my-d™ move and my-d™ move NFC

Extended datasheet

Intelligent 152 byte EEPROM with contactless interface compliant to ISO/IEC 14443-3 Type A and support of NFC Forum Type 2 Tag operation

Key features

Contactless interface

- Physical interface and anticollision compliant to ISO/IEC 14443-3 Type A
  - Operation frequency 13.56 MHz
  - Data rate 106 kbit/s in both direction
  - Contactless transmission of data and supply energy
  - Anticollision logic: Several cards may be operated in the field simultaneously
- Unique identification number (7 byte double-size UID) according to ISO/IEC 14443-3 Type A
- Read and write distance up to 10 cm and more (influenced by external circuitry i.e. reader and inlay design)

152 byte EEPROM

- Organized in 38 blocks of 4 bytes each
- 128 bytes freely programmable user memory
- 24 bytes of service area reserved for UID, configuration, LOCK bytes, OTP block and manufacturer data
- Read and write of 128 bytes of user memory in less than 100 ms
- Programming time per block < 4 ms
- Endurance minimum 10,000 erase/write cycles1)
- Data retention minimum 5 years1)

Privacy features

- 32-bit of One Time Programmable (OTP) memory area
- Locking mechanism for each block
- Block lock mechanism
- Optional 32-bit password for read/write or write access
- Optional password retry counter
- Optional 16-bit value counter

Data protection

- Data integrity supported by 16-bit CRC, parity bit, command length check
- Anti-tearing mechanism for OTP, password retry counter and value counter

NFC Forum operation

- Compliant to NFC Forum Type 2 Tag operation
- Support of static and dynamic memory structure according to NFC Forum Type 2 Tag operation
- SLE 66R01P: UNINITIALIZED state, may be configured to INITIALIZED state
- SLE 66R01PN: Pre-configured NFC memory with empty NDEF message (INITIALIZED state, non-reversible)

---

[1] Values are temperature dependent.

Electrical characteristics

- On-chip capacitance 17 pF ± 5%
- ESD protection minimum 2 kV
- Ambient temperature (T_A) -25°C … +70°C (for the chip)

About this document

Scope and purpose

This Extended datasheet describes features, functionality and operational characteristics of SLE 66R01P(N).

Intended audience

This document is primarily intended for system and application developers.

Table of contents

Table of contents

List of tables

List of figures

1 Sales codes and delivery forms

This chapter provides information about available delivery forms and pin/pad descriptions.

Table 1 **Sales codes and delivery forms**

Sales codes	Package	Total memory/user memory[1]
SLE 66R01P TSNP	PG-TSNP-2-3	152/128 bytes
SLE 66R01P C	Wafer sawn/unsawn	
SLE 66R01P NB	NiAu Bumped (sawn wafer)	
SLE 66R01PN TSNP	PG-TSNP-2-3	
SLE 66R01PN C	Wafer sawn/unsawn	
SLE 66R01PN NB	NiAu Bumped (sawn wafer)	

1) Total memory size includes the service area whereas user memory size is freely programmable for user data.

Note: The ordering codes for the individual sales code and package combinations are available on request.

1.1 Bare die

For more details (die dimensions, pad size, pad location, etc..,), please refer to the wafer specification document [7].

1.1.1 Pin description bare die

The my-d™ move/my-d™ move NFC provides a contactless interface. Table 2 lists pin/pad definitions and pin/pad functions.

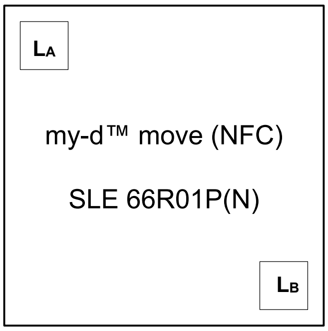


Figure 1 **Pin configuration bare die**

Table 2 **Pin/pad description and function**

Symbol	Function
L_A	Antenna connection
L_B	Antenna connection

1.2 SMD package

The following package is available:

- PG-TSNP-2-3

Table 3 Pad/pin description

Pad number	Pin description
1	Antenna connection
2	Antenna connection

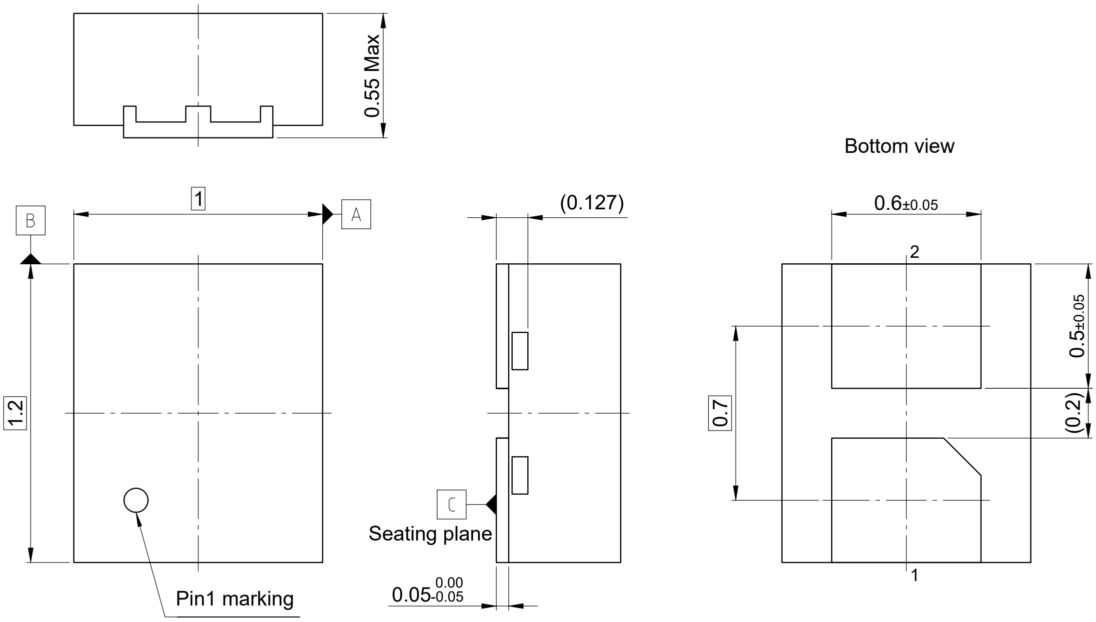
The figures in the sections below show the following aspects of the package:

- Package outline and pin layout: It shows the package dimensions of the device in the individual packages
- Package footprint: It shows footprint recommendations
- Tape and reel packing
- Sample marking pattern: It describes the productive sample marking pattern on the package

Notes:

1. *The drawings are for information only and not drawn to scale. More detailed information about package characteristics and assembly instructions is available on request.*
2. *Unless specified otherwise, all figure dimensions are given in mm.*

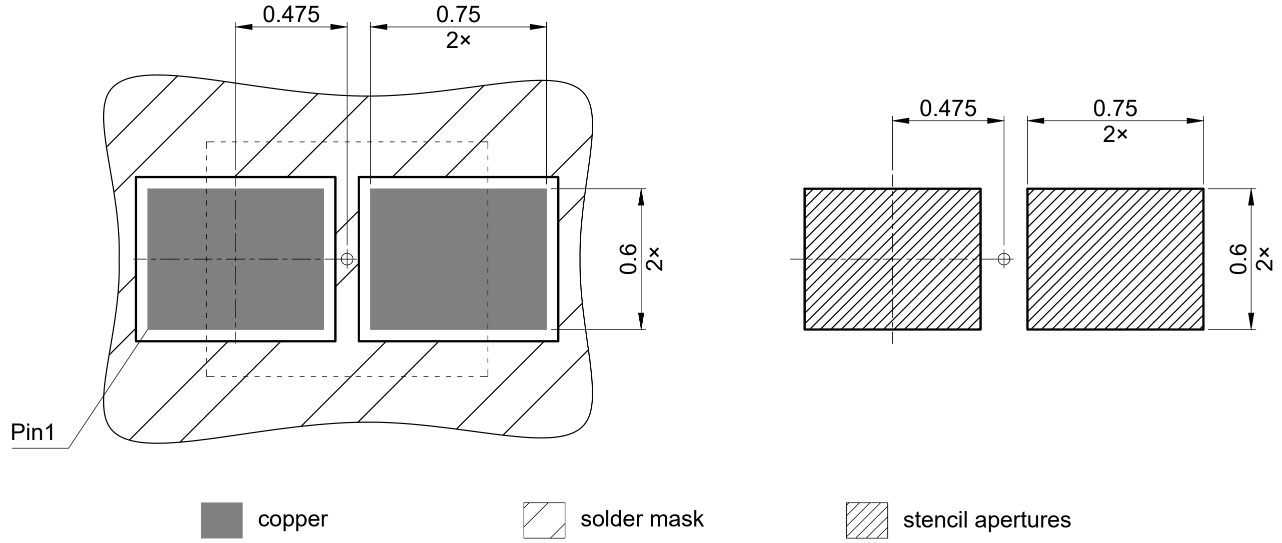
1.2.1 Package outline and pin layout



All dimensions are in units mm
The drawing is in compliance with ISO 128-30, Projection Method 1 [⊲⊕]
Drawing according to ISO 8015, general tolerances ISO 2768-mK

Figure 2 PG-TSNP-2-3 package outline and pin layout

1.2.2 Package footprint



All dimensions are in units mm
All pads are non-solder mask defined

Figure 3 PG-TSNP-2-3 package footprint

1.2.3 Tape and reel packing

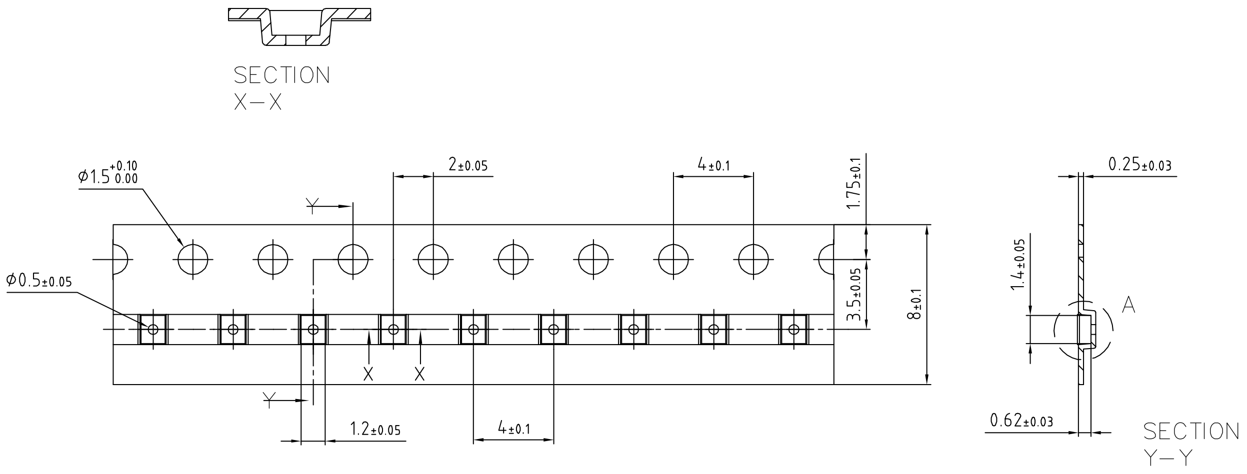


Figure 4 PG-TSNP-2-3 tape and reel packing

1.2.4 Production sample marking pattern

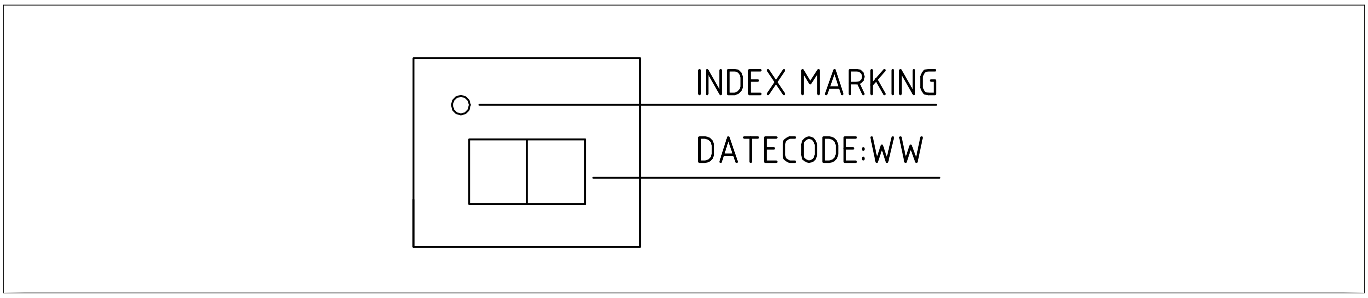


Figure 5 PG-TSNP-2-3 sample marking pattern

Table 4 Marking pattern

Indicator	Description
☐☐	Datecode
<WW>	Production week[1]

---

[1] It is inserted during fabrication

2 my-d™ product family

my-d™ products are available both in plain mode with open memory access and in secure mode with memory access controlled by authentication procedures. The my-d™ product family provides users with different memory sizes, features NFC Forum Type 2 Tag functionality and incorporates security features to enable considerable flexibility in the application design.

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

In plain mode access to the memory is supported by both 4 byte blocks 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 codes (MAC) and customized access conditions protect the memory against unauthorized access.

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

Configurable value counters featuring anti-tearing functionality are suitable for value token applications, such as limited use transportation tickets.

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

The my-d™ move family is designed for cost-optimized applications and its implemented command set eases the usage in existing applications and infrastructures.

2.1 my-d™ move and my-d™ move NFC

The my-d™ move and my-d™ move NFC are part of Infineon's my-d™ product family and are designed to meet the requirements of the increasing NFC market demanding smart memories. They are compliant with ISO/IEC 14443-3 Type A, ISO/IEC 18092 and NFC Forum Type 2 Tag operation.

128 bytes of memory can be arranged in static or dynamic memory structures for NFC applications.

my-d™ move and my-d™ move NFC products also feature configurable value counters which support anti-tearing protection.

Privacy features like password protection including password retry counter provide basic security to the applications.

Based on SLE 66R01P, SLE 66R01PN already contains a pre-configuration of the NFC memory indicating the INITIALIZED state according to the definition of the NFC Forum Type 2 Tag life cycle. Due to that, the my-d™ move NFC is ready to be used in NFC infrastructures.

my-d™ move and my-d™ move NFC products are suited for a broad range of applications like public transport, event ticketing or smart posters.

2.2 Application segments

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

Table 5 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 System overview

The system consists of a host system, one or more SLE 66R01P/SLE 66R01PN Tags or other ISO/IEC 14443-3 Type A compliant cards and an ISO/IEC 14443-3 Type A compatible contactless reader. Alternatively, since the SLE 66R01P and SLE 66R01PN can be used in NFC Forum Type 2 Tag memory structures, an NFC Forum device in card reader/writer mode can be used to operate the chip.

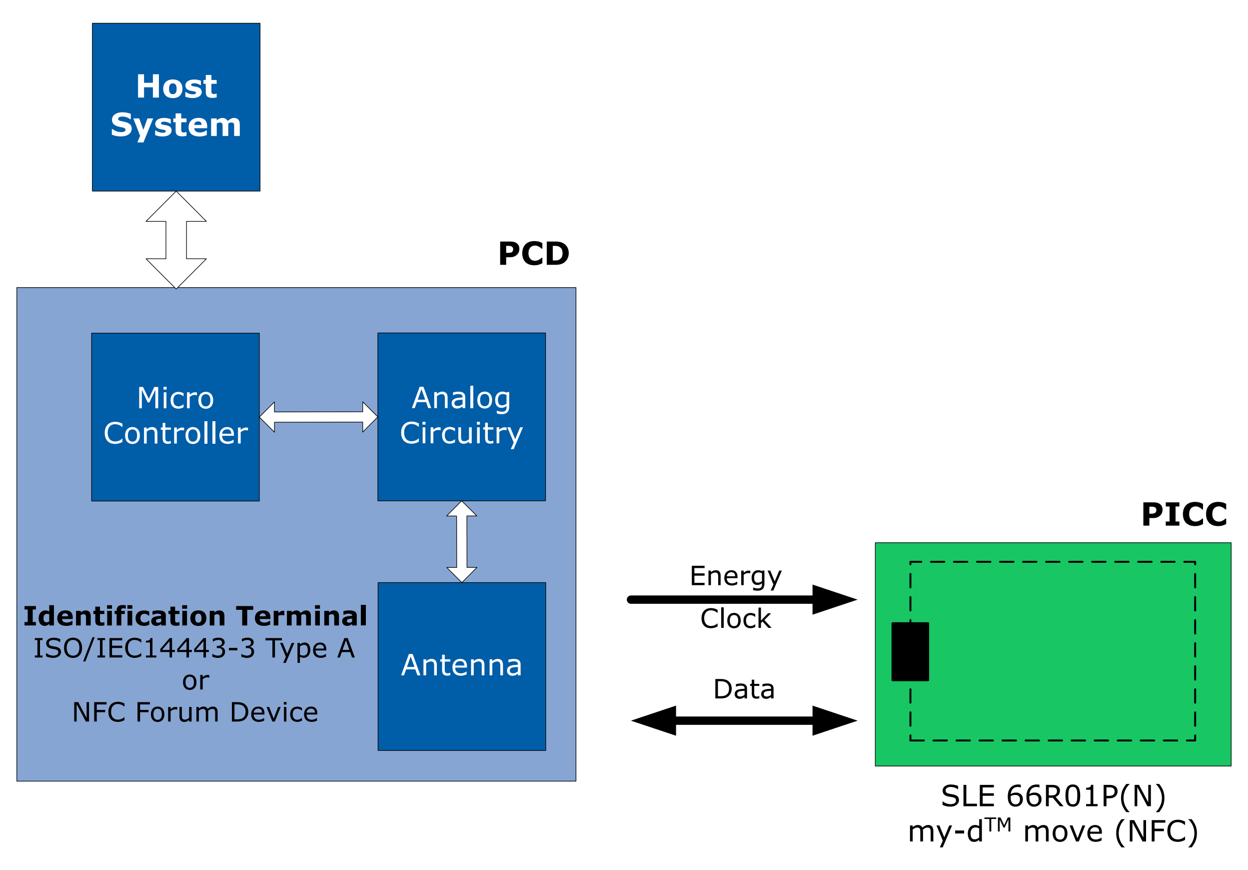


Figure 6 SLE 66R01P and SLE 66R01PN contactless system overview

4 Product overview

The SLE 66R01P and SLE 66R01PN are part of the Infineon my-d™ product family and support Infineon's transport and ticketing strategy and are designed to meet the requirements of NFC applications.

They are compliant with ISO/IEC 14443-3 Type A and NFC Forum Type 2 Tag operation.

4.1 Circuit description

The SLE 66R01P and SLE 66R01PN are made up of an EEPROM memory unit, an analog interface for contactless operation, a data transmission path and a control unit. Figure 7 illustrates the main blocks of the SLE 66R01P and SLE 66R01PN.

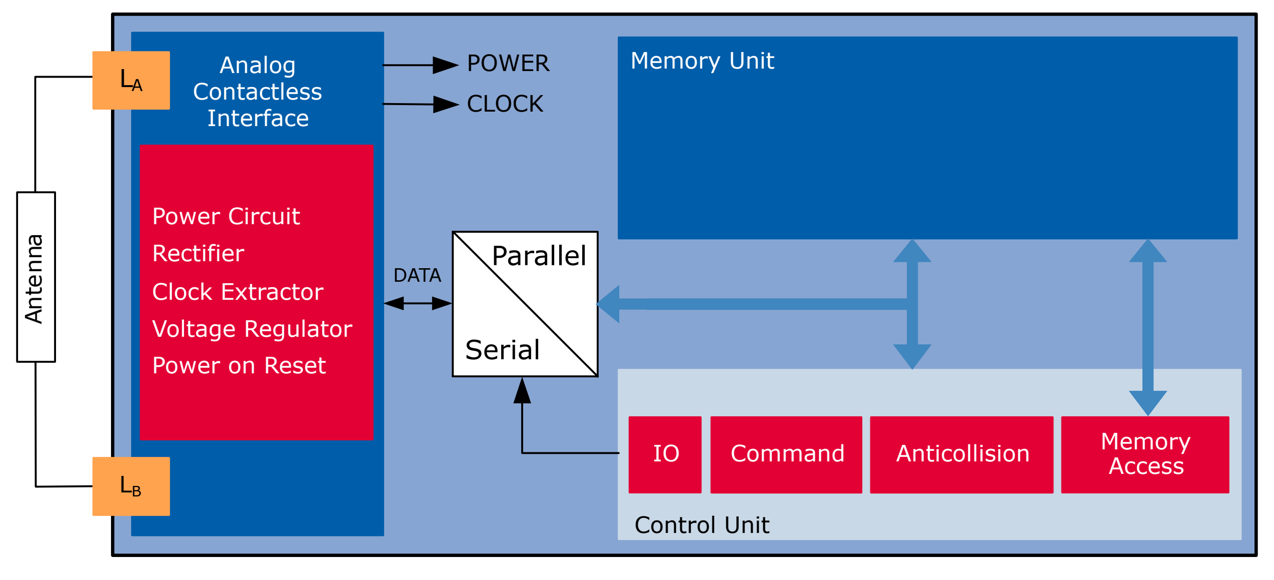


Figure 7 **Block diagram of the SLE 66R01P and SLE 66R01PN**

The SLE 66R01P and SLE 66R01PN comprise the following three parts:

- **Analog contactless interface**
  - The analog contactless interface contains the voltage rectifier, voltage regulator and system clock to supply the IC with appropriate power. Additionally, the data stream is modulated and demodulated
- **Memory unit**
  - The memory unit consists of 38 blocks of 4 bytes each
- **Control unit**
  - The control unit decodes and executes all commands. Additionally, the control unit is responsible for the correct anticollision flow

4.2 Memory overview

The total amount of addressable memory is 152 bytes organized in blocks of 4 bytes each.

The general structure comprises Service Areas as well as User Areas:

- 24 bytes of service and administration data (located in Service Area 1 and 2) reserved for:
  - 7 byte double-size UID
  - Configuration data
  - LOCKx bytes

  - OTP memory
  - Manufacturing data
- 128 bytes of user memory (located in User Area 1 and 2) reserved for:
  - User data
  - Value counter

Additionally the password and password retry counter are available and accessible via dedicated commands.

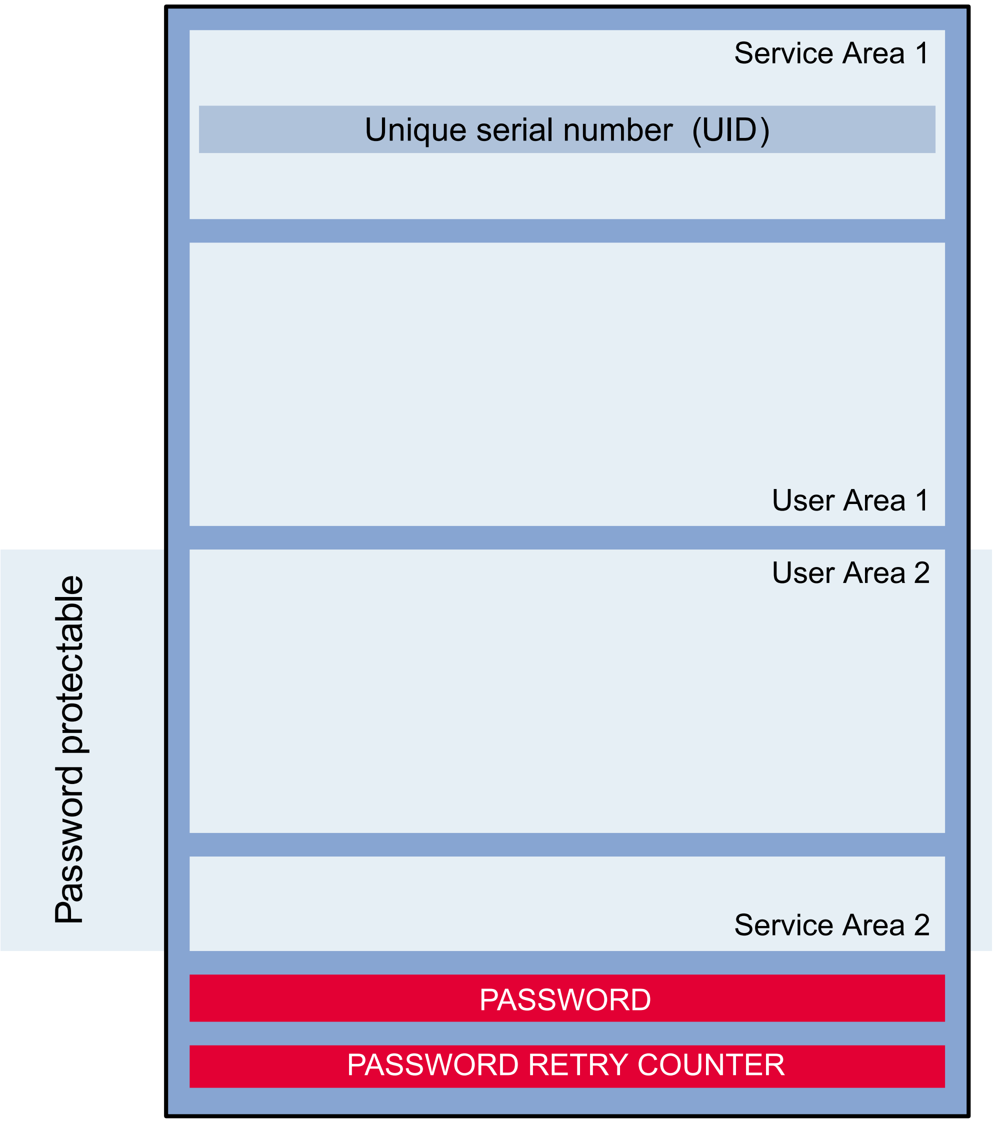


Figure 8 SLE 66R01P and SLE 66R01PN memory overview

4.2.1 Service Area 1

Service Area 1 contains:

- The 7 byte UID which is programmed at the manufacturing of the chip and cannot be changed
- CONFIG byte to enable the password (including: The password retry counter) and the value counter functionality
- LOCK0, LOCK1 bytes to enable an irreversible write-protection for the blocks located in User Area 1
- 32 bits of the One-Time-Programmable (OTP) memory block can irreversibly be programmed from 0_B to 1_B

4.2.2 User Area 1

48 bytes (12 blocks, 4 bytes each) of memory for user data.

4.2.3 User Area 2

User Area 2 contains:

- 80 bytes (20 blocks, 4 bytes each) of user memory for user data. These memory blocks can be used to store user data. This portion of the memory may be protected with a 32-bit password
- A 16-bit value counter may be activated providing a mechanism to store some value (points, trips, ...) on the my-d™ move and my-d™ move NFC chip

4.2.4 Service Area 2

Service Area 2 contains:

- Lock bytes LOCK2 to LOCK5 to enable an irreversible write-protection for the blocks located in User Area 2
- Manufacturing data (programmed during manufacturing of the chip) which cannot be changed

4.3 Memory overview for NFC Forum Type 2 Tag

The memory organization is configurable according to the NFC Forum Type 2 Tag operation specification. Static or dynamic memory structures are supported.

Figure 9 illustrates the principle of the SLE 66R01P and SLE 66R01PN as an NFC Forum Type 2 Tag compatible chip. The memory can be accessed with NFC Forum Type 2 Tag commands.

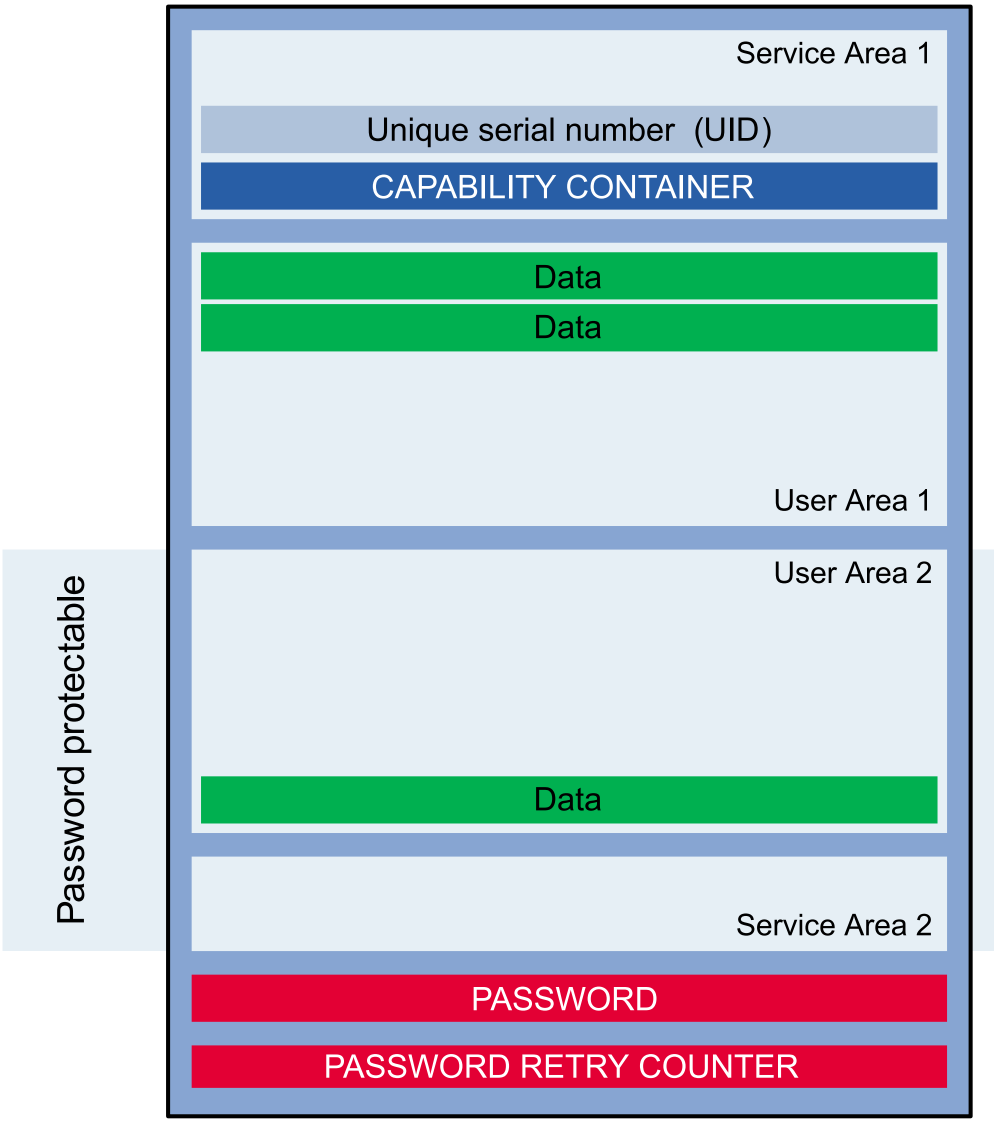


Figure 9 **SLE 66R01P and SLE 66R01PN NFC Forum Type 2 Tag memory structure**

Based on SLE 66R01P and SLE 66R01PN already contains a pre-configuration of the NFC memory indicating the INITIALIZED state according to the definition of the NFC Forum Type 2 Tag life cycle. With this pre-configuration the my-d™ move NFC can be immediately used in NFC infrastructures.

For details regarding the NFC initialization of my-d™ move and my-d™ move NFC please refer to the Application Note "How to operate my-d™ devices in NFC Forum Type 2 Tag infrastructures".

Attention: ***The pre-configuration of SLE 66R01PN is non-reversible and the my-d™ move NFC cannot be overwritten and used as plain, standard my-d™ move anymore.***

4.4 UID coding

To identify SLE 66R01P and SLE 66R01PN chip the manufacturer code and a chip family identifier are coded into the UID as described in Table 6. The chip family identifier can be used to determine the basic command set for the chip.

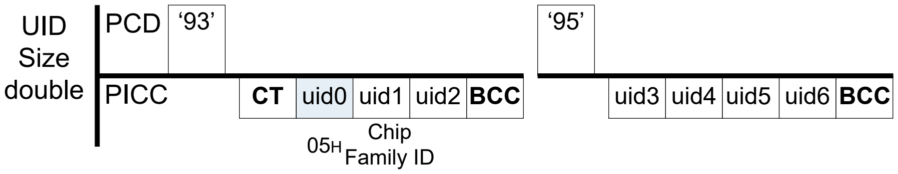


Figure 10 SLE 66R01P and SLE 66R01PN double-size UID

Table 6 UID coding

UID field	Value	Description
uid0	05_H	IC manufacturer code
uid1	$3X_H$	Chip family identifier Higher Nibble: 0011_B: my-d™ move and my-d™ move NFC Lower Nibble: Part of the UID number

4.5 Supported standards

SLE 66R01P and SLE 66R01PN support the following standards:

- ISO/IEC 14443 Type A (Parts 1, 2, and 3) [2] [3] [4] tested according to ISO/IEC 10373-6 [5] (PICC test and validation)
- NFC Forum Type 2 Tag operation specification

4.6 Command set

The SLE 66R01P and SLE 66R01PN are compliant with the ISO/IEC 14443-3 Type A standard.

A set of standard ISO/IEC 14443-3 Type A command is implemented to operate the chip.

Additionally NFC Forum Type 2 Tag commands and a my-d™ move and my-d™ move NFC specific command set is implemented. This facilitates access to the on-chip integrated memory and supports the execution of password and counter functionality.

5 Memory organization

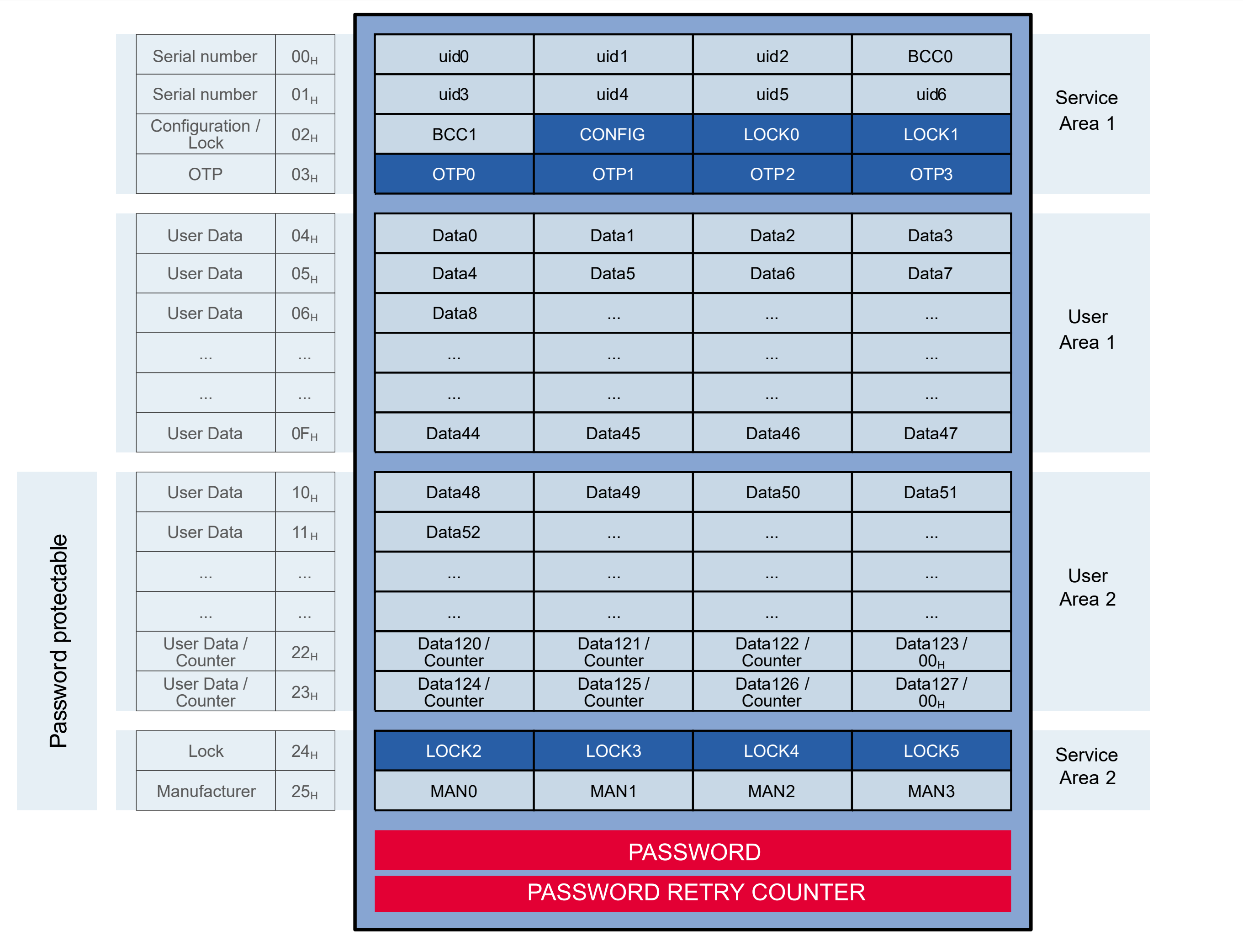
The total amount of user memory is 152 byte. It is organized in blocks of 4 bytes each.

It comprises:

- 128 bytes for user data
- 24 bytes for UID, OTP, locking information, IC configuration and manufacturer information

Additionally the password and password retry counter are allocated in non-addressable part of the memory and are accessible via dedicated commands only.

Figure 11 shows the memory structure of the SLE 66R01P and SLE 66R01PN chip.



	Serial number	00_H	uid0	uid1	uid2	BCC0	Service Area 1
	Serial number	01_H	uid3	uid4	uid5	uid6	
	Configuration / Lock	02_H	BCC1	CONFIG	LOCK0	LOCK1	
	OTP	03_H	OTP0	OTP1	OTP2	OTP3	
	User Data	04_H	Data0	Data1	Data2	Data3	User Area 1
	User Data	05_H	Data4	Data5	Data6	Data7	
	User Data	06_H	Data8	...	...	...	
	...	...	...	...	...	...	
	...	...	...	...	...	...	
	User Data	$0F_H$	Data44	Data45	Data46	Data47	
Password protectable	User Data	10_H	Data48	Data49	Data50	Data51	User Area 2
	User Data	11_H	Data52	...	...	...	
	...	...	...	...	...	...	
	...	...	...	...	...	...	
	User Data / Counter	22_H	Data120 / Counter	Data121 / Counter	Data122 / Counter	Data123 / 00_H	
	User Data / Counter	23_H	Data124 / Counter	Data125 / Counter	Data126 / Counter	Data127 / 00_H	
	Lock	24_H	LOCK2	LOCK3	LOCK4	LOCK5	Service Area 2
	Manufacturer	25_H	MAN0	MAN1	MAN2	MAN3	
			PASSWORD				
			PASSWORD RETRY COUNTER				

Figure 11 my-d™ move and my-d™ move NFC memory organization

5.1 User memory Area 1 and 2

Blocks from address 04_H to 23_H belong to the user memory Area (1 and 2). This part of the memory is readable/ writable as well as lockable against unintentional overwriting using a locking mechanism.

Moreover the user memory Area 2 above the address 10_H can be protected with a password against unintentional reading or reading/writing.

5.2 Service Area 1 and 2

The Service Area 1 (block address 00_H to 03_H) contains:

- 7 byte double-size UID (plus two bytes of UID BCC information)
- Configuration byte
- LOCK0 and LOCK1 to lock the OTP block and blocks in the user Area 1
- 32-bit OTP memory

The Service Area 2 (block address 24_H to 25_H) contains:

- LOCK2 - LOCK5 to lock blocks in user Area 2
- Manufacturer data

5.2.1 Unique identifier (UID)

The 9 bytes of the UID (7 byte UID +2 bytes BCC information) are allocated in block 00_H, block 01_H and byte 1 of block 02_H of the my-d™ move and my-d™ move NFC memory. All bytes are programmed and locked during the manufacturing process. These bytes cannot be changed.

For the content of the UID the following definitions apply:

- SLE 66R01P and SLE 66R01PN support Cascade Level 2 UID according to the ISO/IEC 14443-3 Type A which is a 7 byte unique number

The table below describes the content of the UID including the BCC information.

Table 7 **UID description**

Cascade Level 2 - double-size UID										
UID byte	CT[1]	uid0[2]	uid1[3]	uid2	BCC0[4]	uid3	uid4	uid5	uid6	BCC1[4]

[1] CT is the Cascade Tag and designates CL2. It has a value of 88_H. Please note that CT is hardwired and not stored in the memory.

[2] uid0 is the manufacturer code: 05_H.

[3] uid1 is the Chip Family Identifier. The higher significant nibble identifies a my-d™ move and my-d™ move NFC chip (0011_B). The lower significant nibble of uid1 is part of the serial number.

[4] BCCx are the UID CLn checkbytes calculated as Exclusive-OR over the four previous bytes (as described in ISO/IEC 14443-3 Type A [4]). BCCx is stored in the memory and read-out during the anti-collision.

5.2.2 Configuration byte

The configuration byte defines the configurable functionality of the my-d™ move and my-d™ move NFC. It is allocated in byte 1 of block 02_H. At delivery all bits of the configuration byte are set to 0_B. Note that the configuration byte is One Time Programmable (OTP) byte. Bits allocated in this byte can only be logically set to 1_B, which is an irreversible process i.e. bits can not be reset to 0_B afterwards.

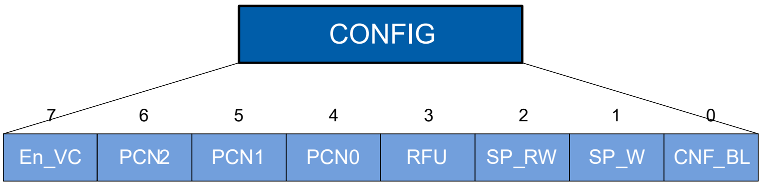


Figure 12 **Configuration byte**

Table 8 **Configuration byte definition**

Configuration bit	Abbreviation	Description
Configuration byte Lock	CNF_BL	0_B ... configuration byte programmable 1_B ... configuration byte locked
Set password for write access	SP-W	0_B ... the write password is not active 1_B ... the write password is active for write Commands which are applied to all blocks starting from the address 10_H
Set password for read and write access	SP_WR	0_B ... the read and write password is not active 1_B ... the read and write password is active for read, write and decrement commands for all blocks above address $0F_H$
RFU	RFU	Reserved for the future use
Initial value of the password retry counter	PCN2 PCN1 PCN0	000_B ... default setting 111_B ... maximal initial value (7_D) Password retry counter is only active if the initial value is different than 0_D
16-bit value counter	En_VC	0_B ... value counter is not configured, blocks 22_H and 23_H are user data blocks 1_B ... value counter is set, blocks 22_H and 23_H are reserved for the 16-bit value counter

Note: The CNF_BL bit is active immediately active after writing. To activate the new configuration of SP-W, SP-WR and VCRN 16 bits the execution of REQA or WUPA commands is required. The new value of the password retry counter (PCN2, PCN1 and PCN0 bits) is active immediately, i.e. is read each time the information is required (during the execution of the access command).

5.2.2.1 Locking mechanism for the configuration byte

The my-d™ move and my-d™ move NFC is delivered with all bits of configuration byte set to 0_B (refer to Configuration byte). The issuer should define the functionality of a chip as required (set e.g. write and/or read/write password, the password retry counter, the 16-bit value counter etc.) and lock the configuration byte. Once the configuration byte is locked no further changes to the configuration byte are possible.

Note: If all three BL bits in the LOCK0 byte are set to 1_B, block 02_H is locked. It is then not possible to change the value of this particular block (02_H) anymore.

5.2.3 Locking mechanism

Bytes LOCK0, LOCK1 allocated in block 02_H and LOCK2, LOCK3, LOCK4 and LOCK5 allocated in block 24_H represent the one time field programmable bits which are used to lock the blocks in the specified address range from block 03_H (OTP Block) to 23_H.

Each block in this range can be individually locked to prevent further write access. A locking mechanism of each block is irreversible, i.e. once the locking information of a particular block (Lx) is set to 1_B it can not be reset back to 0_B anymore. Figure 13 illustrates the locking bytes with the corresponding locking bits.

Furthermore, it is possible to freeze the locking information of some memory areas by setting block locking (BL) bits e.g. if the bit BL 15-10 is set to 1_B then the locking information for the corresponding area (L10 to L15) is not changeable any more. See the example in Table 9.

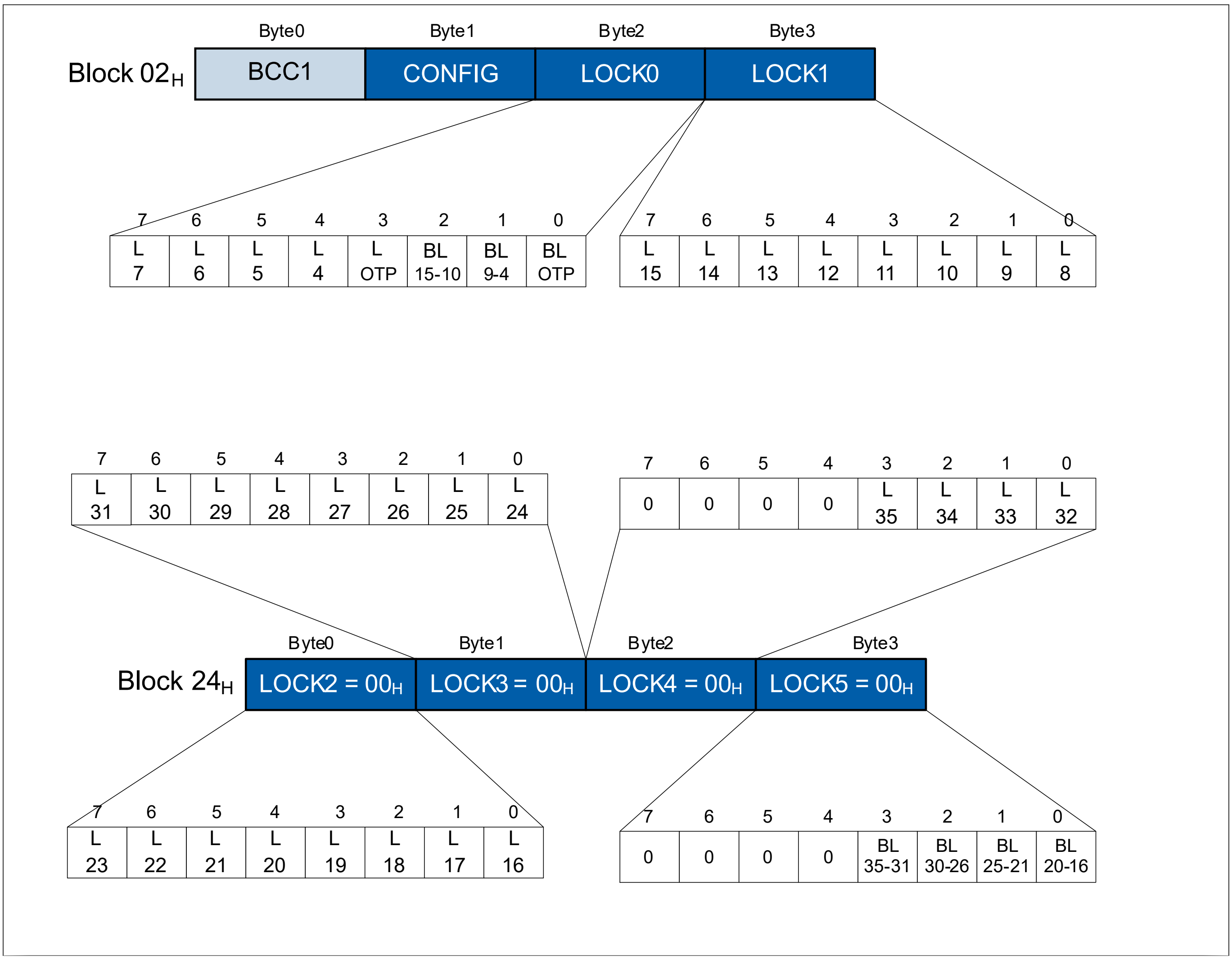


Figure 13 **Locking and block locking mechanism**

The write one block (WR1B) command should be used to set the locking or block locking information of a certain block.

If WR1B is applied to block 02_H then:

- The byte 0 (BCC1) will not be changed
- The byte 1 (configuration byte) will be changed only if it is not locked

If WR1B is applied to block 24_H then:

- The byte 2 [7..4] = Lock4[7..4] and
- The byte 3 [7..4] = Lock5[7..4] will not be changed neither

The locking and block locking for a certain block is active immediately after writing. That means that it is not necessary to execute the REQA or WUPA command in order to activate the locking.

Note: *If all three BL bits in the LOCK0 byte are set to 1_B then Block 02_H is locked. It is not possible to change the locking bits of this block any more. The same applies for block 24_H. If BL bits of the LOCK5 byte are set to 1_B then this block is locked. In this case the SLE 66R01P and SLE 66R01PN responds with NACK to a corresponding Write command.*

Table 9 Example for OTP block lock and block lock

BL OTP	L OTP	OTP block state
0_B	0_B	OTP block unlocked
0_B	1_B	OTP block locked
1_B	0_B	OTP block unlocked and can not be locked ever more
1_B	1_B	OTP block locked

An anti-tearing mechanism is implemented for lock bytes on the SLE 66R01P and SLE 66R01PN. This mechanism prevents a stored value to be lost in case of a tearing event. This increases the level of data integrity and it is transparent to the customer.

5.2.4 OTP block

The block 03_H is a One Time Programmable (OTP) block. Bits allocated in this block can only be logically set to 1_B, which is an irreversible process i.e. bits can not be reset to 0_B afterwards.

The write one block (WR1B) command should be used to program a specific OTP value. Incoming data of the WR1B command are bit-wise OR-ed with the current content of the OTP block and the result is written back to the OTP block.

Table 10 Writing to OTP block (block 03_H) from the user point of view

OTP block	Representation bit-wise	Description
Initial value	$0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000_B$	Production setting
Write $[55550003]_H$	$0101\ 0101\ 0101\ 0101\ 0000\ 0000\ 0000\ 0011_B$	Bit-wise “OR” with previous content of block 03_H
Write $[AA55001C]_H$	$1111\ 1111\ 0101\ 0101\ 0000\ 0000\ 0001\ 1111_B$	Bit-wise “OR” with previous content of block 03_H

An anti-tearing mechanism is implemented for the OTP block on the my-d™ move and my-d™ move NFC. This mechanism prevents the stored value to be lost in case of a tearing event. This increases the level of data integrity and is transparent to the customer.

5.2.5 Manufacturer block (25_H)

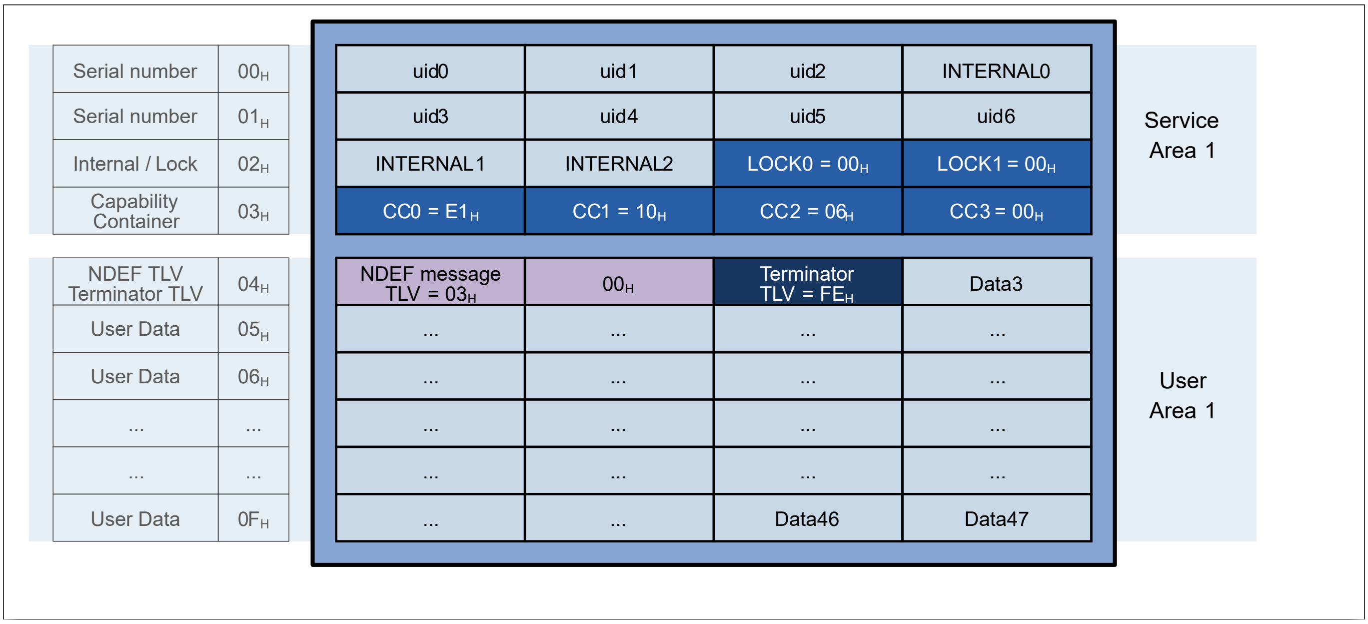
The manufacturer block is used to store the my-d™ move and my-d™ move NFC internal on-chip configuration data and the manufacturing data such as Week and Year of production, lot and wafer counter etc. This block is programmed and locked at manufacturing.

5.3 Memory organization for NFC Forum Type 2 Tag

This section describes how to map the my-d™ move and my-d™ move NFC memory into the memory structures defined in the NFC Forum Type 2 Tag technical specification. This enables the usage of the my-d™ move and my-d™ move NFC as an NFC Forum Type 2 Tag compatible chip.

5.3.1 NFC Forum static memory structure

The static memory structure is applied to a NFC Forum Type 2 Tag with a memory size equal to 64 bytes (see Figure 14). Blocks 04_H to $0F_H$ are available to store user data.



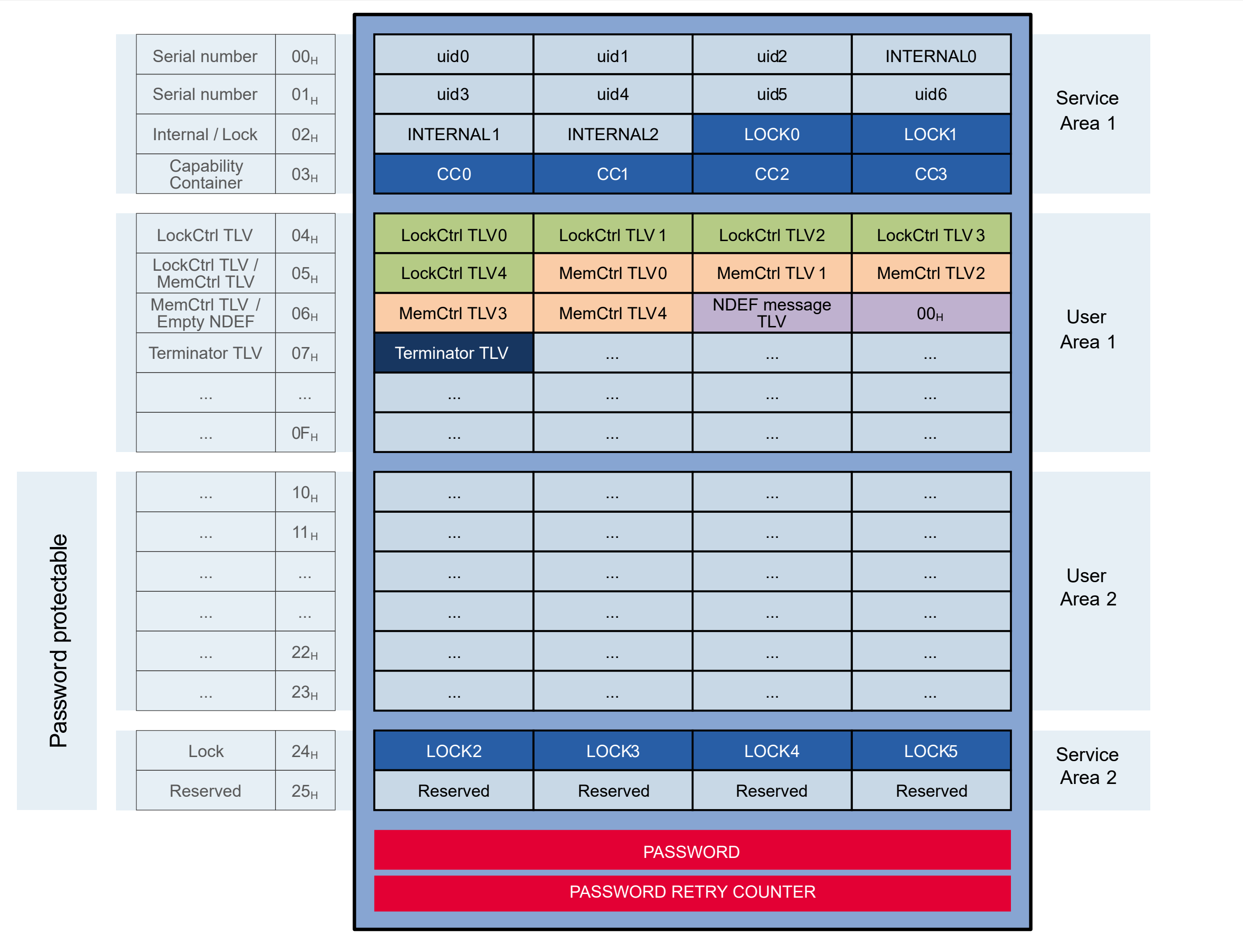
Serial number	00_H	uid0	uid1	uid2	INTERNAL0	Service Area 1
Serial number	01_H	uid3	uid4	uid5	uid6	
Internal / Lock	02_H	INTERNAL1	INTERNAL2	LOCK0 = 00_H	LOCK1 = 00_H	
Capability Container	03_H	CC0 = $E1_H$	CC1 = 10_H	CC2 = 06_H	CC3 = 00_H	
NDEF TLV Terminator TLV	04_H	NDEF message TLV = 03_H	00_H	Terminator TLV = FE_H	Data3	User Area 1
User Data	05_H	...	...	...	...	
User Data	06_H	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	
User Data	$0F_H$	...	...	Data46	Data47	

Figure 14 **Static memory structure**

The static memory structure is characterized by the NDEF message TLV (03_H) starting at block address 04_H. The NFC data shown in Figure 14 is an empty NDEF message (see Table 12).

5.3.2 NFC Forum dynamic memory structure

The dynamic memory structure can be applied to NFC Forum Type 2 Tags with bigger memories than 64 bytes. Figure 15 shows a generic memory layout with a dynamic memory structure (based on the my-d™ move and my-d™ move NFC chip).



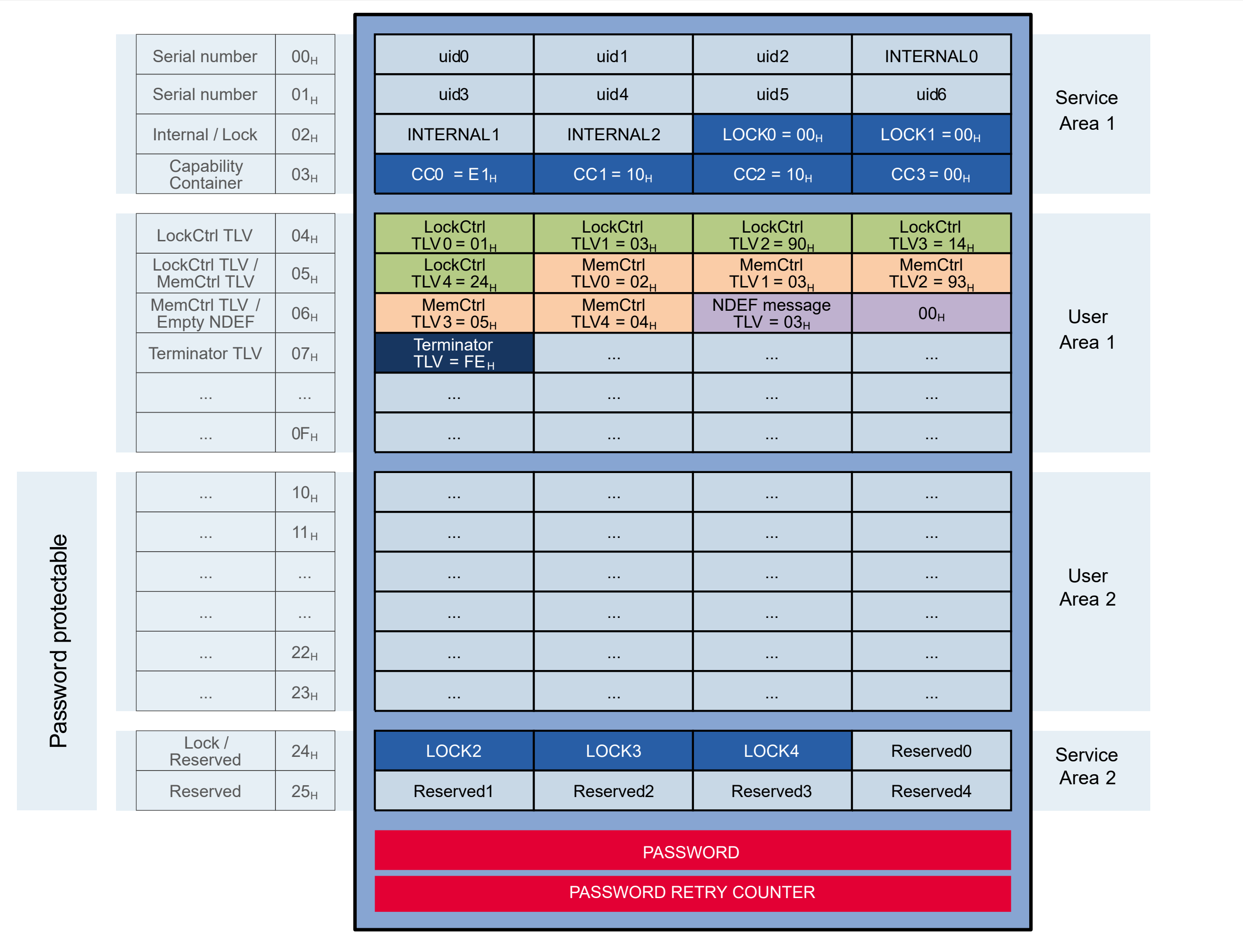
	Serial number	00_H	uid0	uid1	uid2	INTERNAL0	Service Area 1
	Serial number	01_H	uid3	uid4	uid5	uid6	
	Internal / Lock	02_H	INTERNAL1	INTERNAL2	LOCK0	LOCK1	
	Capability Container	03_H	CC0	CC1	CC2	CC3	
	LockCtrl TLV	04_H	LockCtrl TLV0	LockCtrl TLV 1	LockCtrl TLV2	LockCtrl TLV 3	User Area 1
	LockCtrl TLV / MemCtrl TLV	05_H	LockCtrl TLV4	MemCtrl TLV0	MemCtrl TLV 1	MemCtrl TLV2	
	MemCtrl TLV / Empty NDEF	06_H	MemCtrl TLV3	MemCtrl TLV4	NDEF message TLV	00_H	
	Terminator TLV	07_H	Terminator TLV	...	...	...	
	...	...	...	...	...	...	
	...	$0F_H$	...	...	...	...	
Password protectable	...	10_H	...	...	...	...	User Area 2
	...	11_H	...	...	...	...	
	...	...	...	...	...	...	
	...	...	...	...	...	...	
	...	22_H	...	...	...	...	
	...	23_H	...	...	...	...	
	Lock	24_H	LOCK2	LOCK3	LOCK4	LOCK5	Service Area 2
	Reserved	25_H	Reserved	Reserved	Reserved	Reserved	
			PASSWORD				
			PASSWORD RETRY COUNTER				

Figure 15 **Generic NFC Forum Type 2 Tag dynamic memory layout (based on SLE 66R01P/SLE 66R01PN)**

Compared to the static memory structure the dynamic memory structure is characterized by the NDEF message TLV starting after the lock control TLV and memory control TLV (the lock control TLV starts at block 04_H).

Within a dynamic memory structure dynamic lock bytes and reserved bytes might be located at any address in the data area (see LOCK2 - LOCK5, reserved shown in Figure 15). The location and the number of bytes used for these purposes are defined by the settings of the lock control TLV respectively memory control TLV.

The following example for a dynamic memory structure (shown in Figure 16) focuses on my-d™ move and my-d™ move NFC.



Serial number	00_H	uid0	uid1	uid2	INTERNAL0	Service Area 1
Serial number	01_H	uid3	uid4	uid5	uid6	
Internal / Lock	02_H	INTERNAL1	INTERNAL2	LOCK0 = 00_H	LOCK1 = 00_H	
Capability Container	03_H	CC0 = $E1_H$	CC1 = 10_H	CC2 = 10_H	CC3 = 00_H	
LockCtrl TLV	04_H	LockCtrl TLV0 = 01_H	LockCtrl TLV1 = 03_H	LockCtrl TLV2 = 90_H	LockCtrl TLV3 = 14_H	User Area 1
LockCtrl TLV / MemCtrl TLV	05_H	LockCtrl TLV4 = 24_H	MemCtrl TLV0 = 02_H	MemCtrl TLV1 = 03_H	MemCtrl TLV2 = 93_H	
MemCtrl TLV / Empty NDEF	06_H	MemCtrl TLV3 = 05_H	MemCtrl TLV4 = 04_H	NDEF message TLV = 03_H	00_H	
Terminator TLV	07_H	Terminator TLV = FE_H	...	...	...	
...	...	...	...	...	...	
...	$0F_H$	...	...	...	...	
...	10_H	...	...	...	...	User Area 2
...	11_H	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	
...	22_H	...	...	...	...	
...	23_H	...	...	...	...	
Lock / Reserved	24_H	LOCK2	LOCK3	LOCK4	Reserved0	Service Area 2
Reserved	25_H	Reserved1	Reserved2	Reserved3	Reserved4	
		PASSWORD				
		PASSWORD RETRY COUNTER				

Figure 16 **Example of an NFC Forum Type 2 Tag dynamic memory layout (based on SLE 66R01P/SLE 66R01PN)**

If a NFC Forum Type 2 Tag compliant chip with lock control TLV and memory control TLV is required, NFC Forum Type 2 Tag specific data such as capability container, lock control TLV, memory control TLV, NDEF message and terminator TLV should be written to the memory according to the given hardware configuration.

Figure 16 holds valid lock control TLV and the memory control TLV settings within a dynamic memory structure specially suited for the my-d™ move and my-d™ move NFC devices. For my-d™ move and my-d™ move NFC the position of the static and dynamic lock bytes is hard-wired and it is not possible to change their position in the memory.

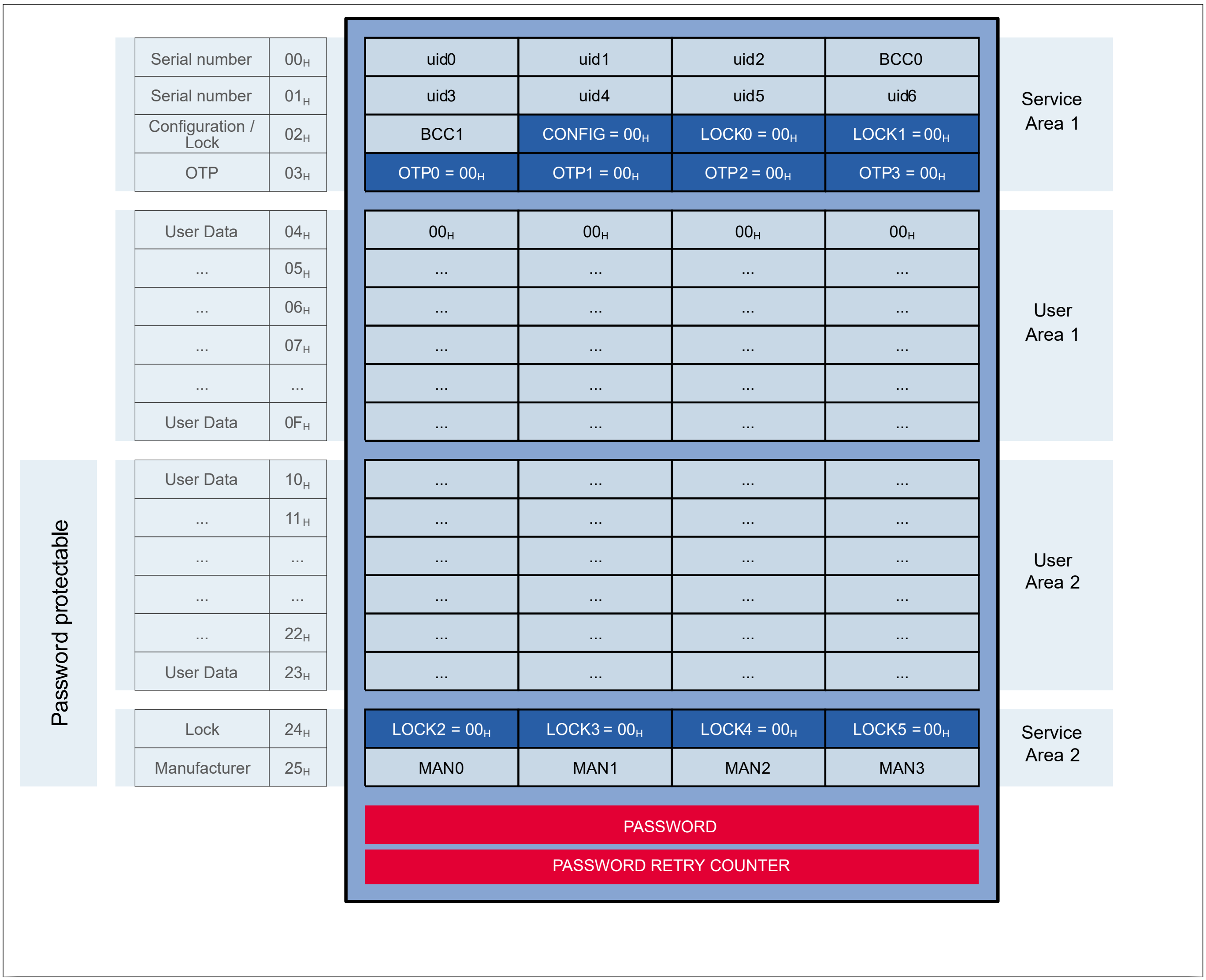
- Static lock bytes LOCK0 and LOCK1 are allocated in block 2, bytes 2 and 3. LOCK0 and LOCK1 are used to lock blocks from address 00_H to $0F_H$
- Dynamic lock bytes LOCK2 to LOCK5 are allocated in block 24_H. These LOCKx bytes are used to lock blocks starting from address 10_H. The position and the number of dynamic lock bits is coded into the lock control TLV as shown above. In this example 20 lock bits are required to lock the user memory blocks 10_H to 23_H. Furthermore the memory control TLV defines the location and number of reserved bytes in the memory

5.4 Transport configuration

Figure 15 shows the memory overview of SLE 66R01P and SLE 66R01PN. The following sections provide details about the initial memory content of these devices.

5.4.1 Transport configuration my-d™ move

The transport configuration of SLE 66R01P contains the following information:



	Serial number	00_H	uid0	uid1	uid2	BCC0	Service Area 1
	Serial number	01_H	uid3	uid4	uid5	uid6	
	Configuration / Lock	02_H	BCC1	CONFIG = 00_H	LOCK0 = 00_H	LOCK1 = 00_H	
	OTP	03_H	OTP0 = 00_H	OTP1 = 00_H	OTP2 = 00_H	OTP3 = 00_H	
	User Data	04_H	00_H	00_H	00_H	00_H	User Area 1
	...	05_H	...	...	...	...	
	...	06_H	...	...	...	...	
	...	07_H	...	...	...	...	
	...	...	...	...	...	...	
	User Data	$0F_H$	...	...	...	...	
Password protectable	User Data	10_H	...	...	...	...	User Area 2
	...	11_H	...	...	...	...	
	...	...	...	...	...	...	
	...	...	...	...	...	...	
	...	22_H	...	...	...	...	
	User Data	23_H	...	...	...	...	
	Lock	24_H	LOCK2 = 00_H	LOCK3 = 00_H	LOCK4 = 00_H	LOCK5 = 00_H	Service Area 2
	Manufacturer	25_H	MAN0	MAN1	MAN2	MAN3	
			PASSWORD				
			PASSWORD RETRY COUNTER				

Figure 17 my-d™ move transport configuration

- Service Area 1 contains:
  - Predefined UID (incl. BCC bytes); Read-only
  - CONFIG, LOCK0, LOCK1 set to 00_H
  - LOCK0, LOCK1 set to 00_H
  - OTP0 - OTP3 set to 00_H
- User Area 1:
  - All data bytes set to 00_H
- User Area 2:
  - All data bytes set to 00_H

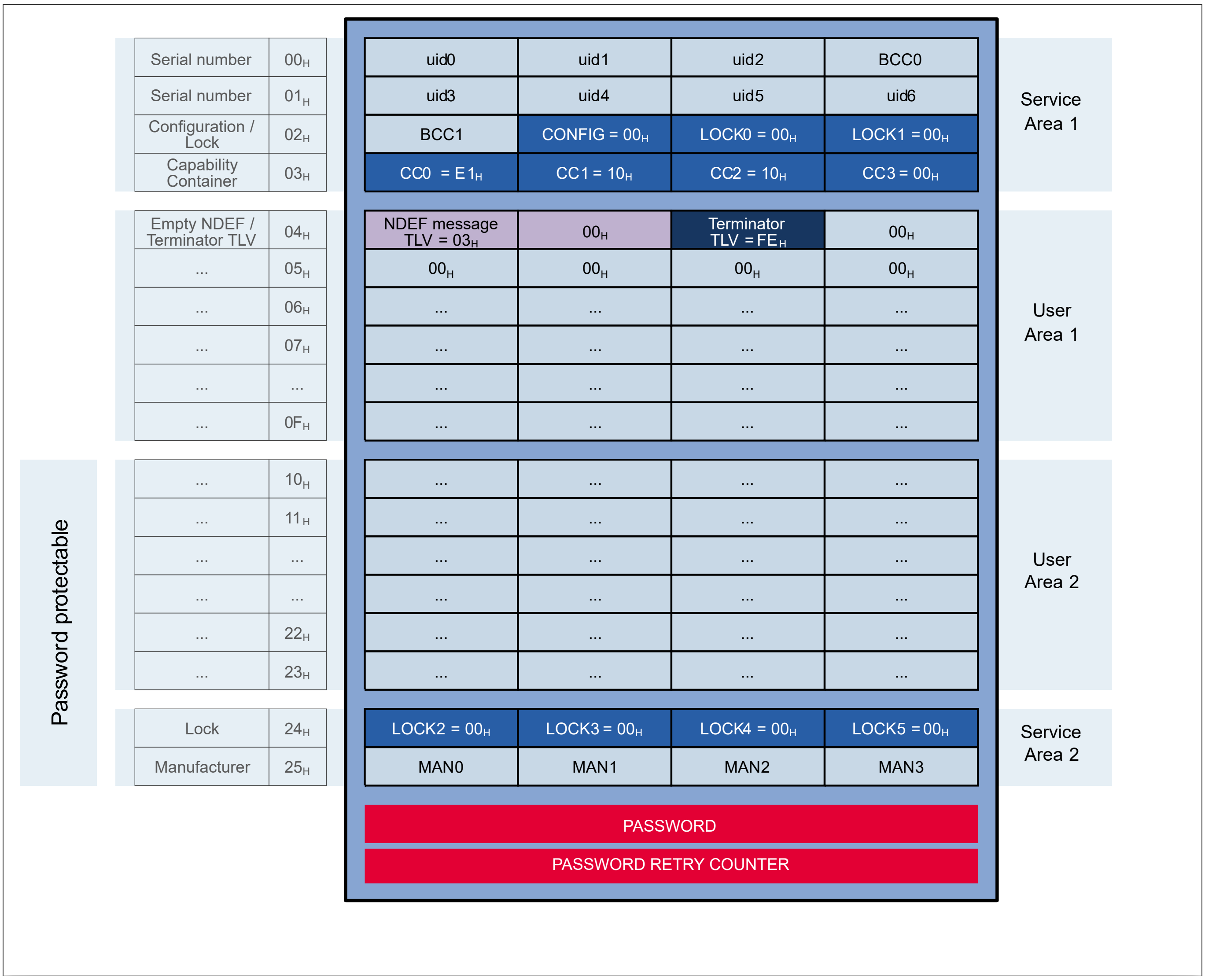
- Service Area 2 contains:
    - LOCK2 - LOCK5 set to 00_H
    - Manufacturer data; Read-only
- Password set to 00_H 00_H 00_H 00_H
- Password retry counter
    - Deactivated by the setting of the CONFIG byte

The SLE 66R01P may be configured to INITIALIZED state according to the definition to the NFC Forum Type 2 Tag life cycle by writing.

- Capability container bytes (see Table 11) to block 03_H
- Empty NDEF message TLV including; Terminator TLV (see Table 12) to block 04_H

5.4.2 Transport configuration my-d™ move NFC

SLE 66R01PN is delivered in the INITIALIZED state (life cycle) according to the NFC Forum Type 2 Tag specification.



	Serial number	00_H	uid0	uid1	uid2	BCC0	Service Area 1
	Serial number	01_H	uid3	uid4	uid5	uid6	
	Configuration / Lock	02_H	BCC1	CONFIG = 00_H	LOCK0 = 00_H	LOCK1 = 00_H	
	Capability Container	03_H	CC0 = $E1_H$	CC1 = 10_H	CC2 = 10_H	CC3 = 00_H	
	Empty NDEF / Terminator TLV	04_H	NDEF message TLV = 03_H	00_H	Terminator TLV = FE_H	00_H	User Area 1
	...	05_H	00_H	00_H	00_H	00_H	
	...	06_H	...	...	...	...	
	...	07_H	...	...	...	...	
	...	...	...	...	...	...	
	...	$0F_H$	...	...	...	...	
Password protectable	...	10_H	...	...	...	...	User Area 2
	...	11_H	...	...	...	...	
	...	...	...	...	...	...	
	...	...	...	...	...	...	
	...	22_H	...	...	...	...	
	...	23_H	...	...	...	...	
	Lock	24_H	LOCK2 = 00_H	LOCK3 = 00_H	LOCK4 = 00_H	LOCK5 = 00_H	Service Area 2
	Manufacturer	25_H	MAN0	MAN1	MAN2	MAN3	
			PASSWORD				
			PASSWORD RETRY COUNTER				

Figure 18 my-d™ move NFC transport configuration

- Service Area 1 contains:
    - Predefined UID; Read-only

  - CONFIG, LOCK0 and LOCK1 set to 00_H
  - OTP0 - OTP3 contains the CAPABILITY CONTAINER (see Table 11)
- User Area 1:
  - Contains empty NDEF message TLV including terminator TLV (= FE_H) as indicated in Table 12
  - All other data bytes set to 00_H
- User Area 2:
  - All data bytes set to 00_H
- Service Area 2 contains:
  - LOCK2 - LOCK5 set to 00_H
  - Manufacturer data; Read-only
- Password set to 00_H 00_H 00_H 00_H
- Password retry counter
  - Deactivated by the setting of the CONFIG byte

Table 11 **Capability container settings for my-d™ move and my-d™ move NFC**

Chip type	**CC0**	**CC1**[1]	**CC2**[2]	**CC3**
SLE 66R01PN	$E1_H$	10_H (may be changed to 11_H if needed)	10_H	00_H

[1] my-d™ move and my-d™ move NFC also support version 1.1 of the NFC Forum Type 2 Tag specification.
[2] CC2 indicates the memory size of the data area of the Type 2 Tag; the given values represent the maximum values for the chips.

Table 12 defines the empty NDEF message TLV (identified with the Tag field value of 03_H). The length field value is set to 00_H; due to that the value field is not present.

The terminator TLV (FE_H) is the last TLV block in the data area.

Table 12 **Empty NDEF message**

NDEF message TLV			**Terminator TLV**		
Tag	**Length**	**Value**	**Tag**	**Length**	**Value**
03_H	00_H	-	FE_H	-	-

Note: *The pre-configuration of SLE 66R01PN is non-reversible and the my-d™ move NFC cannot be overwritten and used as plain, standard my-d™ move anymore.*

6 Password

An issuer can protect the blocks above address $0F_H$ with a 32-bit write and/or read/write password by enabling the password functionality.

The issuer can enable the password functionality by setting the bit 1 (SP-W) of the configuration byte[2] for write password access and/or bit 2 (SP-WR) of the configuration byte for read/write password access (see Configuration byte).

The new configuration is activated after the next transition to the IDLE/HALT state is executed.

The my-d™ move and my-d™ move NFC is delivered without password protection i.e. default value of the SP-W and SP-WR bits is 0_B.

Table 13 **Access rights**

SP-WR	SP-W	Access right
0_B	0_B	Read plain/write plain (default setting)
0_B	1_B	Read plain/write protected
1_B	X_B	Read protected/write protected

There is only one 32-bit password value for both read and/or read/write access.

6.1 Password block

The password block holds 32-bit of password data and is stored in a memory location which is accessible with dedicated commands only. The initial value of the password block is 00_H 00_H 00_H 00_H and should be changed after delivery. The set password SPWD[3] command is used to change the content of the password block.

- If the my-d™ move and my-d™ move NFC is not configured for password protection i.e. bits for SP-W or SPWR are not set, the password block will be overwritten with new password data
- If the my-d™ move and my-d™ move NFC is configured for password protection i.e. if SP-W and/or SP-WR bits are set, the password block will be overwritten with new password data only after the chip has been successfully verified with the Access ACS[4] command

6.2 Password retry counter

A password retry counter counts the number of incorrect accesses to a password protected my-d™ move and my-d™ move NFC. The number of incorrect accesses can be predefined by setting the bits [6:4] of the configuration byte. This number is called the initial value of the password retry counter.

The password retry counter is active if the number of incorrect accesses is higher than 0_D i.e. bit [6:4] of the configuration byte are NOT all set to zero. The write one block (WR1B) command should be used to overwrite the password retry counter value. The initial value of the password retry counter is active immediately after it is written.

To prevent any further changes on a predefined password retry counter value it is recommended to lock the configuration byte. Once the configuration byte is locked, the status of an initial counter value is locked, i.e. are no further changes to these bits are possible.

The my-d™ move and my-d™ move NFC is delivered with a disabled password retry counter i.e. the initial value of the password retry counter is equal to 000_B. The maximum value of the password retry counter is 7_D, and valid values which activate the usage of the password retry counter are in the range from 1_D to 7_D.

Figure 19 shows how to configure the password functionality on the my-d™ move and my-d™ move NFC.

---

[2] For more information about configuration byte see Configuration byte.

[3] For more information about SPWD command see Set password (SPWD).

[4] For more information about ACS command see Access (ACS).

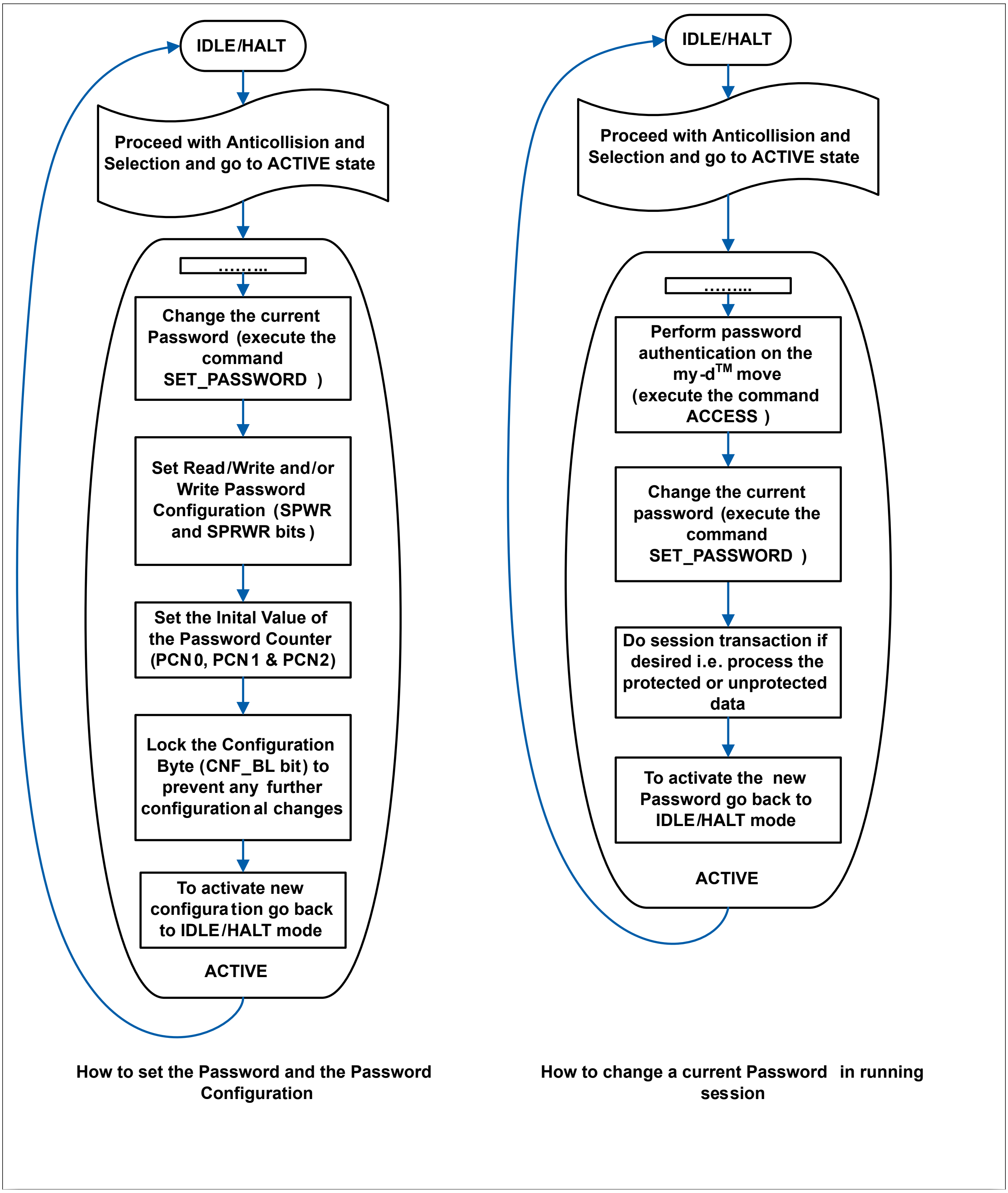


Figure 19 Password and password retry counter configuration

6.3 Anti-tearing mechanism for password retry counter

The password retry counter block is stored in the non-directly accessible part of the memory and for data protection reasons stored redundantly (anti-tearing). This mechanism prevents a stored value of being lost in case of a tearing event. This increases the level of data integrity and is transparent to the customer.

During the execution of the access command the my-d™ move and my-d™ move NFC performs the following actions:

- Compares the incoming password and the password stored in the my-d™ move and my-d™ move NFC
- Pass retry counter enabled:
    - Resets the password retry counter if the password matches. The my-d™ move and my-d™ move NFC responds with an ACK
    - Increments the password retry counter if the passwords do not match and if the password counter has not reached the highest possible value and my-d™ move and my-d™ move NFC responds with a NACK
    - If the password retry counter has already reached the highest possible value (initial password retry counter value), then no further increase is done. The my-d™ move and my-d™ move NFC responds with a NACK
- Depending on the setting of the access bits the access to the memory above block $0F_H$ is granted:
    - SP-W = 1_B: Read access only, no write access
    - SP-RW = 1_B: No read and no write access

7 16-bit value counter functionality

The value counter is a 16-bit value, which provides a mechanism to store some value (points, money…) on a my-d™ move and my-d™ move NFC chip. Normally it is only possible to decrement this value. However, if certain conditions are met it is also possible to reload the counter to an arbitrary 16-bit value. The availability of the value counter in the my-d™ move and my-d™ move NFC is configurable by setting the bit 7 of the configuration byte.

7.1 Value counter format

If configured two 4 byte blocks, 22_H and 23_H, are reserved for the storage of the value counter value. The my-d™ move and my-d™ move NFC supports the detection of an interrupted or corrupted (teared) counter programming operation of the value counter. For the purpose the concept of **redundant saving** of the value counter as well as **temporarily double saving** of the value counter value during the programming process is implemented.

The redundant saving means, that the value counter is represented in the dedicated block by a 3 byte value: Counter LSB, inverted counter LSB and counter MSB. The fourth byte of the block is not used for the counter and carries 00_H data. Counter LSB carries the lower value and counter MSB carries the higher value of the value counter in hexadecimal representation.

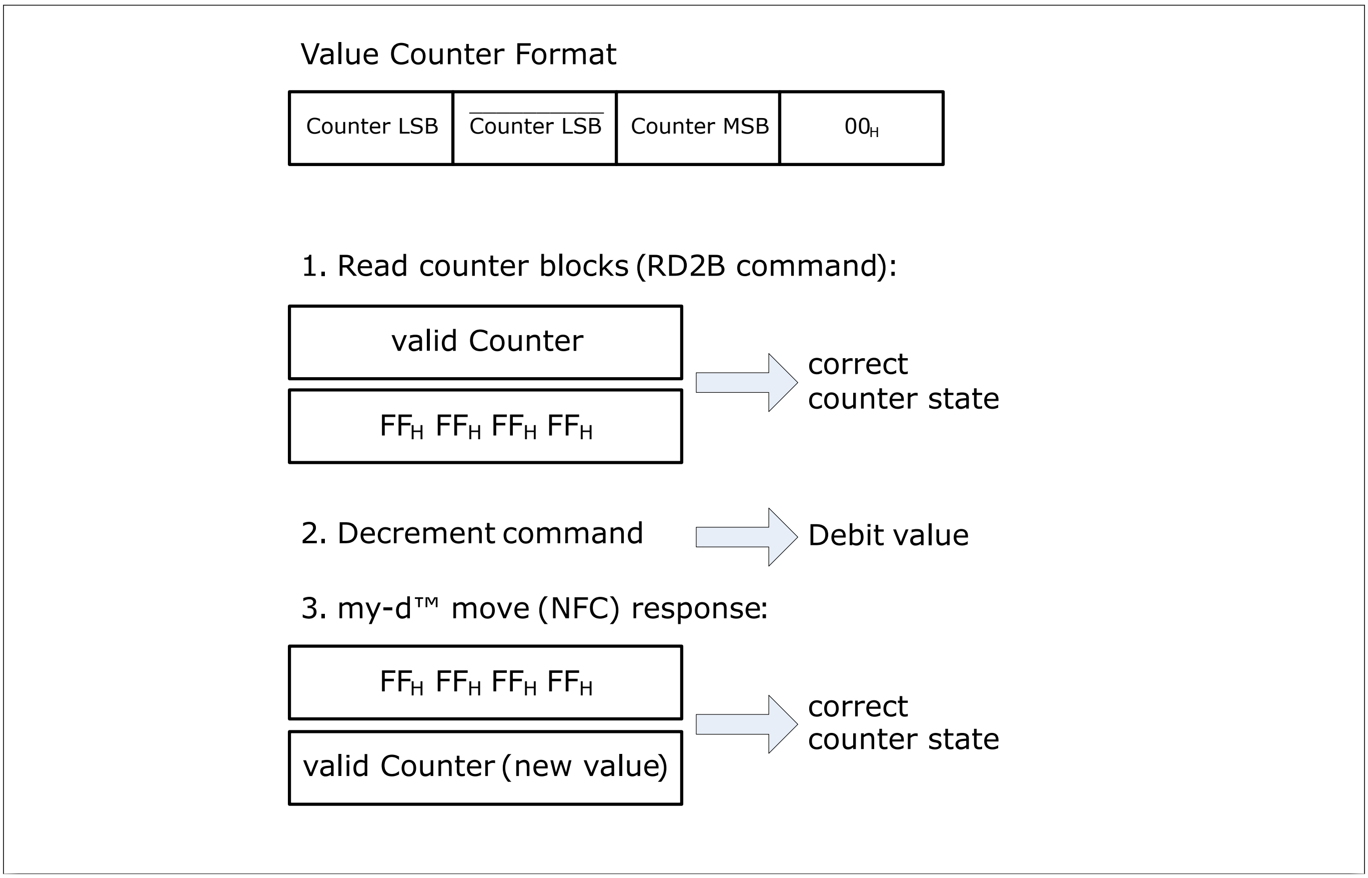
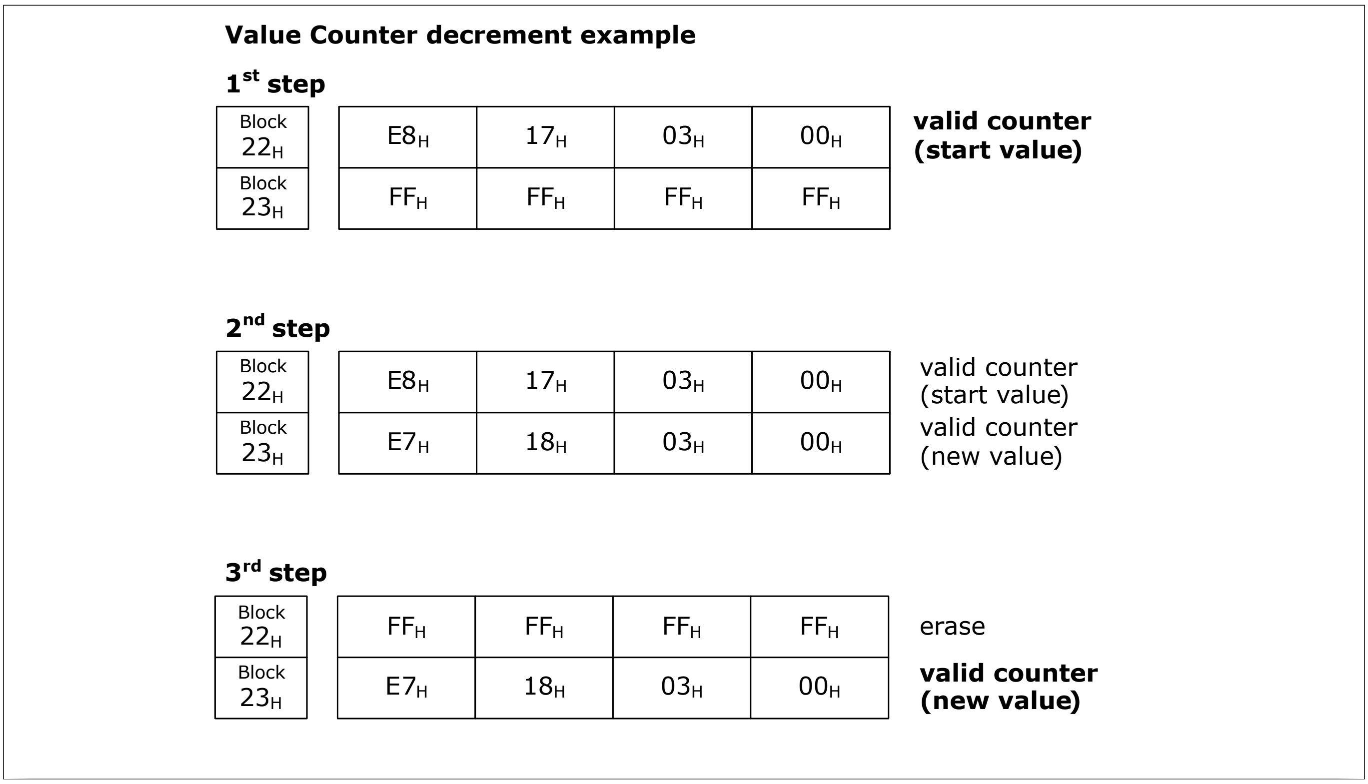


Figure 20 Value counter-principle

For example: The value $1000_D = 03E8_H$ → value counter LS byte = $E8_H$ and value counter MS byte = 03_H. The value counter block looks like: Byte3 .. Byte0 = $000317E8_H$; where 00_H represents the data in byte3.

The temporarily double saving means that value counter is stored twice in two different memory blocks. Figure 21 shows an example for the value counter representation and the decrementing of the value 1000_D by 1_D.

During the programming process of the new value counter, one block holds the current valid value and the other block is used to write the new counter value. At the end of programming cycle the current valid value, becomes an invalid value while it is erased (all bytes set to FF_H) and the other one holds the new valid value.



Value Counter decrement example

1st step

Block 22_H	$E8_H$	17_H	03_H	00_H	**valid counter (start value)**
Block 23_H	FF_H	FF_H	FF_H	FF_H	

2nd step

Block 22_H	$E8_H$	17_H	03_H	00_H	valid counter (start value)
Block 23_H	$E7_H$	18_H	03_H	00_H	valid counter (new value)

3rd step

Block 22_H	FF_H	FF_H	FF_H	FF_H	erase
Block 23_H	$E7_H$	18_H	03_H	00_H	**valid counter (new value)**

Figure 21 **Value counter decrement example**

7.2 Loading and reading of value counter

Loading of the value counter is done by either:

- Using WR2B command to address 22_H
  - [$A1_H$] [22_H] [$CNT0_H$, $\overline{CNT0}_H$, $CNT1_H$, 00_H, FF_H, FF_H, FF_H, FF_H] [$CRC0_H$, $CRC1_H$]
- Using two WR1B commands to address 22_H and 23_H
  - [$A2_H$] [22_H] [$CNT0_H$,$\overline{CNT0}_H$,$CNT1_H$, 00_H] [$CRC0_H$, $CRC1_H$]
  - [$A2_H$] [23_H] [FF_H,FF_H,FF_H,FF_H] [$CRC0_H$, $CRC1_H$]
- It is also possible to use Compatibility Write command to initialize the counter, but this is not recommended

It is crucial to initialize both value counter blocks for the correct counter operation.

Reading of value counter is done by either:

- Using RD2B command to addresses 22_H
  - [31_H] [22_H] [$CRC0_H$, $CRC1_H$]
- Using RD4B command to addresses 22_H
  - [30_H] [22_H] [$CRC0_H$, $CRC1_H$]
- Using DCR16 command with parameter 0000_H
  - [$D0_H$] [0000_H] [$CRC0_H$, $CRC1_H$]

7.3 Decrementing value counter and anti-tearing

The DCR16 command is used to decrement the value counter value. For more details refer to the command description in Decrement command (DCR16).

During the execution of the DCR16 command the my-d™ move and my-d™ move NFC performs the following actions:

- Read both value counter blocks
- Determine the correct valid value counter state. Therefore the values stored in blocks 22_H and 23_H are compared
    - Normally one of the counter value blocks is erased or has an incorrect format and the other block holds the valid counter value
    - If both counter values are correctly formatted, the higher value is chosen as the valid counter value. Note that at least one of the counters must be formatted correctly. Otherwise, the value counter block is corrupted and no further decrement of the value counter is possible
    - If both blocks carry invalid values (incorrect format) no further decrement of the value counter is possible. The my-d™ move and my-d™ move NFC then responds with a NACK
- Compares the received parameter and the valid counter value:
    - If the received parameter is equal or lower than the valid counter value the my-d™ move and my-d™ move NFC decrements the valid value by the received parameter, programs this value to the previous invalid value, erases the previous valid value and replies the newly written value
    - If the received parameter is higher then the valid value no decrement is possible and the my-d™ move and my-d™ move NFC responds with a NACK

7.4 Protection mechanisms for the value counter

The my-d™ move and my-d™ move NFC offers some methods to protect the value counter. The following measures should be considered to prevent unauthorized changes.

- The password
    - If a write password is configured i.e. the bit SP-W is set, then the execution of write commands (WR1B, WR2B or CPTWR) on value counter blocks 22_H and 23_H is possible only after password verification
    - If a read/write password is configured i.e. the bit SP-WR is set, then the execution of read commands RD2B and RD4B and decrement command DCR16 on value counter blocks 22_H and 23_H is possible only after password verification
- The locking mechanism for value counter
    - After the configuration of the value counter it is strongly recommended to lock both blocks 22_H and 23_H in order to prevent any unauthorized changes. The locking of blocks 22_H and 23_H is done by changing the locking information of the LOCK4 byte. If the bits 2 and 3 of the LOCK4 byte are set then both value counter blocks are locked
- Writing of the value counter block
    - If blocks 22_H and 23_H are locked then no further overwriting of their values with write commands is possible. Note that if one of the blocks is locked and the other one is not, then it is possible to change the data of the unlocked block by using WR1B command. For this reason it is important to lock both blocks in order to prevent unintentional harm to value counter (i.e. unintentional overwriting or setting an incorrect value or a value with an incorrect format)
- Reading and decrement of the value counter block
    - If blocks 22_H and 23_H are locked then reading and decrementing is still possible. Note that depending on the chip configuration, password verification may be required

8 Communication principle

This chapter describes the functionality of the SLE 66R01P and SLE 66R01PN.

8.1 Communication between a card (PICC) and a reader (PCD)

It is recommended to read the ISO/IEC 14443-3 Type A and NFC Forum Type 2 Tag specifications in conjunction with this document to understand the communication protocol as well as the functionality of the SLE 66R01P and SLE 66R01PN as it is based on these specifications.

8.2 State diagram

The SLE 66R01P and SLE 66R01PN fully compliant to ISO/IEC 14443-3 Type A. All operations on this IC are initiated by an appropriate reader and controlled by the internal logic of the my-d™ move and my-d™ move NFC.

Figure 22 illustrates the state diagram of SLE 66R01P and SLE 66R01PN.

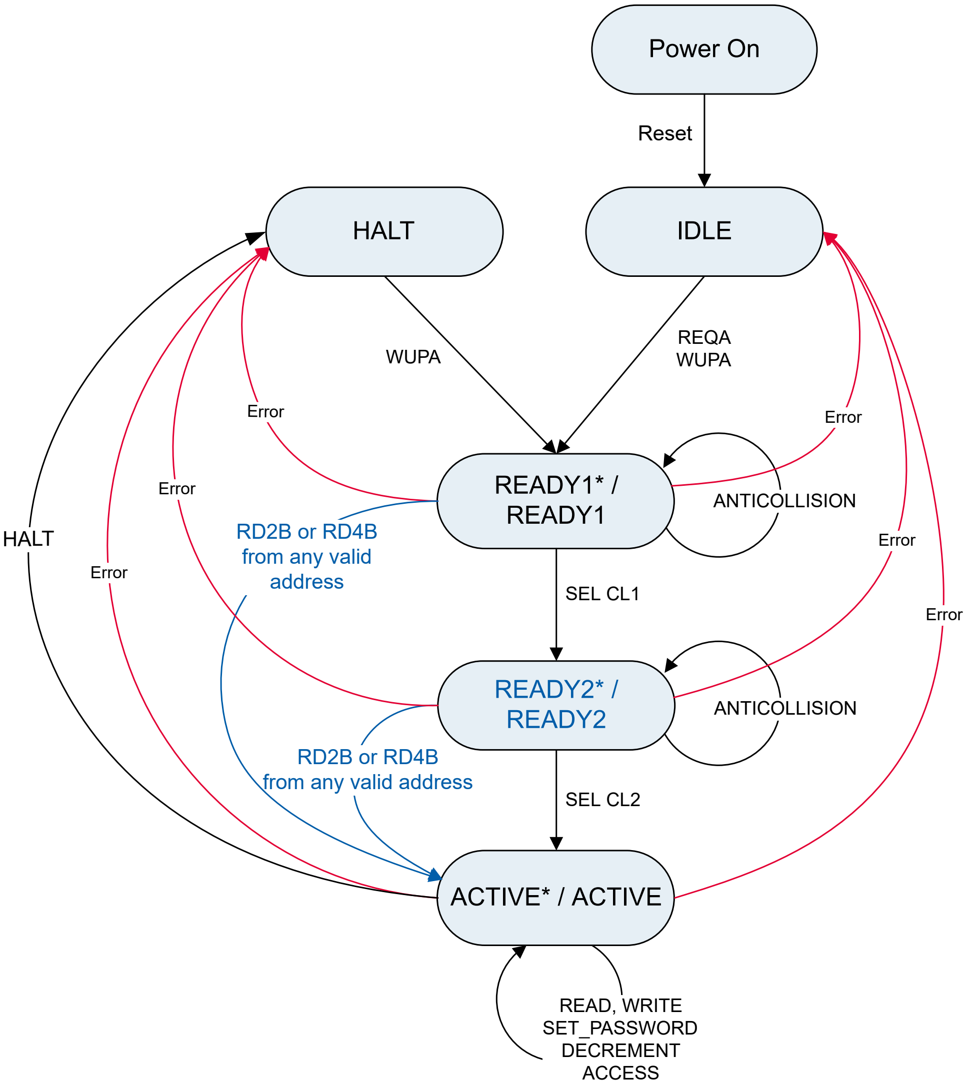


Figure 22 SLE 66R01P and SLE 66R01PN state diagram

Prior to any memory access the card has to be selected according to the ISO/IEC 14443-3 Type A. If the my-d™ move and my-d™ move NFC is configured to be password protected, a password verification is required to access the memory.

If an unexpected command is received, the chip always returns to IDLE or HALT state, depending from which path it came from (the red paths in the state diagram).

8.2.1 IDLE/HALT state

After Power On, the SLE 66R01P and SLE 66R01PN is in IDLE state.

If REQA or WUPA is executed in this state, the SLE 66R01P and SLE 66R01PN transit to the READY1 state. Any other command is interpreted as an error and the chip stays in IDLE state without any response.

If the HLTA command is executed in ACTIVE/ACTIVE* state, the SLE 66R01P and SLE 66R01PN will transit to HALT state. The HALT state can be left only if the chip receives a WUPA command. Any other command is interpreted as an error and the SLE 66R01P and SLE 66R01PN stays in the HALT state without any response.

8.2.2 READY1/READY1* state

In READY1/READY1* state the first part of the UID can be resolved by using ISO/IEC 14443-3 Type A anticollision and/or select commands.

After the select command is executed properly the IC transits to READY2/READY2* state in which the second part of the UID can be resolved. The answer to a select command in READY1/READY1* state is Select Acknowledge (SAK) for Cascade level 1, which indicates that the UID is incomplete and the next Cascade level has to be started to resolve the whole UID (see also ISO/IEC 14443-3 Type A).

However, the SLE 66R01P and SLE 66R01PN can directly transit from READY1/ READY1* state to ACTIVE/ACTIVE* state if a read command RD2B or R4BD with a valid address is executed. Note if more than one SLE 66R01P and SLE 66R01PN is in the reader field, all ICs are selected after the execution of the read command, although all of them have different UIDs.

Any other command or any other interruption is interpreted as an error and the SLE 66R01P and SLE 66R01PN return to IDLE or HALT state without any response, depending from which state it has come from.

8.2.3 READY2/READY2* state

In READY2/READY2* state the second part of the UID can be resolved using ISO/IEC 14443-3 Type A anticollision and/or select commands.

After the select command is executed properly the IC transits to ACTIVE/ACTIVE* state in which memory can be accessed. The answer to a select command in READY2/READY2* state is SAK for Cascade level 2, which indicates that the UID is complete and the selection process is finished.

However, the SLE 66R01P and SLE 66R01PN can directly transit from READY2/READY2* state to ACTIVE/ACTIVE* state if a read command RD2B or RD4B is executed. Any valid block address can be used in the read command. Note that if more than one SLE 66R01P and SLE 66R01PN is in the reader field, all ICs are selected after the execution of the read command, although all of them have different UIDs.

Any other command or any other interruption is interpreted as an error and the SLE 66R01P and SLE 66R01PN return to IDLE or HALT state without any response, depending from which part it has come from.

8.2.4 ACTIVE/ACTIVE* state

In the ACTIVE/ACTIVE* state memory access commands can be executed.

If SLE 66R01P and SLE 66R01PN is configured to have read/write or write password protection, a password verification is required to access the protected memory pages. In case of successful password verification, read/

write access to the whole memory is possible. If no verification is done or the password verification fails, the memory area above block $0F_H$ is locked according to the access rights in the configuration byte.

The ACTIVE/ACTIVE* state is left if the HLTA command is executed properly; the SLE 66R01P and SLE 66R01PN then transit to HALT state and wait until a WUPA command is received.

If any error command is received, the SLE 66R01P and SLE 66R01PN sends “No Response” (NR) or “Not Acknowledge” (NACK) and transits to IDLE or HALT state, depending from which state it has come from.

8.2.5 HALT state

The HLTA command sets the SLE 66R01P and SLE 66R01PN in the HALT state. The SLE 66R01P and SLE 66R01PN sends no response to the HLTA command. In the HALT state the IC can be activated again by a Wake-UP command (WUPA).

Any other data received is interpreted as an error, the SLE 66R01P and SLE 66R01PN sends no response and remains in HALT state.

The exact behavior of a particular command in any of the states above is also described in the specific command description.

8.3 Start up

120 µs after entering the powering field (after the field reset) the SLE 66R01P and SLE 66R01PN is ready to receive a command. If a command is send earlier, the response to this command is not defined.

8.3.1 Startup sequence of the SLE 66R01P and SLE 66R01PN

Each time after the execution of a REQA or WUPA, the SLE 66R01P and SLE 66R01PN reads the configuration byte and sets its internal states accordingly, refer to Figure 23. This information is not updated until the next execution of REQA or WUPA commands in IDLE or HALT state even when the CONFIG byte is changed in the EEPROM.

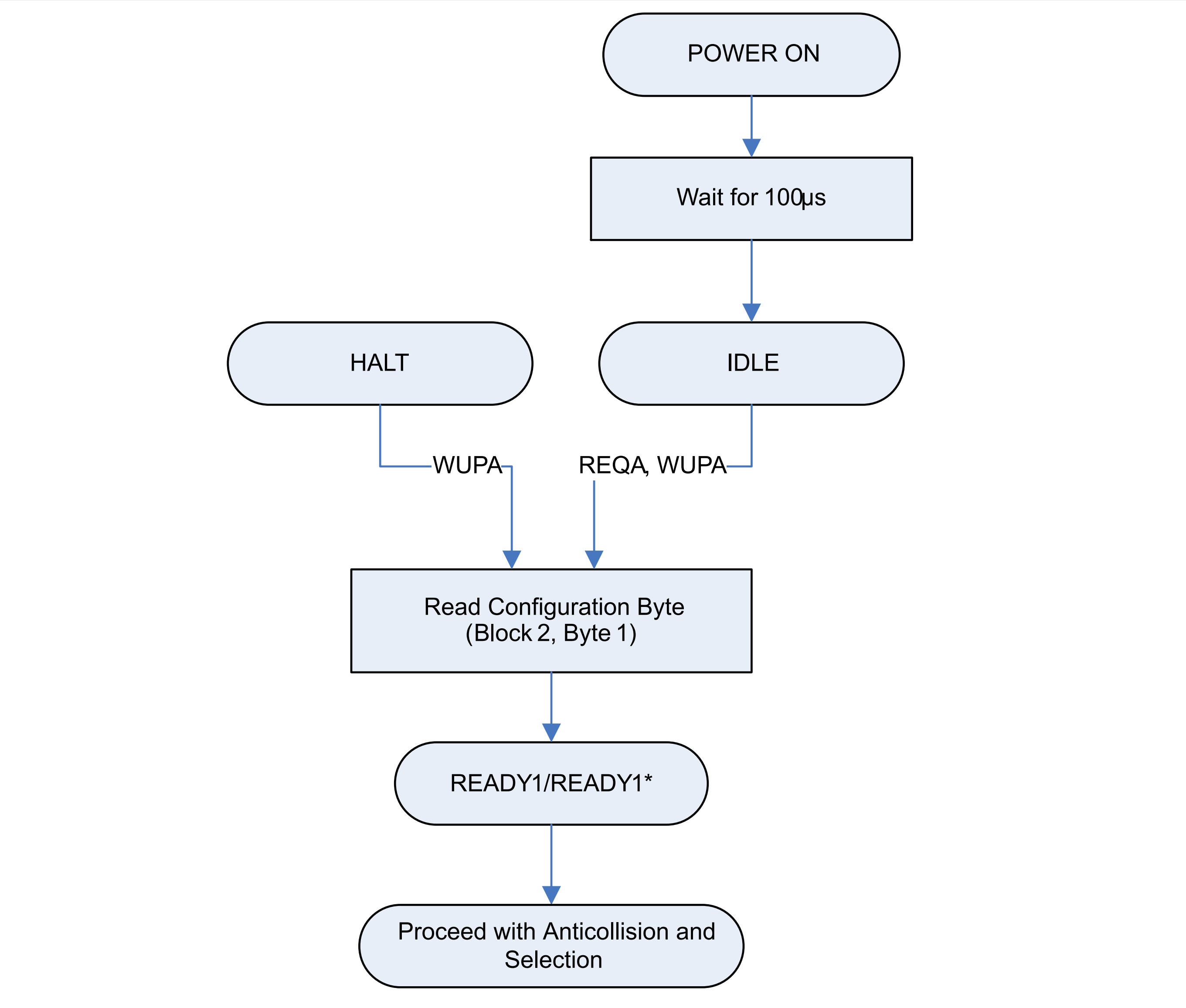


Figure 23 **Start up sequence**

8.4 Frame delay time

For information about frame delay time (FDT), please refer to ISO/IEC 14443-3 Type A specification. Generally the FDT is measured between the last rising edge of the pause transmitted by the PCD and the falling edge of the first load modulation within the start bit transmitted by the my-d™ move and my-d™ move NFC. If more then one ISO/IEC 14443-3 Type A compatible chip is in the operating field of the reader all of them must respond in a synchronous way which is needed for the anticollision procedure.

For detailed timings see Table 2 of ISO/IEC 14443-3 Type A Specification [4].

Note: The response timing of a particular SLE 66R01P and SLE 66R01PN command is given in the specific command description. However, the timing values are rounded and are not on a grid according the ISO/IEC 14443-3 Type A.

8.5 Error handling

The SLE 66R01P and SLE 66R01PN responds to valid frames only. Table 14 describes the behavior for different error cases.

Table 14 Behavior in case of an error

Current states	Command or error	Response SLE 66R01P and SLE 66R01PN	Next state
IDLE/HALT READY1/READY1* READY2/READY2*	Invalid Opcode	NR[1]	IDLE/HALT[2]
	Parity, Miller error, CRC	NR	IDLE/HALT
	Command too short or too long	NR	IDLE/HALT
	Invalid address	NR	IDLE/HALT
	Other errors	NR	IDLE/HALT
ACTIVE/ACTIVE*	Invalid Opcode	NR	IDLE/HALT
	Parity, Miller Error, CRC	NACK1	IDLE/HALT
	Command too short or too long	NR	IDLE/HALT
	Invalid address	NACK0	IDLE/HALT
	Other errors	NACK0	IDLE/HALT

1) RD4B and RD2B commands in READY1/READY1* and READY2/READY2* exceptionally behave as in ACTIVE/ACTIVE* state.
2) The SLE 66R01P and SLE 66R01PN returns to IDLE or HALT state depending on the state where it has come from.

9 Command set

9.1 Supported ISO/IEC 14443-3 Type A command set

Table 15 describes the ISO/IEC 14443-3 Type A command set which is supported by the SLE 66R01P and SLE 66R01PN.

For a detailed command description refer to the ISO/IEC 14443-3 Type A functional specification.

Table 15 ISO/IEC 14443-3 Type A command set

Command	Abbreviation	Op-Code	Description
Request A	REQA	26_H	Short frame command Type A request to all ISO/IEC 14443-3 Type A compatible chips in IDLE state
Wake Up A	WUPA	52_H	Short frame command Type A Wake Up request to all ISO/IEC 14443-3 Type A compatible chips
Anticollision	AC	93_H NVB_H 95_H NVB_H	Cascade level 1 with the number of valid bits Cascade level 2 with the number of valid bits
Select	SELA	93_H 70_H, 95_H 70_H	Select the UID of Cascade level 1 Select the UID of Cascade level 2
Halt A	HLTA	50_H	Set a chip to a HALT state Important remark: The parameter field of the HLTA command represents the valid address range which is 00_H - 25_H

9.2 Memory access command set

The command set of the SLE 66R01P and SLE 66R01PN comprises the NFC Forum Type 2 Tag commands as well as proprietary commands which are additionally implemented to increase data transaction time and increase the protection of the data stored in the memory.

Table 16 lists the memory access command set of the SLE 66R01P and SLE 66R01PN.

Table 16 my-d™ move and my-d™ move NFC memory access command set

Command	Abbreviation	Op-Code	Description
Read 4 blocks(1)	RD4B	30_H	This command reads 16 bytes of data out of the memory starting from the specified address A Roll-Back mechanism is implemented: • If block $0F_H$ is reached the read continues from block 00_H • If block 25_H is reached the read continues from block 00_H
Write 1 block(2)	WR1B	$A2_H$	If write access is granted, this command programs 4 bytes of data to the specified memory address
Compatibility write command	CPTWR	$A0_H$	This command sends 16 bytes to the SLE 66R01P and SLE 66R01PN but writes only the first 4 bytes of the incoming data to the specified memory address

(table continues...)

Table 16 (continued) my-d™ move and my-d™ move NFC memory access command set

Command	Abbreviation	Op-Code	Description
Read 2 blocks[3]	RD2B	31_H	This command reads 8 bytes out of the memory, starting from the specified address. A Roll-Back mechanism is implemented: • If block $0F_H$ is addressed, the read continues from block 00_H • If block 25_H is addressed, the read continues from block 00_H
Write 2 blocks	WR2B	$A1_H$	If write access is granted, this command writes 8 bytes to the specified address memory. Note that the programming time is 4 ms
Set password	SPWD	$B1_H$	This command sets the 4 byte password to the my-d™ move and my-d™ move NFC
Access [4]	ACS	$B2_H$	This command verifies the password to the my-d™ move and my-d™ move NFC
Decrement	DCR16	$D0_H$	This command decrements an existing value counter value to a lower value and writes the result to the value counter block

1) NFC Forum Type 2 Tag read command.

2) NFC Forum Type 2 Tag write command.

3) By using RD2B and WR2B commands, total user memory of 128 bytes can be written and re-read within approximately 100 ms (excluding anti-collision and taking into account a short reader turnaround time, less then 100 µs).

4) If the my-d™ move and my-d™ move NFC is configured to use a write or read/write password, the appropriate memory access operations are possible only after password verification.

9.2.1 Read 4 Blocks (RD4B)

RD4B command reads 16 bytes of data out of the memory starting from the specified address.

The valid address range is 00_H to 25_H.

If any other address is specified the SLE 66R01P and SLE 66R01PN responds with a NACK. A Roll-Back mechanism is implemented:

- If e.g. block $0E_H$ is addressed blocks $0E_H$, $0F_H$, 00_H and 01_H are replied
- If e.g. block 25_H is addressed blocks 25_H, 00_H, 01_H and 02_H are replied

Table 17 Read 4 Blocks (RD4B)

Command length	Code	Parameter	Data	Integrity mechanism	Response
4 bytes	30_H	Valid address range 00_H - 25_H	N.A.	2 bytes CRC (1 parity bit per byte)	16 bytes data +2 bytes CRC or NACK or NR

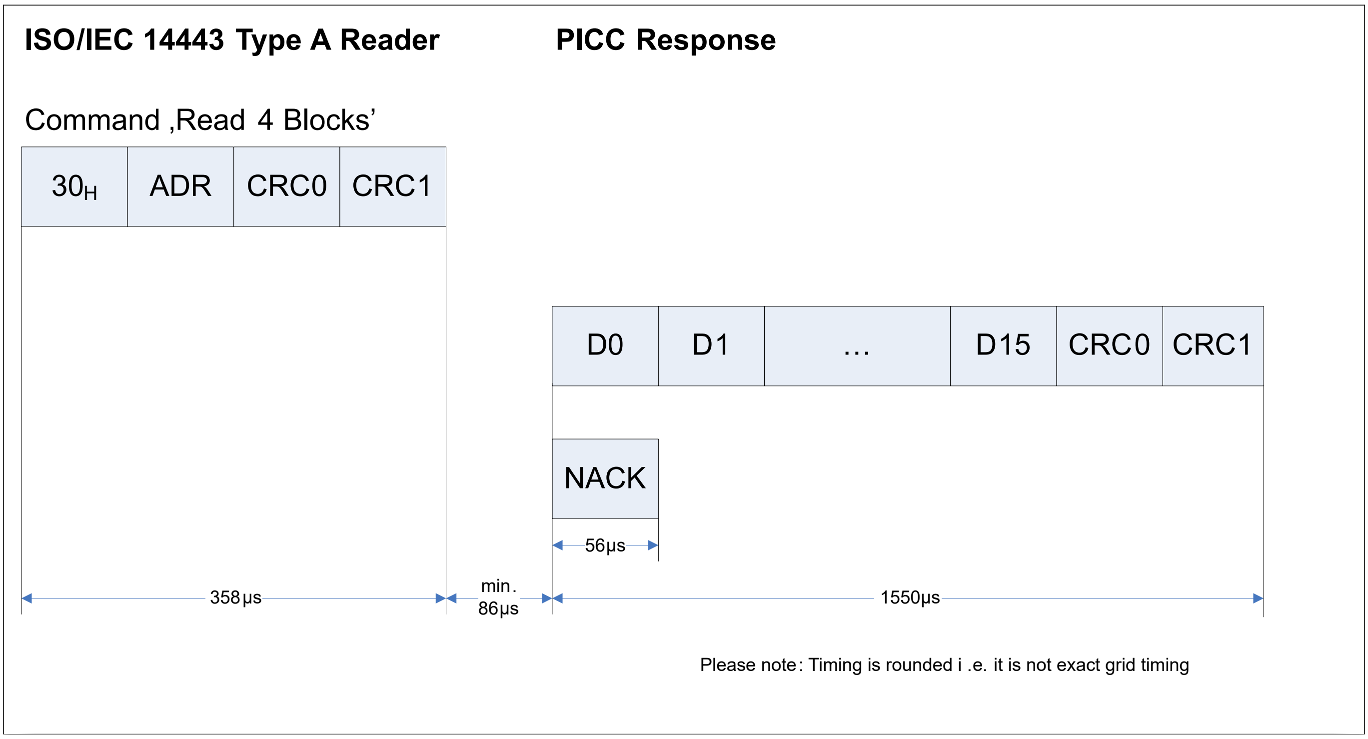


Figure 24 **Read 4 Blocks command**

9.2.2 Write 1 Block (WR1B)

If the write access is granted the WR1B command is used to program 4 bytes of data to the specified address in the memory. This command should be used to program OTP block and locking bytes as well.

The valid address range is from 02_H to 24_H. If any other address is specified the SLE 66R01P and SLE 66R01PN responds with a NACK.

Table 18 **Write 1 Block (WR1B)**

Command length	Code	Parameter	Data	Integrity mechanism	Response
8 bytes	$A2_H$	Valid address range 02_H - 24_H	4 bytes data	2 bytes CRC (1 parity bit per byte)	ACK or NACK or NR

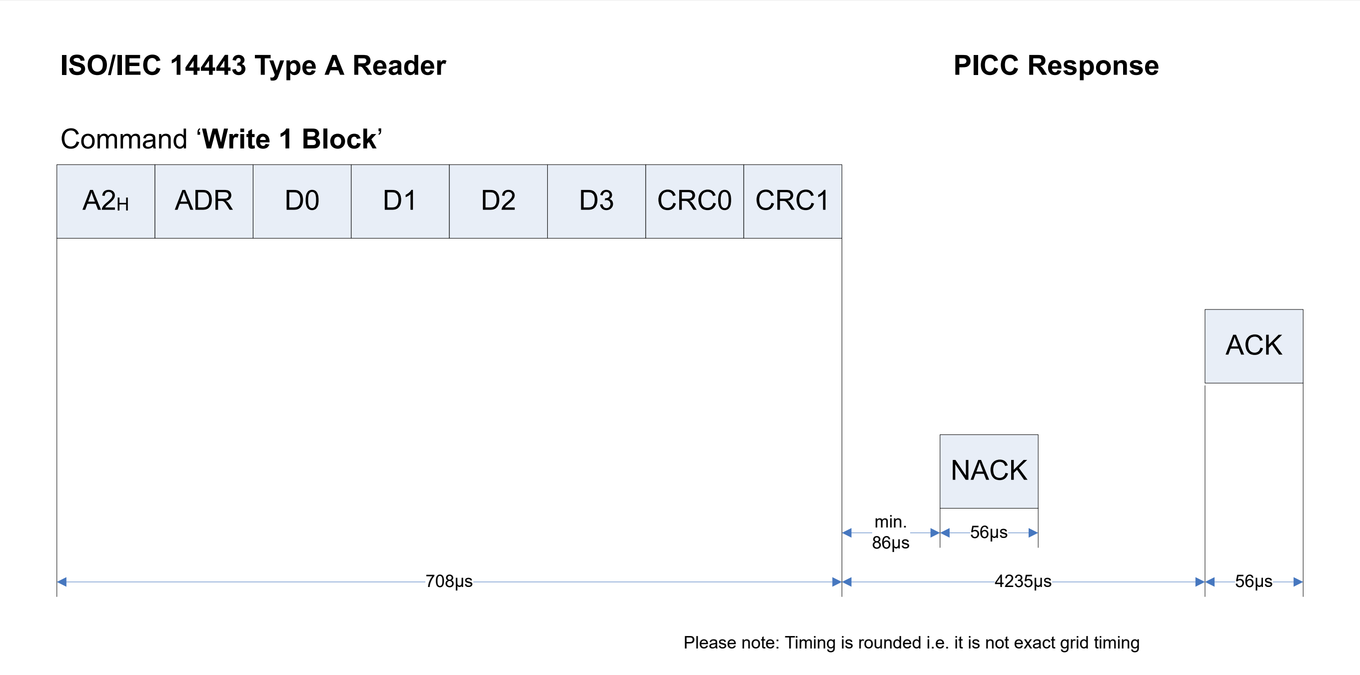


Figure 25 **Write 1 Block command**

9.2.3 Compatibility write command (CPTWR)

If the write access is granted only the four least significant 4 bytes are written to the specified address. The remaining bytes will be ignored by the SLE 66R01P and SLE 66R01PN. It is recommended to set the remaining bytes 04_H - $0F_H$ to 00_H.

Table 19 **Compatibility write (CPTWR)**

Command length	Code	Parameter	Data	Integrity mechanism	Response
20 bytes	$A0_H$	Valid address range 02_H - 24_H	16 bytes data	2 bytes CRC (1 parity bit per byte)	ACK or NACK or NR

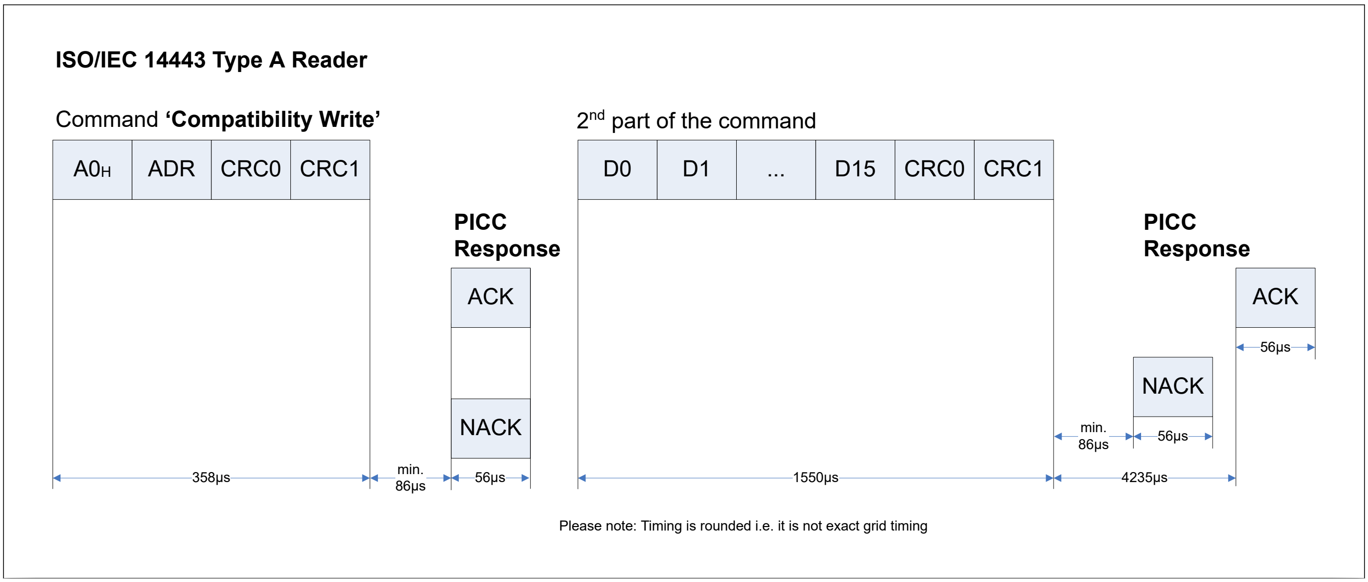


Figure 26 **Compatibility write command**

9.2.4 Read 2 Blocks (RD2B)

RD2B command reads 8 bytes out of the memory, starting from the specified address.

The valid address range is from 00_H to 25_H. If any other address is specified the SLE 66R01P and SLE 66R01PN responds with a NACK. A Roll-Back mechanism is implemented:

- If e.g. block $0F_H$ is addressed blocks $0F_H$ and 00_H are replied
- If e.g. block 25_H is addressed blocks 25_H and 00_H are replied

Table 20 **Read 2 Block (RD2B)**

Command length	Code	Parameter	Data	Integrity mechanism	Response
4 bytes	31_H	Valid address range 00_H - 25_H	N.A.	2 bytes CRC (1 parity bit per byte)	8 bytes data +2 bytes data CRC or NACK Shift or NACK

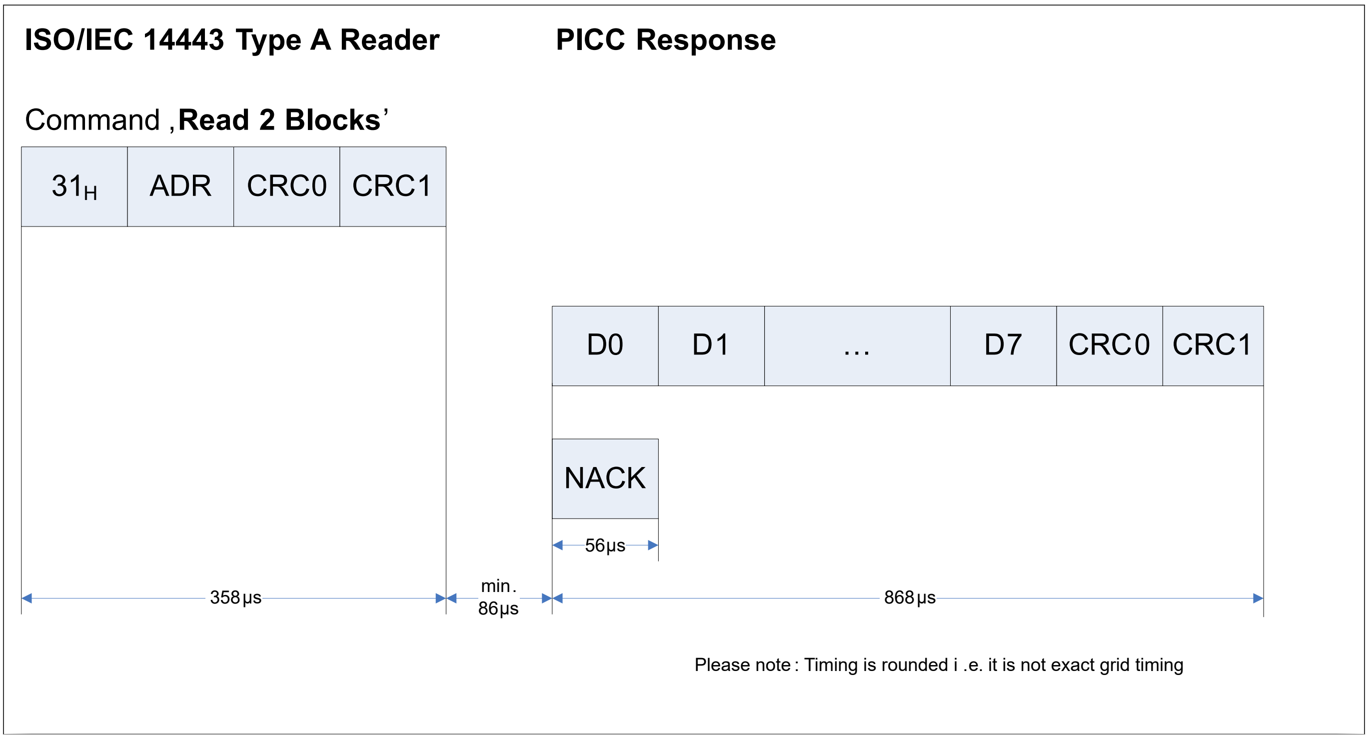


Figure 27 **Read 2 Blocks command**

9.2.5 Write 2 Blocks (WR2B)

If write access is granted, i.e. if both addressed blocks are writable, the WR2B command is used to program two blocks (8 bytes of data) to the specified address in the memory.

The valid address range is 04_H - 22_H. Only even start addresses are allowed. If any other address is specified, the SLE 66R01P and SLE 66R01PN responds with a NACK.

The WR2B command has the same programming time (approximately 4 ms) for writing 8 bytes as the WR1B command which writes 4 bytes of data to the specified memory.

Table 21 **Write 2 Block (WR2B)**

Command length	**Code**	**Parameter**	**Data**	**Integrity mechanism**	**Response**
12 bytes	A1$_H$	Valid address range 04$_H$ - 22$_H$; only even start addresses allowed	8 bytes data	2 bytes CRC (1 parity bit per byte)	ACK or NACK or NR

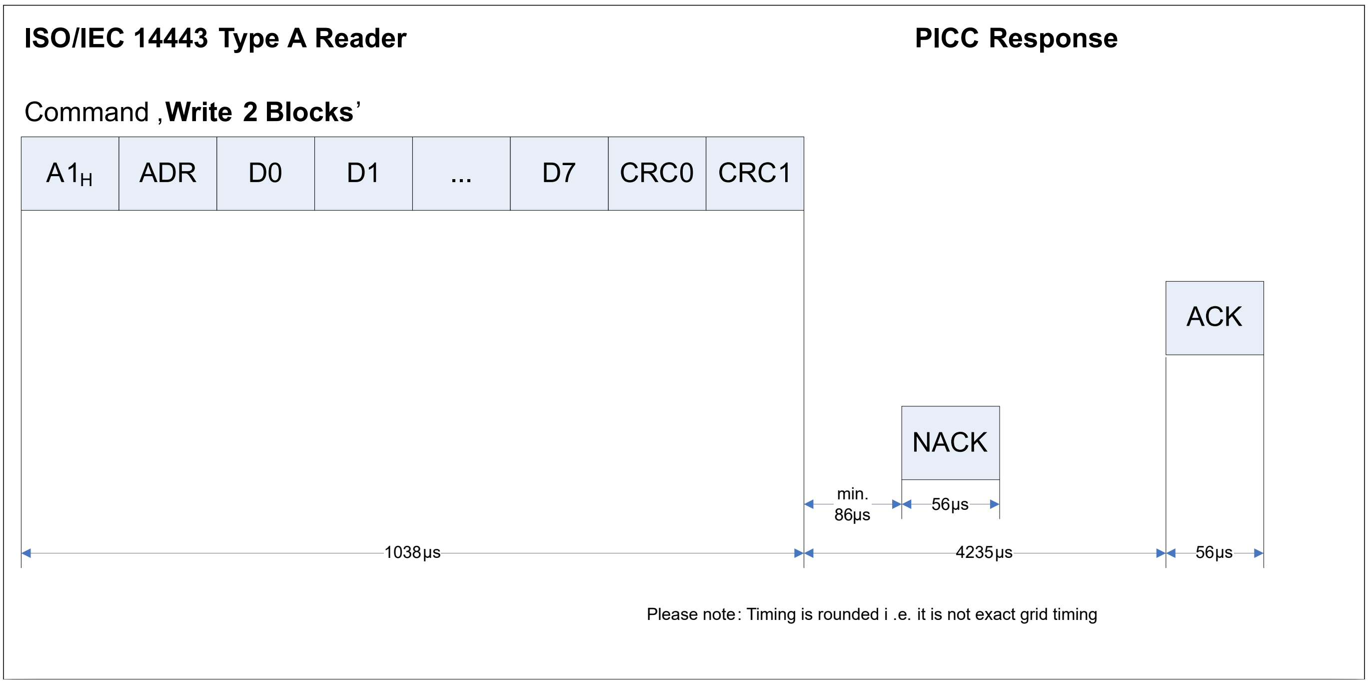


Figure 28 **Write 2 Blocks command**

9.2.6 Set password (SPWD)

The SPWD command writes a new 4 byte password to the dedicated password memory[5]. The newly written value is transmitted in the response.

The SPWD command is always active independently of password configuration. If the SLE 66R01P and SLE 66R01PN is configured for password protection, then the SPWD command can be executed only after a successful password verification.

Table 22 **Set password (SPWD)**

Command length	**Code**	**Parameter**	**Data**	**Integrity mechanism**	**Response**
7 bytes	B1$_H$	N.A.	4 bytes data	2 bytes CRC (1 parity bit per byte)	4 bytes data +2 bytes CRC or NACK or NR

---

[5] For more information about password please refer to Password.

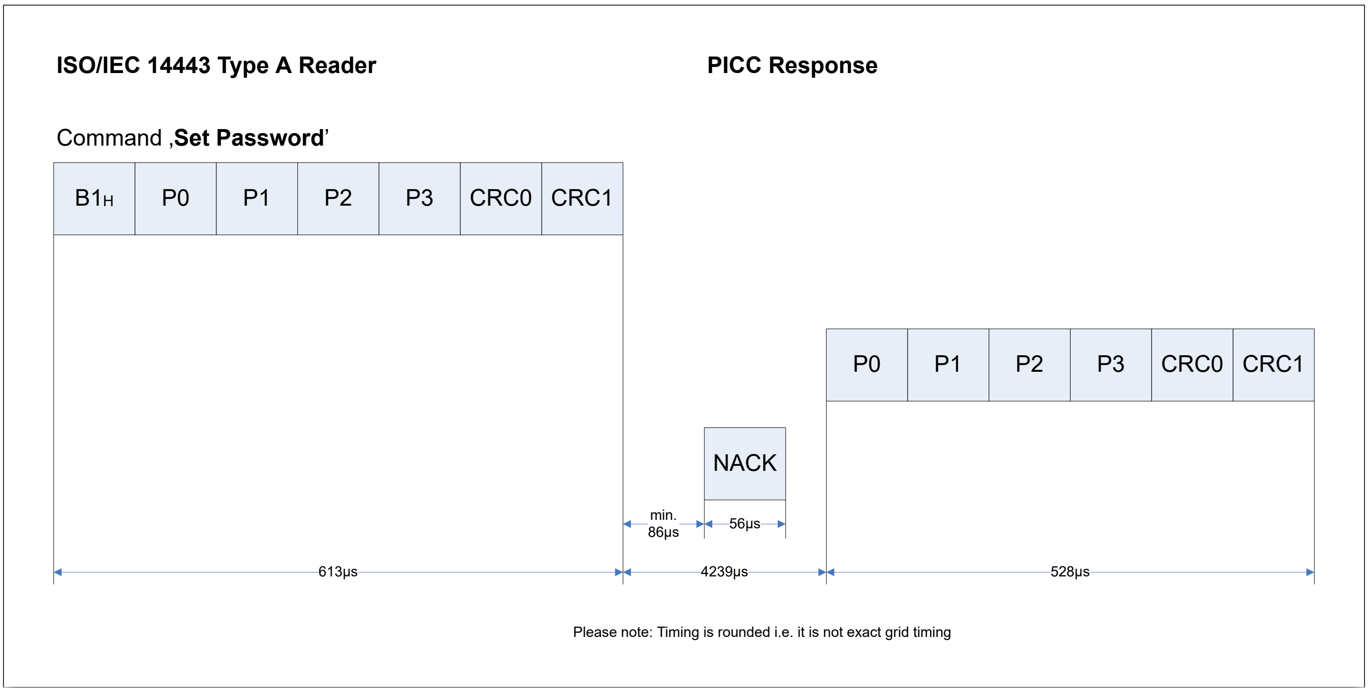


Figure 29 Set password command

Table 23 SPWD - behavior in error case

Error/State	Idle/Halt	Ready	Active	Protected
Invalid Opcode	NR	NR	NR	NR
Parity, Miller	NR	NR	NACK1	NACK1
Command length	NR	NR	NR	NR
CRC	NR	NR	NACK1	NACK1
The selected chip is protected by password	NR	NR	NACK0	N.A.
HV not OK	NR	NR	NR	NR

9.2.7 Access (ACS)

If the my-d™ move and my-d™ move NFC is configured for password protection[6)] the ACS command is used to perform a password verification. If the password verification is successful, memory access to blocks above block 0F$_H$ is granted according to the access rights given in the configuration byte.

Additionally, if the password counter is enabled, the number of unsuccessful password verifications is counted. The ACS command is always active independently on the password and the password retry counter configuration.

---

[6] For more information about password please refer to Password.

- If the password retry counter is not enabled, the my-d™ move responds with ACK or NACK depending on the result of password comparison
- If the password retry counter is enabled, then depending on the result of password comparison the my-d™ move and my-d™ move NFC performs the following actions:
  - If the passwords do not match and the password retry counter holds a lower value than its initial value, the my-d™ move increments the password retry counter and responds with a NACK
  - If the passwords match and the password retry counter holds a lower value then its initial value, the my-d™ move resets the password retry counter and responds with a ACK
  - In any other case the my-d™ move responds with a NACK and limits access to blocks above block $0F_H$ according to access rights stored in the configuration byte

Table 24 Access (ACS)

Command length	Code	Parameter	Data	Integrity mechanism	Response
7 bytes	$B2_H$	N.A.	4 bytes data	2 bytes CRC (1 parity bit per byte)	ACK or NACK or NR

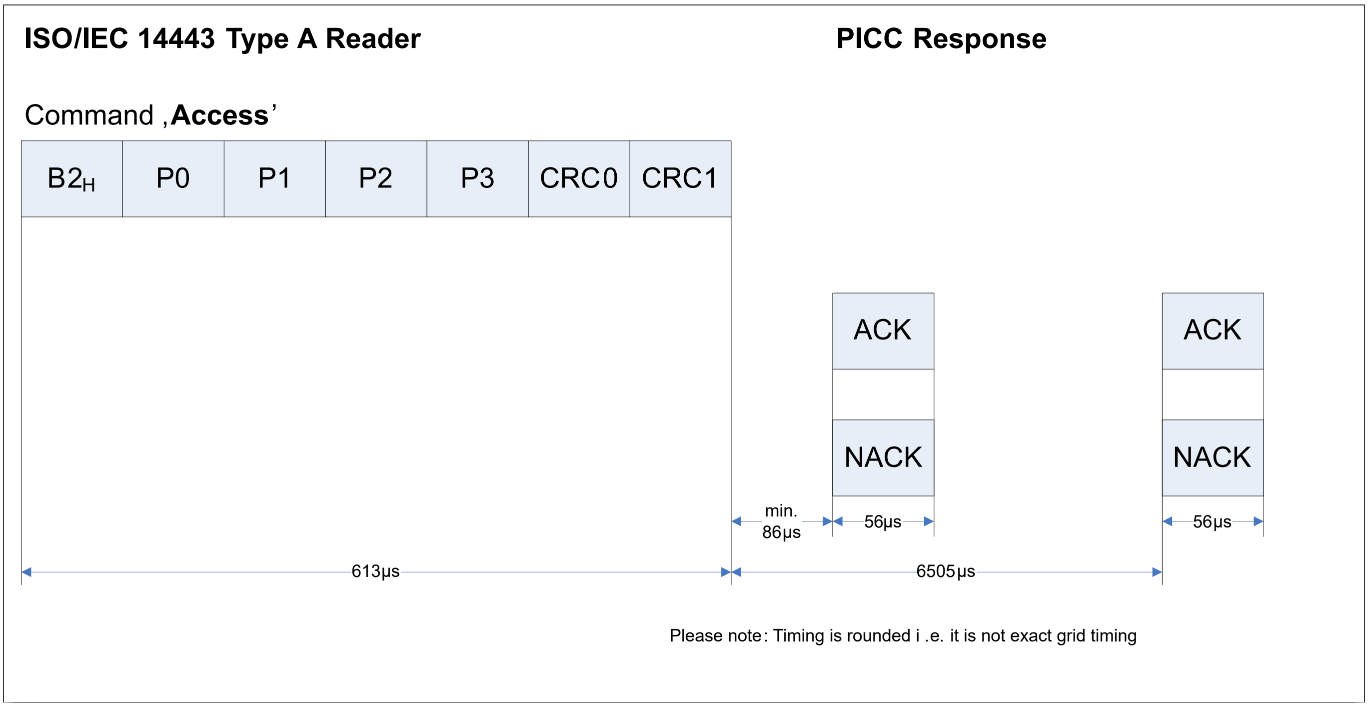


Figure 30 Access command

Figure 31 shows the flow diagram of the access command.

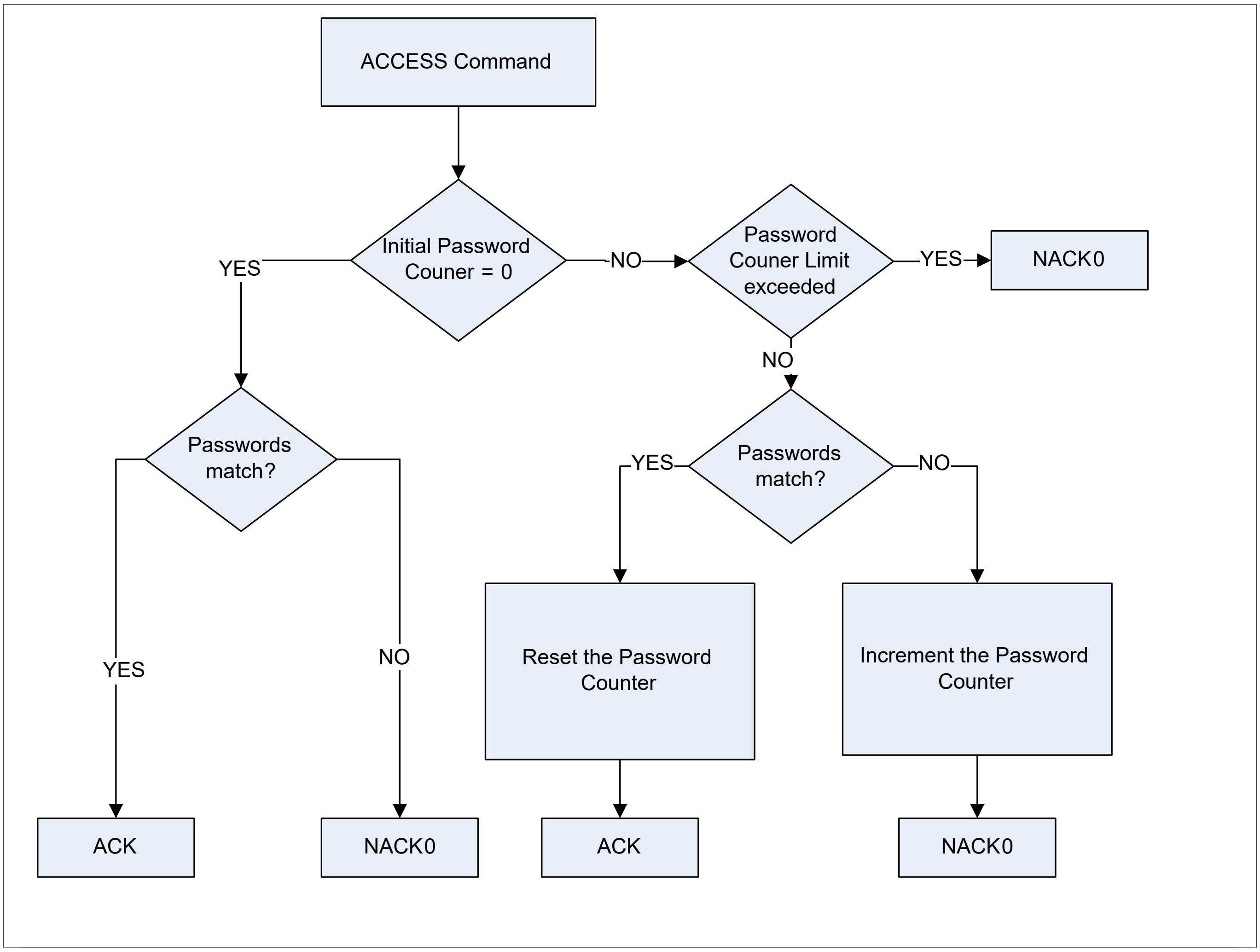


Figure 31 Flow diagram of the ACS command

Table 25 ACS - behavior in error case

Error/State	Idle/Halt	Ready	Active	Protected
Invalid Opcode	NR	NR	NR	NR
Parity, Miller	NR	NR	NACK1	NACK1
Command length	NR	NR	NR	NR
CRC	NR	NR	NACK1	NACK1
Password counter limit exceeded	NR	NR	NACK0	NACK0
Passwords do not match	NR	NR	NACK0	N.A.
HV not OK	NR	NR	NR	NR

9.2.8 Decrement command (DCR16)

The DCR16 command decrements the current value counter value by the received parameter and writes the new value to the value counter block. If this command is executed properly, the my-d™ move and my-d™ move

NFC responds the new written value. Note that the parameter has to be lower or equal to the current value counter value.

Table 26 Decrement (DCR16)

Command length	Code	Parameter	Data	Integrity mechanism	Response
5 bytes	D0$_H$	2 bytes; LSB = CNT0 MSB = CNT1	N.A.	2 bytes CRC 1 parity bit per byte	• If the parameter is lower or equal to the current value counter value, the response is the new decremented value: 2 bytes data +2 bytes CRC • If the parameter is 0000$_H$ the response is the current value counter value • If the parameter is higher than the current value counter value the response is a NACK

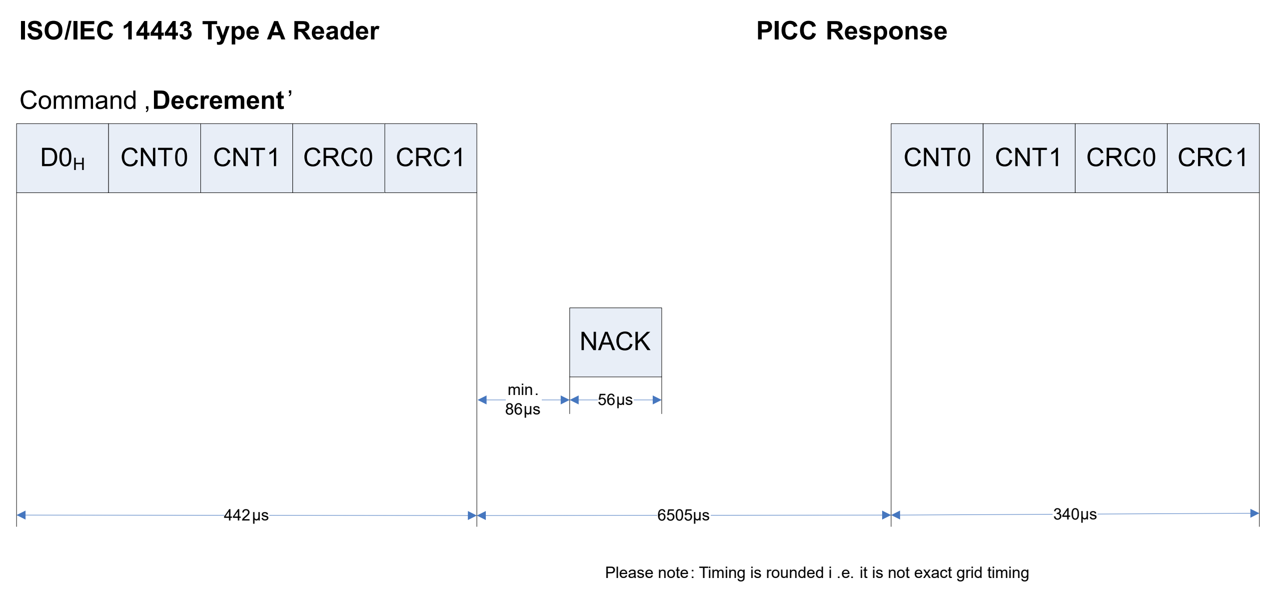


Figure 32 Decrement command

After receiving the correct DCR16 command, the my-d™ move and my-d™ move NFC performs the following actions:

- Checks the format of the current value counter by reading blocks 22$_H$ and 23$_H$
- Determines the valid and the invalid value counter value
- Decrements the current valid value by the received parameter
- Expands the result to the correct value counter format
- Writes the new value counter value, in the correct format, to the previously determined invalid block
- Erases the current valid value counter value to FF$_H$ FF$_H$ FF$_H$ FF$_H$

In case of a successful programming of a value counter value, the my-d™ move and my-d™ move NFC sends the new written value of the value counter block back. If the programming was unsuccessful (due to insufficient power) “No Response” is replied.

In case of any other logical error or if the value counter block is corrupted (i.e. both blocks have an incorrect format) a NACK is replied.

Table 27 **DCR16 - behavior in error case**

Error/State	Idle/Halt	Ready	Active	Protected
Invalid Opcode	NR	NR	NR	NR
Parity, Miller	NR	NR	NACK1	NACK1
Command length	NR	NR	NR	NR
CRC	NR	NR	NACK1	NACK1
VCNTR16 not enabled	NR	NR	NACK0	NACK0
The selected chip is protected by password	NR	NR	NACK0	NACK0
Both counter blocks corrupted	NR	NR	NACK0	NACK0
Current VCNTR16 to low	NR	NR	NR	NR
HV not OK	NR	NR	NR	NR

The figure below presents the flow diagram of the decrement command.

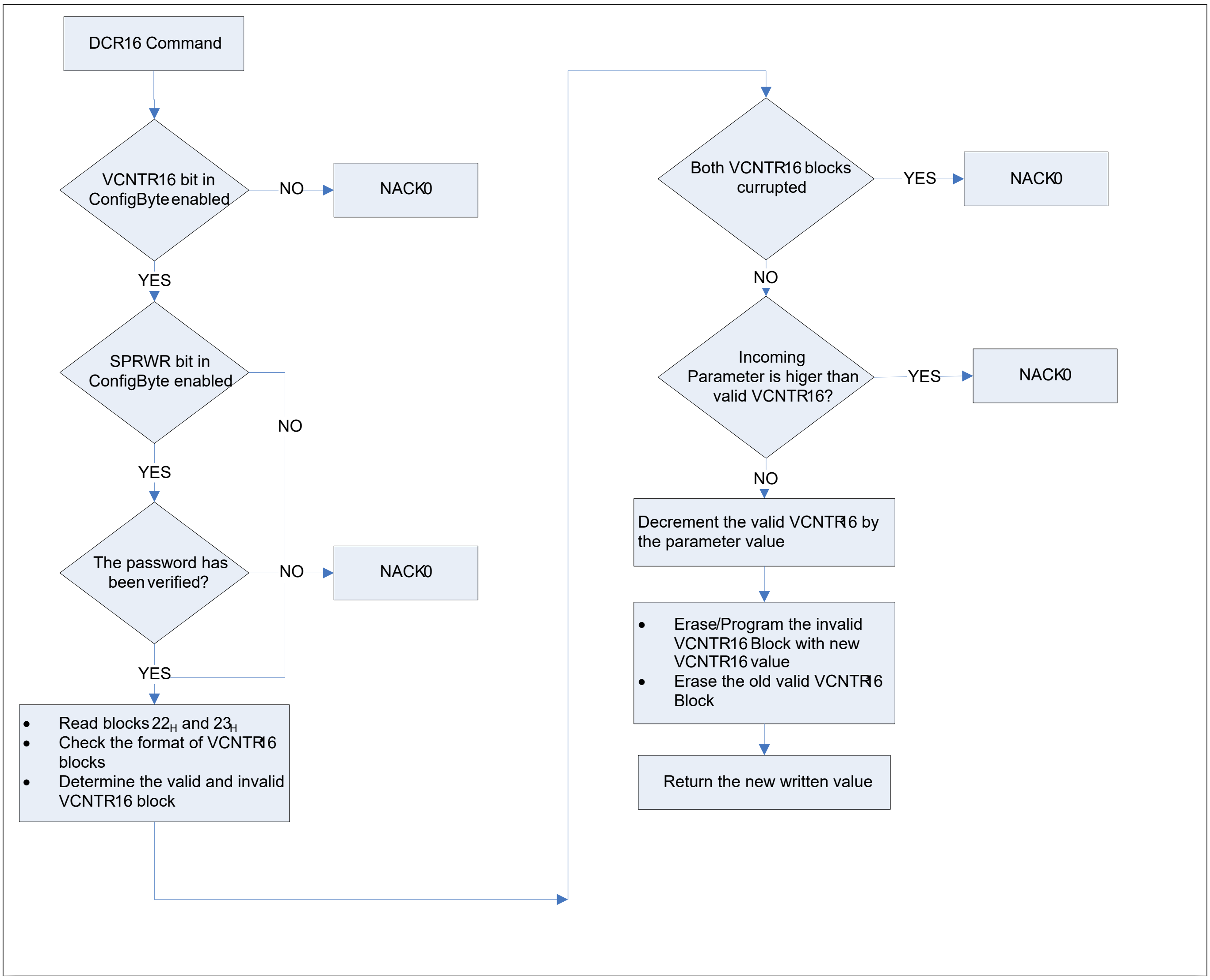


Figure 33 **Decrement command flow**

9.2.9 HLTA command

The HLTA command is used to set the SLE 66R01P and SLE 66R01PN into the HALT state. The HALT state allows users to separate already identified chips. Contrary to the definition in the ISO/IEC 14443-3 Type A standard, the SLE 66R01P and SLE 66R01PN accept as a parameter the whole address range of 00_H to 25_H with correct CRC for a proper execution of a HLTA command.

Table 28 Halt (HLTA)

Command length	Code	Parameter	Data	Integrity mechanism	Response
4 bytes	50_H	Valid address range 00_H - 25_H	N.A.	2 bytes CRC 1 parity bit per byte	NACK or NR

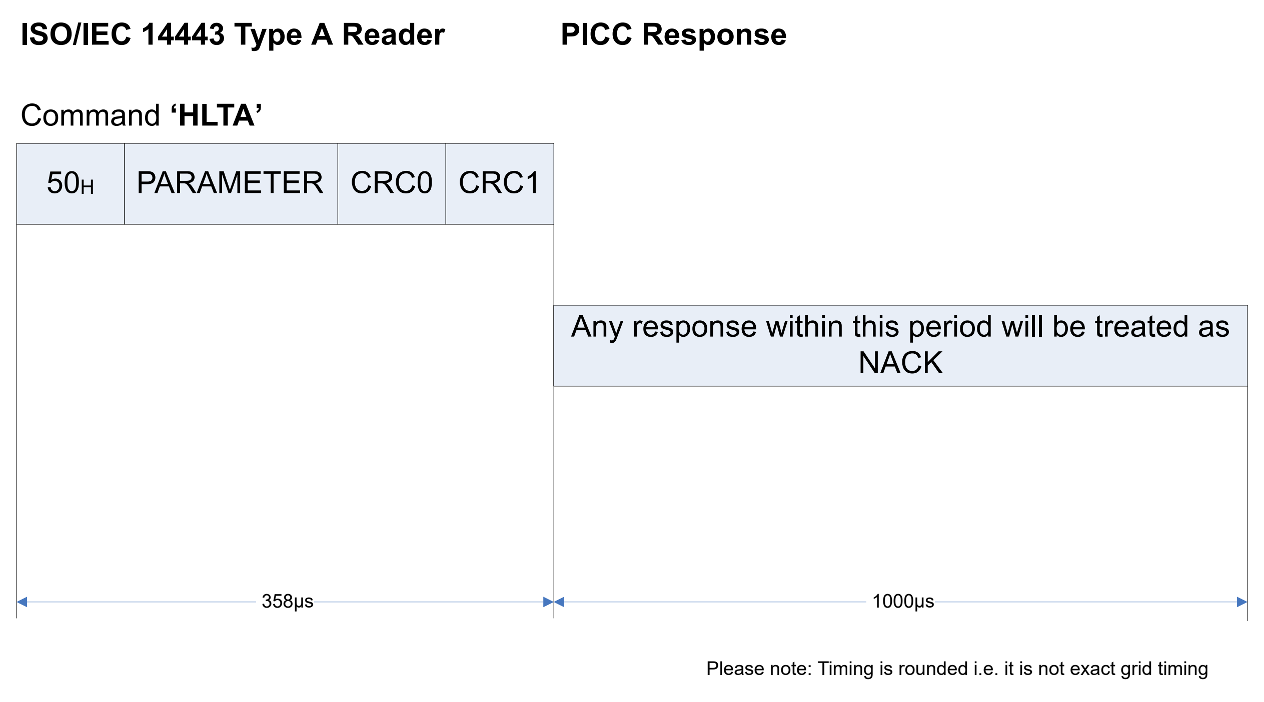


Figure 34 HLTA command

9.3 my-d™ move and my-d™ move NFC responses

The following sections list valid responses of the SLE 66R01P and SLE 66R01PN.

9.3.1 Command responses

The Acknowledge (ACK) and Not-Acknowledge (NACK) are command responses of the SLE 66R01P and SLE 66R01PN.

Table 29 ACK and NACK as responses

Response	Code (4 bits)	Integrity mechanism
ACK	1010_B (A_H)	N.A.
NACK0	0000_B (0_H)	N.A.

(table continues...)

Table 29 **(continued) ACK and NACK as responses**

Response	Code (4 bits)	Integrity mechanism
NACK1	0001_B (1_H)	N.A.
NR[1]	N.A.	N.A.

[1] Depending on the current state, the SLE 66R01P and SLE 66R01PN does not respond to some errors.

The response code is A_H for ACK and 0_H or 1_H for NACK. The ACK and NACK are sent as 4-bit response with no CRC and/or parity.

9.3.2 my-d™ move and my-d™ move NFC identification data

During the anti-collision the SLE 66R01P and SLE 66R01PN sends responses to the REQA and SEL commands.

Table 30 **Summary of SLE 66R01P and SLE 66R01PN identification data**

Code	Data	Description
ATQA	0044_H	Answer to request, response to REQA and WUPA command, hard coded 2 bytes. Indicates a double-size UID
SAK (cascade level 1)	04_H	Select Acknowledge answer to selection of 1st cascade level. Indicates that the UID is incomplete
SAK (cascade level 2)	00_H	Select Acknowledge answer to selection of 2nd cascade level. Indicates that the UID is complete
CT	88_H	Cascade Tag indicates that UID is not single size UID

10 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 ambient temperature $T_A = 25°C$ and the given supply voltage.

10.1 Electrical characteristics

$f_C = 13.56$ MHz sinusoidal waveform, voltages refer to VSS.

Table 31 Electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Chip input capacitance L_A-L_B	C_{IN}	16.15	17	17.85	pF	$V_{AB\ peak} = 3.0$ V, $f_C = 13.56$ MHz, $T_A = 25°C$
Chip load resistance L_A-L_B	R_{IN}	3	4.5	6	kΩ	$V_{AB\ peak} = 3.0$ V, $f_C = 13.56$ MHz, $T_A = 25°C$
Endurance (erase/write cycles)(1)		10^4				–
Data retention(1)		5			Years	
EEPROM erase and write time	t_{prog}			3.8	ms	Combined erase + write; excluding time for command/response transfer between interrogator and chip, $T_A = 25°C$
ESD protection voltage (L_A, L_B pins)	V_{ESD}	2			kV	JEDEC STD EIA/JESD22 A114-B
Ambient temperature	T_A	-25		+70	°C	For chip
Junction temperature	T_J	-25		+110	°C	For chip

1) Values are temperature dependent.

10.2 Absolute maximum ratings

Stresses above the maximum values listed here may cause permanent damage to the device. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including EEPROM data retention and erase/write endurance. Maximum ratings are absolute ratings; exceeding only one of these values may cause irreversible damage to the integrated circuit (IC). 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 Extended datasheet is not implied.

Table 32 **Absolute maximum ratings**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input peak voltage between L_A-L_B	V_{INpeak}			6	V	
Input current through L_A-L_B	I_{IN}			30	mA	
Storage temperature	T_S	-40		+125	°C	

References

ISO/IEC

[1] ISO/IEC 18092:2013: *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1) (Second edition)*; 2013-03

[2] ISO/IEC 14443-1:2018: *Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics (Fourth edition)*; 2018-04

[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 14443-3:2018: *Cards and security devices for personal identification – Contactless proximity objects – Part 3: Initialization and anticollision (Fourth edition)*; 2018-07

[5] ISO/IEC 10373-6:2020: *Cards and security devices for personal identification — Test methods — Part 6: Contactless proximity objects*

NFC Forum

[6] NFC Forum: *Type 2 Tag Technical Specification (Version 1.2)*; 2021-09-27

Infineon Technologies

[7] *SLE66R01xx Wafer Specification*; 2021-07 https://www.infineon.com/dgdl/Infineon-Chip_Specification_SLE_66R01xx-AdditionalProductInformation-v01_00-EN.pdf

Glossary

CRC

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

ECC

error correction code (ECC)
A method for controlling errors in data on an unreliable transfer channel. The sender adds an ECC redundancy information and the receiver is able to verify the data and correct a limited amount of errors.

EEPROM

electrically erasable programmable read-only memory (EEPROM)

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.

FDT

frame delay time (FDT)

IC

integrated circuit (IC)

IEC

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

ISO

International Organization for Standardization (ISO)

LSB

least significant byte (LSB)

MAC

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

MSB

most significant byte (MSB)

NFC

near field communication (NFC)

PCD

proximity coupling device (PCD)
A reader device for NFC cards.

PICC

proximity integrated circuit card (PICC)
A contactless smart card which can be read without inserting it into a reader device.

RFU

reserved for future use (RFU)

RoHS

Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)
EU rules restricting the use of hazardous substances in electrical and electronic equipment to protect the environment and public health.

SMD

surface-mounted device (SMD)

TLV

tag length value (TLV)

TSNP

thin small no-lead package (TSNP)

UID

unique identifier (UID)

Revision history

Reference	Description
Revision 4.0, 2023-08-14	
All	• Updated Sales codes and delivery forms and References • Added SMD package details and RoHS compliance
Revision 3.1, 2022-08-12	
Application segments	Updated Table 5
Revision 3.0, 2021-12-21	
All	• Migrated to latest IFX template and updated editorial changes • Added About this document, References sections, glossary entries and Figure 22
Revision 2.0, 2019-06-26	
All	Updated trademarks and major changes since last release
Revision 1.0, 2011-11-24	
All	Initial release

RoHS compliance

On January 27, 2003 the European Parliament and the council adopted the directives:

- 2002/95/EC on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment ("RoHS")
- 2002/96/EC on Waste Electrical and Electrical and Electronic Equipment ("WEEE")

Some of these restricted (lead) or recycling-relevant (brominated flame retardants) substances are currently found in the terminations (e.g. lead finish, bumps, balls) and substrate materials or mold compounds.

The European Union has finalized the Directives. It is the member states' task to convert these Directives into national laws. Most national laws are available, some member states have extended timelines for implementation. The laws arising from these Directives have come into force in 2006 or 2007.

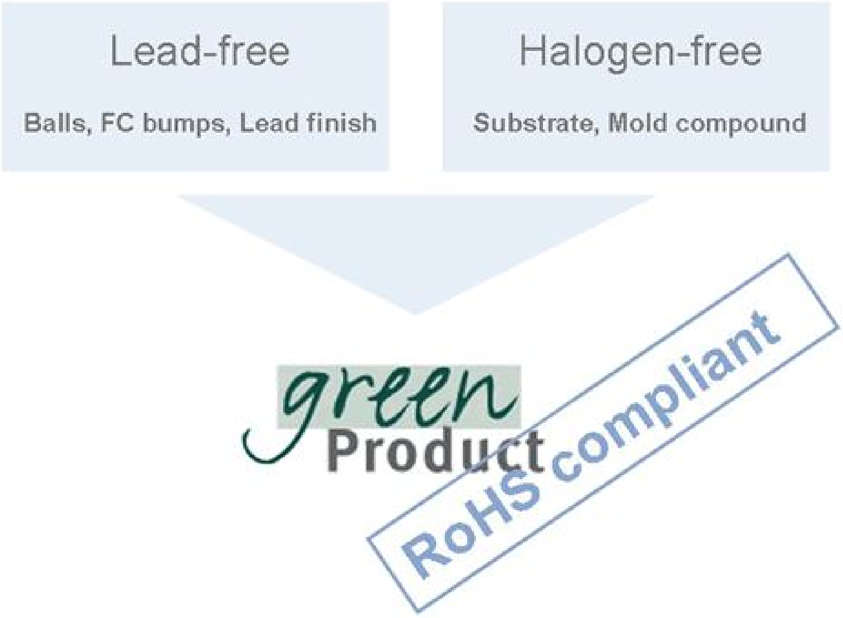
The electro and electronic industry has to eliminate lead and other hazardous materials from their products. In addition, discussions are on-going with regard to the separate recycling of certain materials, e.g. plastic containing brominated flame retardants.

Infineon is fully committed to giving its customers maximum support in their efforts to convert to lead-free and halogen-free[7)] products. For this reason, Infineon's "Green Products" are ROHS-compliant.

Since all hazardous substances have been removed, Infineon calls its lead-free and halogen-free semiconductor packages "green." Details on Infineon's definition and upper limits for the restricted materials can be found here.

The assembly process of our high-technology semiconductor chips is an integral part of our quality strategy. Accordingly, we will accurately evaluate and test alternative materials in order to replace lead and halogen so that we end up with the same or higher quality standards for our products.

The use of lead-free solders for board assembly results in higher process temperatures and increased requirements for the heat resistivity of semiconductor packages. This issue is addressed by Infineon by a new classification of the Moisture Sensitivity Level (MSL). In a first step the existing products have been classified according to the new requirements.



---

[7] Any material used by Infineon is PBB and PBDE-free. Plastic containing brominated flame retardants, as mentioned in the WEEE directive, will be replaced if technically/economically beneficial.

Trademarks

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

Edition 2023-08-14

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2023 Infineon Technologies AG

All Rights Reserved.

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

Email:
CSSCustomerService@infineon.com

Document reference
IFX-wxz1597749380665

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.