SLE 66R35E7 / SLE 66R35E7H

Intelligent 1kByte Memory chip with NRG and 7-byte UID

Extended datasheet

Devices

- SLE 66R35E7
- SLE 66R35E7H

Features

- Intelligent 1 kByte Memory Chip with NRG (ISO/IEC 14443-3 type A with CRYPTO1) and 7-byte Unique Identification (UID)
- Physical Interface and Anticollision compliant to ISO/IEC14443-2 and -3 Type A
  - Operation frequency 13.56 MHz
  - Data rate 106 kbit/s
- 1 kByte EEPROM
  - Block organization of memory, 16 Sectors with fixed 4 blocks of 16 bytes each
  - User definable access conditions for each memory block
- Security Features
  - 7-byte Unique Identification (UID)
  - Support of 4-byte Random number (RND-ID) and 4-byte fixe non-unique number (FNUID)
  - Features Short-Cut Anticollision scheme to realize backward compatibility to installed infrastructures supporting 4-byte single size UIDs only
  - Mutual three-pass authentication between card and reader for basic security
  - Selective memory access control secured by authentication and access conditions
  - Data encryption for RF channel
  - Dedicated Value Counter
- SLE 66R35E7H implements an adopted SAK parameter value supporting 4-byte infrastructure compatibility

About this document

Scope and purpose

This document describes the features, functionality and operational characteristics of SLE 66R35E7(H).

Intended audience

This document is primarily intended for system and application developers.

Table of contents

Table of contents

Table of contents

List of figures

List of figures

List of tables

Features

Intelligent 1 kByte Memory Chip with NRG and 7-byte Unique IDentification Number

Contactless Interface

- Physical Interface and Anticollision compliant to ISO/IEC14443-2 and -3 Type A
  - Operation frequency 13.56 MHz; data rate 106 kbit/s
  - Contactless transmission of data and supply energy
  - Anticollision logic: several cards may be operated in the field simultaneously
  - Features Short-Cut Anticollision scheme to realize backward compatibility to installed infrastructures supporting 4-byte single size UIDs only
- Read and Write Distance up to 10 cm and more (influenced by external circuitry i.e. reader and inlay design)
- Short transaction times: typical ticketing transaction < 100 ms; transaction possible when card is moving

1 kByte EEPROM

- Block organization of memory, 16 Sectors with fixed 4 blocks of 16 bytes each
- EEPROM updating time per block < 4 ms
- Endurance > 100.000 erase/write cycles[1]
- Data Retention > 10 years[1]
- User definable access conditions for each memory block

Security Features

- 7-byte Unique IDentifier (UID) according to ISO/IEC 14443-3 Type A
- Support of 4-byte Random Number (RND-ID) and 4-byte fixed non-unique number (FNUID) according to ISO/IEC 14443-3 Type A
- Mutual three-pass authentication between card and reader for basic security
  - 48-bit key length
  - 2 keys per sector enabling key management
  - Transport key at chip delivery
- Selective memory access control secured by authentication and access conditions
- Suited to multifunctional applications: Individual key sets are available for each EEPROM sector
- Data encryption for RF channel
- Dedicated Value Counter
- Data integrity supported by CRC, Parity Check, etc.

Electrical characteristics

- On-chip capacitance 18.3 pF + 10 %
- ESD protection typical 2 kV
- Ambient temperature -25 ... +70°C for the chip

[1] Values are temperature dependant

1 Ordering and packaging information

Table 1 Ordering information

Type	Package	Remark
SLE 66R35E7 C	Die (on wafer)	sawn / unsawn
SLE 66R35E7 NB	Die (on wafer)	NiAu-bumps, sawn
SLE 66R35E7 MCC8	MCC8-2-6	
SLE 66R35E7H C	Die (on wafer)	sawn / unsawn
SLE 66R35E7H NB	Die (on wafer)	NiAu-bumps, sawn
SLE 66R35E7H MCC8	MCC8-2-6	

Note: For further information on technology, delivery forms (wafer thickness or height of NiAu-bump) please contact your local Infineon Technologies sales representative (www.infineon.com).

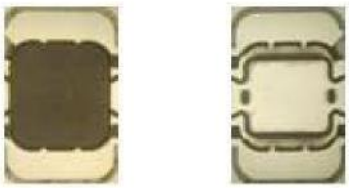

Figure 1 Pin configuration Module Contactless Card - MCC8-2-6 (top / bottom view)

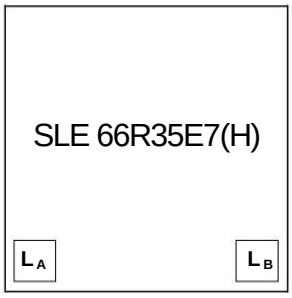

Figure 2 Pad configuration die

Table 2 Pin description and function

Symbol	Function
L_A	Antenna Connection
L_B	Antenna Connection

2 Overview of a NRG system

The SLE 66R35E7(H) is designed to operate in a NRG system. The system consists of a smart card and a card reader together with an antenna. The card's antenna consists of a simple coil with a few turns embedded in plastic.

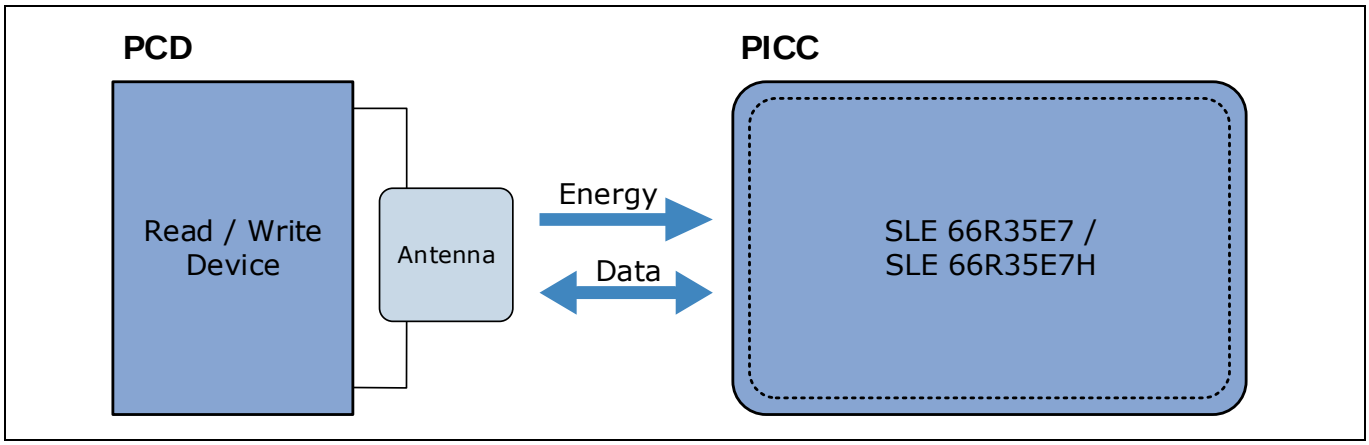

Figure 3 System overview

The operating distance between card and reader antenna is up to 10 cm and more (influenced by external circuitry i.e. reader-antenna configuration).

The RF communication interface transmits at 106 kbit/s resulting in short transaction times, the effect being that a card user can move freely through a reader gate with minimum disruption. A typical ticketing transaction can be handled in less than 100 m/s. Robust contactless transmission means that the card with SLE 66R35E7(H) may also remain in the wallet of the user even if there are coins in it.

An intelligent anticollision function based on the chip's double size unique identifier (uid0-uid6) enables more than one card in the field to operate simultaneously. The anticollision algorithm selects each card individually and enables the execution of a transaction with a selected card is performed correctly without data corruption resulting from other cards in the field.

The SLE 66R35E7(H) supports additional UID configurations allowing to operate SLE 66R35E7(H) in infrastructures running 4-byte (single cascade) anticollision schemes only (short-cut anticollision, Random Number, FNUID). Existing systems can remain unchanged. These options may be configured once during card personalization.

Access to SLE 66R35E7(H) is only allowed after a three-pass authentication. The serial number is unique for each card and cannot be changed. Each data transmission is enciphered. Protection from misuse is done by configurable access conditions that are protected by secret keys used for memory operations such as read or write.

Multi-Application Functionality

The SLE 66R35E7(H) is suited for the use in multi-application schemes, for example combining a transportation fare collection scheme and a ticketing system such as a stadium ticketing. Both applications can be performed with the same card, as hierarchical key management is supported. This means that two different keys for each memory sector can be assigned to enable authentication to that sector.

2.1 Supported standards

The SLE 66R35E7(H) supports the following standards:

- ISO/IEC 14443-1, -2 and -3 Type A [1]
- Tested according to ISO/IEC 10373-6 [2]

2.2 Command set

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

Additionally the SLE 66R35E7(H) specific command set is implemented. This facilitates the access to the on-chip integrated memory, supports the execution of authentication, encryption and decryption of data as well as an increment or a decrement of a dedicated value counter.

3 Circuit Description

SLE 66R35E7(H) consists of an EEPROM memory of 1 kByte organized in 16 sector with 4 blocks each containing 16 bytes, an analog interface for contactless energy and data transmission and a control unit.

The power supply and data are transferred to SLE 66R35E7(H) via an antenna, which consists of a coil with few turns directly connected to the module. No further external components are necessary. The circuit is designed to communicate with a card-reader at an operating distance of up to 10 cm (or more) depending on the reader-antenna configuration.

The chip is designed to meet the cost-optimized requirements of a basic security level. The targeted applications are transport, corporate access, events and loyalty cards with basic security requirements.

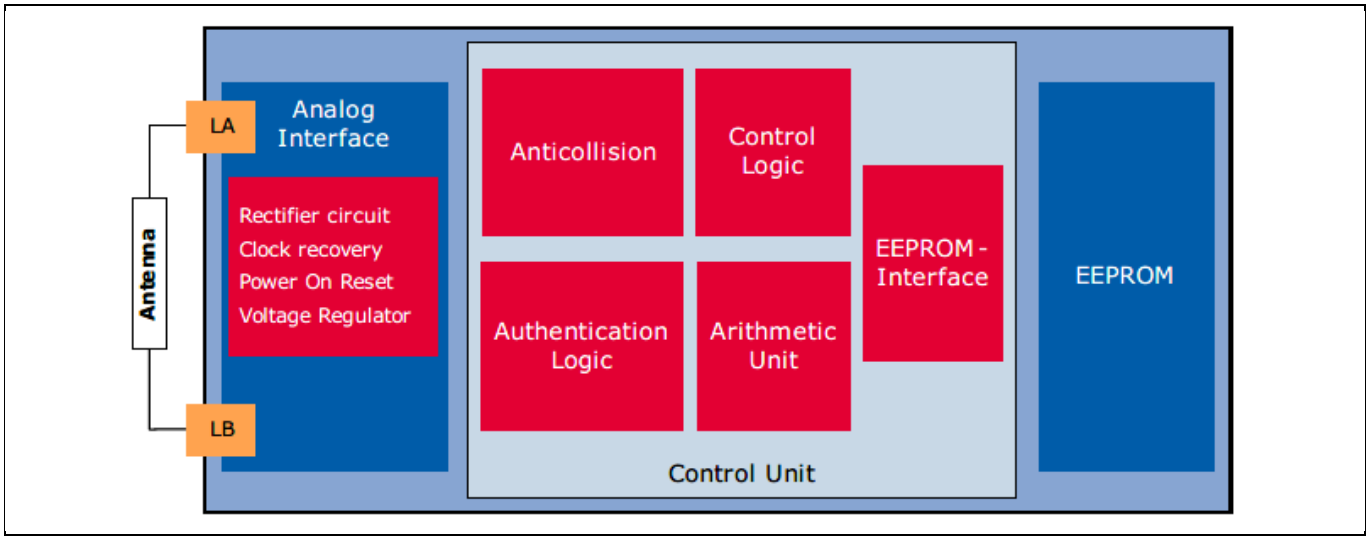

Figure 4 Block diagram

- **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.
- **Anticollision**
  - Internal logic of SLE 66R35E7(H) ensures the recognition of several cards in the field which may be selected and operated in sequence.
- **Authentication Logic**
  - Correct execution of any memory operation can only occur after the authentication procedure with a specific key.
- **Control Logic**
  - Access to a block is defined by the associated access conditions for that block. These are programmed individually for each block in a sector.
- **Arithmetic Unit**
  - Arithmetic Capability: increment and decrement of values stored in a special redundant format.
- **EEPROM:**
  - 1 kByte organized in 16 sectors with 4 blocks by 16 bytes each. The last block of each sector is called "Sector Trailer" and is used to store for a pair of secret keys and programmable access conditions for each block.

4 SLE 66R35E7(H) options

SLE 66R35E7(H) supports systems based on single and double size UIDs:

- 7-byte Unique IDentifier (UID) according to ISO/IEC 14443-3 Type A
- 4-byte Random Number (RND-ID) according to ISO/IEC 14443-3 Type A
- 4-byte fixed non-unique number (FNUID) according to ISO/IEC 14443-3 Type A

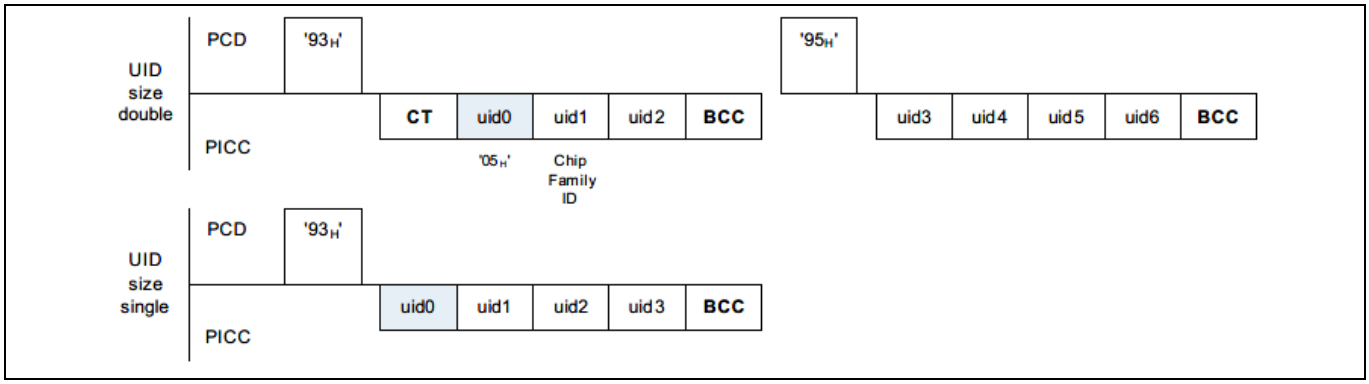

Figure 5 UIDs according to ISO/IEC 14443-3 Type A

4.1 Product overview

Following memory chips with NRG are available (see Table 3):

Table 3 Overview on chip types using NRG technology

Type	UID size	UID type	uid0	Description
SLE 66R35[1] [2]	4-byte	UID	xM_H $P8_H$	Fixed unique number programmed by manufacturer ($M = 1_H, 5_H, 7_H, 9_H$) and ($P = 1_H, 2_H, 3_H, 4_H, 5_H$)
SLE 66R35I	4-byte	FNUID	xF_H	Fixed number, non-unique programmed by manufacturer
SLE 66R35R	4-byte	r-ID	xM_H $P8_H$	Fixed reused identity number programmed by manufacturer ($M = 1_H, 5_H, 7_H, 9_H$) and ($P = 1_H, 2_H, 3_H, 4_H, 5_H$)
SLE 66R35E7(H)	7-byte	UID	05_H	Fixed unique number programmed by manufacturer (delivery default)
	4-byte	FNUID	xF_H	Fixed number, non-unique derived from 7-byte UID (personalization option). The FNUID is not stored in Block 00_H, it is derived from the 7-byte UID stored in Block 00_H. The derived value for the uid0 byte is logically OR-ed with $1F_H$; due to that x may have following values: 1_H, 3_H, 5_H, 7_H, 9_H, B_H, D_H, F_H
	4-byte	RND-ID	08_H	uid1 to uid3 is a random number (RND1 - RND3) (personalization option). The RND-ID is not stored in Block 00_H; a new RND-ID is generated with every power-up.

[1] The available numbers are already exhausted.

[2] Discontinued. Consider to use successor products SLE 66R35I, SLE 66R35R, SLE 66R36E7, SLE 66R35E7H.

SLE 66R35E7(H) options

4.2 Personalization options

SLE 66R35E7(H) can be configured during issuing of a card using the CONFIGURE_UID command (see 7.2.9).

Table 4 UID options

UID Option	Anticollision and selection
UIDF0	7-byte UID only (delivery default)
UIDF1	7-byte UID and optional usage of short-cut anticollision scheme
UIDF2	4-byte Random number (RND-ID) uid0 = 08_H uid1 – uid3 = RND1 – RND3
UIDF3	4-byte Fixed number, non-unique ID (FNUID) uid0 = xF_H ($x = 1_H, 3_H, 5_H, 7_H, 9_H, B_H, D_H, F_H$)

4.3 SLE 66R35E7(H) – 7-byte UID configuration

The SLE 66R35E7(H) is delivered as 7-byte UID device.

Block 00_H is configured as shown in Figure 6.

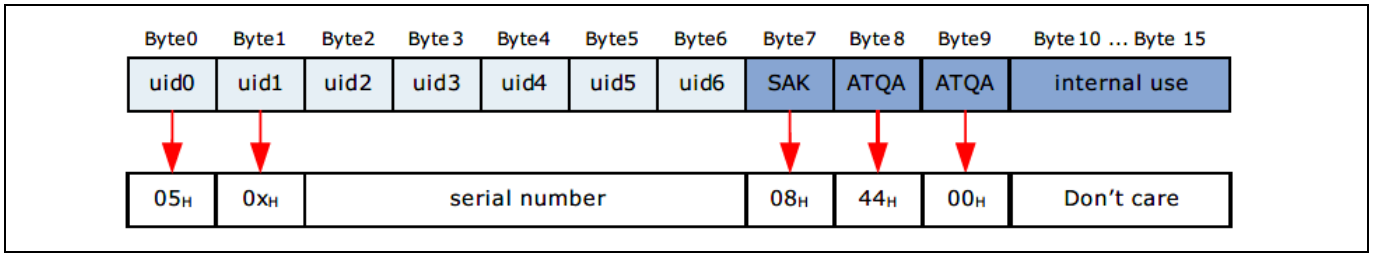

Figure 6 Memory structure block 00_H

- uid0 = 05_H identifies Infineon Technologies as chip manufacturer according to ISO/IEC 7816-6 standard [3]
- uid1 holds the Chip Family Identifier (see Table 5)

Table 5 Chip Family Identifier

uid1 coding[1]	Chip Family	Description
$0x_H$	SLE 66R35E7(H)	NRG product with 7-byte UID
$1x_H$	SLE 66RxxS	my-d™ proximity 2
$2x_H$	SLE 66RxxP	my-d™ NFC
$3x_H$	SLE 66R01P(N)	my-d™ move (NFC)
$7x_H$	SLE 66R01L(N)	my-d™ move lean (NFC)
All other		Please contact Infineon Technologies sales

Note: Please also refer to the application note "Anticollision and UID Options" for further information on UIDs as used for Infineon Products.

[1] 'x_H' is part of the chip serial number.

SLE 66R35E7(H) options

Anticollision for CL1 (Short-cut) and CL2

The SLE 66R35E7(H) supports the both anticollision schemes cascade level 1 (short-cut anticollision) and 2. The short-cut anticollison allows to operate the SLE 66R35E7(H) even in infrastructures with 4-byte (single cascade) anticollision scheme. Existing systems based on CL1 can remain unchanged.

If the Short-cut anticollision scheme has been enabled (UIDF1 Option, in READY2 / READY2* state the chip accepts:

- a READ (Block 00_H) command: the SLE 66R35E7(H) then executes a state transition to ACTIVE / ACTIVE* state. Following authentication commands will use the last four UID bytes sent to the PCD.
    - an AUTHENTICATE command to a sector: the SLE 66R35E7(H) then executes a state transition to the AUTHx state applying the UID bytes used for cascade level 1 selection (SEL CL1).

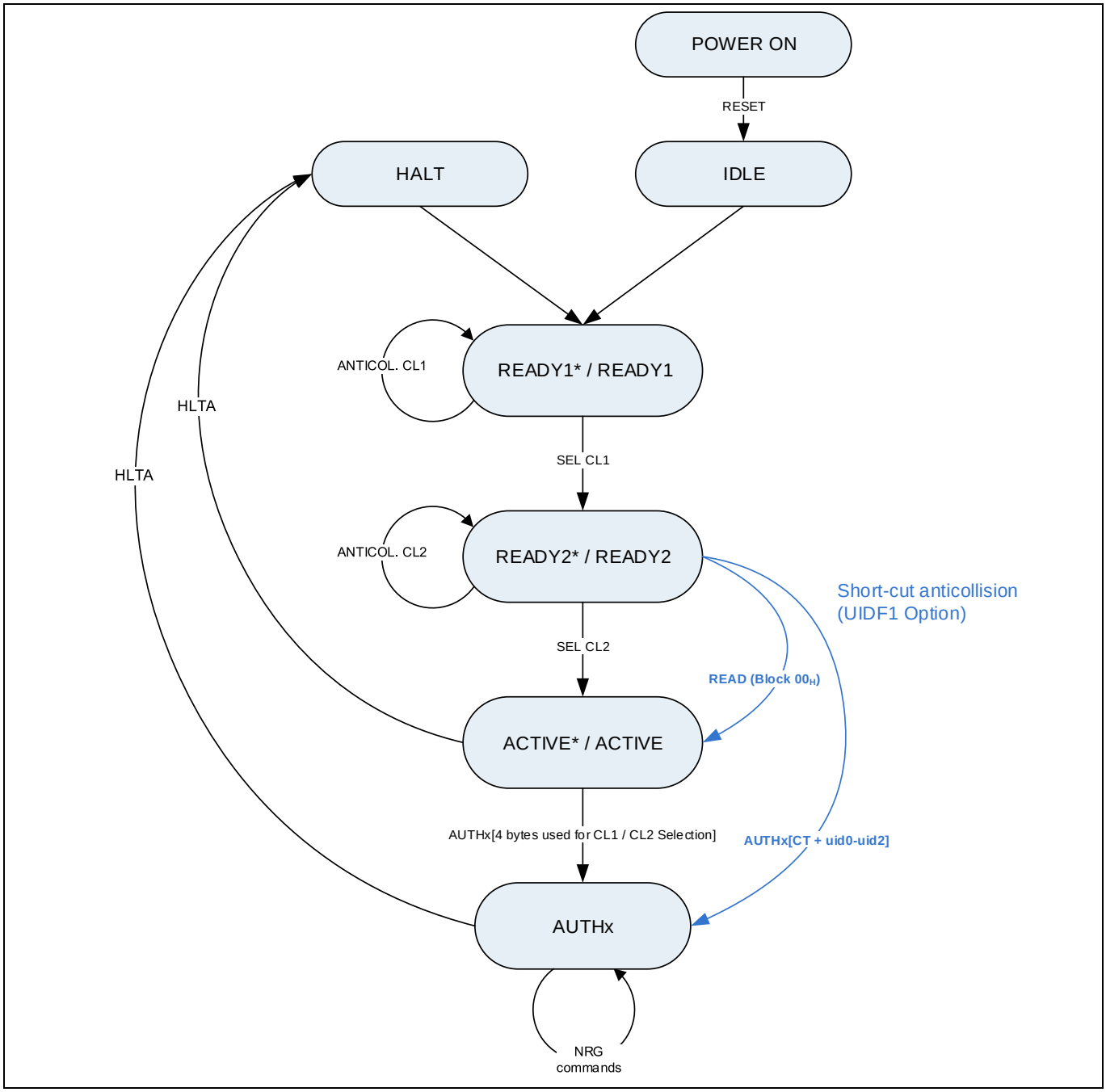

Figure 7 Anticollision for UIDF0 and UIDF1 options

SLE 66R35E7(H) options

4.4 SLE 66R35E7(H) – 4-byte UID configurations

The SLE 66R35E7(H) also supports single cascade anticollision schemes.

- 4-byte Random Number (RND-ID)
- 4-byte fixed non-unique number (FNUID)

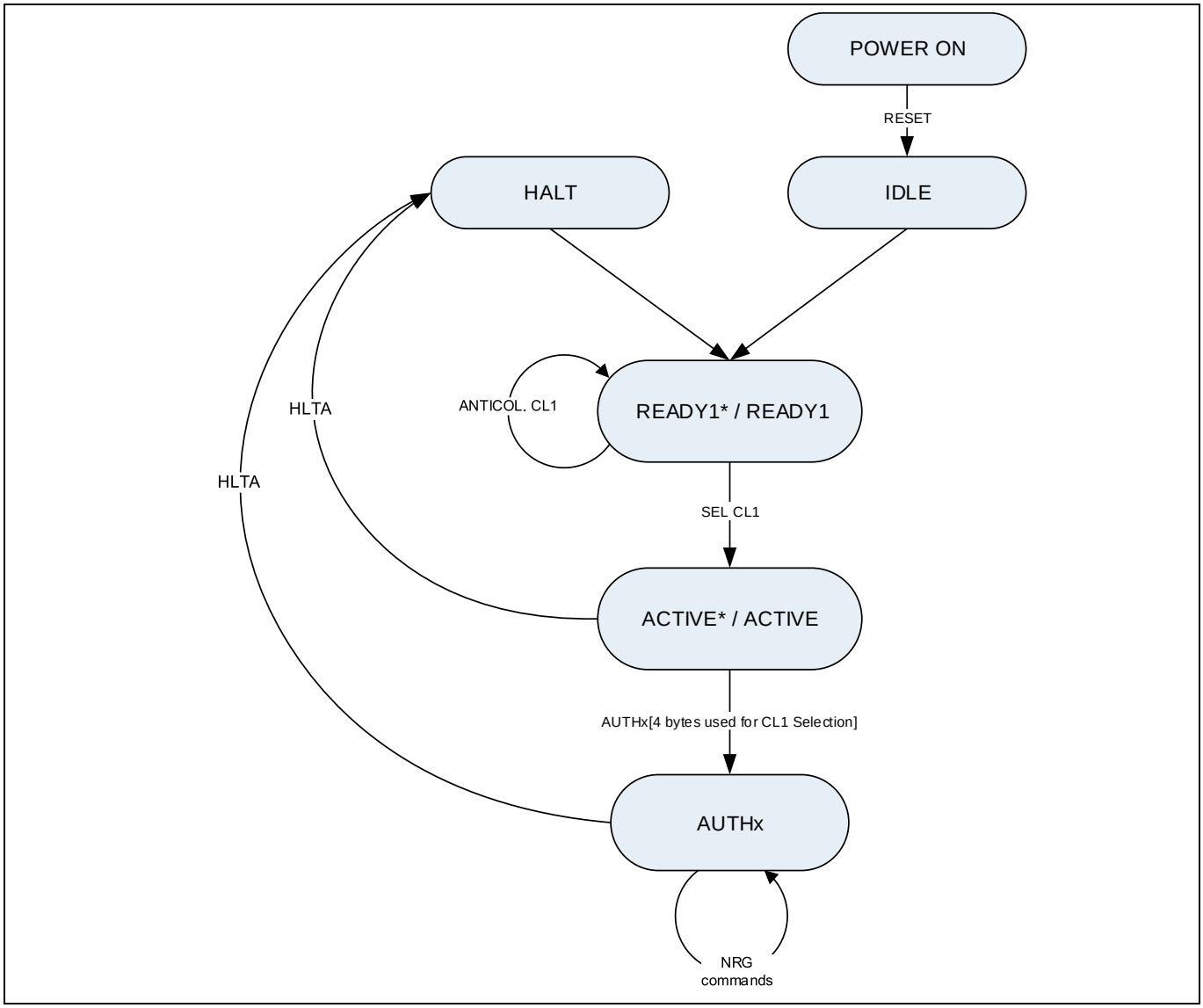

Figure 8 Anticollision for UIDF2 and UIDF3 options

5 Memory organization

The 1024 Byte EEPROM is organized in 16 sectors with 4 blocks of 16 bytes each.

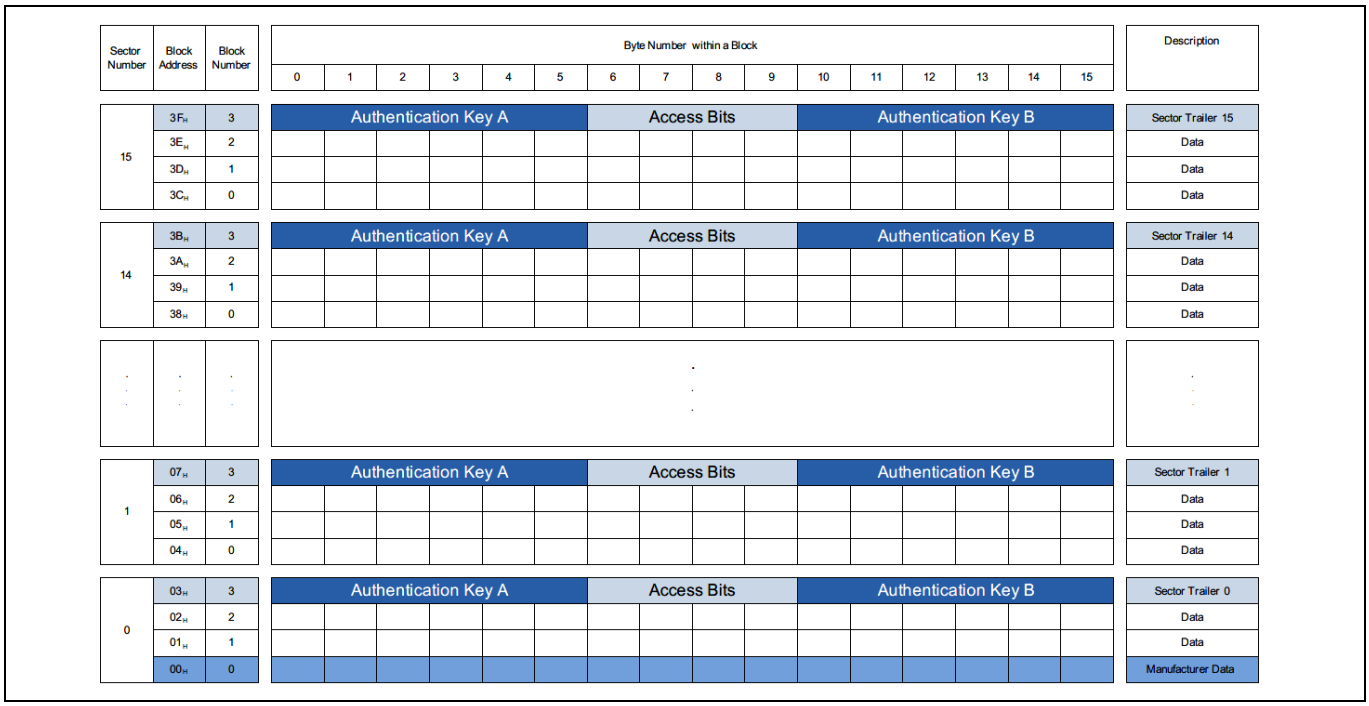

Figure 9 Memory organization

Each sector contains four 16 bytes blocks.

- 3 blocks of data are configurable
  - as Read / Write blocks for storing general data
  - as Value blocks for e.g. electronic purse applications
  - Sector 0, Block 00_H contains Manufacturer Data (serial number, SAK, ATQA, etc.), read only
- the Sector Trailer contains the individual secret authentication Key A and optional Key B as well as the block accesses conditions of the respective sector
  - authentication Key A
  - (optional) authentication Key B
  - access bits to define the access conditions for the specified blocks for every sector individually.

    The Sector Trailer and the data blocks are controlled independently.

A successful authentication procedure for the desired sector has to be carried out to allow access to the memory by the appropriate commands.

Furthermore, the access to the EEPROM is controlled by the access conditions (set by the access bits) depending on the application. Applications for contactless access control (e.g. identification) only require read and write operations whereas in revenue control systems (e.g. public transport applications) additional commands like increment, decrement for direct control of the value stored are provided.

All sectors can be assigned to different applications by use of different keys. The authentication procedure is performed between the Reader and the contactless card automatically. Access to stored data is only permitted after successful authentication to that sector.

In erased state the EEPROM cells are as a 1_B, the written state is represented by a 0_B.

5.1 Manufacturer block SLE 66R35E7(H)

The information within the manufacturer block (Block 00_H, Sector 0) is programmed and locked during the manufacturing process. It is reserved to store:

- 7-byte UID
  - uid0 = 05_H: Manufacturer Code according to ISO/IEC 7816-6 [3]
  - uid1 = $0x_H$:

    higher nibble: 0_H is the Chip Family Identifier for the SLE 66R35E7(H) (fixed during manufacturing)
    lower nibble: x_H is part of the serial number
  - uid2 - uid6 = part of the serial number
- SAK: Select Acknowledge
- ATQA: Answer to Request A
- REV: Revision byte = $E1_H$
- Manufacturer specific data

Figure 10 gives some details on the content of Block 00_H.

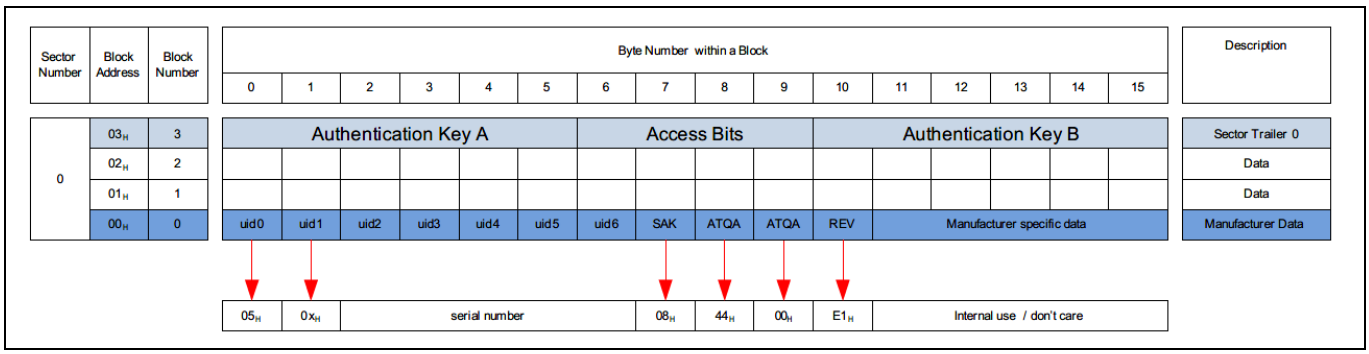

Figure 10 Manufacturer block SLE 66R35E7(H)

5.2 Answer to Request (ATQA) and Select Acknowledge (SAK)

Following valid responses are returned to valid …

- ATQA to REQA or WUPA commands and
- SAK to the SELECT command

Table 6 ATQA and SAK responses SLE 66R35E7

Product	UID Option	ATQA response	SAK Cascade Level 1	SAK Cascade Level 2	Description
SLE 66R35E7	UIDF0	00_H 44_H	$0C_H$	08_H	7-byte UID only (default)
	UIDF1	00_H 44_H	$0C_H$	08_H	7-byte UID with short-cut anticollision enabled
	UIDF2	00_H 04_H	88_H	-	4-byte Random number (RND-ID)
	UIDF3	00_H 04_H	88_H	-	4-byte Fixed number (FNUID)

Memory organization

Table 7 ATQA and SAK responses SLE66R35E7H

Product	UID Option	ATQA response	SAK Cascade Level 1	SAK Cascade Level 2	Description
SLE 66R35E7H	UIDF0	00_H 44_H	$0C_H$	08_H	7-byte UID only (default)
	UIDF1	00_H 44_H	$0C_H$	08_H	7-byte UID with short-cut anticollision enabled
	UIDF2	00_H 04_H	08_H	-	4-byte Random number (RND-ID)
	UIDF3	00_H 04_H	08_H	-	4-byte Fixed number (FNUID)

5.3 Personalization Options

The SLE 66R35E7(H) has a 7-byte UID which is stored in the Block 00_H of Sector 0.

The behavior of the SLE 66R35E7(H) during anticollision, selection and authentication must be configured during the issuing process of this product. Following issuing options are available, labeled with UIDFn (UID Functionality n):

Table 8 UID options for SLE 66R35E7(H)

UID Option	Anticollision and selection	Description
UIDF0	7-byte UID only	Delivery default
UIDF1	7-byte UID with short-cut anticollision enabled	
UIDF2	4-byte Random number (RND-ID)	uid0 = 08_H A new RND-ID is generated during every POWER-UP of the chip.
UIDF3	4-byte Fixed number, non-unique ID (FNUID)	uid0 = xF_H (x = 1_H, 3_H, 5_H, 7_H, 9_H, B_H, D_H, F_H) The FNUID is derived from the 7-byte UID stored in Block 00_H.

The desired configuration is selected using the CONFIGURE_UID command during the issuing process of the SLE 66R35E7(H). Prior to the execution of the CONFIGURE_UID command an authentication to Sector 0 is required. Once executed, the selected functionality (UID option) cannot be changed anymore. The change is irreversible as the selected configuration is locked. A subsequent execution of this command results in NACK response. The new configuration is active after a power-on reset.

Note: The CONFIGURE_UID command must be executed in the personalization process. This is mandatory to lock the UID option settings (even if the default configuration is chosen).

Note: The execution of this command has no influence on the content of the Block 00_H.

Memory organization

UID Information

Table 9 shows the UID information which is retrieved from the different SLE 66R35x variants during the anticollision.

Table 9 UID Information

Product	Option	Cascade Level 1 response					Cascade Level 2 response				
SLE 66R35E7(H)	UIDF0	88_H	05_H	$0x_H$	uid2	BCC0[1]	uid3	uid4	uid5	uid6	BCC1[1]
	UIDF1	88_H	05_H	$0x_H$	uid2	BCC0[1]	uid3	uid4	uid5	uid6	BCC1[1]
	UIDF2	08_H	RND1	RND2	RND3	BCC[2]					
	UIDF3	xF_H	xx_H	xx_H	xx_H	BCC[2]					
SLE 66R35	-	uid0	uid1	uid2	uid3	BCC[3]					
SLE 66R35R	-	uid0	uid1	uid2	uid3	BCC[3]					
SLE 66R35I	-	xF_H	xx_H	xx_H	xx_H	BCC[3]					

Serial Number Check, BCC

According to the ISO/IEC14443-3 Type A the BCC is the UID CLn checkbyte, calculated as exclusive-or over the four previous bytes (as described in ISO/IEC 14443-3 Type A).

5.4 Sector Structure

Each sector has three data blocks (block numbers 0, 1 and 2) and the Sector Trailer block (block number 3).

5.4.1 Data blocks / Value blocks

Each data block can be defined as Read / Write block or as Value block by setting the specific access conditions. According to these conditions data can be read, written, incremented, decremented, restored or transferred to the card after a successful authentication with either authentication Key A or authentication Key B.

Read / Write blocks

A Read / Write block is used to store general application data (valid commands: READ, WRITE).

Value block

The Value blocks allows electronic purse functions to be performed. Valid commands are READ, WRITE, INCREMENT, DECREMENT, RESTORE and TRANSFER. The Value blocks have a fixed data format that permits error detection, error correction and a backup management.

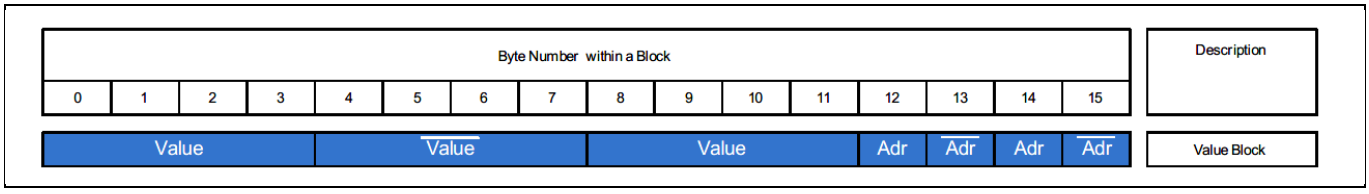

Figure 11 Data structure of a Value block

[1] The BCC0 and BCC1 values are generated during anticollision.

[2] The BCC value is generated during anticollision.

[3] The BCC value is stored within Block 00_H.

Memory organization

- Value is a signed four byte value. For the security and integrity purposes it is stored three times; twice non-inverted and once bit-inverted. Values are stored in 2[s] complement binary format with the most significant bit as a sign bit.

  The value is stored in the big endian order, hence the most significant byte is stored at the highest address of the reserved memory field.
- The address (Adr) signifies a 1-byte block address. It is used to keep the storage address of a block that is particularly useful for implementing a powerful backup management. The address byte is stored four times, twice inverted and twice non-inverted and it can only be changed by a WRITE command. During INCREMENT, DECREMENT, RESTORE and TRANSFER operations the address is not altered.

The WRITE command must also be used to initialize a Value block. The value and the address must be written in the appropriate format. The arithmetic commands INCREMENT, DECREMENT are available to modify the value content, but Value blocks may still be accessed with READ and WRITE commands. The block management commands RESTORE and TRANSFER are available to manage the backup management and programming of the Value blocks.

5.4.2 Sector Trailer

Every sector has a Sector Trailer (block 3 within every sector) containing the authentication keys (Key A and Key B) and the access condition information of the associated sector, i.e. access to the data blocks (0, 1 and 2) and the Sector Trailer itself.

Block Number	Byte Number within a Block																Description
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
3	Authentication Key A						Access Bits				Authentication Key B (optional)						Sector Trailer
2																	Data or Value Block
1																	Data or Value Block
0																	Data or Value Block

Figure 12 Data structure of a Sector Trailer

- Authentication Key A (mandatory): these field contains the cryptographic key A which can never be read (a READ command returns the value 00_H 00_H 00_H 00_H 00_H 00_H.
- Authentication Key B (optional): depending on the access conditions this portion of the Sector Trailer can be read after an authentication or never be read (when used as key; in this case a READ command returns the value 00_H 00_H 00_H 00_H 00_H 00_H).
- If the Key B is readable then it can be used for the authentication however any subsequent access to the memory (Read, Write...) is denied and will result in NACK response.
- Access Bits define the access conditions for each block of the sector and the Sector Trailer.
- Byte 9 of the Sector Trailer is reserved for future use and shall not be checked by the application. It does not contain access condition information and might be used for other application data.

Each sector should have different values for authentication Key A and (the optional) authentication Key B as all sectors can be assigned to different applications offered by different system providers. The authentication procedure is performed between the reader and the SLE 66R35E7(H) card. Only after successful authentication to a sector the access to data blocks is enabled.

5.5 Memory access

The SLE 66R35E7(H) memory can be accessed using a defined memory commands. Before execution of any memory command, the desired card has to be selected via appropriate operation and the three-pass authentication procedure has to be completed. All possible memory operations for an addressed block in the memory depend on key which is used for the authentication as well as on the assigned access conditions stored in the associated sector trailer, see also 5.5.1.

Table 10 Memory access command set

Command	Op-code	Description	Valid for blocks
READ	30_H	Reads the data from an addressed block if access conditions permit an access.	Data block Value block Sector Trailer
WRITE	$A0_H$	Writes the data to an addressed block if access conditions permit an access.	Data block Value block Sector Trailer
DECREMENT	$C0_H$	Decrement the addressed value by the received value and stores the result into the internal buffer.	Value block
INCREMENT	$C1_H$	Increment the addressed value by the received value and stores the result into the internal buffer.	Value block
RESTORE	$C2_H$	Loads the content of an addressed block into the internal buffer. Only allowed if the addressed block in a Value block format.	Value block
TRANSFER	$B0_H$	Writes the content of the internal buffer to the addressed block. The addressed block will be programed in Value block format.	Value block

5.5.1 Access conditions

The access conditions (AC) for every data block and Sector Trailer are stored in byte 6, 7 and 8 of the Sector Trailer of each block. These access bits control the access rights of memory access for different commands and keys. The byte 9 is accessible under the same access condition as for Sector Trailer and can be used for the additional data storage.

Bits $C1_Y$, $C2_Y$ and $C3_Y$ (Y = block number, 0..3), are stored twice (non-inverted and inverted) for data integrity reasons. They define the access conditions for every block inside each sector.

If the format of access condition bits in one specific Sector Trailer is incorrect, an authentication to this sector is still possible, but any subsequent memory access will be rejected.

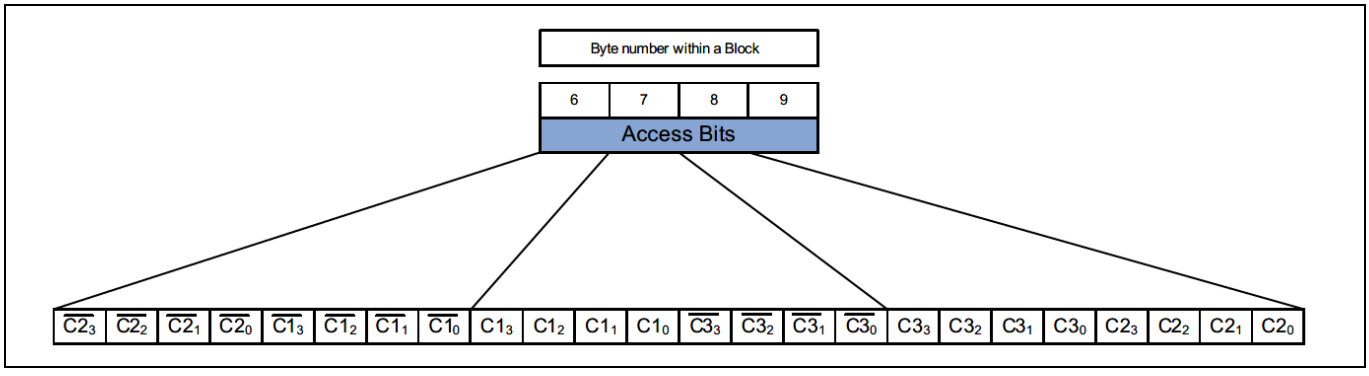

Figure 13 Access conditions

Memory organization

Table 11 Access conditions

Access Bits	Valid for block	Description	Valid commands
$C3_3$ $C2_3$ $C1_3$	3	Sector Trailer	READ, WRITE
$C3_2$ $C2_2$ $C1_2$	2	Data block	READ, WRITE, INCREMENT, DECREMENT, TRANSFER, RESTORE
$C3_1$ $C2_1$ $C1_1$	1	Data block	READ, WRITE, INCREMENT, DECREMENT, TRANSFER, RESTORE
$C3_0$ $C2_0$ $C1_0$	0	Data block	READ, WRITE, INCREMENT, DECREMENT, TRANSFER, RESTORE

5.5.2 Access conditions for Sector Trailer

Depending on the access conditions for the Sector Trailer read / write access to either authentication Key A or Key B or to the access bits is specified as 'Never', 'Key A' or 'Key B'. 'Key A / Key B' means that the access is possible only after an authentication to the sector using authentication Key A or authentication Key B.

Table 12 Access condition for Sector Trailer

Access Bits			Access condition for						Remark
			Authentication Key A		Access Bits[1]		Authentication Key B		
$C3_3$	$C2_3$	$C1_3$	READ	WRITE	READ	WRITE	READ	WRITE	
0	0	0	Never	Key A	Key A	Never	Key A	Key A	Key B may be read[2]
0	0	1	Never	Key B	Key A / Key B	Never	Never	Key B	
0	1	0	Never	Never	Key A	Never	Key A	Never	Key B may be read
0	1	1	Never	Never	Key A / Key B	Never	Never	Never	
1	0	0	Never	Key A	Key A	Key A	Key A	Key A	Transport Configuration
1	0	1	Never	Never	Key A / Key B	Key B	Never	Never	
1	1	0	Never	Key B	Key A / Key B	Key B	Never	Key B	
1	1	1	Never	Never	Key A / Key B	Never	Never	Never	

[1] Access Bits can also be locked which prevents any further changes of the access conditions

[2] The bytes reserved to store for Key B may be used to store data. Access to data blocks is not possible.

5.5.3 Access conditions for data blocks

Depending on the access bits for the data blocks (block number Y = 0...2) the read / write access is specified as ‘Never’, ‘Key A’, ‘Key B’ or ‘Key A / Key B’ (Key A or Key B). The setting of the relevant access bits defines the application and the corresponding applicable commands.

Table 13 Access condition for data blocks

Access Bits (Y = 0 … 2)			Access condition Data block (block number Y = 0 … 2)				Application
$C3_Y$	$C2_Y$	$C1_Y$	READ	WRITE[1]	INCREMENT	DECREMENT TRANSFER RESTORE	
0	0	0	Key A / Key B	Key A / Key B	Key A / Key B	Key A / Key B	Transport Configuration Read / Write / Value block
0	0	1	Key A / Key B	Key B	Never	Never	Read / Write block
0	1	0	Key A / Key B	Never	Never	Never	Read / Write block
0	1	1	Key A / Key B	Key B	Key B	Key A / Key B	Value block
1	0	0	Key A / Key B	Never	Never	Key A / Key B	Value block
1	0	1	Key B	Never	Never	Never	Read / Write block
1	1	0	Key B	Key B	Never	Never	Read / Write block
1	1	1	Never	Never	Never	Never	Read / Write block

[1] Write access conditions do not apply for Block 00_H of Sector 0.

5.6 Transport configuration

At delivery the memory is predefined. After a successful authentication with either Key A or Key B of a sector the respective data can be accessed.

- Data area is set to 00_H as default
- Key A and Key B are set to FF_H FF_H FF_H FF_H FF_H FF_H as default

Reading of Key A is never allowed, thus the value 00_H 00_H 00_H 00_H 00_H 00_H is read. Sector Trailer byte 9 is set arbitrary.

Sector Number	Block Address	Block Number	Byte Number within a Block 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	$3F_H$	3	00_H	00_H	00_H	00_H	00_H	00_H	FF_H	07_H	80_H	xx_H	Authentication Key B						Sector Trailer 15
	$3E_H$	2																	Data
	$3D_H$	1																	Data
	$3C_H$	0																	Data
14	$3B_H$	3	00_H	00_H	00_H	00_H	00_H	00_H	FF_H	07_H	80_H	xx_H	Authentication Key B						Sector Trailer 14
	$3A_H$	2																	Data
	39_H	1																	Data
	38_H	0																	Data
. . .	. . .	. . .	. . .																. . .
1	07_H	3	00_H	00_H	00_H	00_H	00_H	00_H	FF_H	07_H	80_H	xx_H	Authentication Key B						Sector Trailer 1
	06_H	2																	Data
	05_H	1																	Data
	04_H	0																	Data
0	03_H	3	00_H	00_H	00_H	00_H	00_H	00_H	FF_H	07_H	80_H	xx_H	Authentication Key B						Sector Trailer 0
	02_H	2																	Data
	01_H	1																	Data
	00_H	0	05_H	$0x_H$	uid2	uid3	uid4	uid5	uid6	08_H	44_H	00_H	$E1_H$	Manufacturer specific data					Manufacturer Data

Figure 14 Memory map - Transport Configuration SLE 66R35E7(H)

6 Communication Principle

6.1 State diagram

The SLE 66R35E7(H) is fully compliant to the ISO/IEC 14443-3 Type A specification.

All operations are initiated by an appropriate reader and controlled by the internal logic of the SLE 66R35E7(H). Prior to any memory access the card has to be selected according to the ISO/IEC 14443-3 Type A anticollision and selection scheme.

After the anticollision and selection the reader may enter the protected state by performing the authentication procedure to any sector by sending the AUTHENTICATE command (either with Key A or with Key B and a valid block address). Any other command will cause an error and the SLE 66R35E7(H) will return either to IDLE or to HALT state.

Figure 15 shows the state diagram of the SLE 66R35E7(H).

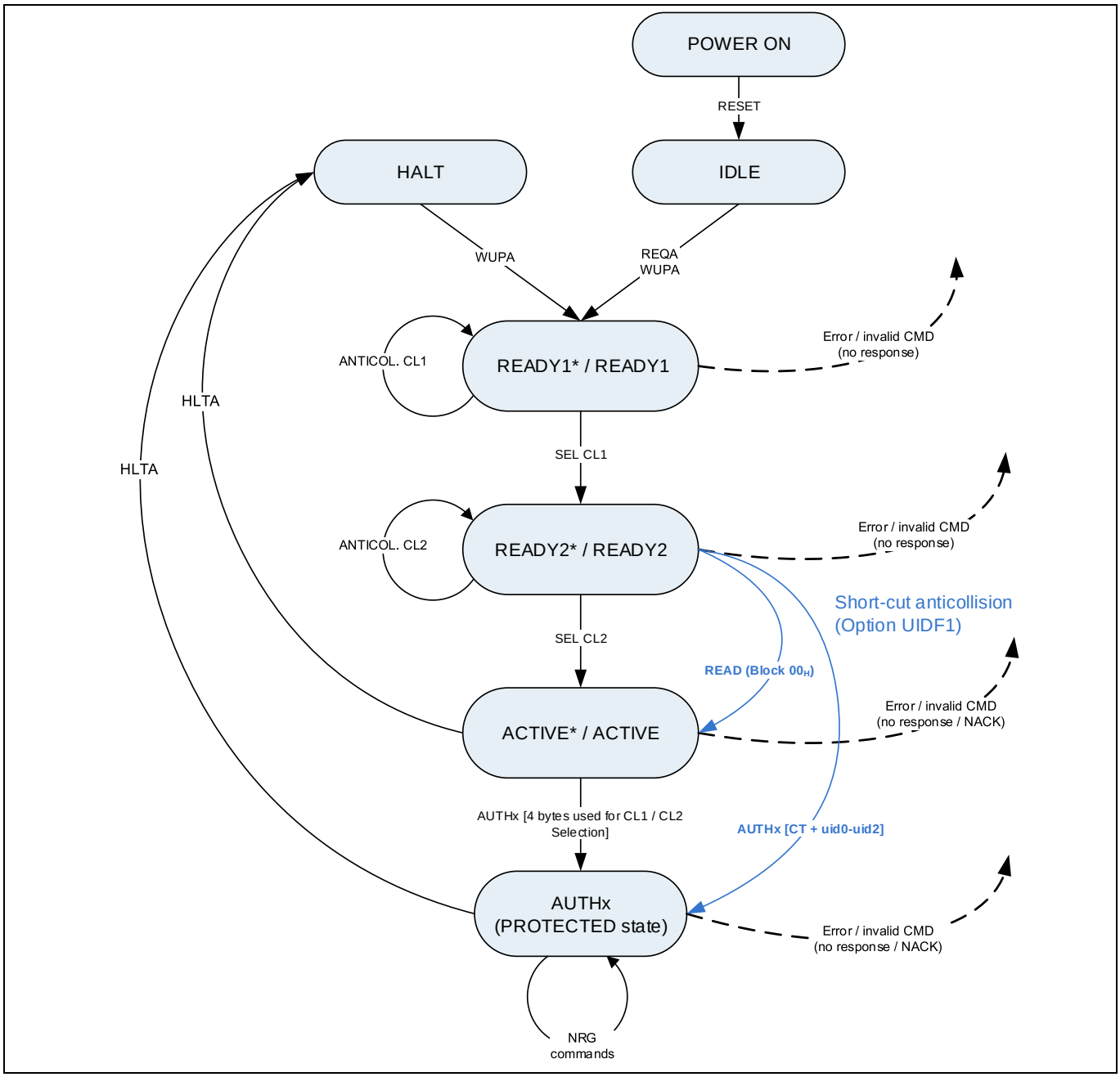

Figure 15 SLE 66R35E7(H) state diagram (UIDF0 and UIDF1 option)

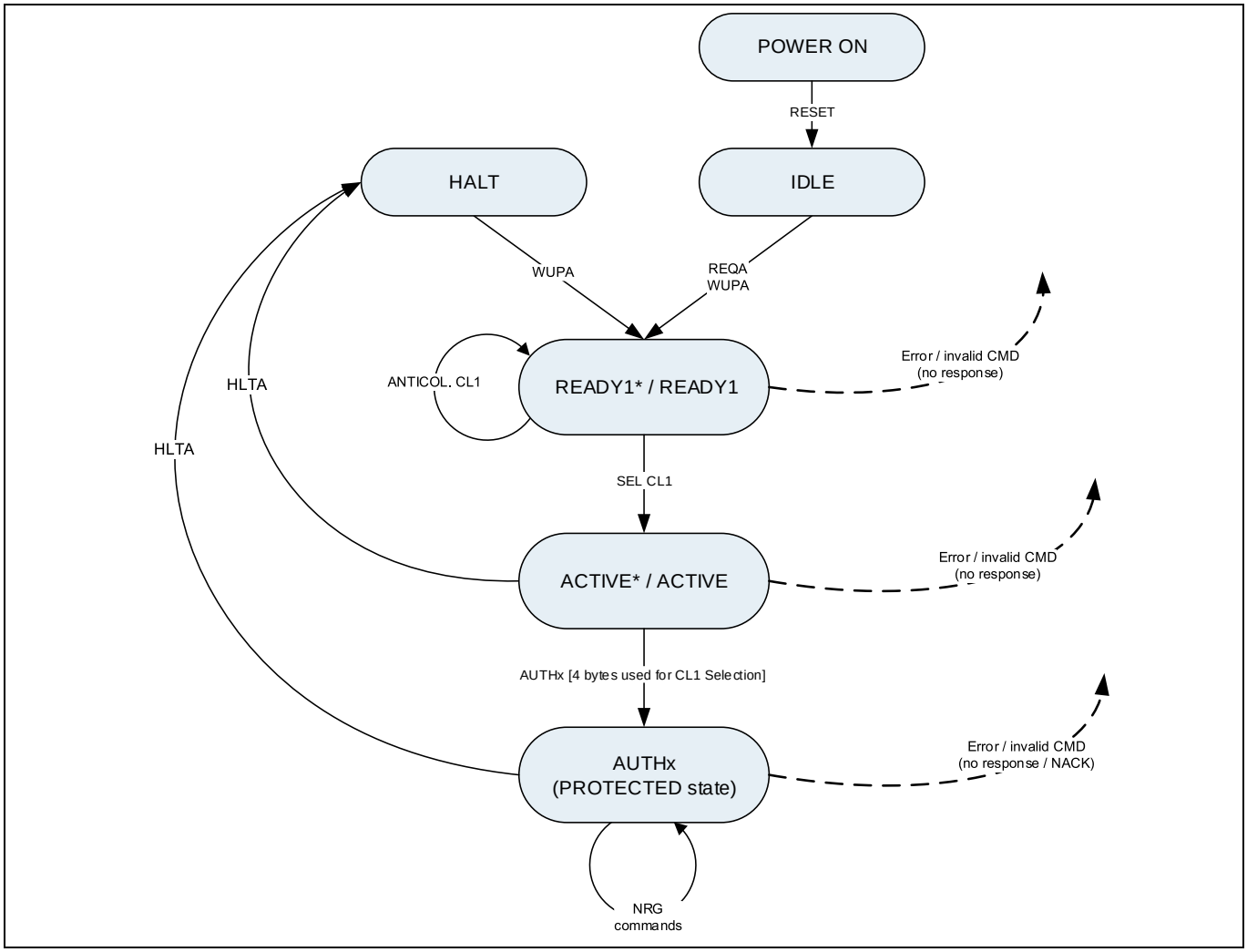

Figure 16 SLE 66R35E7(H) state diagram (UIDF2 and UIDF3 option)

6.1.1 IDLE state

After POWER ON, the SLE 66R35E7(H) is in IDLE state.

If REQA or WUPA command is executed in this state, the SLE 66R35E7(H) transits to READY1 state. Any other command is interpreted as an error and the SLE 66R35E7(H) stays in IDLE state without any response.

6.1.2 READY1 / READY1* state

In READY1 / READY1* state:

- for 7-byte UIDs the first part of the UID can be retrieved by using ISO/IEC 14443-3 Type A Anticollision and/or Select commands. After the Select command is executed the IC transits to READY2 / READY2* state in which the second part of the UID can be retrieved. The answer to a Select command in READY1 / READY1* state is Select Acknowledge (SAK) for cascade level 1 (CL1), 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).
  Any other command or any other interruption is interpreted as an error and the SLE 66R35E7(H) returns back to IDLE or HALT state without any response, depending from which state it came from.
- for 4-byte UIDs (UIDF2 and UIDF3 options) the whole UID can be retrieved by using ISO/IEC 14443-3 Type A Anticollision and Select commands. After the Select command is executed properly the IC transits to ACTIVE / ACTIVE* state. The answer to a Select command in READY1 / READY1* state is Select Acknowledge (SAK), which indicates that the UID is complete (see also ISO/IEC 14443-3 Type A).

Communication Principle

Any other command or any other interruption is interpreted as an error and the SLE 66R35E7(H) returns back to IDLE or HALT state without any response, depending from which state it came from.

6.1.3 READY2 / READY2* state

This state is only valid for the SLE 66R35E7(H) configured to have a 7-byte UID (UIDF0 and UIDF1 options). In READY2 / READY2* state the second part of the 7-byte UID can be retrieved using ISO/IEC 14443 Type A Anticollision and/or Select commands. After the Select command is successfully executed the IC transits to ACTIVE / ACTIVE* state. The Answer to a Select command in READY2 / READY2* state is SAK for cascade level 2 (CL2), which indicates that the UID is complete and the selection process is finished.

The exception is made for SLE 66R35E7(H) with Short-cut functionality (UIDF1) which can directly transit from READY2 / READY2* state to

- ACTIVE / ACTIVE* state if READ (Block 00_H) command is executed
- PROTECTED state if an AUTHENTICATE command to any valid sector is executed

Any other command or any other interruption is interpreted as an error and the SLE 66R35E7(H) returns back to IDLE or HALT state without any response, depending from which part it has come from.

Short-cut Functionality

If the Short-cut functionality is enabled (UIDF1) and the SLE 66R35E7(H) in READY2 / READY2* state receives

- a valid READ (Block 00_H) command it executes the state transition from READY2 / READY2* to the ACTIVE / ACTIVE* state.
- a valid AUTHENTICATE command it executes the state transitions from READY2 / READY2* state to the PROTECTED state.

In both cases the SLE 66R35E7(H) takes the first 4 byte of the UID (CT, uid0, uid1 and uid2) which were used in the READY1 / READY1* state to initialize its CRYPTO1 unit at the beginning of the authentication process.

6.1.4 ACTIVE / ACTIVE* state

In ACTIVE / ACTIVE* state during an execution of a valid AUTHENTICATE command 4 bytes of the UID are used to initialize the CRYPTO1. Depending on the UID configuration (UIDFx) the 4 bytes are chosen differently.

For more information please refer to the Table 14.

Table 14 Initialization parameter for the CRYPTO1 unit

Personalization option	Parameter used to initialize the CRYPTO1 registers	Description
UIDF0	uid3, uid4, uid5, uid6	7-byte UID product
UIDF1	CT, uid0, uid1, uid2	7-byte UID product with Short-cut functionality enabled
UIDF2	08_H, RND1, RND2, RND3	4-byte Random ID (RND-ID) configured during the personalization
UIDF3	xF_H, xx_H, xx_H, xx_H	4-byte Fixed number, non-unique ID (FNUID) configured during the personalization

Communication Principle

The ACTIVE / ACTIVE* state is left with a HLTA command. The SLE 66R35E7(H) transits to HALT state and waits until a WUPA command is received.

If any error is detected the SLE 66R35E7(H) sends “No Response” (NR) or “Not Acknowledge” (NACK) and transits to IDLE or HALT state depending on the previous state.

6.1.5 PROTECTED state (AUTHx)

In the PROTECTED State SLE 66R35E7(H) memory access commands can be executed. These commands can be applied to the currently authenticated sector in any order, including the authentication of another sector with the following exceptions and recommendations:

- arithmetic commands such as INCREMENT and DECREMENT shall only be applied to blocks in Value block format
- successful execution of a RESTORE, INCREMENT or DECREMENT command is recommended before executing the TRANSFER command
- SLE 66R35E7(H)exits the PROTECTED state upon reception of the HLTA command or in a case of an error

6.1.6 HALT state

The HLTA command sets the SLE 66R35E7(H) in the HALT state. The SLE 66R35E7(H) sends no response to the HLTA command. The HALT state is left by a WAKE-UP A (WUPA) request. Any other data received is interpreted as an error, the SLE 66R35E7(H) sends no response and remains in HALT state.

6.2 Start up

Latest 250 µs after entering the powering field the SLE 66R35E7(H) is ready to receive a command.

6.3 Frame Delay Time

For detailed timings see ISO/IEC 14443-3 Type A Standard.

Note: The response timing of a particular command in specified in the command description.

6.4 Error handling

The SLE 66R35E7(H) responds to valid frames only. In case of any error the SLE 66R35E7(H) returns to its initial state, either IDLE or HALT state. Depending on the error type, the SLE 66R35E7(H) responds either with a Not Acknowledge (NACK) or does not respond (NR).

Table 15 lists ACK and NACK responses.

Table 15 ACK and NACK responses

Response	Code (4 bits)[1]
ACK	1010_B
NACK0	0000_B
NACK1	0001_B
NACK4	0100_B
NACK5	0101_B
NR[2]	n.a.

[1] No integrity mechanism, the response is encrypted.

[2] NR = no response. Depending on the state the does not send a response on errors.

Communication Principle

Table 16 describes the behavior of the SLE 66R35E7(H) in different error cases.

Table 16 Behavior in case of error

Current States	Command or Error	Response	Next State
IDLE / HALT READY1 / READY1* READY2 / READY2*	Invalid op-code	NR	IDLE / HALT
	Parity, Miller or CRC error	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 op-code	NR	IDLE / HALT
	Parity, Miller, CRC error	NACK1 or NACK5	IDLE / HALT
	Command too short or too long	NR	IDLE / HALT
	Invalid address	NACK0 or NACK4	IDLE / HALT
	Other errors	NACK0 or NACK4	IDLE / HALT

6.5 Data integrity

Reliable data transmission in the contactless communication link is supported by following mechanisms:

- 16 bit CRC (Cyclic Redundancy Check) for each data transmission
- Parity bits for each byte
- Monitoring of protocol sequence
  - bit coding to distinguish between "1", "0" and “no information”
  - bit stream analysis
  - bit count checking

6.6 Three-pass authentication

A basic security level is provided using a three-pass authentication between the SLE 66R35E7(H) and the reader. The three-pass authentication sequence is split into following steps:

- The reader selects the sector to be accessed by addressing a block within this sector. The reader transmits the AUTH command using either authentication Key A or Key B.
- SLE 66R35E7(H) reads the secret key and the associated access conditions from the Sector Trailer. Then SLE 66R35E7(H) transmits a random number as a challenge to the reader (step 1).
- The reader calculates the response using the secret key and the challenge from SLE 66R35E7(H). The reader transmits its response together with its own challenge (random number) to SLE 66R35E7(H) (step 2).
- SLE 66R35E7(H) verifies the reader response. Then SLE 66R35E7(H) calculates the response to the challenge from the reader and returns it to the reader (step 3).
- The reader verifies the received response to its own challenge.

After the first random challenge (step 1) further data transmission is encrypted.

6.7 Memory access / operations

After a mutual authentication any of the following operations may be performed:

- READ block
- WRITE block
- DECREMENT: decrements the content of a Value block and stores the result in an internal data register
- INCREMENT: increments the content of a Value block and stores the result in an internal data register
- RESTORE: moves the content of a Value block into an internal data register
- TRANSFER: writes the content of the temporary internal data register to a block

7 Command set

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

Table 17 describes the ISO14443-3 Type A command set which is supported by SLE 66R35E7(H).

Table 17 ISO/IEC 14443-3 Type A command set

Command	Abbreviation	Command 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 (NVB) Cascade level 2 with the Number of Valid Bits (NVB)
Select	SELA	93_H 70_H, 95_H 70_H	Select the UID of Cascade level 1 Select the UID of Cascade level 2
HaltA	HLTA	50_H[1][2]	Sets a chip to a HALT state

For a detailed command description please refer to ISO/IEC 14443-3 Type A standard.

7.2 Memory access command set

There are two command types implemented:

- One step commands:
  - the PCD sends a command, the PICC sends a response
- Two step commands:
  - the PCD sends the first command, the PICC sends the first response
  - if the PCD does not detect an error the PCD sends the second command and the PICC responds with the answer to the second command

The command set of the SLE 66R35E7(H) is listed in Table 18.

Table 18 SLE 66R35E7(H) command set

Command	Abbreviation	Command Op-code	Description
Authenticate with Key A	AUTHA	60_H	Authentication with Key A to the sector in which the address block is located.
Authenticate with Key B	AUTHB	61_H	Authentication with Key B to the sector in which the address block is located.
READ	RD	30_H	Reads the data from an addressed block if access conditions permits access.
WRITE	WR	$A0_H$	Writes the data to an addressed block if access conditions permits the access.

[1] SLE 66R35E7(H) accepts also command op-code values $5x_H$.

[2] Within the parameter field of the HLTA command values from 00_H to $3F_H$ are accepted.

Command set

Command	Abbreviation	Command Op-code	Description
DECREMENT	DCR	$C0_H$	Decrement the addressed value by the received value and writes the result into the internal transfer buffer.
INCREMENT	INC	$C1_H$	Increment the addressed value by the received value and writes the result into the internal transfer buffer.
RESTORE	RSTR	$C2_H$	Loads the content of an addressed block into the transfer buffer. Only allowed if the addressed block in a value block format. Data is lost in case of power loss.
TRANSFER	TRFR	$B0_H$	Writes the content of the transfer buffer to the addressed block. The addressed block will be programed in value block format.
CONFIGURE_UID	CFG_UID	40_H	The CONFIGURE_UID command is used to set the desired UID functionality.

The data in the command are always sent LSByte first. Within a byte the LSBit is sent first

7.2.1 AUTHENTICATE (AUTHA and AUTHB)

AUTHA or AUTHB command performs the authentication using either Key A or Key B to a sector. The specified address indicates the block number. The valid address range is 00_H to $3F_H$. If any other address is specified the SLE 66R35E7(H) replies with an error message. This command shall be executed after the SLE 66R35E7(H) has been selected.

When the short-cut anticollision scheme is enabled (UIDF1 option) the behavior is different. Here SLE 66R35E7(H) accepts an AUTHENTICATE command already in READY2 / READY2* (after the selection of the cascade level 1). In this case a transition to PROTECTED state (AUTHx) is directly executed (see Figure 15).

The AUTHENTICATE command is performed as a three-pass authentication:

- Step 1:
  The PCD sends the AUTHA or AUTHB command to the PICC. The paramenter, a valid block address, indicates the sector for the authentication. The PICC decodes this command and replies with a challenge, TokenRB, which is a 32 bit random number[1)].
- Step 2:
  The PCD generates a 64 bit TokenAB. The PCD encrypts its own 32 bit random number RA as well as the value RB' which is a modified RB value and sends it to the PICC. The PICC receives and encrypts the received value. Finally the PICC compares the received RB' it to its own RB'.
- Step3:
  If the values are identical the PICC will repond the next challenge, TokenBA, which is encrypted value RB" confirming its authenticity. Otherwise an error (NR) will break the authentication. The PCD verifies the response and if no error is detected it allows further memory access i.e. both PCD and PICC are authenticated to each other.

Table 19 AUTHENTICATE command step 1

Command	Parameter	Integrity Mechanism
AUTHA or AUTHB	**Block address**	**CRC**
60_H or 61_H	00_H - $3F_H$	2 bytes CRC

Response
TokenRB
32 bit random number or NR

Command set

Table 20 AUTHENTICATE command step 2

Command	Parameter	Integrity Mechanism	Response
AUTHA or AUTHB	**Block address**	**CRC**	**TokenBA or NR**
-	64 bit Token	-	32 bit random number or NR

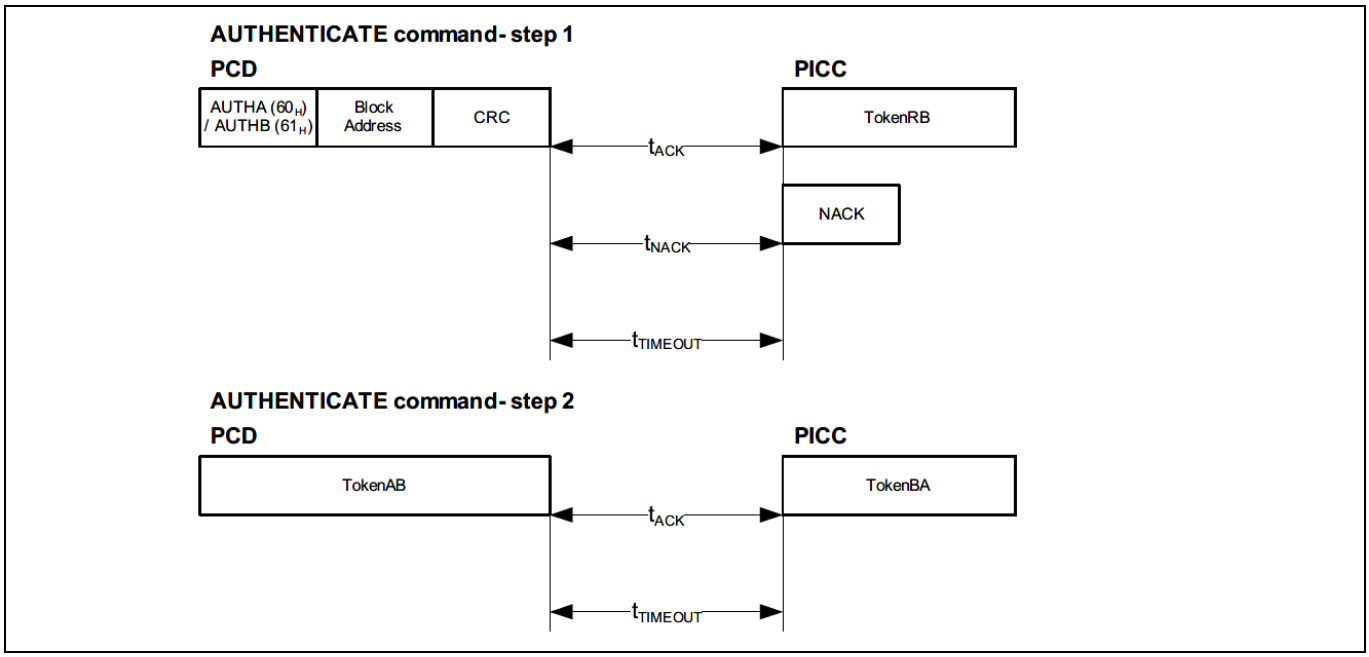

Figure 17 AUTHENTICATE command

Table 21 Timing AUTHENTICATE command

AUTHENTICATE	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
Command step 1	147.82 µs	t_{nonNVM}	86.11 µs	t_{nonNVM}	$t_{nonNVM} \leq 950$ µs
Command step 2	86.11 µs	t_{nonNVM}	86.11 µs	t_{nonNVM}	$t_{nonNVM} \leq 950$ µs

Command set

7.2.2 READ (RD)

The READ command reads 16 bytes from the specified block address in the memory:

- if the specified address is allocated in a previously authenticated sector
- if the access conditions for the adressed block allow read access

When the short-cut anticollision scheme is enabled the SLE 66R35E7(H) accepts a READ (Block 00_H) command in READY2 / READY2* (after the selection of the cascade level 1, no successful authentication required). In this case the SLE 66R35E7(H) performs a state transistion to ACTIVE / ACTIVE* state.

Table 22 READ command

Command	Parameter	Integrity Mechanism	Response
READ	**Block address**	**CRC**	**DATA + CRC**
30_H	00_H - $3F_H$	2 bytes CRC	16 bytes data + 2 bytes CRC or NACK or NR

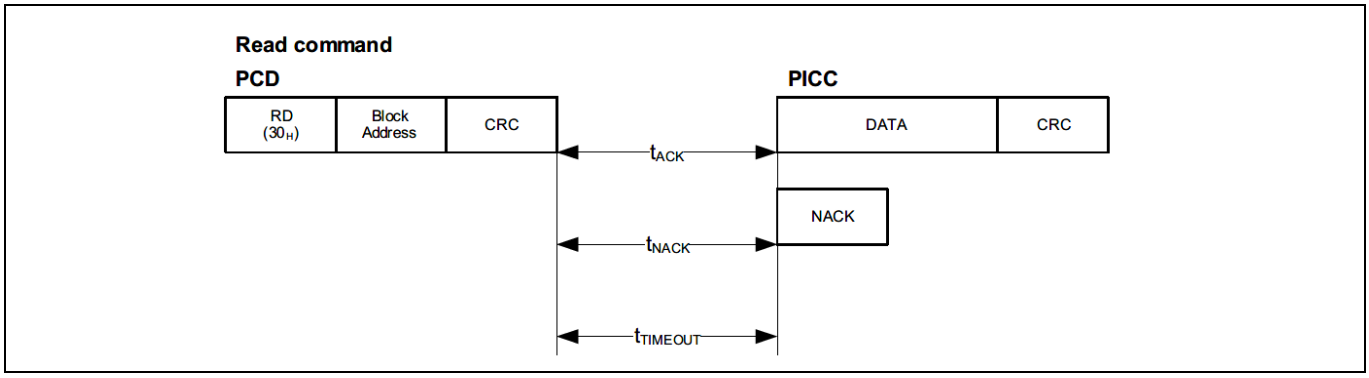

Figure 18 READ command

Table 23 Timing READ command

READ	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
	95.98 µs	t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$ µs

Command set

7.2.3 WRITE (WR)

The WRITE command writes 16 bytes to the specified address in the memory:

- if the specified address is allocated in a previously authenticated sector
- if the access conditions for the adressed block allow write access

Note: The Block 00_H is never writable independent on the access conditions.

Table 24 WRITE command step 1

Command	Parameter	Integrity Mechanism	Response
WRITE	**Block address**	**CRC**	
$A0_H$	00_H – $3F_H$	2 bytes CRC	ACK or NACK or NR

Table 25 WRITE command step 2

Command	Parameter	Integrity Mechanism	Response
WRITE	**DATA**	**CRC**	
-	16 bytes data	2 bytes CRC	ACK or NACK or NR

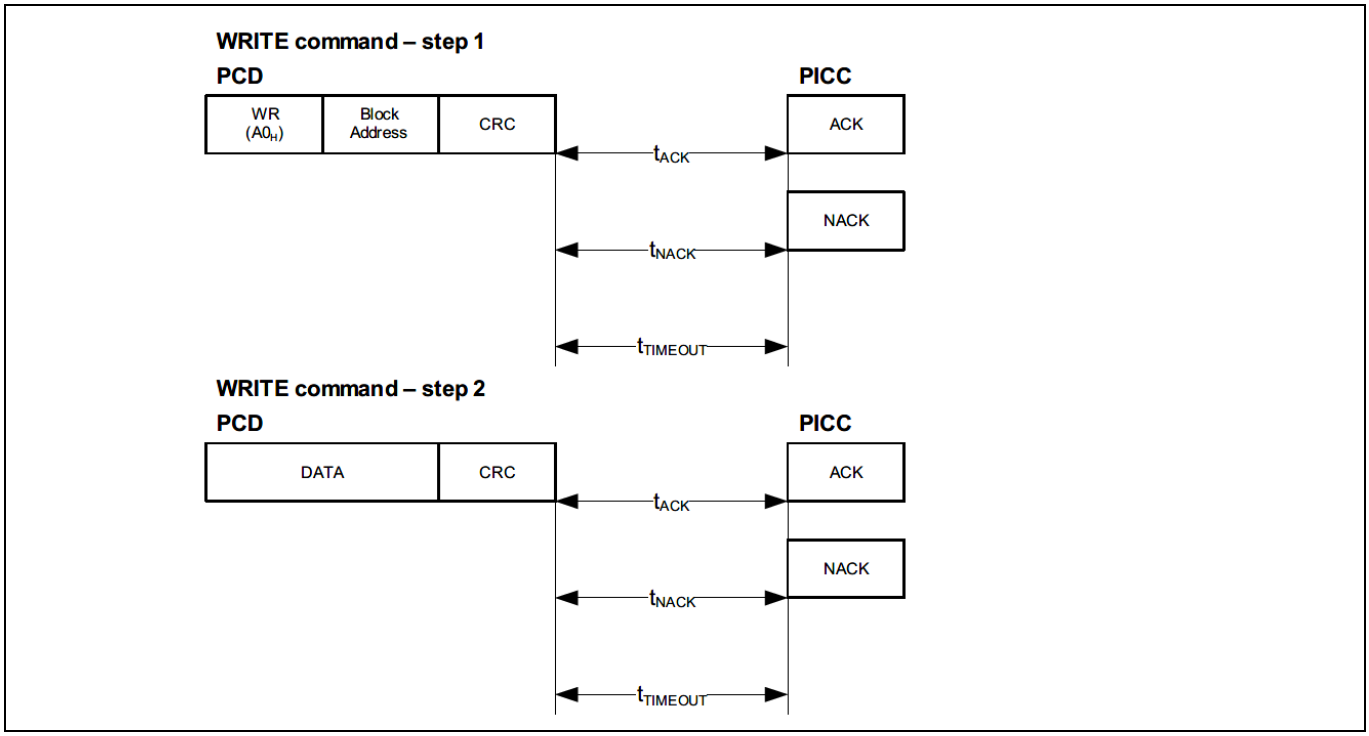

Figure 19 WRITE command

Table 26 Timing WRITE command

WRITE	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
Command step 1	86.38 µs	t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$ µs
Command step 2	3546.73 µs	t_{wrNVM}	86.11 µs	t_{wrNVM}	$t_{wrNVM} \leq 9500$ µs

7.2.4 DECREMENT (DCR)

The DECREMENT command reads out the content of the addressed value block (block address) and decrements it by the value given in the command data field. The conditions are the following:

- the specified block address is allocated in a previously authenticated sector
- the data at specified block address is stored in a value block format
- the access conditions for the adressed block allow decrement operation

The decremented data is stored internally and can be written to any authenticated data block using the TRANSFER command.

Table 27 DECREMENT command step 1

Command	Parameter	Integrity Mechanism	Response
DECREMENT	**Block address**	**CRC**	
$C0_H$	00_H - $3F_H$	2 bytes CRC	ACK or NACK or NR

Table 28 DECREMENT command step 2

Command	Parameter	Integrity Mechanism	Reponse
DECREMENT	**Value**	**CRC**	
-	4 byte counter value[1]	2 bytes CRC	Nack or NR[2]

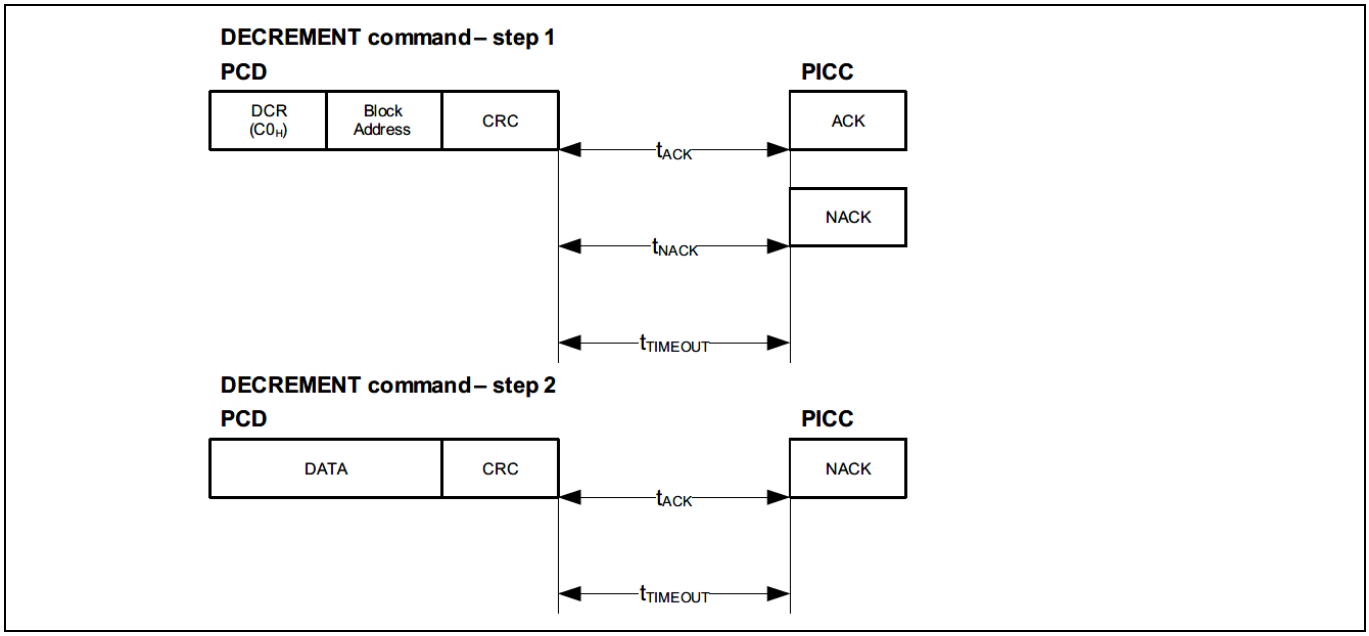

Figure 20 DECREMENT command

Table 29 Timing DECREMENT command

Decrement	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
Command step 1	256.53 µs	t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$ µs
Command step 2	-	t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$µs

[1] The value is a 4 byte signed integer value and should be bigger than zero and positive. Please note that the sign (most significant bit of the value) will be ignored e.g. a decrement by $7F_H\ FF_H\ FF_H\ FF_H$ or $FF_H\ FF_H\ FF_H\ FF_H$ returns the same result.

[2] In the case of successful decrement there is NR (no response).

7.2.5 INCREMENT (INC)

The INCREMENT command internally reads the value block out of the specified block address. The value is incremented by the given value in command data field under the following conditions:

- the specified block address is allocated in a previously authenticated sector
- the data at the specified block address are stored in a value block format
- the access conditions for the adressed block allow decrement access

The incremented data is stored internally and can be written to any authenticated data block using the TRANSFER command.

Table 30 INCREMENT command step 1

Command	Parameter	Integrity Mechanism	Response
INCREMENT	**Block address**	**CRC**	
$C1_H$	00_H - $3F_H$	2 bytes CRC	ACK or NACK or NR

Table 31 INCREMENT command step 2

Command	Parameter	Integrity Mechanism	Response
INCREMENT	**Value**	**CRC**	
-	4 byte counter value[1]	2 bytes CRC	NACK or NR[2]

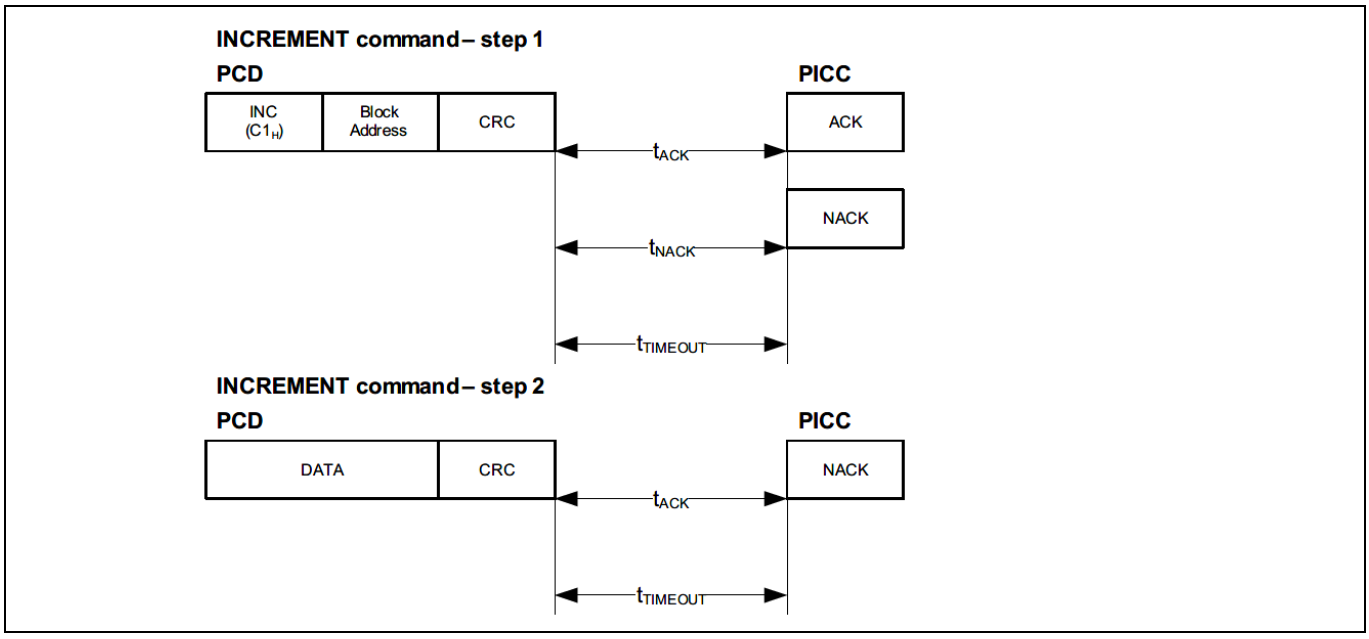

Figure 21 INCREMENT command

Table 32 Timing INCREMENT Command

Increment	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
Command step 1	256.53 µs	t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$ µs
Command step 2		t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$ µs

[1] The value is a 4 byte signed integer value and should be bigger than zero and positive. Please note that the sign (most significant bit of the value) will be ignored e.g. a decrement by $7F_H\ FF_H\ FF_H\ FF_H$ or $FF_H\ FF_H\ FF_H\ FF_H$ returns the same result.

[2] In the case of successful increment there is NR (no response)

Command set

7.2.6 RESTORE (RSTR)

The RESTORE command reads the value (4 byte) and the address (1 byte) data from the specified block address in the memory and stores it into the Transfer Buffer under the following conditions:

- the specified address is allocated in an authenticated sector

The restored data can be written to any authenticated block by the subsequent TRANSFER command.

Table 33 RESTORE command step 1

Command	Parameter	Integrity Mechanism	Response
RESTORE	**Block address**	**CRC**	
$C2_H$	00_H - $3F_H$	2 bytes CRC	ACK or NACK or NR

Table 34 RESTORE command step 2

Command	Parameter	Integrity Mechanism	Response
RESTORE	**DATA**	**CRC**	
-	4 byte data	2 bytes CRC	NACK or NR

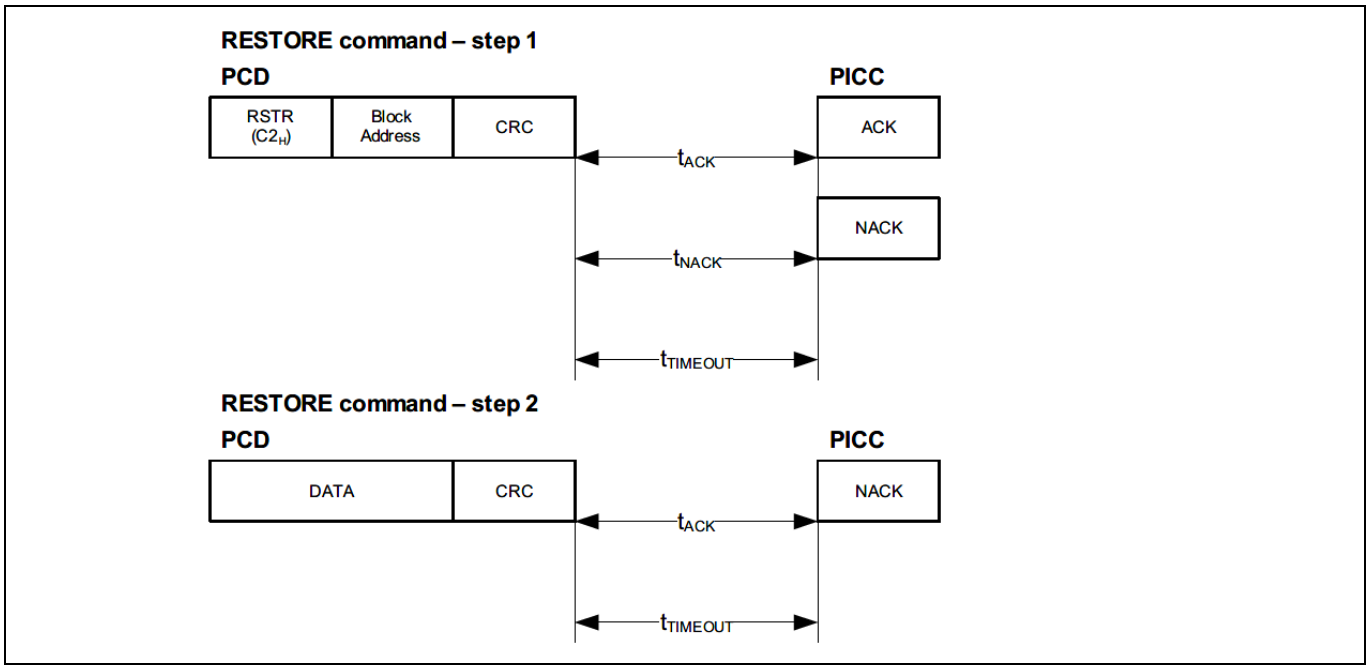

Figure 22 RESTORE command

Table 35 Timing RESTORE command

RESTORE	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
Command step 1	256.53 µs	t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$ µs
Command step 2		t_{rdNVM}	86.11 µs	t_{rdNVM}	$t_{rdNVM} \leq 4750$µs

Command set

7.2.7 TRANSFER (TRFR)

The TRANSFER command programs the data to the specified block address using the RESTORE, INCREMENT or DECREMENT command under the following conditions:

- the specified block address is allocated in a authenticated sector
- pre-condition is a properly executed INCREMENT, DECREMENT or RESTORE command

The TRANSFER command completes a preceeding INCREMENT or DECREMENT or RESTORE operation. It is possible to transfer value blocks between different sectors.

Note: Consecutive TRANSFER commands will cause a NACK response.

Table 36 TRANSFER command

Command	Parameter	Integrity Mechanism	Response
RESTORE	**Block address**	**CRC**	
$B0_H$	00_H - $3F_H$	2 bytes CRC	ACK or NACK or NR

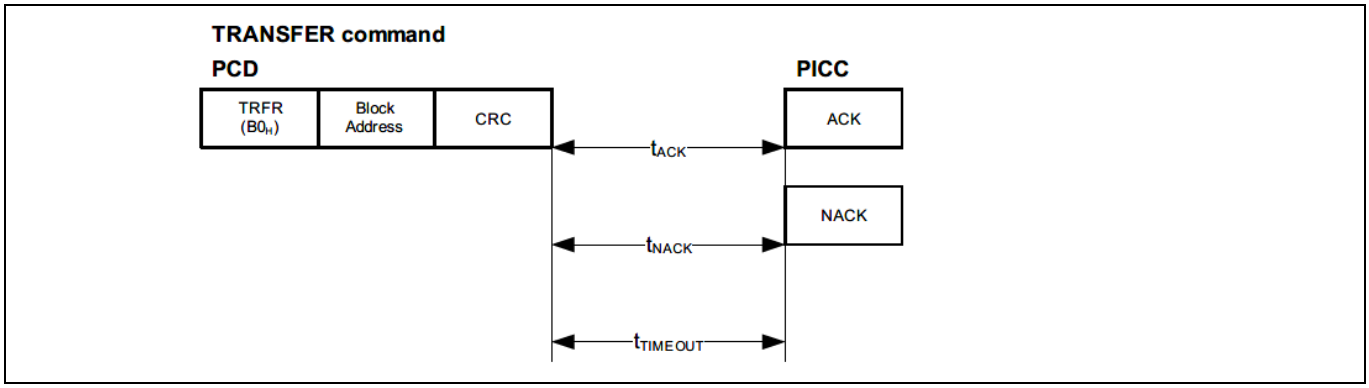

Figure 23 TRANSFER command

Table 37 Timing TRANSFER command

TRANSFER Command	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
	3546.73 µs	t_{wrNVM}	86.11 µs	t_{wrNVM}	$t_{wrNVM} \leq 9500$ µs

Command set

7.2.8 HLTA

The HLTA command sets the SLE 66R35E7(H) to the HALT state. The HALT State allows the user to separate already identified SLE 66R35E7(H) from each other.

Table 38 HLTA command

Command	Parameter	Integrity Mechanism
HLTA	**Block address**	**CRC**
50_H	00_H - $3F_H$	2 bytes CRC

Response
NACK or ACK

Note: The HLTA command will be sent plain in ACTIVE state and encrypted in PROTECTED state. If the command is not received properly the SLE 66R35E7(H) replies a NACK.

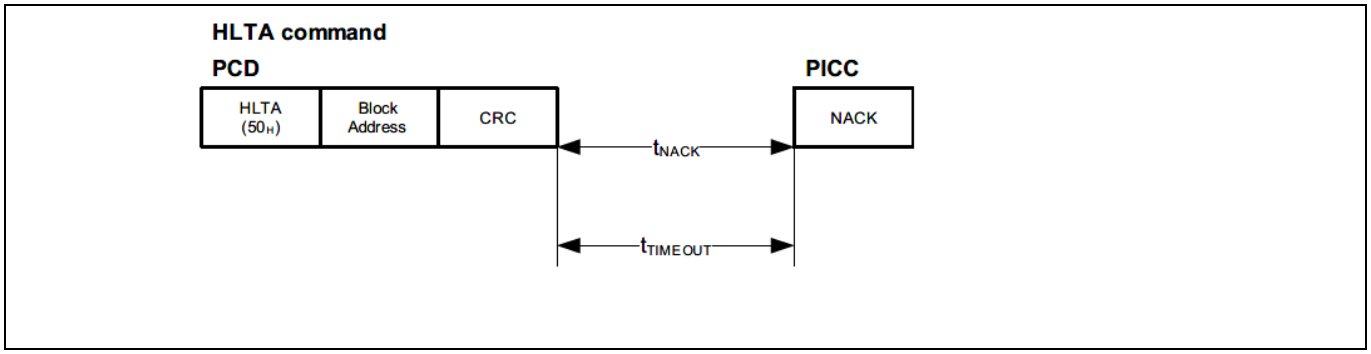

Figure 24 HLTA command

Table 39 Timing HLTA command

HLTA Command	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
			86.11 µs	t_{nonNVM}	$t_{nonNVM} \leq 950$ µs

Command set

7.2.9 CONFIGURE_UID

The CONFIGURE_UID command is used to set the desired UID functionality of the SLE 66R35E7(H). The command can be executed only after a successful authentication to Sector 00_H.

It is strongly recommended to execute the CONFIGURE_UID command in a secured and stable environment. Once this command carried out successfully the chosen UID functionality is locked and not changeable anymore. Any subsequent CONFIGURE_UID command will cause NACK response.

The new configuration is active after a POWER_ON reset only!

Table 40 CONFIGURE_UID command

Command	Parameter	Integrity Mechanism	Response
CFG_UID	**UID Option**	**CRC**	
40_H	see Table 41	2 bytes CRC	ACK or NACK or NR

Table 41 UID options

UID Option	Code	Anticollision and selection
UIDF0	00_H	7-byte UID only (delivery default)
UIDF1	40_H	7-byte UID with short-cut anticollision enabled
UIDF2	20_H	4-byte random ID (RND-ID) uid0 = 08_H (accord. to ISO/IEC 14443-3)
UIDF3	60_H	4-byte fixed number, non-unique ID (FNUID) uid0 = xF_H (accord. to ISO/IEC 14443-3)
All others		RFU

Note: The CONFIGURE_UID command must be executed in the personalization process. This is mandatory to lock the UID option settings (even if the default configuration is chosen).

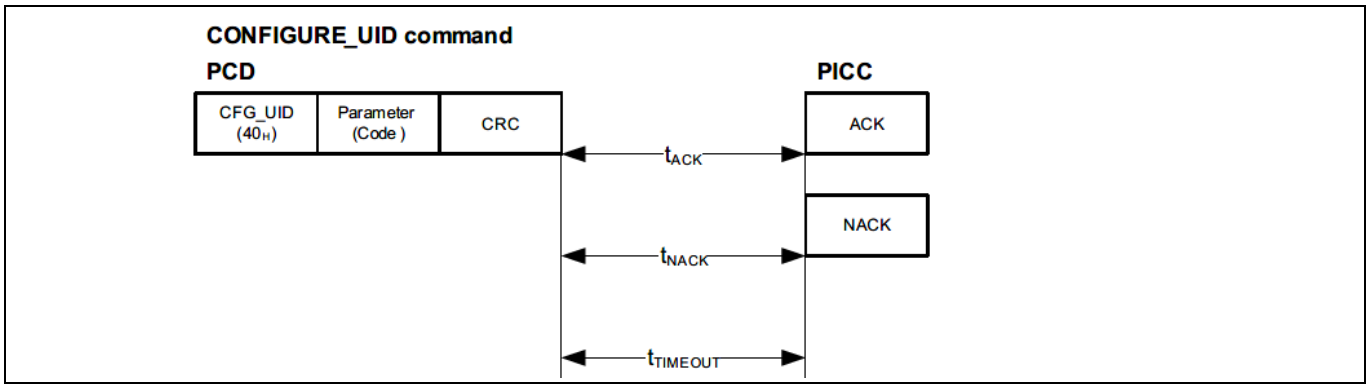

Figure 25 CONFIGURE_UID command

Table 42 Timing CONFIGURE_UID command

CONFIGURE_UID	$t_{ACK\ min}$	$t_{ACK\ max}$	$t_{NACK\ min}$	$t_{NACK\ max}$	$t_{TIMEOUT}$
	3600.00 µs	t_{wrNVM}	86.11 µs	t_{wrNVM}	$t_{wrNVM} \leq 9500$ µs

8 Performance and Operational Characteristics

The electrical characteristics ensure the operation of the SLE 66R35E7(H) over the listed range.

Typical characteristics specify mean values expected over the production spread. If not otherwise specified typical characteristics apply at $T_{ambient}$ = 25° C and the given supply voltage.

8.1 Electrical Characteristics

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

Table 43 Electrical Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Chip input capacitance L_A – L_B	C_{IN}	17.3	18.3	19.3	pF	$V_{AB\ RMS}$ = 2.0 V, f_{CAR} = 13.56 MHz, $T_{ambient}$ = 25 °C Tolerance +/- 5%
Chip load resistance L_A – L_B	R_{IN}		4.5		kΩ	$V_{AB\ RMS}$ = 2.0 V, f_{CAR} = 13.56 MHz, $T_{ambient}$ = 25 °C
Endurance (erase / write cycles)[1]		10^5				–
Data retention[1]		10			years	
EEPROM Erase and Write time	t_{prog}			3.8	ms	Combined erase + write; excluding time for command / response transfer between interrogator and chip, $T_{ambient}$ = 25 °C
ESD Protection voltage (L_A, L_B pins)	V_{ESD}	2			kV	JEDEC STD EIA / JESD22 A114-B
Ambient temperature	$T_{ambient}$	-25		+70	°C	for chip
Junction temperature	$T_{junction}$	-25		+110	°C	for chip

[1] Values are temperature dependent.

8.2 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. 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.

Table 44 Absolute Maximum Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Input peak voltage between $L_A - L_B$	V_{INpeak}			6	V_{peak}	
Input current through $L_A - L_B$	I_{IN}			50	mA	
Storage temperature	$T_{storage}$	-40		+125	°C	

References

[1] ISO/IEC 14443 Identification cards – Contactless integrated circuit(s) cards Proximity cards, Parts 1, 2 and 3

[2] ISO/IEC 10373-6 Identification cards – Test methods – Proximity cards

[3] ISO/IEC 7816-6 Identification cards – Integrated circuit cards Interindustry data elements for interchange

Revision history

Reference	Description
Revision 3.0, 2021-05-28	
all	Document classification changed Editorial changes
Revision 2.0, 2020-08-19	
all	New document template Editorial changes Adding description for SLE 66R35E7H product version.
Ordering and packaging information	Delivery form MCC2-2-1 removed
Revision 1.1, 2017-05-12	
all	Major review
Revision 1.0, 2017-03-28	
all	Initial version

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

Edition 2021-05-28

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
csscustomerservice@infineon.com

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.

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

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.