical key management
- Multilevel security structure possible

---

1 Values are temperature dependent

Key features

- Individual access rights for each key within a sector for each page
- Only one sector can be opened at a time
- Each page can be locked against rewriting → read-only
- Data integrity is supported by 16-bit CRC (ISO/IEC 3309) and 32-bit MAC (after authentication)
- Access protection of EEPROM by transport keys on chip delivery

Smart electronic article surveillance (EAS)

- Easy integration into existing infrastructure
- On/off EAS switch feature

Electrical characteristics

- ESD protection minimum 2 kV
- Ambient temperature -25°C ... +70°C (for the chip)
- Chip capacitance 23.1 pF ± 5%
- High on-chip capacitance chip available (97 pF ± 5%) allowing small tag antenna designs

About this document

Scope and purpose

This Extended datasheet describes features, functionality, and operational characteristics of my-d™ vicinity secure.

Intended audience

This document is primarily intended for system and application developers.

Table of contents

Table of contents

List of tables

List of tables

List of figures

1 Ordering and packaging information

Table 1 Ordering information my-d™ vicinity

Type	Package	Total[1] /user memory [bytes]	Total/user pages[2]	Ordering code
SRF 55V02S C	Wafer unsawn/sawn	320/224	32/28	On request
SRF 55V02S NB	NiAu Bumped			
SRF 55V02S MCC8	P-MCC8-2-6			
SRF 55V10S C	Wafer unsawn/sawn	1280/992	128/124	
SRF 55V10S NB	NiAu Bumped			
SRF 55V10S MCC8	P-MCC8-2-6			

1) Total memory size and page count includes the Service Area and the 2 administrative bytes per page whereas user memory size and page count is freely programmable for user data
2) Page size 8 bytes, accessible via ISO custom commands

Table 2 Ordering information my-d™ vicinity high on-chip capacitance

Type	Package	Total[1] /user memory [bytes]	Total/user pages[2]	Ordering code
SRF 55V02S HC C	Wafer unsawn/sawn	320/224	32/28	On request
SRF 55V02S HC NB	NiAu Bumped			
SRF 55V10S HC C	Wafer unsawn/sawn	1280/992	128/124	
SRF 55V10S HC NB	NiAu Bumped			

1) Total memory size and page count includes the Service Area and the 2 administrative bytes per page whereas user memory size and page count is freely programmable for user data
2) Page size 8 bytes, accessible via ISO custom commands

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

Pin description

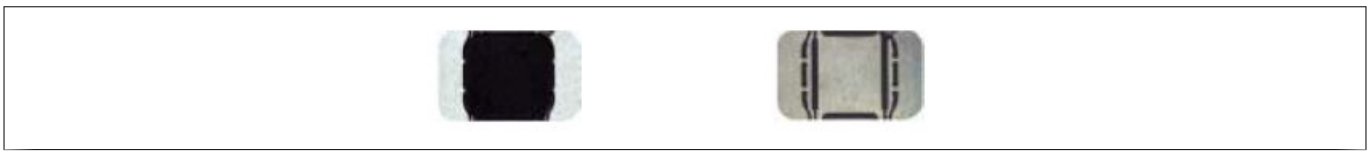


Figure 1 Pin configuration module contactless card-MCC8 (top/bottom view)

1 Ordering and packaging information

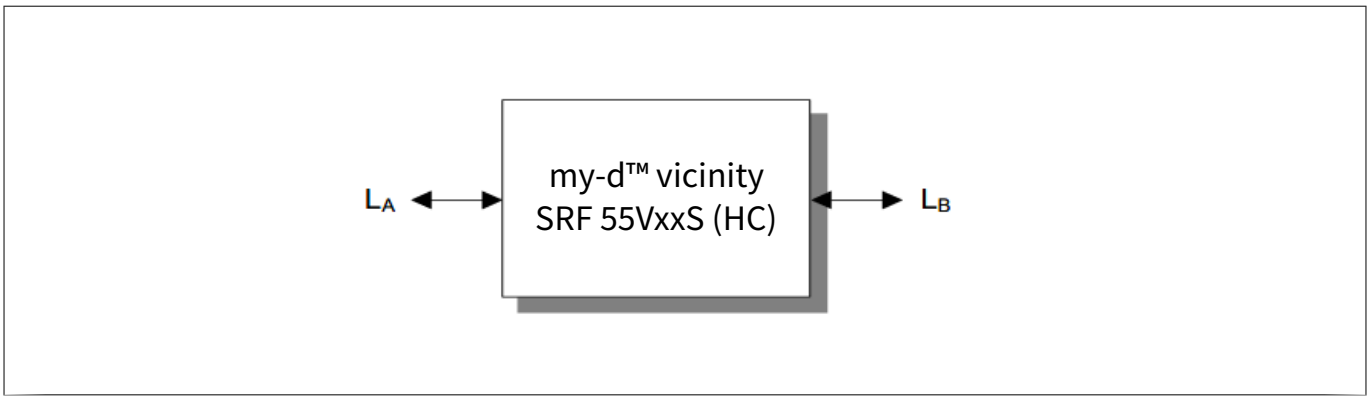


Figure 2 Pad configuration die

Table 3 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 basic security and design flexibility. The my-d™ family of contactless memories supplies the user with different memory sizes and incorporates security features to enable considerable flexibility in the application design.

2.1 Product variants-plain/secure operation, high on-chip capacitance

The my-d™ products are available in the following configurations:

- Plain mode with open memory access
- Secure mode with both memory access controlled by authentication procedures (up to 14 sectors) and plain mode operation (plain sector)
- Additional small tag antenna designs are possible with the HC variant providing a high on-chip capacitance chip for small communication distances

Applications may start with the my-d™ ICs in plain mode operation and individual page locking; for more complex applications various settings in secure mode can be used for multi-user or multi-application configurations.

In plain mode access to the memory is supported by both 4-byte block as well as 8-byte page structure.

In secure mode a cryptographic algorithm based on a 64-bit key is available. Mutual authentication, message authentication code (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 applications.

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

2.2 General memory structure

The fundamental structure of my-d™ vicinity products consists of the following memory structure:

- **User Area** → For storing user data
- **Service Area** → Storing the unique identifier (UID) number and manufacturer data
- **Administration Area** → For storing
  - Sector index (SI), defining either plain or secure memory access
  - Access condition (AC) holding information on access rights (example: Read/write, read-only)

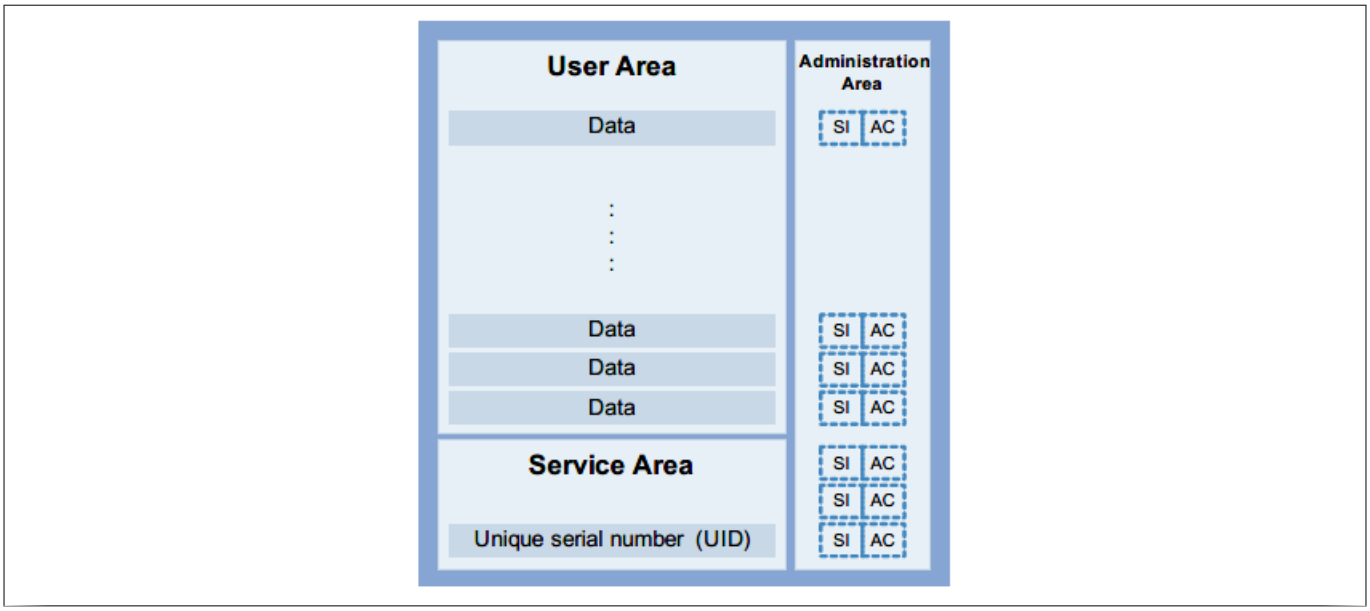


Figure 3 General memory structure of my-d™ products

Communication

The physical contactless interface and communication protocols are defined for vicinity by ISO/IEC 15693. The my-d™ products support a set of standardized commands. Additionally, custom commands are also implemented for example: 8-byte page memory access and optionally authentication (secure variant).

Security

The memory can be accessed without security precautions (i.e: Authentication) in plain mode.

The secure variants additionally require the mutual authentication procedure before memory access is granted.

2.3 Application segments

The my-d™ products are optimized for personal and object identification. Please find the following table for some dedicated examples:

Table 4 my-d™ family product overview

Product	Application
my-d™ move-SLE 66R01P	Public transport, smart posters, NFC device pairing
my-d™ move NFC-SLE 66R01PN	Public transport, smart posters, NFC device pairing
my-d™ move lean-SLE 66R01L	Public transport, smart posters, NFC device pairing
my-d™ move lean NFC-SLE 66R01LN	Public transport, smart posters, NFC device pairing
my-d™ vicinity plain-SRF 55VxxP	Factory automation, healthcare, ticketing, access control
my-d™ vicinity plain HC-SRF 55VxxP HC	Ticketing, brand protection, loyalty schemes, Ski passes
my-d™ vicinity secure-SRF 55VxxS	Ticketing, brand protection, loyalty schemes, access control
my-d™ vicinity secure-SRF 55VxxS HC	Supply chain management, library management, product authentication, amusement ticketing, access control

3 my-d™ vicinity secure-SRF 55VxxS (HC)

The my-d™ vicinity products are based on ISO/IEC 15693 [5] or ISO/IEC 18000-3 Mode 1 [7] standards for contactless vicinity cards. The my-d™ vicinity secure family additionally features my-d™ vicinity commands and my-d™ cryptographic algorithm. The products are targeting personal identification, access and event ticketing, amusement, and entertainment with basic security requirements.

The my-d™ vicinity family focuses on flexible memory and sector configuration.

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 control unit and an authentication unit.

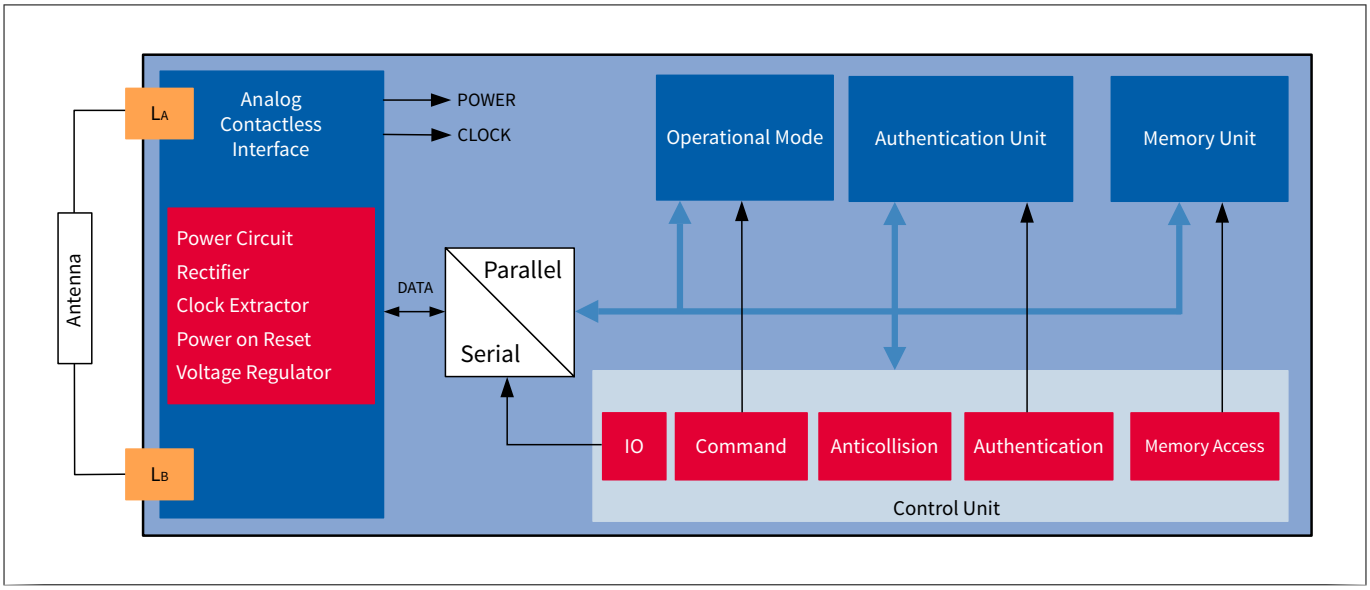


Figure 4 Block diagram of the my-d™ vicinity

- **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 configuration of the my-d™ vicinity. The memory is accessed according to plain or protected mode when the VICC is selected
- **Memory unit**
  - The memory unit consists of up to 1280 bytes of memory organized in up to 128 pages each of 8 users 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
- **Authentication unit**
  - The Authentication Unit generates random numbers, calculates and verifies the message authentication codes (MAC)

3.2 Memory principle

The my-d™ vicinity chip features secure memory access. The user/key memory with its flexible organization 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 accessible plain sector is available for general-purpose use.

Memory is organized in 4 areas:

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

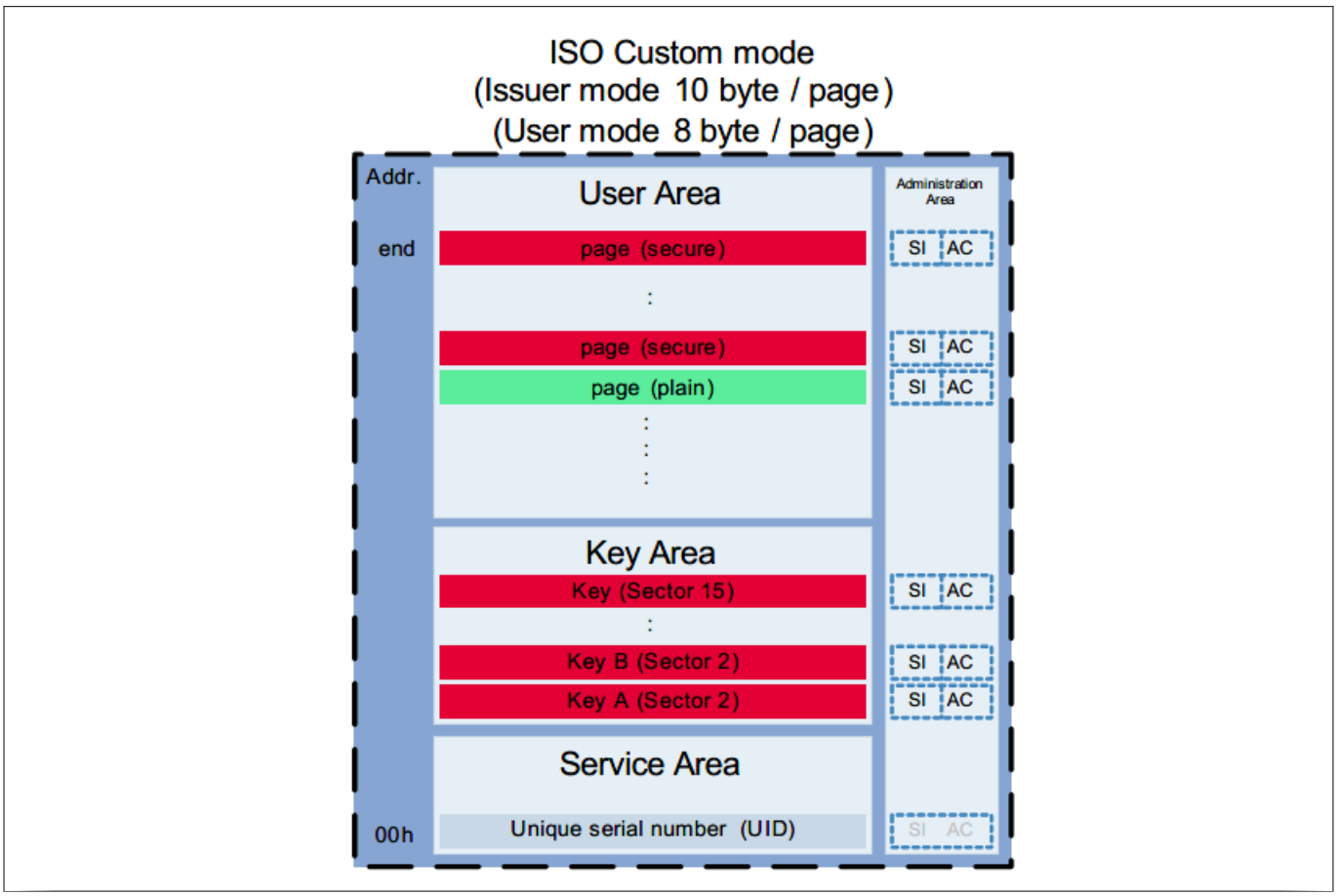


Figure 5 my-d™ vicinity memory organization

The **User Area**[2] stores user data in flexible numbers of sectors, from 0 to 15, with configurable number of pages (up to 124 pages), where sector 0 is the plain sector[3] and sector 1 is reserved for authentication counters.

The **Key/User Area** stores the 8-byte key(s) and user data. Two 8-byte keys per sector with different access rights are available to enable hierarchical key management. The number of key pages depends on how many secure sectors the chip can support.

The **Service Area** stores the UID, manufacturer data, configuration data as well as authentication counter. This information is programmed at the manufacture of the chip and cannot be changed. Data are accessible via ISO custom commands only, except the UID being available also via the inventory command.

2 Pure 'User Area' present only with SRF 55V10S
3 Data in the plain sector are accessible both via ISO optional and ISO custom commands

The **Administration Area** stores 2 bytes of information about page administration (sector index and access condition).

- Sector index (SI) defines plain memory access
- Access condition (AC) holds information on access rights (for example: Read/write, read-only)

The sector index and access condition of each page store each bit non-inverted and inverted to ensure data integrity. Data are accessible via ISO custom commands only

3.3 System overview

The system consists of a host system (that is computer with database), one or more my-d™ vicinity secure or other ISO/IEC 15693 [5] compliant cards and tags (VICC) and an ISO/IEC 15693 [5] compatible contactless reader (VCD) with an antenna.

Operation in protected areas of a my-d™ vicinity in secure mode requires mutual authentication between the card and the reader. To achieve system security, the my-d™ security algorithm has to be integrated into the reader[4].

Optionally, the EasySAM SLF9620 can be used. This device incorporates the security algorithm and a key management system including the diversification of Masterkeys. Additionally AES and TDES is supported enabling data encryption methods. EasySAM is a CC EAL5+ certified product.

To access plain pages on an SRF 55VxxS (HC), the my-d™ security algorithm is not required on the reader.

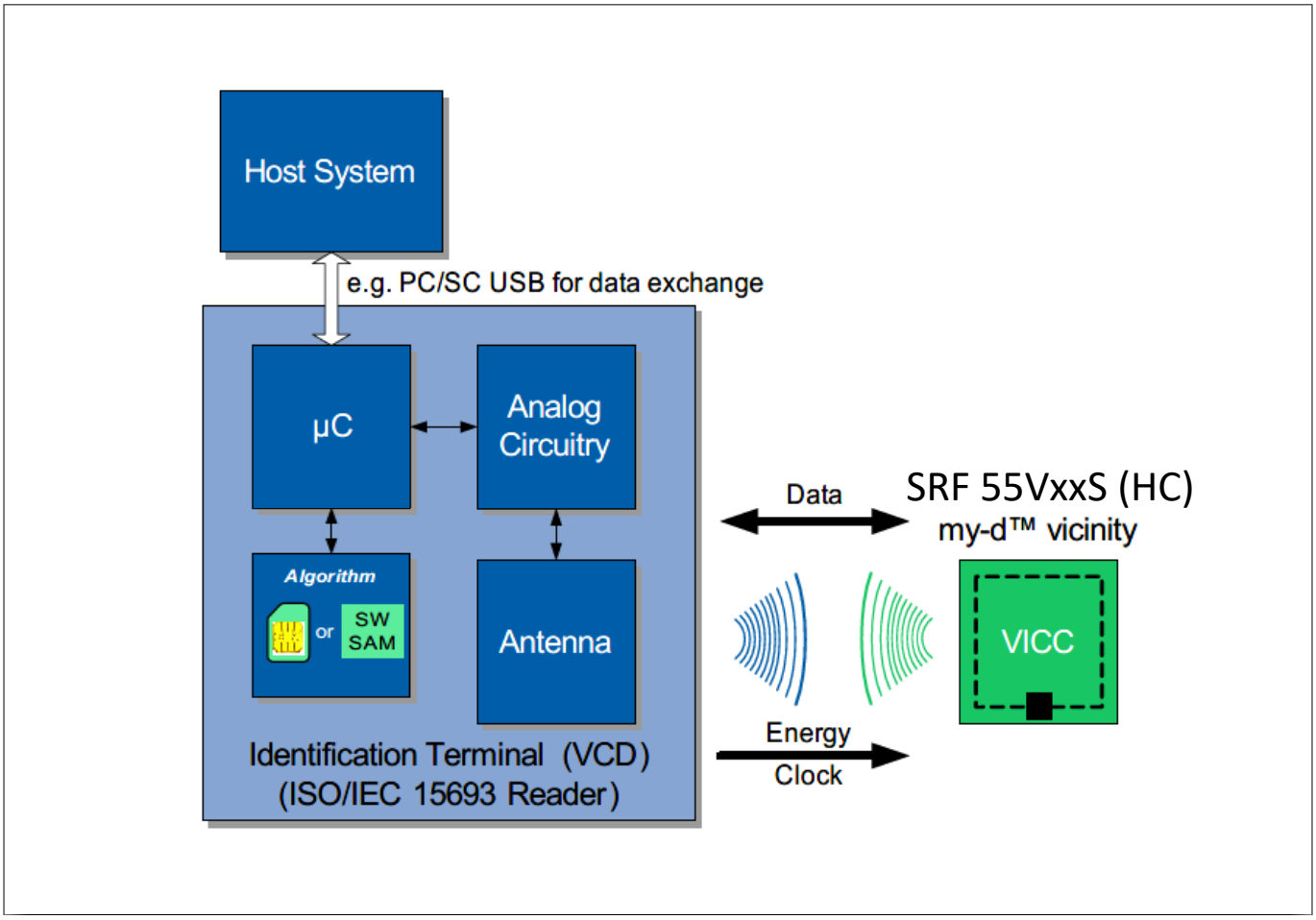


Figure 6 my-d™ vicinity secure RFID system

[4] A license can be obtained from Infineon Technologies for integration of the algorithm into the reader.

3.4 Product versions

ISO/IEC 15693 [5] or ISO/IEC 18000-3 Mode 1 [7] respectively define procedures to identify VICCs being in the reader field. The unique identification (UID) number is used to perform the anticollision procedure identifying each VICC. Then a reader (VCD) is able to recognize the Infineon chip functionality is based on the UID as described.

3.4.1 UID coding

To identify the different types of my-d™ vicinity contactless memories chip type information is coded into the UID according to the format defined in ISO/IEC 15693-3 [6].

The following table briefly describes the values for the different chip versions.

Table 5 UID coding

Type	Byte 7	Byte 6	Byte 5	Byte 4 ... Byte 0
	ISO	IC Mfg code	IC manufacturer serial number	
			Chip ID byte	Unique number
SRF 55V02P (HC)	$E0_H$	05_H	40_H	XX_H XX_H XX_H XX_H XX_H
SRF 55V10P (HC)	$E0_H$	05_H	00_H	XX_H XX_H XX_H XX_H XX_H
SRF 55V02S (HC)	$E0_H$	05_H	50_H	XX_H XX_H XX_H XX_H XX_H
SRF 55V10S (HC)	$E0_H$	05_H	10_H	XX_H XX_H XX_H XX_H XX_H

The 64-bit unique identification (UID) number is stored in the Service Area in page 00_H and programmed by the IC manufacturer. According to ISO/IEC 7816-6 [2] the IC manufacturer code (IC Mfg code) for Infineon is 05_H. The UID is unique for each single IC within the ISO/IEC 15693 world and cannot be changed.

3.4.2 Memory sizes

The my-d™ vicinity contactless memories are available with the following memory sizes:

Table 6 Memory size of my-d™ vicinity (in bytes)

Type	Memory		
	Total	Service Area[1)]	User Area (addressable memory)
			ISO custom
SRF 55V02P (HC)	320	24	232
SRF 55V10P (HC)	1280	24	1000
SRF 55V02S (HC)	320	32	224
SRF 55V10S (HC)	1280	32	992

1) Addressable only via ISO custom command

4 Memory, access rights, and chip states

Memory size and organization describe the memory structure of the my-d™ vicinity secure chip.

Counter values are detailed in Counter format and operations.

Chip mode gives an overview of the chip mode and describes access conditions.

4.1 Memory size and organization

The my-d™ vicinity in secure mode has a memory size of up to 1280 bytes organized in up to 128 pages.

Each page consists of 8 bytes for data storage +2 bytes for administrative purposes. 4 pages ('00_H' to '03_H') are defined as Service Area. In the erased state, the EEPROM cells are read as logical "1", the written state is represented by a logical "0".

Table 7 shows detailed memory organization of the SRF 55V02S on delivery.

Table 7 Memory organization for SRF 55V02S (manufacturer configuration[1])

Memory location	Page address	Byte number within a page								Administration area	
										Sector index	Access condition
		0	1	2	3	4	5	6	7	8	9
Key/User Area	$1F_H$	Key B [15]/User data								59_H	AA_H
	$1E_H$	Key A [15]/User data								59_H	AA_H
	...	...								...	...
	07_H	Key B [3]/User data								59_H	AA_H
	06_H	Key A [3]/User data								59_H	AA_H
	05_H	Key B [2]/User data								59_H	AA_H
	04_H	Key A [2] (transport key)								59_H	99_H
Service Area	03_H	Authentication counter								56_H	55_H
	02_H	AFI[2]	AC_{AFI}[3]		Manufacturer data					55_H	66_H
	01_H		IT[4]	AN[5]	Issuer data/user data					59_H	AA_H
	00_H	Unique identification number								55_H	46_H

1) The values of the access conditions and key index are defined in the testing phase and may change in future revisions
2) AFI byte according to ISO/IEC 15693
3) Access condition for AFI byte
4) Issuer tag
5) Configuration of the authentication counter page

Table 8 shows detailed memory organization of the SRF 55V10S on delivery.

Table 8 Memory organization for SRF 55V10S (manufacturer configuration[1])

Memory location	Page address	Byte number within a page								Administration area	
										Sector index	Access condition
		0	1	2	3	4	5	6	7	8	9
User Area	$7F_H$	User data								59_H	AA_H
	$7E_H$	User data								59_H	AA_H
	$7D_H$	User data								59_H	AA_H
	...	...								...	...
	21_H	User data								59_H	AA_H
	20_H	User data								59_H	AA_H
Key/User Area	$1F_H$	Key B [15]/User data								59_H	AA_H
	$1E_H$	Key A [15]/User data								59_H	AA_H
	...	...								...	...
	07_H	Key B [3]/User data								59_H	AA_H
	06_H	Key A [3]/User data								59_H	AA_H
	05_H	Key B [2]/User data								59_H	AA_H
	04_H	Key A [2] (transport key)								59_H	99_H
Service Area	03_H	Authentication counter								56_H	55_H
	02_H	AFI[2]	AC_{AFI}[3]						Manufacturer data	55_H	$F6_H$
	01_H		IT[4]	AN[5]					Issuer data/user data	59_H	AA_H
	00_H	Unique identification number								55_H	46_H

1) The values of the access conditions and key index are defined in the testing phase and may change in future revisions
2) AFI byte according to ISO/IEC 15693
3) Access condition for AFI byte
4) Issuer tag
5) Configuration of the authentication counter page

Note: The available space of user data in the 'Key/User Area' depends on the number of secure sectors to be supported. For each secure sector two pages from the 'Key/User Area' is used to store the sector keys. Available user data are always 96 pages (768 user bytes), regardless of how many secure sectors were configured.

For more details about access conditions and sector index refer to Access conditions and Sector index.

Table 9 Memory size of my-d™ vicinity secure

Type	Memory		Address space	Number of pages
	User	Administration		
SRF 55V02S	256 bytes	64 bytes	00_H...$1F_H$	32
SRF 55V10S	1024 bytes	256 bytes	00_H...$7F_H$	128

(table continues...)

Table 9 (continued) Memory size of my-d™ vicinity secure

Type	Memory		Address space	Number of pages
	User	Administration		
my-d™ vicinity in secure mode is organized in 4 areas:				
Area	**byte 0 to byte 7**		**byte 8 to byte 9**	
User Area	• Stores user data in a flexible number of sectors with configurable size • Located from page 20_H to page $7F_H$ (Pure 'User Area' present only with SRF 55V10S)		**Administration Area** • Sector index • Access rights • 2-byte per page	
Key Area/User Area	• Stores keys and user data • The number of key pages depends on how many secure sectors the chip shall support • Located from page 04_H to page $1F_H$			
Service Area	• Stores manufacturing data and personalization data as well as the predefined authentication counter • Located from page 00_H to page 03_H			

Note: The SRF 55VxxS (HC) does not support an automatic redundancy check for the data storage. It is recommended to protect important data by the application (for example: Redundant data).

- In issuer mode all 10 bytes are accessible by read and write commands
- In user mode only the 8 data bytes can be read or written with the page-oriented commands, bytes 8 and 9 can only be written using the 'Write Byte' command

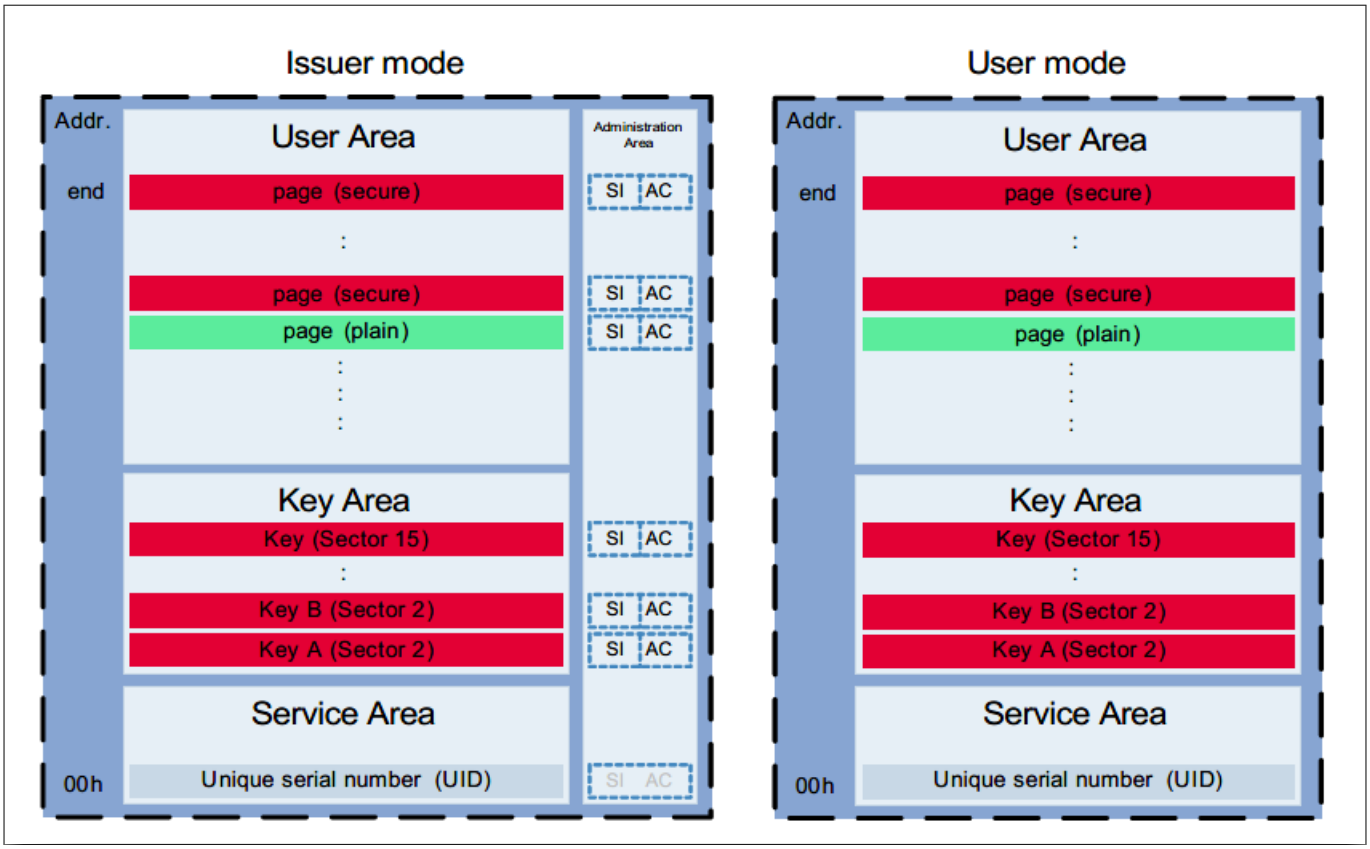


Figure 7 Issuer/user mode

SRF 55VxxS (HC) is delivered with predefined authentication counter and all data secured in sector 2 by a predefined transport key, stored in page 4. The transport key is delivered together with secure chips. The transport key is required to configure the my-d™ vicinity secure for the application.

One or more sectors may be defined to enable several independent applications on the SRF 55VxxS (HC) (multi-application). Each secure sector needs a different key pair. Pages allocated to a certain sector will have an access condition which will be assigned to an appropriate key. Two sectors are mandatory, sector 0 (plain sector) and sector 1 (authentication counter sector). Up to 14 sectors (sectors 2 up to 15) are configurable according to the application requirements.

After a chip is selected, sector 0 will be opened for access. Memory access to pages allocated to this sector is performed without authentication. Depending on the access conditions assigned to those plain pages, data may be read-only, read/write, or restricted write (value counter).

Authentication is mandatory to access pages that are allocated to a protected sector (sector number 2 and above). The authentication will be performed between a card and a reader, using the same secret key on both sides. After successful authentication, a secure sector will be opened and access to the pages belonging to this sector can be performed. In this case, the integrity of all data which are transmitted via the air interface is secured by a message authentication code (MAC). The MAC is generated with the key assigned to the accessed sector.

4.1.1 Service area

The Service Area consists of 4 pages to store:

- **Page 00_H**: Holds the unique identification (UID) number which is individual for each chip
- **Page 01_H**: Holds Issuer tag, authentication counter configuration and Issuer data
- **Page 02_H**: Holds the AFI byte and the access condition for the AFI. Also, manufacturing data are located within this page
- **Page 03_H**: Holds the authentication counter value, which is predefined at delivery for the secure variants. However, one chip could have more authentication counters, and they can be placed elsewhere in the user memory. Pages holding an authentication counter are allocated to sector 1 and have access condition 56_H

4.1.1.1 Unique identification number (page 00_H)

The 64-bit unique identification (UID) number is stored at manufacturing and can not be changed later on. The UID is programmed by the IC manufacturer according to the format defined in ISO/IEC 15693-3 [6].

In the following table please find the detailed definition of the UID as used by Infineon.

Table 10 Description of the UID coding

Bit (63...56)	Bit (55...48)	Bit (47...40)	Bit (39...00)
ISO[1] $E0_H$	IC Mfg code[2] 05_H	IC manufacturer serial number	
		Chip ID byte	Unique number

1) According to ISO/IEC 15693-3 this byte is assigned to $E0_H$
2) According to ISO/IEC 7816-6 the IC manufacturer code (IC Mfg code) for Infineon is assigned to 05_H

Table 11 Chip ID byte (byte 5 of UID)

Bit 47	Bit 46	Bit 45	Bit 44	Bit 43	Bit 42	Bit 41	Bit 40
EEPROM size			Security bit	Chip type			

Table 12 Chip ID byte: EEPROM size, security bit

Bit (47...45)	Bit 44	Meaning	Comment
000_B	-	10 kbit	SRF 55V10P (and SRF 55V10S)
010_B	-	2.5 kbit	SRF 55V02P (and SRF 55V02S)
Other	-	RFU	Reserved for future use
-	0_B	Chip supports plain mode only	SRF 55VxxP
-	1_B	Chip supports secure mode	SRF 55VxxS

Table 13 Chip ID byte: Chip type

Code Bit (43...40)	Meaning	Comment
0000_B	my-d™ vicinity IC functionality	-
$0xxx_B$	Backwards compatible to my-d™ vicinity functionality	Chip supports at least the functionality described in this document
$1xxx_B$	RFU	Used to identify chips that are not backwards compatible to my-d™ products

(table continues...)

Table 13 (continued) Chip ID byte: Chip type

Code Bit (43...40)	Meaning	Comment

Note: A reader or an application shall check the "chip type" bits (UID bits 43…41) to ensure the operation with a chip out of the my-d™ vicinity family. UID bit 43 set to "0" means that at least the chip supports the functionality described in this document. This is a measure to ensure backward compatibility of future ICs of the my-d™ product family with existing infrastructure.

4.1.1.2 Issuer data, issuer tag, and authentication counter configuration (page 01_H)

Issuer data such as expiry date, application identifier, and country code, etc.., are typically stored in page 01_H.

At delivery, this page is allocated to sector 2. For proper operation the issuer page 1 must be protected by assigning it to a secure sector or setting its access condition to read-only after initialization of the chip.

Issuer Tag

Due to the fact, that the user can design the sectors of the chip (that is number of sectors, sector size, and keys to be used), the chip needs to be formatted before use. This is done in the so called 'issuer mode'. After issuing, the chip is then used in its dedicated application. During use in the application, the chip shall be in the 'user mode', where no changes to the sector-setup are accepted. To switch between 'user mode' and 'issuer mode' a special tag inside the service area is used: The issuer tag.

The issuer tag is located in byte 1 of page 1 (high nibble). In issuer mode, the issuer tag is set to A_H. If the issuer tag is changed to any value besides A_H, the user mode is activated after the next power-on reset.

Table 14 Settings of issuer tag

Description	High nibble of byte 1 of page 01_H
Issuer mode	A_H
User mode	Not A_H

Note: The access conditions of page 01_H holding the issuer tag must be set in the field to:

- *Either read-only (AC = 66_H), or*
- *Key protected by authentication (that is: Allocated to a sector 2 to 15 to ensure appropriate system security.)*

Authentication counter configuration

In the current version of SRF 55VxxS (HC), the write of a new value to the authentication counter page of the memory is optional. This option is controlled by a lower nibble of byte 1 of page 1 (AN).

The definition of the memory bits are described in Table 15.

Table 15 Configuration of authentication counter page

Description	Lower nibble of byte 1 of page 1 (AN)
Authentication counter would NOT be written to the memory	A_H
Authentication counter would be written to the memory	Not A_H

4.1.1.3 Manufacturer data and AFI (page 02_H)

The manufacturer page is located on page 02_H. It contains the AFI byte (byte 00_H), the access condition for the AFI (byte 01_H) and data which are programmed and locked at manufacture.

Table 16 Definition of page 02_H

Bit (63...16)	Bit (15...08)	Bit (07...00)
Manufacturer data	AC_{AFI}	AFI byte

Table 17 Definition of the AFI byte

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
As defined in ISO/IEC 15693				-	EAS bit	-	-

4.1.1.4 Authentication counter (page 03_H)

By default page 03_H contains the authentication counter (for more details refer to Authentication counter format) which is mandatory to operate the chip in a secure mode.

It provides a higher security level by changing the content of the counter during each authentication.

The authentication counter is always allocated to sector 1 and is written to page 03_H during the ICs testing phase. Further authentication counter can be defined by allocating a page to sector 1 and by applying the counter format.

The authentication counter can neither be read nor written with the standard custom commands.

Access is possible with authentication commands only.

During step 3 of the authentication process (see also Authentication) VCD will return a new authentication counter value and a new random number to my-d™ vicinity. The my-d™ vicinity will then perform a "restricted write authentication" and write the new authentication counter value to the dedicated page in the memory.

Note: There is no change in the way authentication process works, see Authentication. If the write to authentication counter page is disabled, the authentication counter is never changed in the memory. VCD should still send the "restricted write authentication" command in step 3 of the authentication. Upon receiving this, if the lower nibble of byte 1 page 1 is A_H, my-d™ vicinity ignores the write/erase process to the authentication counter in the memory. As for the long authentication process (see Authentication) after authentication step 3, the my-d™ vicinity will again return the new authentication counter to the VCD. In this case, the authentication counter being sent back is always being re-read from the memory.

4.1.2 Key/user area

Pages 04_H to $1F_H$ (31_D) are either key pages or user-data pages. The mandatory keys for the authentication of protected sectors are stored in this area. Up to 14 pairs of keys equal to the number of protected sectors may be defined in the key area.

The ‘Key/User Area’ can be structured in one or several sectors defined by the user during the issuing process. For every new sector, a new pair of keys has to be defined.

A sector consists of one or several pages with the same sector index. A page always belongs to a sector. Access to a page is defined by the associated access conditions of the page. The sector index of the page is bound to the sector number and references to the authentication keys of this sector. The data format of the page can be either counter-format or 8-byte data (for more details about counter-format refer to Counter format and operations).

Key pages have a special ‘write only’ access condition, so that keys may be overwritten with new keys, but keys never can be read out of the memory (for more details about access conditions refer to Access conditions).

Each pair of keys (key A and key B) for one sector is stored in sequence starting from page 04_H and ending at $1F_H$ if all keys are required. Key A is always stored in even pages and key B is always in the subsequent odd page.

Table 18 Key number hard-wired to pages and allocated sector

Pages of the key A - B	04_H-05_H	06_H-07_H	08_H-09_H	$0A_H$-$0B_H$	$0C_H$-$0D_H$	...	$1C_H$-$1D_H$	$1E_H$-$1F_H$
Allocated sector number	2	3	4	5	6	...	14	15
Key A and B number	2	3	4	5	6	...	14	15
Corresponding sector index	59	5A	65	66	69	...	A9	AA

For more details about connection between sector number and sector index refer to Sector index.

After the definition the number of sectors, the size of each sector, and the corresponding keys, the remaining pages in the key area can also be used as data pages. These pages **must not** have the access conditions ‘write only’ or will be interpreted as key.

Tip: It is recommended to allocate a key page to sector 2…15 to protect the page against unauthorized access.

4.1.3 User area

The pure ‘User Area’ exists only with SRF 55V10S, the pages from 20_H to $7F_H$ (32_D to 127_D) are reserved for user data only (additionally, pages not used for keys in the ‘Key/User Area’ may store user data too).

The ‘User Area’ can be structured in one or several sectors defined by the user during the issuing process. For every new sector, a new pair of keys has to be defined.

A sector consists of one or several pages with the same sector index. A page always belongs to a sector. Access to a page is defined by the associated access conditions of the page. The sector index of the page is bound to the sector number and references to the authentication keys of this sector. The data format of the page can be either counter-format or 8-byte data (for more details about counter format refer to Counter format and operations).

4.1.4 Administration area

To each page, two administration bytes are assigned. One byte holds the access conditions (for more details refer to Access conditions) and other byte holds the sector index of the page (for more details refer to Sector index).

During the process of formatting the memory, the user writes the value of these 2 bytes. This is called the ‘issuing process’. All pages with the same sector index belong to the same sector and can only be accessed with the dedicated pair of keys belonging to that sector.

This structure allows a very flexible key handling, establishing a key hierarchy and flexible memory access for each page.

The access condition byte and the sector index byte are corruption protected. Each bit in each byte is stored non-inverted and inverted. That induces each nibble of each byte has the next value: 5, 6, 9, and A (refer to Value counter format for definition of redundant bits).

4.2 Chip mode

This section describes the two chip modes, which are determined by the memory content.

4.2.1 Issuer mode

The card issuer uses this mode to prepare a new and blank card for later use. In this mode, the desired initial user data as well as the card sectorisation is programmed into the memory.

When an issuer mode, data is read and written 10 bytes at a time. The whole row inside the memory is affected at once. (for the memory map of the my-d™ vicinity secure refer to Table 7 and Table 8) writing 10 bytes at once allows quick access to the user data (8 bytes) as well as the access condition (1-byte) and the sector index (1-byte) of the addressed page within single read and/or write commands.

On delivery, the chip is in issuer mode. The memory is key protected by a transport key and is organized in one user sector (sector 2). For all pages of sector 2, the access conditions are set to read/write (AC = AA_H) with the transport key defined in the testing phase.

This means, after power up sector 0 is opened and all pages belonging to sector 0 (pages with sector index 55_H) are readable. After authentication with the transport key, all other pages belonging to sector 2 (pages with sector index 59_H) are also readable and writable.

While in issuer mode, read access to all pages with access conditions allowing a read independent of plain or protected to be granted. (Keys are never readable!) write operations are only possible to the already opened sector (sector 0 for plain, or according to secure sector respectively). The number of sectors is defined by the number of independent applications the chip shall support. Each application (an application herein is equivalent to a sector) needs a different key pair that allows being secure regardless to another application. The definition of number and size of sectors is done by setting byte 8 of each page according to Sector index.

The issuer mode is terminated with a write command setting the high nibble of byte 1 on page 01_H to a value 'Not A_H' (see Table 14). In consequence, the chip is then in user mode.

By denying write access to page 01_H, an unauthorized change to the issuer tag is prevented. Using hierarchical keys to obtain access to the issuer page allows only dedicated VCDs to alter the issuer tag.

4.2.2 User mode

The user mode is provided for the normal chip operation. In user mode, read/write commands affect only the 8 bytes of user data inside a page.

Additionally, the command 'Write Byte' (for more details refer to Write Byte command) allows modifying access conditions and key indexes, if the page has to write access at all and if the page is not a key page.

Note: In user mode, a key can be changed after authentication to the sector the key is in. Keys may only be overwritten, but never read out.

4.2.3 Selection of a sector

In ISO/IEC 15693-3 [6], the selection procedure of a VICC is defined. After a successful select command, the sector 0 is opened by default. The memory commands can be executed within sector 0 according to the access conditions of each page (see Access conditions). When operating within the sector 0 (plain sector) all commands are sent without a message authentication code (MAC) extension.

To open a secure sector it is required to start an authentication sequence and therefore the key of that sector must be known to the VCD (see Authentication). After successful authentication, the applied sector is opened and protected memory operations can be executed. Protected memory commands are the same as standard memory commands, but each command has a 4-byte MAC extension in the request data and the VICC also sends a MAC extension in the response data for each command call. As long as the protected sector is opened, all data exchange is secured by the attached MAC values.

The MAC value for each command is calculated by the VCD, using a secure access module (SAM): The MAC values being sent back from the VICC is calculated within the VICC itself.

This MAC protected data transmission provides a very high-security level (for more details about authorizing a sector refer to Authentication).

It is not possible to open more than one sector simultaneously. In case of a communication error, that is reception of a wrong MAC, the operation is denied, the sector is closed and sector 0 is open again.

When a secure sector is opened and data from the plain sector shall be read next, log out from the current secure sector must be performed. There is no special command for the log out, this is simply done by performing an invalid authentication to an arbitrary secure sector. As a consequence, the open secure sector is closed and sector 0 (plain sector) is open again.

4.2.4 Access conditions

Each sector consists of one or more pages. Each page has individual access rights, which apply when a sector is open. For each key of the two keys per sector, the following access rights are defined:

- Read-only
  The page can be read but not written
- Write
  The page can be read and written
- Read and restricted write
  The page can be read but counter rules[5)] apply for writing
- Write only
  This access right is used for the key area only

Each page has two access rights which are activated according to the key which has been used to open the sector which belongs to the page. This allows the implementation of a multilevel security structure.

The access conditions for a page are described in Table 19 and Table 20. Access conditions are stored in byte 9 of each page

Table 19 Access conditions byte, key-dependent (byte 9 of each page)

Bit number	7	6	5	4	3	2	1	0
Description	AC for key B				AC for key A			

5 Writing is only done if the new value is lower than the actual value

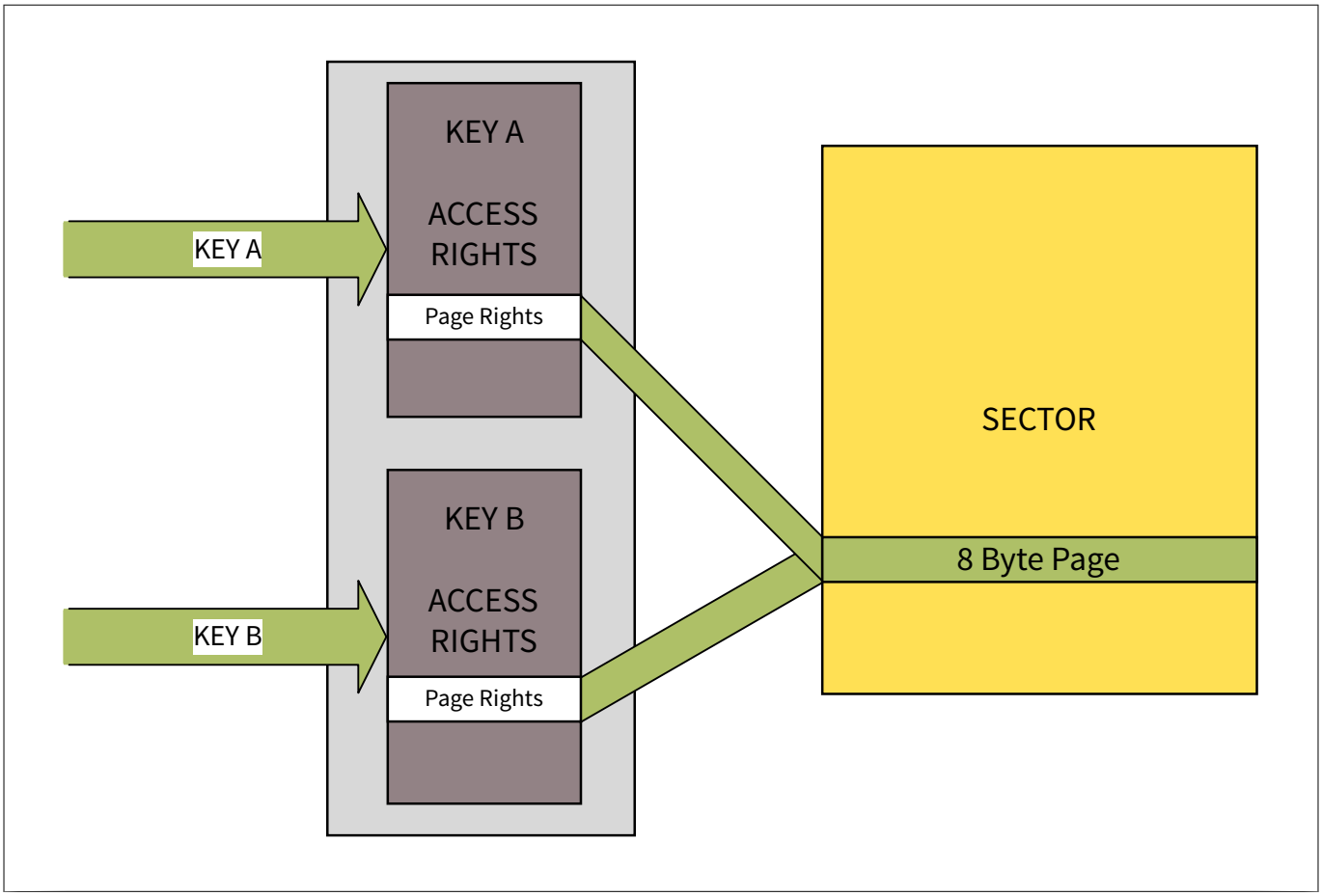


Figure 8 Access condition and keys

Byte 9 of each memory page is used to hold the access condition byte for the page depending on the key used during the authentication procedure.

Table 20 Access conditions and rights

Access condition	Access rights		Comments
	Key B	Key A	
'55_H'	Read/restricted write	Read/restricted write	Counter
'56_H'	Read/restricted write	Read only	Counter
'59_H'	None	Write only	Key[1)]
'$5A_H$'	Read/restricted write	Read/write	Counter
'65_H'	Read only	Read/restricted write	Counter
'66_H'	Read only	Read only	User data
'69_H'	None	Write only	Key[1)]
'$6A_H$'	Read only	Read/write	User data
'95_H'	Write only	None	Key[1)]
'96_H'	Write only	None	Key[1)]
'99_H'	Write only	Write only	Key[1)]
'$9A_H$'	Write only	None	Key[1)]

(table continues...)

Table 20 (continued) Access conditions and rights

Access condition	Access rights		Comments
	Key B	Key A	
'$A5_H$'	Read/write	Read/restricted write	Counter
'$A6_H$'	Read/write	Read only	User data
'$A9_H$'	None	Write only	Key[1)]
'AA_H'	Read/write	Read/write	User data
Any other value	None	None	Invalid AC

1) The access conditions for keys only apply if the indexed page is located in the Key Area, the values are mandatory to define the relevant page as a key. A key access right of a page in the User Area locks the page for further access.

In case where non-protected sectors are involved (sector 0 and sector 1), access conditions for key A are verified only.

The access condition 'write only' does only apply for key definitions. If only one key has this access right, the other key can not be used for authentication to that sector.

When in user mode, access conditions may be changed by using the command 'write byte' (for more details refer to Write Byte command), if the page has to write access at all and if the page is not a key page.

Note: For pages allocated to sector 0 (that is plain mode) only access conditions read-only (AC = 66_H), read/write (AC = AA_H) and read/restricted write (AC = 55_H) is meaningful.

Change of access conditions of a page is possible with read/write access only.

4.2.5 Sector index

The memory of SRF 55VxxS (HC) can be structured in several sectors. Each sector consists of several pages. A page is allocated to a sector by programming the "sector index" accordingly. This sector index refers to the (pair of) keys in the key area. Using the dedicated keys of that sector is mandatory to open a protected sector. All sectors besides sector 0 (plain sector) and sector 1 (authentication counter) are protected. Pages within sector 0 are not key protected and are to be opened without authentication.

Byte 8 of each memory page is used to hold the sector index. Sector 0 is opened after the power-up of the VICC. This sector is defined as a plain sector, which means IC commands can be performed on sector 0 pages without authentication.

Each of the keys has also a sector index. This means, that all or part of the keys can be grouped into a sector or more sectors as well. Therefore this makes it possible to authenticate a key sector by its own key or by another key and build hierarchical key management.

Table 21 Sector index byte

Sector number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sector index	55_H	56_H	59_H	$5A_H$	65_H	66_H	69_H	$6A_H$	95_H	96_H	99_H	$9A_H$	$A5_H$	$A6_H$	$A9_H$	AA_H

Note: The plain sector (no 0) has always sector index of 55_H. Plain data must be allocated to sector 0, secure to sectors 2...15.

4.3 Counter format and operations

Each page of the data area may be defined as a counter page. A counter page is a single 8-byte page which is initialized with two 4-byte counters and the access conditions set accordingly.

Counter data are accessible via ISO custom commands only.

4.3.1 Counter mechanism

The concept incorporates that a counter page is divided into two counters with one counter being valid where the other is normally 00_H, 00_H, 00_H, 00_H. This principle allows supporting an anti-tearing mechanism.

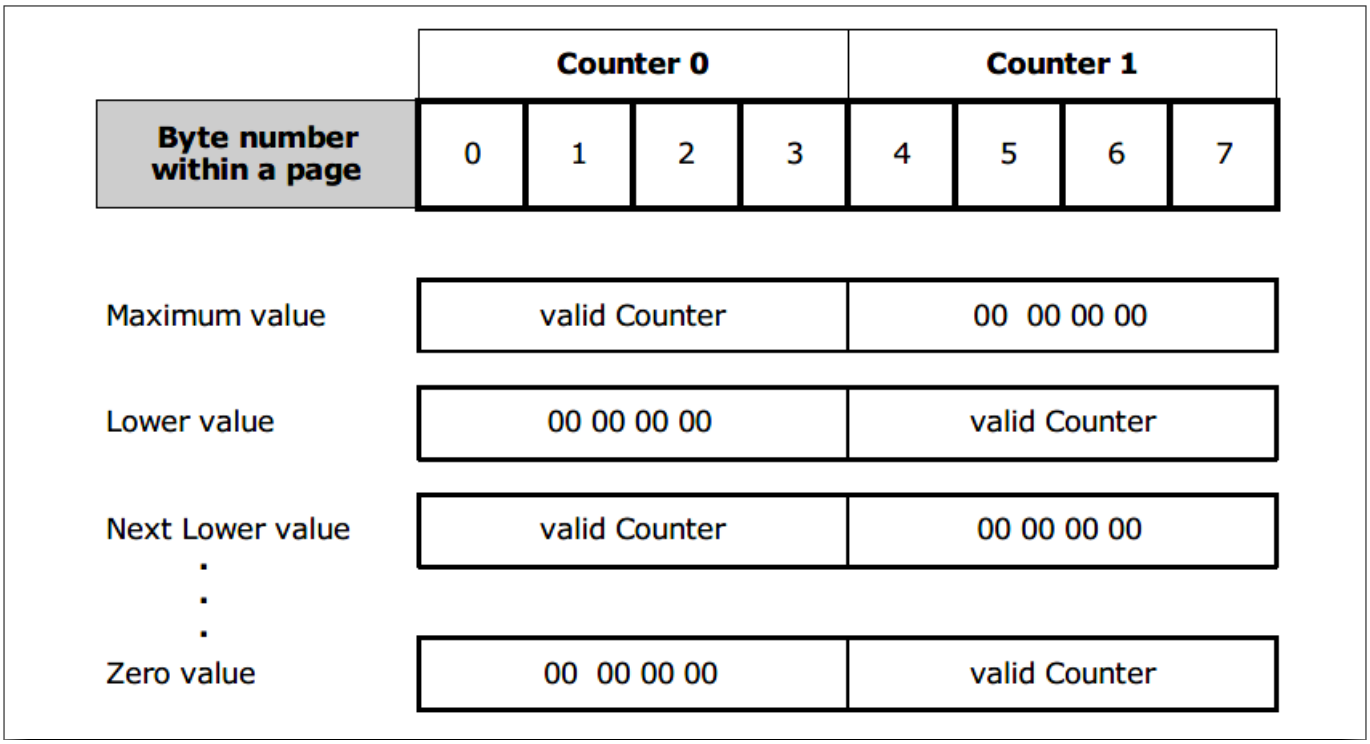


Figure 9 Counter mechanism

So a normal decreased counter page always contains 4-byte with a valid counter value and the other 4-byte set to '00_H, 00_H, 00_H, 00_H'. Cases with 4-byte containing a valid counter and the other 4-byte with any value indicate an aborted counting operation, for further information please refer to Anti-tearing.

Counting is done by transmitting counter data fulfilling the condition "lower than previous value".

- Debit the value counter
  - Using the 'Restricted Write' or 'Restricted Write and Reread' command. With each successful command SRF 55VxxS (HC) switches from counter 0 to counter 1 and vice versa
- Lower byte/LSB is transmitted first
- Authentication counter

Used by the "Authenticate" command; the authentication sequence requires a new value of the authentication counter in the command transmitted by the VCD.

The counter data must fulfill a dedicated counter format to ensure data redundancy.

4.3.2 Anti-tearing

SRF 55VxxS (HC) supports the detection of an interrupted counting operation due to the concept of using two counters on a page defined as a counter page.

A malfunction of the counting may be caused by a power loss during the update of the counter data stored in the EEPROM. Due to physical characteristics, the change of EEPROM data requires an erase/write cycle. So, the chip needs several intermediate states during a counter update. Especially during the erase and write also random data may appear because of the physical process.

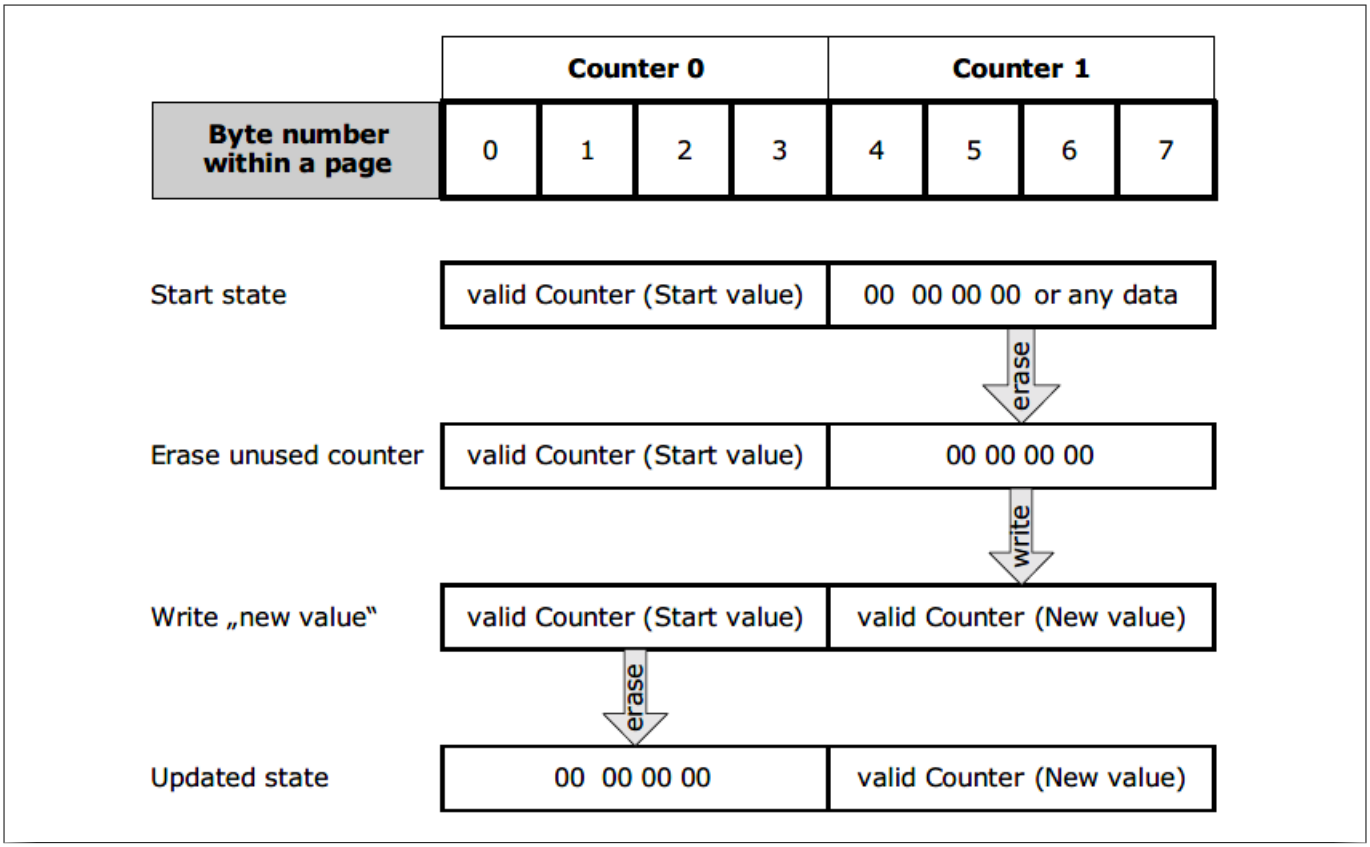


Figure 10 Intermediate counter states

So a normal counting operation looks as follows:

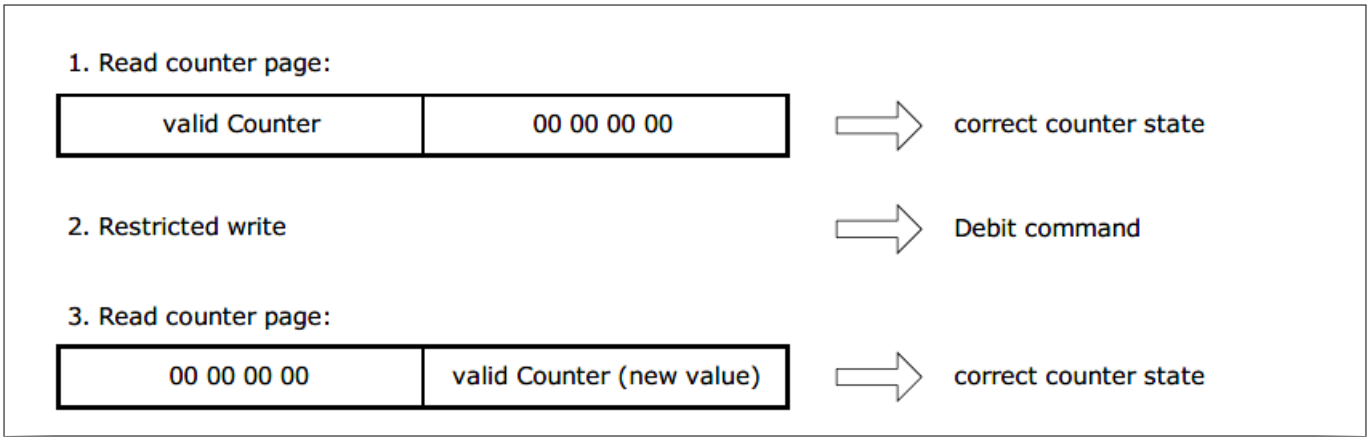


Figure 11 Counter update sequence

If the initial read of a counter page looks like the following operation, this indicates a previously interrupted counting operation:

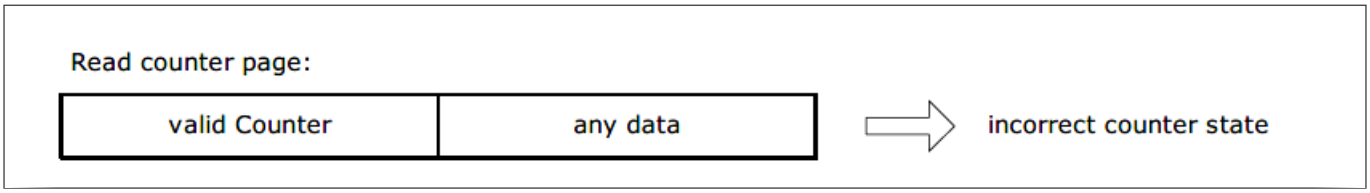


Figure 12 Incorrect counter state

The anti-tearing mechanism is controlled by the VCD software and is based on the two value counters per counter page. It ensures that in case of power loss at least one correct value is stored in the counter.

The following procedure is executed by the **VCD**:

1. **Determine the actual counter**: Read the value counter page with a 'Read' command and separate counter 0 from counter 1
   - Case a) Valid counter is the actual counter

     Only one counter data is valid (the other holds either all bits set to zero or a corrupted counter format).
   - Case b) Higher value is actual counter

     The card was torn during the last operation: Both counters have a valid counter format.
2. **Calculate the new counter value**: New counter value **must** be lower than the actual counter value and has to be sent to the chip in the correct counter value format
3. The **new counter value is programmed** to the non-actual counter with a 'Restricted Write' or 'Restricted Write and Reread' command to the SRF 55VxxS (HC)
4. Finally, the old counter value (actual counter) is cleared by the chip (all bits set to zero) and the new counter value becomes the new actual counter

Programming and clearing the counter value pages are processed in one EEPROM erase/write cycle and one EEPROM erase operation. First, the invalid counter value (or lower value) will be erased and programmed with the new value. Then the old valid value will be erased from all zeroes. If there is any interrupt (example: Power loss etc.) at least one counter will have a valid format and data. With this check and backup procedure, a reader can always determine if the 'Restricted Write' command has been performed correctly or not. Additionally, at least the old counter data is always available until the new counter data is programmed.

4.3.3 Value counter pages

Each page in the data area of the memory allocated either to a plain or a secure sector may be configured and used as a counter value page. A counter value page is a single 8-byte page that is programmed with a dedicated counter format (see Figure 13 and the following explanation). The counter can hold values from 0 to 65535.

4.3.3.1 Value counter format

SRF 55VxxS (HC) supports a value counter with a range of 2^{16} (0 to 65535) units.

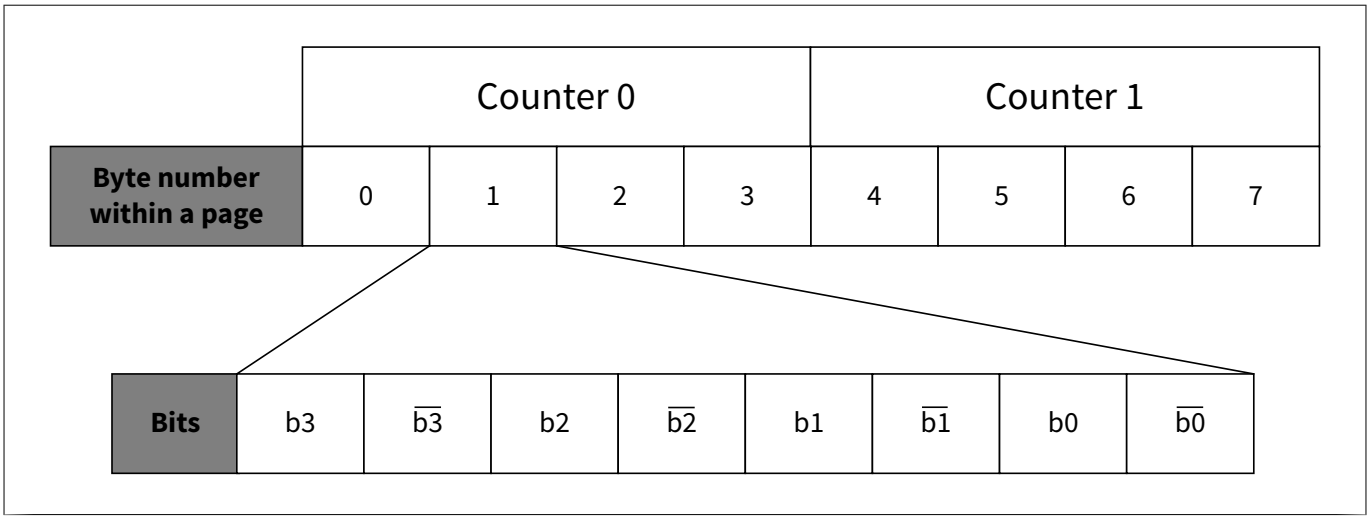


Figure 13 Data structure of a value counter page

The counter page consists of two counters of 4-byte length to support backup/anti-tearing. For data security and integrity reasons, each data bit is stored twice: Non-inverted and inverted (see Figure 13). One 2-byte value is therefore extended to a 4-byte value for example the one-byte value 0000 0001_B (01_H) is extended to 0101010101010110_B (5556_H). The two counters stored on a counter page (counter 0 and counter 1) must always have different values. This counter format is mandatory to perform the on-chip redundancy and anti-tearing functionality included in the 'Restricted Write' command for the counter block as well as a data integrity check (see Anti-tearing).

4.3.3.2 Initialization of a value counter page

The following steps have to be performed to initialize a page as value counter:

- Initialize the counter value page using the 'Write' and 'Write Byte' commands
- The data to be written to the page must have a counter format (see Value counter format)
- The access condition has to be set to read/restricted-write (see Access conditions)

Example:

To set the counter value 1010_H to one of the plain pages in user memory, an issuer has to:

- Write 8 bytes with the 'Write' command; in this case, the data will be '55 56 55 56 00 00 00 00_H'
- Set the access condition for this page to 55_H with the 'Write Byte' command

Then, the value counter page is ready to be used and can be performed by any 'Restricted Write' command.

- Use the 'Restricted Write' command to decrement the value by 1 by sending $100F_H$ in counter value format 'AA 55 56 55_H', low significant byte first

4.3.4 Authentication counter format

The authentication counter limits the number of accesses to the protected sectors to a predefined value. Therefore, the counter can only be decremented but not reloaded. Within every authentication procedure, the counter is decremented by an application-defined value. Access to protected sectors requires a valid authentication counter in sector 1. If the authentication counter becomes zero or if no decrement is possible with the applied decrement value, an application using this counter can not authenticate protected sectors anymore.

For authentication of different sectors, the same as well as different authentication counters can be used. But all authentication counters must be referenced to sector 1 in the sector index.

Concerning the byte and value organization, the authentication counter resembles the value counter. The bit redundancy of the 4-byte authentication counter is reduced due to an extended value range to 2 bits per byte (only the low nibble is corruption checked; see Figure 14).

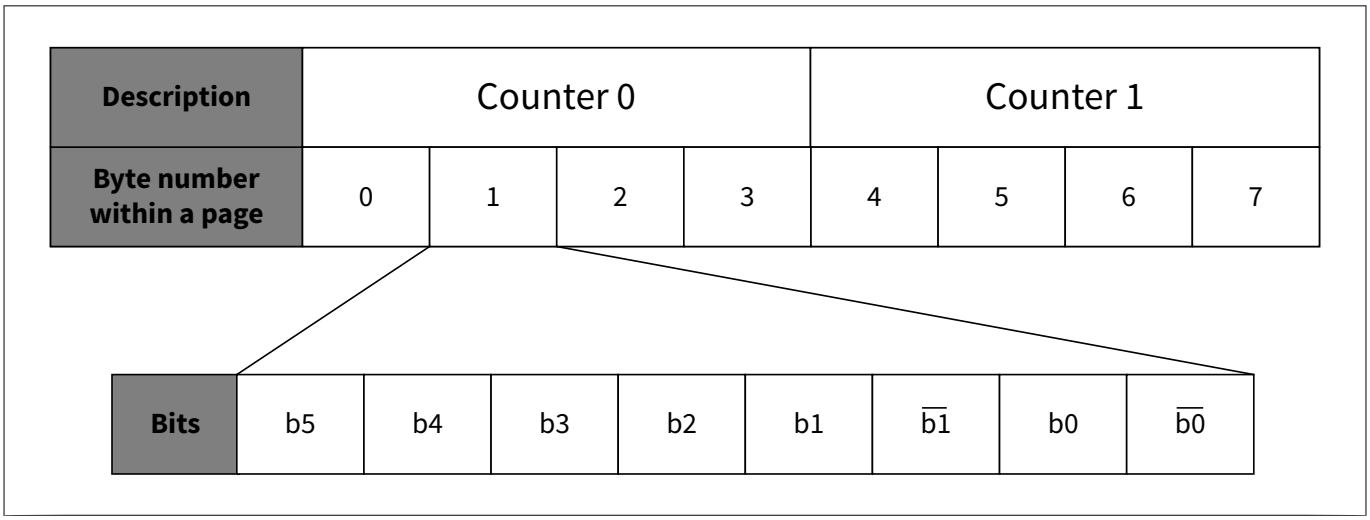


Figure 14 Bit redundancy and arrangement of authentication counter bytes

This dedicated counter format with 6 value bits in each byte provides an extended counter range of 0 to 2^{24} -1 (= 16777215).

During the authentication sequence, the VICC sends first the 8-byte value of the authentication page. The VCD has to separate counter 0 from counter 1 and select the actual authentication counter. Then, the VCD defines the new value of the authentication counter according to the dedicated value and sends this 4-byte authentication counter back to the VICC.

Within each authentication process, depending on the configuration of the authentication counter page (for more details refer to Authentication counter (page 03_H)), the authentication counter is replaced with a specific command by a lower value than the actual value (refer to Authenticate B: Authentication step 3).

Modifying the authentication counter, together with the use of random number and sector index, makes data and MAC, exchanged during two subsequent authentications, different.

The initialization of an authentication counter must be done by the Write command (access conditions have to be set accordingly). The VCD software is responsible for the correct counter format sent either during the initialization or authentication procedure.

5 Frames and command set

The communication from VCD to VICC and from VICC to VCD is according to ISO/IEC 15693. The standard defines the following command types:

- Mandatory commands
- Optional commands
- Custom commands
- Proprietary commands

5.1 ISO command frame

The ISO command frame for the communication from VCD to VICC is according to ISO/IEC 15693-3 [6].

The request format consists of the following fields:

- Flags
- Command opcode
- Parameter field
- Data field
- CRC

These fields are embedded into the general request format and are enframed by a start of frame (SOF) and an end of frame (EOF).

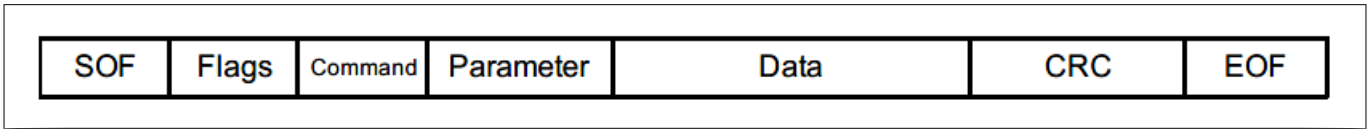


Figure 15 General request format

Flags and parameter settings are defined in ISO/IEC 15693-3 [6].

5.1.1 Supported ISO/IEC 15693-3 commands

The following commands are implemented in the my-d™ vicinity:

Table 22 my-d™ vicinity supported ISO/IEC 15693-3 commands[1)]

Command code	Command type	Function	Available modes[2)]
01_H	Mandatory	Inventory	U
02_H	Mandatory	Stay quiet	A
20_H	Optional	Read single block	A/S/U
21_H	Optional	Write single block	A/S/U
22_H	Optional	Lock block	A/S/U
23_H	Optional	Read multiple blocks	A/S/U
25_H	Optional	Select	A
26_H	Optional	Reset to ready	A/S/U
27_H	Optional	Write AFI	A/S/U
28_H	Optional	Lock AFI	A/S/U

(table continues...)

Table 22 (continued) my-d™ vicinity supported ISO/IEC 15693-3 commands[1)]

Command code	Command type	Function	Available modes[2)]
$2C_H$	Optional	Get multiple block security status	A/S/U
$A0_H$	Custom	my-d™ vicinity specific command set	A/S/U

1) Read single block, Write single block, Lock block, Read multiple blocks and Get multiple block security status commands can be applied only if the page in secure memory is plain (sector index is set to 55_H, meaning sector 0) and the chip mode is in user mode. Commands will be executed on 4-byte blocks. Depending on the block access condition and the command that is sent to the my-d™ vicinity, the data will be read/written to one or more blocks. For the available address range see chapter Memory Organization in [1]

2) U → non-addressed, A → addressed, S → selected according to ISO/IEC 15693-3

5.1.2 Error codes

To ease the system integration, the following listed error codes (as defined by ISO/IEC 15693) must be implemented:

Table 23 Error codes

Error code	Meaning	Type
$0F_H$	Error with no information given or a specific error code is not supported	ISO
01_H	The command is not supported, that is command code is not recognized	ISO/custom
10_H	The specified block/page is not available (does not exist)	ISO
11_H	The specified block is already locked and it cannot be locked again	ISO
12_H	The specified block is locked and its content cannot be changed	ISO
$A0_H$	Error during authentication or the wrong MAC	Custom
$A1_H$	Access denied for example: • Read from secure pages without authentication • The page is locked and its content cannot be changed	Custom

5.1.3 Inventory

The transponder performs an anticollision sequence after receiving a valid inventory request.

Table 24 Inventory request format

SOF	Flags	Inventory command opcode	Optional AFI	Mask length	Mask value	CRC16	EOF
-	8-bit	8-bit	8-bit	8-bit	(0 to 64) bit	16-bit	-

The transponder response contains the data storage format identifier (DSFID) and unique identifier (UID) number.

Table 25 Inventory response format

SOF	Flags	DSFID	UID	CRC16	EOF
-	8-bit	8-bit	64-bit	16-bit	-

Please refer to the ISO/IEC 15693-3 [6] standard for more details on the request and response formats.

5.1.4 Stay quiet

After receiving a valid stay quiet request the transponder enters the quiet state. There is no response to a stay quiet command.

Table 26 Stay quiet request format

SOF	Flags	Stay quiet command opcode	UID	CRC16	EOF
-	8-bit	8-bit	64-bit	16-bit	-

Please refer to the ISO/IEC 15693-3 [6] standard for more details on the request and appropriate state transitions.

5.2 Specific commands of my-d™ vicinity

The my-d™ vicinity specific commands are embedded in the data section of the ISO command frame.

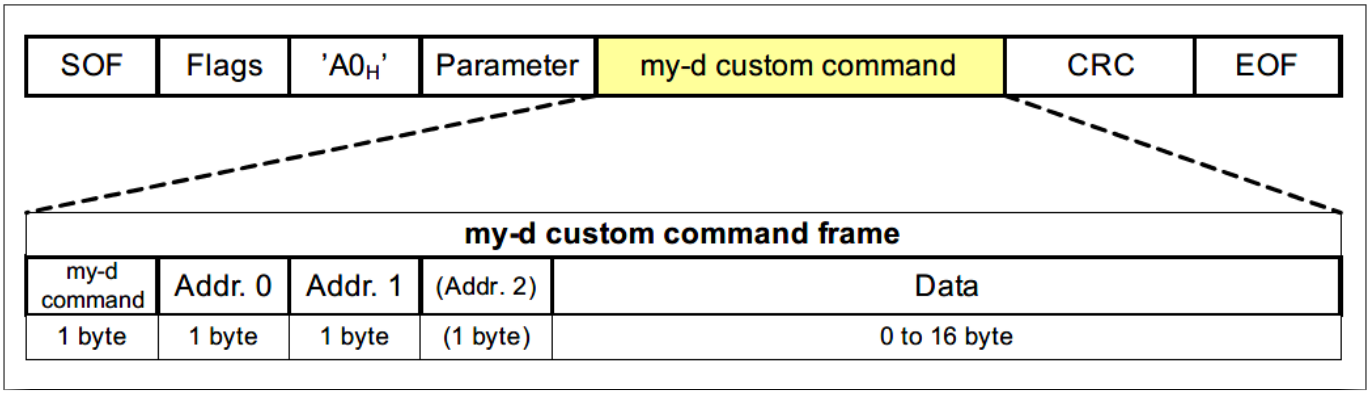


Figure 16 my-d™ vicinity specific commands

Table 27 ISO command frame with embedded my-d™ custom command frame

Field	Value	Description
SOF	Start of frame	According to ISO/IEC 15693-3 [6]
Flags	-	According to ISO/IEC 15693-3 [6]
ISO command code	$A0_H$	Used to indicate my-d™ custom command
Parameter	05_H [UID]	IC manufacturer code for Infineon + optionally UID of the VICC
my-d™ custom command	As defined for my-d™	For more details please see the following
Address 0	Page address	Page address of my-d™ vicinity
Address 1	00_H	Reserved for future use
Address 2	Byte address of a page	Only for 'Write Byte' command
CRC	Cyclic redundancy check	According to ISO/IEC 15693-3 [6]
EOF	End of frame	According to ISO/IEC 15693-3 [6]

- Timing of VICC response according to ISO/IEC 15693
- Error handling according to ISO/IEC 15693
- Addr.1 must be '00_H' (reserved for future use)
- Addr.2 for the 'Write Byte' command only, must not be sent with all other commands

Note: The my-d™ custom command can be applied to 8-byte my-d™ pages only. Depending on the block access condition the data will be read/written to/from a page (for the available address range refer to Memory size and organization).

Command list of my-d™ vicinity secure:

After the "power-on", memory operations can be executed. Before each command execution, the key index and the access conditions are checked. If the sector is protected, authentication has to be executed before. Besides sector 0 and sector 1, all sectors are protected that is an authentication has to be executed to get access to the pages of the sector.

Table 28 Command codes of my-d™ vicinity secure

my-d™ vicinity command[1]	Code	Comment	T1 [µs] [2] [3]
Read	10_H	Reads one page of the memory and transmits it to the VCD	320
Write	30_H	Writes data to the specified page	$4352/f_c + n * 4096/f_c \pm 32/f_c$
Write and Reread	$B0_H$	Write data to the specified page and read the page after writing the data; page data is transmitted to VCD instead of ACK	$4352/f_c + n * 4096/f_c \pm 32/f_c$
Restricted Write	00_H	Dedicated write command to counter pages; the counter is only overwritten if the new value is lower than the old one and counter format set	$4352/f_c + n * 4096/f_c \pm 32/f_c$
Restricted Write and Reread	80_H	Restricted Write command to decrement counter data; after writing the counter is read again and the data is transmitted instead of an ACK	$4352/f_c + n * 4096/f_c \pm 32/f_c$
Authenticate A	20_H	Initializes the authentication sequence, reads the authentication counter and creates random number; a successful authentication replies an ACK	$4352/f_c + n * 4096/f_c \pm 32/f_c$
Authenticate B	$A0_H$	Initializes the authentication sequence, reads the authentication counter and creates random number; a successful authentication replies the reduced authentication counter page	$4352/f_c + n * 4096/f_c \pm 32/f_c$
Write Byte	90_H	Overwrites the data of the specified byte	$4352/f_c + n * 4096/f_c \pm 32/f_c$

1) Timing for ISO commands is defined according to ISO/IEC 15693
2) According to ISO/IEC 15693: Typical VICC waiting time before transmitting its response after reception of an EOF from the VCD
3) Timing conditions for write alike requests are defined according to the ISO/IEC 15693. The number “n” depends on the VCD-VICC configuration. For more details see also application note: “my-d™ response times” (f_c = 13.56 MHz)

Note: Whenever a plain page is accessed with a my-d™ vicinity custom command, the response is the same as described in this document and the data size is 8 bytes per page.

***Attention*: Whenever the content of a plain page (8-byte page) should be changed with a my-d™ vicinity custom write command as stated in this section (write, write and reread, restricted write, restricted write and reread, write byte), both the higher and lower nibble of the access conditions byte AC must allow the change of the whole page. Otherwise, the tag responds with error code $A1_H$ as defined above. In addition, if a whole page (8 bytes) should be locked then both nibbles of AC must indicate this; that is both nibbles must be 6_H.**

Whenever a plain page is to be changed with an ISO optional command, only the access conditions of an accessed block is checked.

5.2.1 Read command

ISO command code = '$A0_H$'.

my-d™ vicinity embedded command code = '10_H'.

The 'Read' command reads one page of the memory (8-byte in user mode, 10-byte in issuer mode).

When applying the read command to a page in the plain sector, the MAC value of 32 bits must be omitted. There is also no MAC value used, when in issuer mode.

Table 29 my-d™ vicinity "Read": Request format

SOF	Flags	Command code	Parameters	Data				CRC	EOF
-	8-bit	'$A0_H$'	'05_H', [UID]	'10_H'	Addr.0	'00_H'	MAC	16-bit	-

Table 30 my-d™ vicinity "Read": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 31 my-d™ vicinity "Read": Data-field

Code	Meaning	Comment
'10_H'	Command code for "Read"	8-bit
Addr.0	Page address to be read	8-bit Address range for SRF 55V10S '00_H' - '$7F_H$' Address range for SRF 55V02S '00_H' - '$1F_H$'
'00_H'	RFU	8-bit
MAC	Message authentication code (applies only in user mode)	32-bit; Ensures the integrity and authenticity of the data being read

Table 32 Response format user mode (no errors)

SOF	Flags	Data		CRC	EOF
-	'00_H'	64-bit Page content	32-bit MAC	16-bit	-

Table 33 Response format issuer mode (no errors)

SOF	Flags	Data			CRC	EOF
-	'00_H'	64-bit Page content	8-bit Sector index	8-bit Access conditions	16-bit	-

Table 34 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.2.2 Write command

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = '30_H'.

The 'Write' command performs an erase - write cycle in the specified page (8-byte are written in user mode, 10-byte in issuer mode). In case of successful programming of the page, the VICC sends back an acknowledge frame consisting of 3 bytes (see below). In case of an error or if the access condition is set to read only an error code ('$0F_H$') is transmitted by the VICC (see below).

When applying the write command to a page in the plain sector, the MAC value of 32 bits must be omitted. There is also no MAC value used, when in issuer mode.

Table 35 my-d™ vicinity "Write": Request format

SOF	Flags	CMD	Parameters	Data					CRC	EOF
-	8-bit	'$A0_H$'	'05_H', [UID]	'30_H'	Addr.0	'00_H'	Page data	MAC	16-bit	-

Table 36 my-d™ vicinity "Write": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 37 my-d™ vicinity "Write": Data-field

Code	Meaning	Comment
'30_H'	Command code for "Write"	8-bit
Addr.0	Page address	8-bit Address range for SRF 55V10S '00_H' - '$7F_H$' Address range for SRF 55V02S '00_H' - '$1F_H$'
'00_H'	RFU	8-bit
Page data	Page data to be written	• 64-bit page data when in user mode • 80-bit page data when in issuer mode: 64-bit page data plus 8-bit sector index plus 8-bit access conditions
MAC	Message authentication code (applies only in user mode)	32-bit; Ensures the integrity and authenticity of the data being written

Table 38 Response format (no errors)

SOF	Flags	CRC	EOF
-	'00_H'	16-bit	-

Table 39 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code [1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.2.3 Write and Reread command

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = '$B0_H$'.

The 'Write and Reread' command is a special command to read data immediately after having written it. This command combines the write (8-byte are written in user mode, 10-byte in issuer mode) and read command (8-byte in user mode, 10-byte in issuer mode). Instead of signaling an acknowledge frame consisting of 3 bytes (see Write command), the written data is transmitted back to the VCD. With this command, the correct execution of the write command and the actual contents of the page can be verified. In case of an error or if the access condition is set to read only an error code ('$0F_H$') is transmitted by the VICC (see below). The command and response length depends on the actual mode.

When applying the Write and Reread command to a page in the plain sector, the MAC value of 32 bits must be omitted. There is also no MAC value used, when in issuer mode.

Table 40 my-d™ vicinity "Write and Reread": Request format

SOF	Flags	CMD	Parameters	Data					CRC	EOF
-	8-bit	'$A0_H$'	'$A0_H$' [UID]	'$B0_H$'	Addr.0	'00_H'	Page data	MAC	16-bit	-

Table 41 my-d™ vicinity "Write and Reread": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 42 my-d™ vicinity "Write and Reread": Data-field

Code	Meaning	Comment
'$B0_H$'	Command code for "Write and Reread"	8-bit
Addr.0	Page address	8-bit Address range for SRF 55V10S '00_H' - '$7F_H$' Address range for SRF 55V02S '00_H' - '$1F_H$'
'00_H'	RFU	8-bit
Page data	Page data to be written	• 64-bit page data when in user mode • 80-bit page data when in issuer mode: 64-bit page data plus 8-bit sector index plus 8-bit access conditions
MAC	Message authentication code (applies only in user mode	32-bit; Ensures the integrity and authenticity of the data being written

Table 43 Response format user mode (no errors)

SOF	Flags	Data		CRC	EOF
-	'00_H'	64-bit Page content	32-bit MAC	16-bit	-

Table 44 Response format issuer mode (no errors)

SOF	Flags	Data			CRC	EOF
-	'00_H'	64-bit Page content	8-bit Sector index	8-bit Access conditions	16-bit	-

Table 45 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.2.4 Restricted Write command

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = '00_H'.

The 'Restricted Write' command is used for setting and overwriting value counters and the authentication counter. To set the new and lower value of a counter, a read command on the counter page has to be executed previously (see Read command). After the determination of the actual counter value, the new value can be set. Only the new counter value (4 bytes) in the counter value format (see Counter format and operations) has to be transmitted.

In case of successful programming of the page, the VICC sends back an acknowledge frame consisting of 3 bytes (see below). In case of an error or if the access condition is set to read only an error code ('$0F_H$') is transmitted by the VICC (see below).

When applying the Restricted Write command to a page in the plain sector, the MAC value of 32 bits must be omitted. There is also no MAC value used, when in issuer mode.

Table 46 my-d™ vicinity "Restricted Write": Request format

SOF	Flags	CMD	Parameters	Data					CRC	EOF
-	8-bit	'$A0_H$'	'05_H' [UID]	'00_H'	Addr.0	'00_H'	Page data	MAC	16-bit	-

Table 47 my-d™ vicinity "Restricted Write": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 48 my-d™ vicinity "Restricted Write": Data-field

Code	Meaning	Comment
'00_H'	Command code for "Restricted Write"	8-bit
Addr.0	Page address	8-bit Address range for SRF 55V10S '00_H' - '$7F_H$' Address range for SRF 55V02S '00_H' - '$1F_H$
'00_H'	RFU	8-bit
Page data	New counter value	32-bit new counter value when in user mode: • Counter value in special counter value data format 48-bit page data when in issuer mode: • 32-bit new counter value in special counter value data format plus 8-bit sector index plus 8-bit access conditions
MAC	Message authentication code (applies only in user mode)	32-bit; Ensures the integrity and authenticity of the data being written

Table 49 Response format (no errors)

SOF	Flags	CRC	EOF
-	'00_H'	16-bit	-

Table 50 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.2.5 Restricted Write and Reread command

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = '80_H'.

The 'Restricted Write and Reread' command is used for setting and overwriting value counters and the authentication counter and reading them back in one turn. To set the new and lower value of a counter, a Read command on the counter page has to be executed previously (see Read command). After the determination of the actual counter value, the new value can be set. Only the new counter value (4 bytes) in the counter value format (see Counter format and operations) has to be transmitted.

In case of successful programming of the page the VICC sends back the new value of the counter.

In case of an error or if the access condition is set to read only an error code ('$0F_H$') is transmitted by the VICC (see below).

When applying the Restricted Write and Reread command to a page in the plain sector, the MAC value of 32 bits must be omitted. There is also no MAC value used, when in issuer mode.

Table 51 my-d™ vicinity "Restricted Write and Reread": Request format

SOF	Flags	CMD	Parameters	Data					CRC	EOF
-	8-bit	'$A0_H$'	'05_H' [UID]	'80_H'	Addr.0	'00_H'	Page data	MAC	16-bit	-

Table 52 my-d™ vicinity "Restricted Write and Reread": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 53 my-d™ vicinity "Restricted Write and Reread": Data-field

Code	Meaning	Comment
'80_H'	Command code for "Restricted Write and Reread"	8-bit
Addr.0	Page address	8-bit Address range for SRF 55V10S '00_H' - '$7F_H$' Address range for SRF 55V02S '00_H' - '$1F_H$'
'00_H'	RFU	8-bit
Page data	New counter value	32-bit new counter value when in user mode: • Counter value in special counter value data format 48-bit page data when in issuer mode: • 32-bit new counter value in special counter value data format plus 8-bit sector index plus 8-bit access conditions
MAC	Message authentication code (applies only in user mode)	32-bit; Ensures the integrity and authenticity of the data being written

Table 54 Response format user mode (no errors)

SOF	Flags	Data		CRC	EOF
-	'00_H'	64-bit Page content	32-bit MAC	16-bit	-

Table 55 Response format issuer mode (no errors)

SOF	Flags	Data			CRC	EOF
-	'00_H'	64-bit Page content	8-bit Sector index	8-bit Access conditions	16-bit	-

Table 56 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.2.6 Write Byte command

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = '90_H'.

The 'Write Byte' command writes one byte to the specified address. In case of successful programming, the VICC sends back an acknowledge frame consisting of 3 bytes (see below). In case of an error or if the access condition is set to read only an error code ('$0F_H$') is transmitted by the VICC (see below).

When applying the Write Byte command to a page in the plain sector, the MAC value of 32 bits must be omitted.

Table 57 my-d™ vicinity "Write Byte": Request format

SOF	Flags	CMD	Parameters	Data						CRC	EOF
-	8-bit	'$A0_H$'	'05_H' [UID]	'90_H'	Addr.0	'00_H'	Byte address	Byte value	MAC	16-bit	-

Table 58 my-d™ vicinity "Write Byte": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 59 my-d™ vicinity "Write Byte": Data-field

Code	Meaning	Comment
'90_H'	Command code for "Write Byte"	8-bit
Addr.0	Page address	8-bit Address range for SRF 55V10S '00_H' - '$7F_H$' Address range for SRF 55V02S '00_H' - '$1F_H$'
'00_H'	RFU	8-bit
Byte address	Byte address in page	8-bit Address range from '00_H' - '09_H'
Byte value	Byte data to be written	8-bit user data
MAC	Message authentication code (applies only in user mode)	32-bit; Ensures the integrity and authenticity of the data being written

Table 60 Response format (no errors)

SOF	Flags	CRC	EOF
-	'00_H'	16-bit	-

Table 61 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.3 Authentication

Mutual authentication allows verifying that both VCD and VICC are authentic. The authentication sequence is split into three steps:

Sequence step 1: (command **Authenticate A**, for more details refer to Authenticate A: Authentication step 1). The VCD sends the page address of the authentication counter (CntAddr) and the page address of the authentication key (KeyAddr, page of the key as defined in Table 18).

The command Authenticate A initiates a challenge of the VICC to the VCD. The VICC transmits a random number and the data of the authentication counter page. If an error occurs, an error code ('$0F_H$') is transmitted by the VICC, further on the authentication is terminated and the VICC opens sector 0 again.

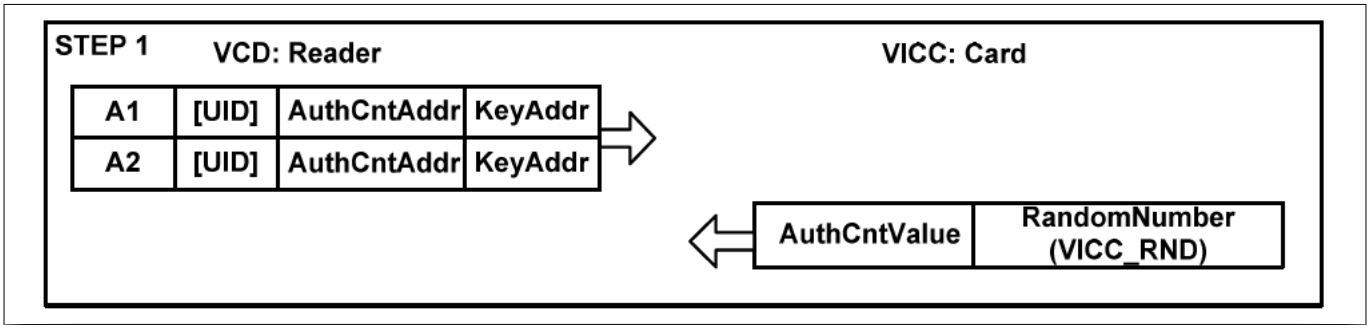


Figure 17 Authentication sequence step 1

Sequence step 2: The VCD calculates the response upon the challenge from the VICC. For that purpose, the sector key must be known to the VCD. This can be done using a security authentication module (SAM). The SAM holds all or just a subset of application keys. It also holds the algorithms to calculate the response to the challenge of the VICC. As a result, the VCD transmits its response using sequence step 3.

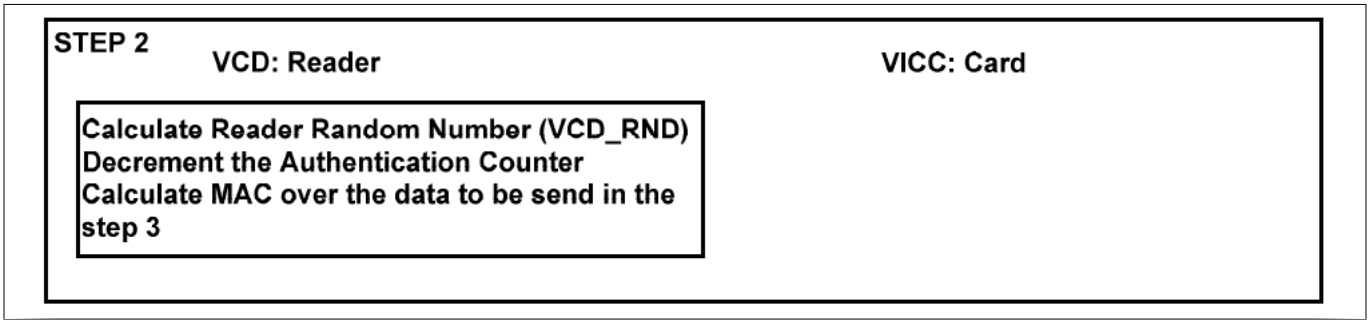
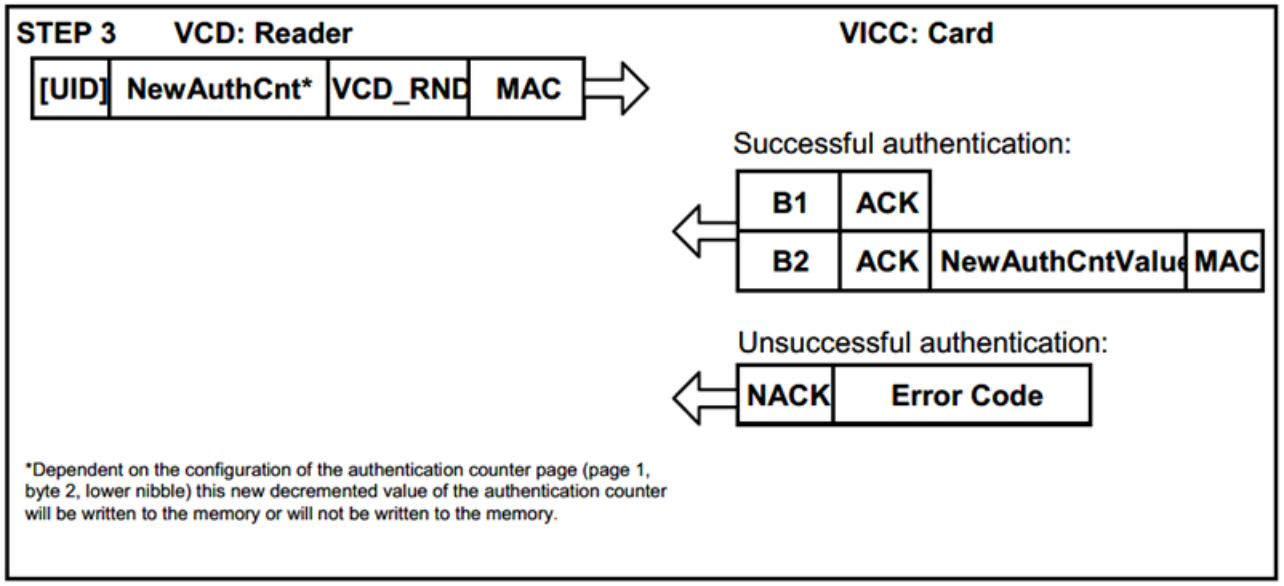


Figure 18 Authentication sequence step 2

Sequence step 3: (command **Authenticate B**, for more details refer to Authenticate B: Authentication step 3). The VCD replies its response to the challenge from step 1 by using the command Authenticate B. Within the command Authenticate B, the VCD sends the new value of the authentication counter, an 8-byte random number, and a MAC over all transferred data. The random number sent by the VCD is the challenge to the VICC to as certain an authentic VICC. Depending on the command sent by the VCD in sequence step 1, the VICC responds with an acknowledge frame or with the data of the authentication counter page if the authentication was successful. If an error had occurred, an error code ('$0F_H$') is transmitted by the VICC, further on the authentication is terminated and the VICC opens sector 0 again.



Note: For more information about the configuration of authentication counter page refer to Authentication counter (page 03_H).

Figure 19 Authentication sequence step 3

After the successful authentication, the VICC is in protected mode and memory operations can be executed within the authenticated sector. It is, that in user mode all commands to the secure sector have to be attached with a MAC value to ascertain data integrity and data authenticity.

In general, a MAC is a data authentication code. It is a one-way hash function with the addition of a secret key. The hash value is the function of both the pre-image (the input data) and the key. Only someone with the key can verify the hash value, that is open a secure sector of the memory of the chip and read/write data out/from it. The idea is that only the legitimate user can ask and get the correct response from the card, because only this user alone has been given the identifying piece of secret information, the secret key.

5.3.1 Authenticate A: Authentication step 1

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = '20_H' or '$A0_H$' respectively.

This command initiates the challenge-response mutual authentication between VCD and VICC. As a response to this command, the value of the authentication counter (Auth_CNT) and a random number (VICC_RND) are transmitted back. These two values are used to calculate the response to the challenge within the VCD.

The Authenticate A command has two variants as follows:

- When using the command code **'20_H' (Authenticate A1)**, the response in step B will be of type ACK/NACK (response B1)
- When using the command code **'$A0_H$' (Authenticate A2)**, the response in step B will be the value of the new authentication counter value secured by a MAC value (response B2)

In case of an error, an error code ('$0F_H$') is transmitted by the VICC and the authentication is aborted and the VICC opens sector 0 again (see below).

Table 62 my-d™ vicinity "Authenticate A": Request format

SOF	Flags	CMD	Parameters	Data				CRC	EOF
-	8-bit	'$A0_H$'	'05_H' [UID]	'20_H' or '$A0_H$'	CntAddr	'00_H'	KeyAddr	16-bit	-

Table 63 my-d™ vicinity "Authenticate A": Parameter-field

Code	Meaning	Comment
05_H	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 64 my-d™ vicinity "Authenticate A": Data-field

Code	Meaning	Comment
'20_H' or '$A0_H$'	Command code for "Authenticate A" • Command code '20_H': Response of sequence B will be of type ACK/NACK (response B1) • Command code '$A0_H$': Response of sequence B will be of type NewAuthCNT and MAC (response B2)	8-bit
CntAddr	Page address of the authentication counter	8-bit Default authentication counter page address: '03_H'
'00_H'	RFU	8-bit
KeyAdd	Page address of the key to be used; there is a fixed assignment between sector number and key page address (see Table 18)	8-bit Address range '04_H' - '$1F_H$'

Table 65 Response format (no errors)

SOF	Flags	Data		CRC	EOF
-	'00_H'	64-bit authentication counter Auth_CNT	64-bit random number from VICC VICC_RND	16-bit	-

Table 66 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.3.2 Authenticate B: Authentication step 3

ISO-command code = '$A0_H$'.

my-d™ vicinity embedded command code = None.

From the VICC's point of view this command must follow immediately to the command 'Authenticate A'. The Authenticate B command concludes the mutual authentication by sending the decremented authentication counter in the authentication counter format (new Auth_CNT) and by sending a challenge random number from the VCD (VCD_RND) to the VICC. Depending on the configuration of the authentication counter page (refer

to Authentication counter (page 03_H)) the VICC will write this new value of the authentication counter to the authentication counter page or the value of the authentication counter page stay unchanged. The VICC will then signal a successful log in either by an ACK/NACK or by replying to the new authentication counter secured by a MAC value.

The response to the Authenticate B command has two variants, depending on which variant was initiated in the Authenticate A command already:

- When having used command code '20_H' with the Authenticate A, the response to Authenticate B will be of type ACK/NACK (response B1)
- When having used command code '$A0_H$' with the Authenticate A, the response to Authenticate B will be the value of the new authentication counter value secured by a MAC value (response B2)

The sequence with the response B1 allows an "accelerated card authentication" for applications, which do not use the authentication counter as an application counter. So, the authentication counter value is not read. The authentication is finished with the next memory command of the VCD, sent with a MAC example: A read command to a page within the secure sector. On successful verification of the MAC of the replied data, the VICC is authenticated to the VCD.

The sequence with the response B2 completes the mutual authentication already when the new value of the authentication counter is sent back to the VCD.

In case of an error, an error code ('$0F_H$') is transmitted by the VICC and the authentication is aborted and the VICC opens sector 0 again (see below).

Table 67 my-d™ vicinity "Authenticate B": Request format

SOF	Flags	CMD	Parameters	Data			CRC	EOF
-	8-bit	'$A0_H$'	'05_H' [UID]	New Auth_CNT	VCD_RND	MAC	16-bit	-

Table 68 my-d™ vicinity "Authenticate B": Parameter-field

Code	Meaning	Comment
'05_H'	IC manufacturer code for Infineon	Mandatory
UID	Unique identification number	Optional

Table 69 my-d™ vicinity "Authenticate B": Data-field

Code	Meaning	Comment
New Auth_CNT	Decremented value of the authentication counter in the authentication counter format, with the bytes holding the value of the counter only!	32-bit (see Authentication counter (page 03_H))
VCD_RND	Random number of the VCD	64-bit
MAC	Message authentication code	32-bit; Ensures the integrity and authenticity of the data being written

Table 70 Response format for response B1 (no errors)

SOF	Flags	CRC	EOF
-	'00_H'	16-bit	-

Table 71 Response format for response B2 (no errors)

SOF	Flags	Data		CRC	EOF
-	'00_H'	64-bit Authentication counter Auth_CNT	32-bit MAC	16-bit	-

Table 72 Response in case of an error: (Error_flag is set)

SOF	Flags	Data	CRC	EOF
-	'01_H'	Error code[1)]	16-bit	-

1) Error code is defined according to ISO/IEC 15693 and Error codes

5.4 Personalization of my-d™ vicinity secure

Prior to the delivery of my-d™ vicinity in security mode, the memory is configured as a transport configuration. Chip, which UID will be defined by the manufacturer (Infineon Technologies), will be delivered in issuer mode, with an already predefined memory allocation for an authentication counter and a transport key. All memory pages which are part of the user area including page 1, which stores the issuer configuration as well as the configuration of the authentication counter page, are stored in sector 2, with sector index 59_H (for more details about memory organization of the SRF 55VxxS (HC) see Table 7 and Table 8).

Personalization steps:

1. After receiving such a card, the user (issuer) has to perform the three-step mutual authentication with the transport key to open sector 2
2. Definition of data/counter pages: Set up one or more sectors, configure the data pages with their access conditions

   Note: Writing of the sector index allocates the page to the indicated sector, further access is only possible after authentication of the relevant sector.

3. Definition of key pages: Set up the corresponding keys

The configuration (personalization) of the IC should be done in the issuer mode. Therefore, before the personalization of my-d™ vicinity IC, it is recommended to check if the issuer mode is set by reading page 1 and to set it if it is not set (for more details about issuer tag refer to Issuer data, issuer tag, and authentication counter configuration (page 01_H)). As the page 1 stores not only the issuer tag but also the configuration bits for the authentication counter (for more details refer to Authentication counter (page 03_H)), Infineon Technologies recommends to keep page 1 writable however secured with the key in one of the sectors which is accessible only by the issuer of the card.

Figure 20 shows the steps which are to be performed when the personalization of my-d™ vicinity IC by the issuer is required.

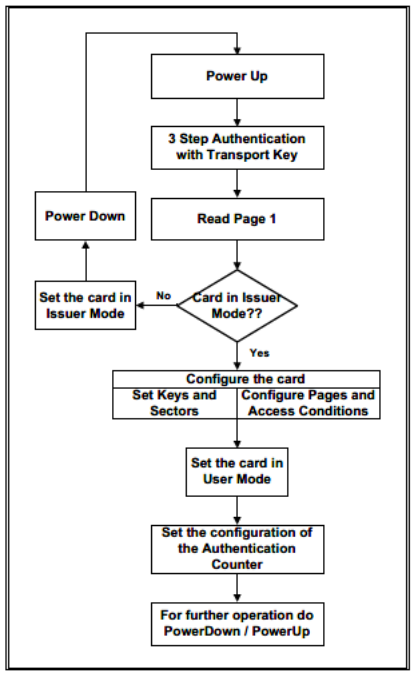


Figure 20 Personalization of my-d™ vicinity in secure mode

5.5 Communication principle

The commands are initiated by the VCD or reader. The internal logic of my-d™ vicinity will decode the command, prove if it is valid and according to the access conditions of the accessed pages that will be executed.

The communication between VCD or reader and the VICC my-d™ vicinity card (with my-d™ vicinity IC on it) will start typically with the identification of the card. After checking for further cards in the field (anticollision process), one card is selected for further communication. All other cards are sent to a quite state however, they are accessible to the user, by sending a command in addressed mode, which will directly address a particular card.

If the card is in secure mode, a three-step mutual authentication ensures that a correct reader and a correct card communicate with each other. Only valid commands, which are sent by a correct reader will be allowed and executed by the corresponding card.

The communication principle between the card and the reader is explained in Figure 21.

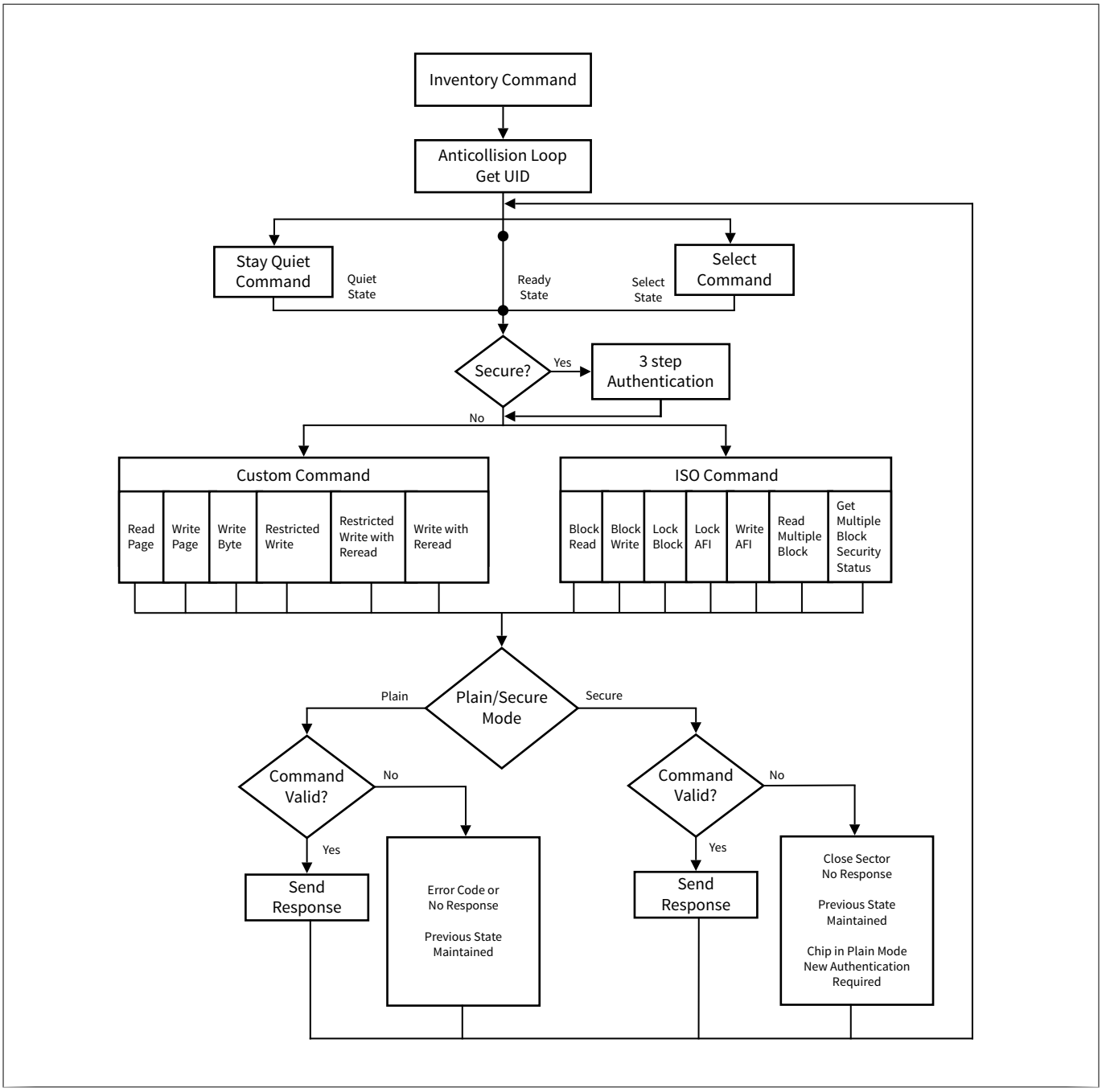


Figure 21 Communication principle

6 EAS functionality

Electronic article surveillance (EAS) functionality is supported by programming the AFI byte using the optional ISO/IEC 15693.

Command ‘Write AFI’ and ‘Lock AFI’.

With EAS enabled, the tag triggers an alarm at a gate VCD by sending a special bit stream after power up without the need of receiving any command from the VCD (Tag talks first). The bit 2 of the AFI byte is used to switch on and off the EAS signal.

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
as defined by ISO-15693					EAS bit		

Figure 22 Definition of the AFI byte

AFI bit 2 set to 1 means the EAS function activated.

AFI bit 2 set to 0 means the EAS function deactivated.

AFI bit 0, 1, and 3 are free and available for the application.

If the EAS function is activated, the tag starts to send the EAS signal as soon it is powered up by the magnetic field of the reader. This fast reaction ensures high reliability. The VCD does not have to send ISO commands to operate the EAS feature.

The EAS signal consists of a bit stream sent at a sub-carrier frequency of 2.4 MHz. By this, the tag does not interfere with standard ISO/IEC 15693 applications.

The bit stream is interrupted by 56 ms breaks. During this break, the tag is ready to accept ISO commands. Each bit stream starts with a SOF followed by logical zeroes and stops after 40 ms with an EOF.

The content of page 2, byte 1, defines the access condition of the AFI byte (for more details refer to Memory size and organization). So the user can change the access condition of the AFI byte from read/write to read only.

The value ‘$0A_H$’ shall make it possible to change the content of the AFI byte with the ISO optional ‘Write AFI’ command. The access condition can be altered to read only with the command ‘Lock AFI’. In that case, the value of the access condition will be ‘06_H’.

Please note that the AFI byte must not be locked so that it is possible to turn the EAS functionality on or off.

7 Operational characteristics

The listed characteristics are ensured over the operating range of the integrated circuit. Typical characteristics specify mean values expected over the production spread. If not otherwise specified, typical characteristics apply at T_A = 25°C and the given supply voltage.

7.1 Electrical characteristics

f_C = 13.56 MHz sinusoidal waveform, voltages refer to V_{SS}.

Table 73 Operating range and conditions

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
EEPROM erase + write time	t_{e+w}	-	-	3.96	ms	Combined erase + write; Excluding time for command/ response transfer between VCD and chip T_A = 25°C
Inputs L_A, L_B						
Chip input capacitance L_A - L_B	C_{AB}	-	23.1	-	pF	V_{AB} RMS = 1.6 V f_C = 13.56 MHz, T_A = 25°C
Chip load resistance L_A - L_B	R_{AB}	-	10	-	kΩ	V_{AB} RMS = 1.6 V f_C = 13.56 MHz, T_A = 25°C

7.2 Absolute maximum ratings

Stresses above those listed may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of this document is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including EEPROM data retention and write/erase endurance.

Table 74 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input peak voltage L_A - L_B	V_A, V_B	-	-	4.2	V	On-chip limitation by the voltage regulator
Input current L_A - L_B	I_{AB}	-	-	100	mA	Maximal current
Pulse voltage (ESD protection L_A, L_B)	V_{ESD}	-	-	2	kV	JEDEC STD EIA/JESD22 A114-B
Endurance[1)] (write/erase cycles)	-	10^5	-	-	-	-
Data retention[1)]	-	10	-	-	Years	-
Operating temperature	T_A	-25	-	+70	°C	For the chip

(table continues...)

Table 74 (continued) Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Storage temperature	T_S	-40	-	+125	°C	For the chip

1) Values are temperature dependent, for further information please contact Infineon Technologies office or representative

References

[1] Infineon Technologies: *SRF55VxxP my-d™ vicinity plain Extended datasheet (Revision 3.0 or later)*; 2022-09-23

[2] ISO/IEC 7816-6:2016: *Identification cards - Integrated circuit cards - Part 6: Interindustry data elements for interchange (Third edition)*; 2016-06

[3] ISO/IEC 14443-2:2020: *Cards and security devices for personal identification – Contactless proximity objects - Part 2: Radio frequency power and signal interface (Fourth edition)*; 2020-07

[4] ISO/IEC 15693-1:2010 *Identification cards — Contactless integrated circuit cards — Vicinity cards — Part 1: Physical characteristics (Second edition)*; 2010-10

[5] ISO/IEC 15693-2:2019: *Cards and security devices for personal identification — Contactless vicinity objects — Part 2: Air interface and initialization (Third edition)*; 2019-04

[6] ISO/IEC 15693-3:2019: *Cards and security devices for personal identification — Contactless vicinity objects — Part 3: Anticollision and transmission protocol (Third edition)*; 2019-04

[7] ISO/IEC 18000-3:2010: *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13.56 MHz (Third edition)*; 2010-11

Glossary

AC

access condition (AC)

AES

Advanced Encryption Standard (AES)
The standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The algorithm described by AES is a symmetric-key algorithm (i.e. the same key is used for both encryption and decryption).

AFI

application family indicator (AFI)

CC

Common Criteria for Information Technology Security Evaluation (CC)
An international standard (ISO/IEC 15408) for computer security certification.

CRC

cyclic redundancy check (CRC)
A procedure that uses a checksum to check the validity of a data transfer.

EAL

evaluation assurance level (EAL)

EAS

electronic article surveillance (EAS)
Securing articles with the use of tags/labels that cause an alarm when activated in security gates at the exit or entry of a building.

EEPROM

electrically erasable programmable read-only memory (EEPROM)

EOF

end of frame (EOF)

ESD

electrostatic discharge (ESD)
The sudden draining of electrostatic charge. Even with small charges, it poses a considerable risk to small semiconductor structures, in particular MOS structures. It is therefore essential to take precautions when dealing with unprotected semiconductors.

IC

integrated circuit (IC)

IEC

International Electrotechnical Commission (IEC)
The international committee responsible for drawing up electrotechnical standards.

IFX

Infineon Technologies AG (IFX)
The stock market acronym for Infineon Technologies AG shares. It is sometimes used in diagrams or tables where the long term hinders readability.

ISO

International Organization for Standardization (ISO)

JEDEC

Joint Electron Device Engineering Council (JEDEC)

LSB

least significant bit (LSB)

MAC

message authentication code (MAC)
Used to prove message integrity.

MCC

module contactless card (MCC)

MSB

most significant bit (MSB)

RFID

radio frequency identification (RFID)

RFU

reserved for future use (RFU)

SAM

secure access module (SAM)
A module based on smart card integrated circuits, and used to enhance the security and cryptography performance in devices. It is commonly used in smart card readers that need to perform secure transactions, for example, payment or ticketing terminals. The module is also referred to as a secure application module.

SI

sector index (SI)

SOF

start of frame (SOF)

TDES

Triple DES (TDES)

UID

unique identifier (UID)

VCD

vicinity coupling device (VCD)

VICC

vicinity integrated circuit card (VICC)

Revision history

Reference	Description
Revision 3.0, 2023-02-14	
All	Migrated to latest template and updated editorial changes
Revision 2.0, 2004-02-29	
All	• IC Manufacturer Code (IC Mfg code) is assigned to '$E0_H$' only • Additional support of ISO optional commands
Revision 1.0, 2003-02-25	
All	Initial release

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2023-02-14

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-sjm1603272921134

Important notice

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, 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.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings

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

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.