



DATASHEET

43NT

NFC Type-2 Tag IC with 144-byte user memory and a configurable pin for RF field indication or tamper evidence detection

Rev 0.2

Features Summary

Highlight Features

- NFC forum type 2 tag
- A configurable pin for three modes:
 - RF field detection
 - Tamper evidence detection
 - Sleep mode
- Dynamic NDEF message
 - contains tamper evidence and rolling code
 - mirrored into original NDEF message
 - can be triggered by tamper status of the tag
- Password protection
- Tag authenticity verification using rolling code (optional)

Interfaces and Peripherals

- RF interface based on ISO14443A, 106 kbps data rate
- True anti-collision
- Configurable output style for RF detector mode
 - Push-Pull Mode
 - Open-Drain Mode
- On-chip capacitance 50 pF

Memory

- 7-byte UID
- Lock byte with anti-tearing protection
- 1 page for OTP memory
- 144-byte user memory
- 8 dedicated pages for configuration functions: Password authentication; Pin configuration; and Rolling code configuration
- EEPROM organization enabling NDEF format and TLV1
- EEPROM erase/write cycle up to 100,000 times
- EEPROM memory retention up to 10 years at 70°C

Operating Conditions

- 13.56MHz operating radio frequency
- Operating temperature from -40 to 85°C

Package

- DOW (Die-on-Wafers)
- DOW with Au-Bump
- Custom packages

Supplementary

- Wafer map - XML, TXT, SECSII
- UID summary

Applications

- NFC-wakeup devices and appliances
- Bluetooth pairing
- WiFi connection
- Smart posters
- Toys
- Anti-tampering sticker and label
- Secure packaging seal
- Product authenticity verification

Revision History

Revision	Date	Description	Change/Updated/Comment
0.1	31 Oct 2016	1 st Release	Electrical characteristic is based on simulation. The information will be updated after silicon characterization.
0.2	8 Dec 2016	Content update	<ol style="list-style-type: none">1. Update Section 1.22. Remove DFN package from Section 2 and 93. Update Table 5-14. Update example in Table 7-2 and 7-35. Update Section 8.1.1. (Add ATQA data)6. Update Section 8.2.1.

Ordering Information

TBD

Content

0. Notation.....	11
0.1 Styles and Fonts for keywords.....	11
0.2 Abbreviation.....	12
1. Functional Overview	13
1.1 Block diagram.....	13
1.1.1 RF Analog-Front-End (RF-AFE).....	13
1.1.2 Digital controller.....	13
1.1.3 EEPROM.....	14
1.1.4 RFD pin control	14
1.2 Typical operating system	14
2. Pin configuration	15
2.1 Pin configuration	15
2.1.1 Die Pad.....	15
3. Specifications.....	16
3.1 Absolute maximum rating.....	16
3.2 Electrical characteristic	16
4. Communication.....	18
4.1 RF interface	18
4.1.1 Downlink.....	18
4.1.2 Uplink.....	19
4.1.3 Frame pattern.....	20
4.1.4 Timing.....	21
4.1.5 State of operation.....	22
5. Memory Configuration	23
5.1 EEPROM Organization	23
5.2 UID	23
5.1 OTP.....	24
5.2 User memory	24
5.3 Dynamic lock byte.....	25
5.3.1 Lock_Key.....	25
5.3.2 Lock_IniV	25
5.4 User Configuration.....	26
5.4.1 User Configuration 0.....	26
5.4.2 User Configuration 1.....	27
5.4.3 Password (PWD) and Password Acknowledge (PACK)	30
5.4.4 KEY and Initial Vector (IV) of Rolling Code function	30
6. Rolling Code Generation	31
6.1 Time Stamp.....	31
6.2 Rolling Code	31

7. Dynamic NDEF Message32

7.1 Dynamic NDEF Data Format 32

7.2 Dynamic NDEF Data Configuration Bits..... 32

7.3 UID+RLC dynamic NDEF example 33

8. Commands35

8.1 Basic RFID commands 35

8.1.1 REQA..... 35

8.1.2 WUPA..... 35

8.1.3 ANTI-COLLISION 36

8.1.4 SELECT 37

8.1.5 HLTA..... 37

8.2 Data accessing commands 38

8.2.1 ReadE2..... 38

8.2.2 WriteE2..... 38

8.2.3 Compatible WriteE2..... 39

8.2.4 PWD_AUTH..... 40

8.2.5 Read_Tamper..... 41

8.3 Response Acknowledge 42

9. Packaging and Dimension.....43

10. Disclaimer.....44

List of Figures

Figure 1-1: Functional block diagram.....	13
Figure 1-2: SIC43NT with RF detect pin operating in an open-drain mode	14
Figure 1-3: SIC43NT with RF detect pin operating in a 1.8V output mode	14
Figure 1-4: SIC43NT operates in tamper evident detection mode	14
Figure 2-1: SIC43NT Die (Top View)	15
Figure 4-1: Example of downlink telegram.....	18
Figure 4-2: Example of uplink telegram.....	19
Figure 4-3: Frame format for RF communication	20
Figure 4-4: Downlink frame delay time	21
Figure 4-5: Uplink frame delay time	21
Figure 4-6: State of operation	22
Figure 5-1: SIC43NT EEPROM memory map.....	23
Figure 5-2: Lock configuration in static memory.....	24
Figure 5-3: OTP behavior in Page 3	24
Figure 5-4: NDEF value in page 0x03 to 0x05 for NFC tag.....	24
Figure 5-5: Memory content in page 0x03 to 0x05 (Lock bit Style 1)	24
Figure 5-6: Memory content in page 0x03 to 0x05 for 144 bytes (Lock bit Style 2)	25
Figure 5-7: Lock configuration of dynamic memory for 144-byte user memory configuration (Lock bit Style 1)	25
Figure 5-8: Lock configuration of dynamic memory for 144-byte user memory configuration (Lock bit Style 2)	25
Figure 5-9: Configuration 0.....	26
Figure 5-10: Field Detect Pin (FDP) configuration	26
Figure 5-11: Configuration 1.....	27
Figure 5-12: Protection configuration.....	28
Figure 5-13: RFDCFG byte configuration.....	29
Figure 5-14: DYN_DATA_CFG byte configuration	30
Figure 6-1: Rolling Code Generation Block Diagram.....	31
Figure 7-1 Dynamic NDEF Message Format.....	32
Figure 8-1: REQA command frame with a response.....	35
Figure 8-2: WUPA command frame with a response	35
Figure 8-3 : ANTI-COLLISION in the cascade level 1 with a response.....	36
Figure 8-4 : ANTI-COLLISION in the cascade level 2 with a response.....	36
Figure 8-5: SELECT level1 command frame with a response	37
Figure 8-6: SELECT level2 command frame with a response	37
Figure 8-7: HALT command frame	38
Figure 8-8: ReadE2 command frame with response.....	38
Figure 8-9: ReadE2 command frame with a negative acknowledgement in response.....	38
Figure 8-10: WriteE2 command frame with an ACK response indicating successful operation.....	39
Figure 8-11: WriteE2 command frame with a NAK response indicating unsuccessful operation	39
Figure 8-12: Two-step operation of Compatible Write E2 with an ACK response	39
Figure 8-13: One-step operation of Compatible Write E2 with a NAK response.....	40
Figure 8-14: Two-step operation of Compatible Write E2 with a NAK response.....	40
Figure 8-15: Successful authentication with matched password	40
Figure 8-16: Fail authentication due to incorrect password	40
Figure 8-17: Fail authentication when authentication counter overflows	41
Figure 8-18: Successful Read_Tamper response.....	41

Figure 8-19: Fail **Read_Tamper** response due to framing error..... 41

Figure 9-1: Die and Wafer Dimension..... 43

List of Tables

Table 0-1: Styles and Fonts for key words	11
Table 0-2: Abbreviation	12
Table 2-1: SIC43NT Pad descriptions	15
Table 3-1: Absolute maximum rating	16
Table 3-2: Operating condition.....	16
Table 3-3: RF front end characteristic.....	16
Table 3-4: Pin characteristics.....	16
Table 3-5: Operation timing.....	17
Table 3-6: EEPROM.....	17
Table 4-1: Sequences for the downlink bit-pattern	18
Table 4-2: Information to code with the downlink sequences.....	18
Table 4-3: Sequences for the uplink bit pattern.....	19
Table 4-4: Uplink data coding	19
Table 4-5: Information to code with the uplink sequences.....	21
Table 5-1: Effect of configuration on Pin RFD	29
Table 6-1: Time Stamp Update Condition.....	31
Table 7-1: NDEF Message Data Field.....	32
Table 8-1: REQA command format.....	35
Table 8-2: WUPA command format	35
Table 8-3: ANTI-COLLISION command format	36
Table 8-4: SELECT command format.....	37
Table 8-5: HLTA command format	37
Table 8-6: ReadE2 command format.....	38
Table 8-7: WriteE2 command format	39
Table 8-8: Compatible WriteE2 command format.....	39
Table 8-9: PWD_AUTH command format.....	40
Table 8-10: Read_Tamper command format.....	41
Table 8-11: 4-bits ACK/NAK.....	42

0. Notation

0.1 Styles and Fonts for keywords

This part defines styles and fonts used for the keywords throughout this document. The keywords are names of signals, registers, pins, states of operations and commands. The styles, fonts, and their indications are shown in Table 0-1.

Table 0-1: Styles and Fonts for key words

Symbol	Indication
<i>Signal</i>	Signal name
Register, Flag	Register name, or Bit name or acknowledge flag
pin <i>RX</i>	Pin name
<i>"State of Operation"</i>	State of operation
<i>Command</i>	Command name for RF interface

- To refer to a register address and a value in a register, a hexadecimal number proceeding with letter "0x" is used. For example, 0x0A.
- To refer to a bit located in a register address, a symbol "." following by a number reflecting the bit location starting from 0 to 7 is used. For example, 0x0A.0 refers to bit 0, least significant bit, in the register 0x0A.
- To refer to a set of consecutive bits located in a register address, a format ".[msb:lsb]" is used after a register value. For example, a value of 0x0A. [3:0] refers to bit 3, 2, 1, and 0 in the register 0x0A.
- To refer to a binary value in some registers, the letter "b" is placed at the end of the binary number, for example "1010b".
- To refer to logic level, the number in single quote '1' and '0' are used to refer to binary logic level.

0.2 Abbreviation

Table 0-2: Abbreviation

Abbreviation	Term
ACK	Positive Acknowledge
AFE	Analog-Front-End
CC	Capability Container in NDEF Format
CRC	Cyclic redundancy check
CT	Cascade tag
EEPROM	Electrically Erasable Programmable Read-Only Memory
EOF	End of Frame
fc	Carrier frequency
FDT	Frame Delay time
NAK	Negative Acknowledge
NDEF	NFC data Exchange format
NFC	Near Field Communication
OTP	One-time program
PACK	Password acknowledge
PWD	Password
RFD	RF detect
SAK	Select Acknowledge
SOF	Start of Frame
UID	Unique Identifier (Unique ID)
TS	Tamper Status
RLC	Rolling Code
IV	Initialization Vector

1. Functional Overview

The SIC43NT is a NFC Forum Type 2 Tag IC with an RF detection pin **RFD**. The RF detection pin is designed to wake up the MCU system from sleep state for applications such as pairing Bluetooth devices, setting WIFI, or wireless authentication. The EEPROM memory can store necessary pairing information for electronic devices and embedded systems. The RF detection pin can be set to: (1) 1.8V output voltage mode, in which the **RFD** pin connected directly to the I/O; or (2) open-drain mode, in which the logic can be translated to MCU VDD level.

Moreover, the **RFD** pin can be configured to operate in tamper evidence detection mode where a tear-able conductor normally connects between the RF detection pin and the tag's ground pin. This mode is designed for anti-tampering applications. A RFID/NFC device can monitor the status of the pin via special commands to check whether the conductor has been cut or still be in a safety state.

The SIC43NT NDEF response can be configured to include Dynamic NDEF data, which contains tamper status of the tag and a rolling code. These two data will be mirrored into the NDEF message at the position corresponding to the dynamic data pointer set by users.

The tamper status indicates whether the tag's **RFD** pin (in tamper evidence detector mode) has been disconnected or not. The rolling code is a one-time generated data that can be used to check authenticity of the tag. It is generated by a secure cipher module with an 80-bit key.

In addition, the tag can be configured to mirror these dynamic data in NDEF message only when a certain condition is met: either mirror data only when the tag is not tampered, or mirror only after the tag has been tampered.

1.1 Block diagram

Figure 1-1 depicts a conceptual block diagram of SIC43NT, mainly consists of four parts as listed below:

- RF Analog Front End (RF-AFE);
- Digital controller;
- EEPROM; and
- RFD control.

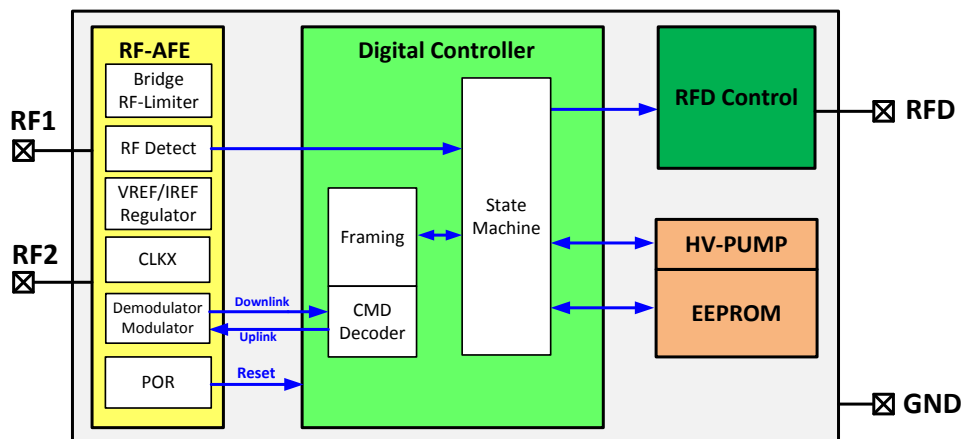


Figure 1-1: Functional block diagram

1.1.1 RF Analog-Front-End (RF-AFE)

The RF Analog-Front-End (RF-AFE), which has the RF1 and RF2 terminals for connecting to an external coil, harvests RF power to supply the internal circuit. The RF-AFE provides facilities for RF communication such as a Modulator for uplink data communication, a Demodulator for downlink data communication, a clock extractor for system clock and data synchronization, and a RF field detector for detecting the presence of RF field.

1.1.2 Digital controller

The digital controller controls data transaction between the RF-AFE and the EEPROM. The digital controller handles operations as follows:

- Decoding incoming RF downlink commands and encoding RF uplink data/response;
- Reading and programing data from/to the EEPROM;

- Presenting RF Detection state to pin **RFD** ;
- Detecting logic present at pin **RFD** in case of tampering mode and store it into EEPROM
- Detecting logic present at pin **RFD** in case of sleep mode.

1.1.3 **EEPROM**

The EEPROM consists of memory blocks and a high-volt generator. The EEPROM memory is used to store an UID, user data, and a memory lock control bit to serve NFC applications. The EEPROM also contains device configuration bits, configuration data for rolling code generator, and tamper evidence of the tag.

1.1.4 **RFD pin control**

The RFD pin control block handles RF detection, sensing sleep control, and detecting tamper evidence. Depending on the configuration bits, pin **RFD** can be either an input or an output. For RF detection, a pin **RFD** is in output mode. For tamper evident detection, a pin **RFD** is in input mode. SIC43NT can be forced into a sleep mode by tying the pin **RFD** to logic '0' before presence of RF field. The Pin functionality and I/O type can be set via device configuration page.

1.2 **Typical operating system**

SIC43NT can be configured in various arrangements as illustrated in Figure 1-2 to Figure 1-4. A loop antenna is directly connected between pin **RF1** and **RF2** for RFID/NFC communication, whereas pin **RFD** can connect to:

- a microcontroller for indicating presence of RF field when I/O is set in an open drain mode;
- a microcontroller for indicating presence of RF field when I/O is set in a 1.8V mode; and
- tear-able conducting material for tamper evident detection.

If neither field detection nor tamper detection feature is required, **RFD** pin can be left unconnected.

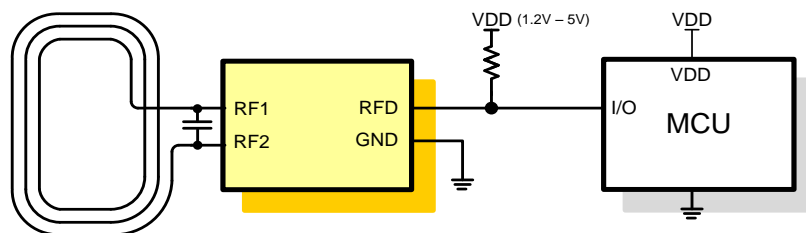


Figure 1-2: SIC43NT with RF detect pin operating in an open-drain mode

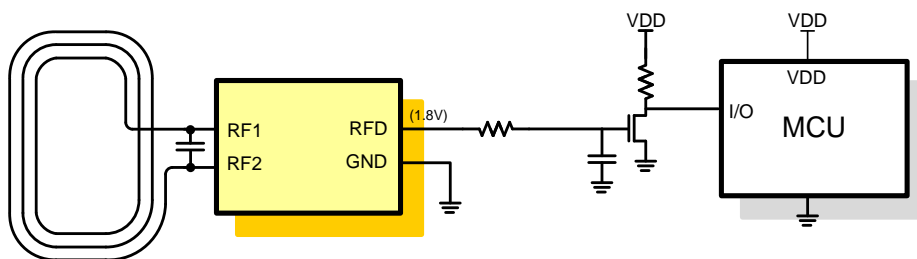


Figure 1-3: SIC43NT with RF detect pin operating in a 1.8V output mode

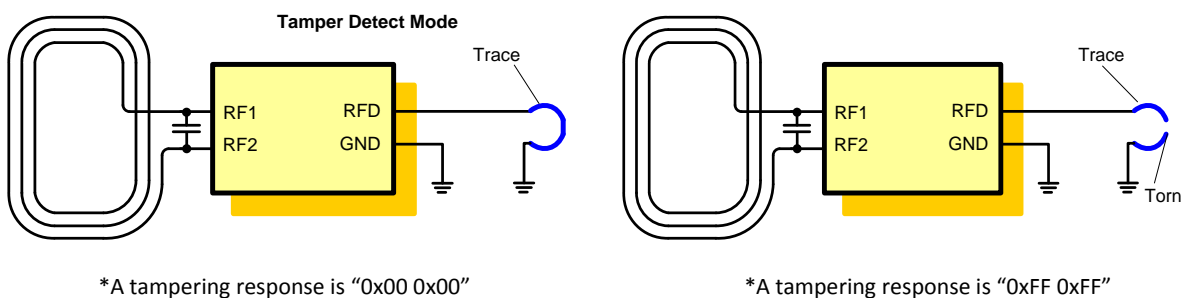


Figure 1-4: SIC43NT operates in tamper evident detection mode

2. Pin configuration

2.1 Pin configuration

2.1.1 Die Pad

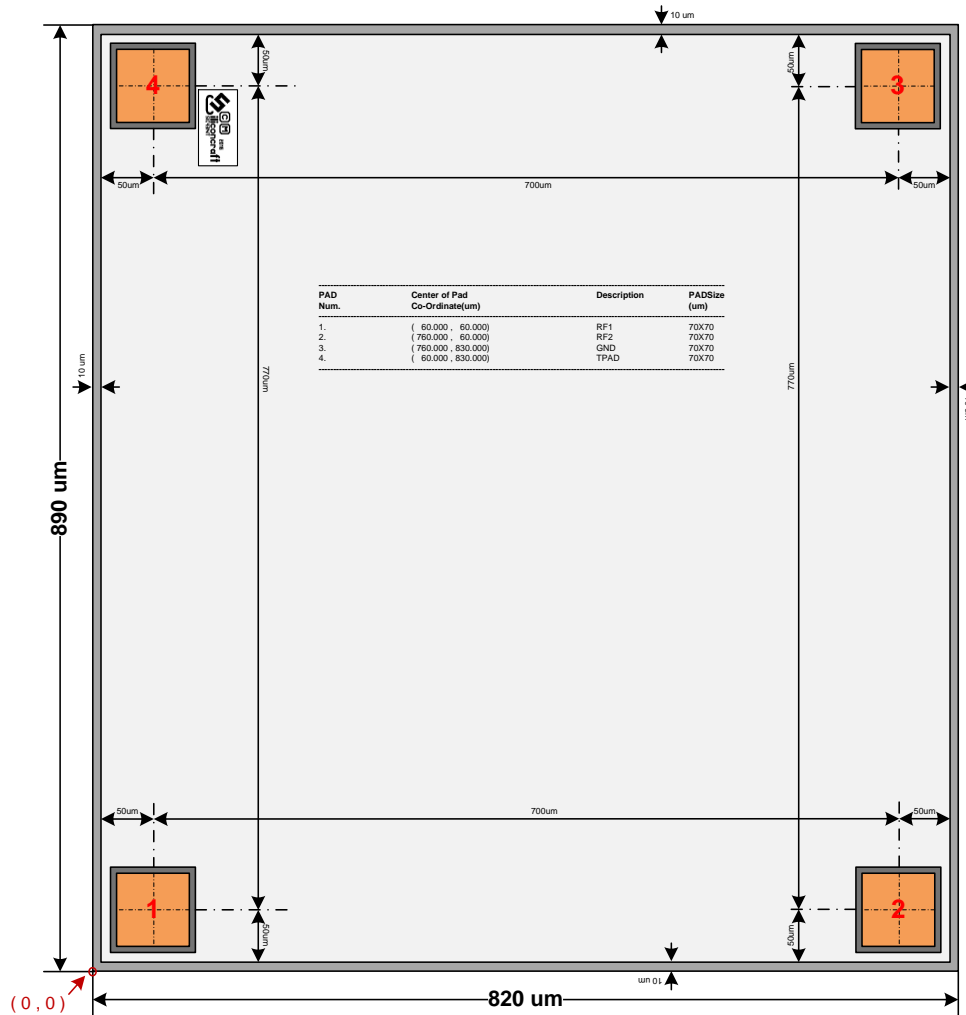


Figure 2-1: SIC43NT Die (Top View)

Table 2-1: SIC43NT Pad descriptions

Pad	Symbol	Type	Center of Pad Co-ordinate	Pad Size(μm)	Description
1	RF1	RF	(60,60)	70x70	RF pin 1 for coil connection
2	RF2	RF	(760,60)	70x70	RF pin 2 for coil connection
3	GND	Power	(760,830)	70x70	Ground
4	RFD	I/O	(60,830)	70x70	RFD pin

3. Specifications

3.1 Absolute maximum rating

Stresses above those listed under absolute maximum ratings may cause permanent damage to the device. Exposure to the absolute maximum rating conditions for an extended period of time may affect the device reliability.

Only one absolute maximum rating can be applied at a time.

Table 3-1: Absolute maximum rating

Parameter	Rating
Voltage on pin RFD	-0.3 V to 5.5 V
RF input current	40mA
Operating temperature range	-40 C to +85 C
Storage temperature range	-40 C to +125 C

3.2 Electrical characteristic

Table 3-2: Operating condition

Parameter	Description	Min	Typ	Max	Unit	Conditions
ESD	Electrostatic discharge tolerance		2		kV	HBM model

Table 3-3: RF front end characteristic

Parameter	Description	Min	Typ	Max	Unit	Conditions
f-op	RF operating frequency		13.56		MHz	
Vcoil-pp	POR threshold			6	Vpk-pk	
	EEPROM programming	6			Vpk-pk	
VRFlimit	RF Limiter Level @ 1mA input		12.5		Vpk-pk	Temp = 25C
	RF Limiter Level @ 10mA input		13.5		Vpk-pk	
Vmod	Modulation Level @ 1mA input		1		Vpk-pk	
	Modulation Level @ 10mA input		2		Vpk-pk	
Irf, max, op	Maximum operating current	10			mA	
Cr	On-chip resonance capacitor	45	50	55	pF	
Yin, RF	Effective input impedance at RF		20		u.mho	2.2 Vrms at RF1/ RF2 RFID read mode, 13.56 MHz, (Guarantee by Design)
TRF_off	Minimum period for RF field-off to ensure reset	10			uS	

Table 3-4: Pin characteristics

Parameter	Description	Min	Typ	Max	Unit	Conditions
C_RFD	GPIO pin capacitance		1.1		pF	
VIL,RFD	Digital logic input Low voltage on FD pin for Sleep mode/Tampering detection mode	-0.3		0.7	V	
VIH,RFD	Digital logic input High voltage on FD pin for Sleep mode/Tampering detection mode	1.2		5	V	
VOL,RFD	Digital logic output low voltage			0.05	V	I Load = 50uA
			0.1	0.5	V	I Load = 4 mA
			0.25	1.2		I Load = 8 mA
VOH,RFD	Digital logic output high voltage for push-pull mode	1.2	1.8	2.1	V	I Load,source = 20uA
Iinlogic1	Logic 1 input current			1	uA	VINH = 5.5V
Iinlogic0	Logic 0 input current			1	uA	VINL = 0
VRFD	Voltage on pin RFD	-0.5		5.5	V	
Zpd-tam	Pull down impedance in tampering detection mode which indicate untempering state			TBD	ohm	

Table 3-5: Operation timing

Parameter	Description	Min	Typ	Max	Unit	Conditions
Tpowerup	Startup time from power up		1000		uS	After burst RF field until chip ready to receive command.
TRFD, RfOff	Field Detection indication reset after RF field absent. (RF field detect pin is set to open drain)	5		10	uS	Logic of pin RFD go to high after RF field immediately absent

Table 3-6: EEPROM

Parameter	Description	Min	Typ	Max	Unit	Conditions
TEEprog	EEPROM programming time		8		mS	From EOF downlink to SOF uplink
RFMINProg	Minimum RF voltage for programming voltage		6		Vpk-pk	
Endurance	Write endurance	100,000			Times	
Retention	Data Retention		10		Years	

4. Communication

The RF communication is based on ISO14443A. This section describes the RF interface behaviour.

4.1 RF interface

The RF interface of SIC43NT is based on the standard for contactless smart cards ISO14443A-2. According to ISO standard, PCD and PICC are referred throughout the document as NFC/RFID device and SIC43NT/tag/transponder/chip, respectively.

SIC43NT activates itself by energizing RF field generated by its companion NFC/RF device. When the transponder is powered up and internal supply voltage is higher than the POR threshold, the chip initiates itself and waits silently for an operational command and then starts transmitting in uplink as a response.

4.1.1 Downlink

In downlink, the RF device starts sending a command to the transponder by interrupting the field. The downlink communication takes place using 100% ASK modulation with the Miller coding. The transmission bit-rate is 106 kbps ($f_c/128$). Figure 4-1 depicts an example of downlink telegram.

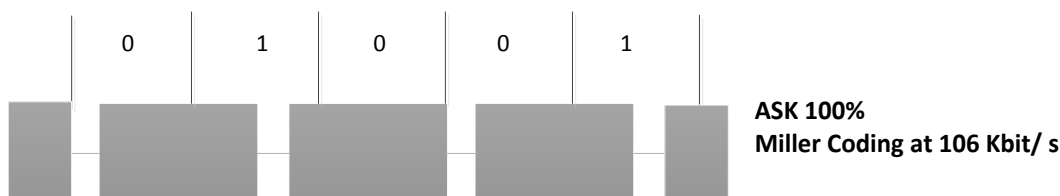


Figure 4-1: Example of downlink telegram

4.1.1.1 Downlink bit pattern

Downlink bit pattern is based on the ISO 14443 type-A protocol as defined in Table 4-1 and Table 4-2.

Table 4-1: Sequences for the downlink bit-pattern

Sequence X	After a time of $64/f_c$ a “pause” shall occur
Sequence Y	For the full bit duration ($128/f_c$) no modulation shall occur
Sequence Z	At the beginning of the bit duration a “pause” shall occur

Table 4-2: Information to code with the downlink sequences

Logic ‘1’	Sequence X
Logic ‘0’	Sequence Y with the following two exceptions: If there are two or more contiguous ‘0’s, sequence Z shall be used from the second ‘0’ on If the first bit after a “start of frame” is ‘0’, sequence Z shall be used to represent this and any ‘0’s which follow directly thereafter
Start of communication	Sequence Z
End of communication	Logic ‘0’ followed by Sequence Y
No information	At least two Sequence Y

4.1.2 Uplink

After SIC43NT executes a command from NFC device and starts transmission in uplink as a response, SIC43NT communicates with an NFC/RFID device by load modulation through inductive coupling field. The uplink bit pattern is defined based on ISO14443 type A. The uplink bit definition is described in Table 4-3 and Table 4-4. The uplink data is encoded in Manchester format with subcarrier frequency of 847 KHz ($f_c/16$). One-bit duration is 8 periods of the subcarrier, equivalent to bit-rate of 106 kbps ($f_c/128$). Figure 4-2 depicts an example of data encoding in uplink telegram.

Table 4-3: Sequences for the uplink bit pattern

Sequence D	The carrier shall be modulated with the subcarrier for the first half (50%) of the bit duration
Sequence E	The carrier shall be modulated with the subcarrier for the second half (50%) of the bit duration
Sequence F	The carrier is not modulated with the subcarrier for one-bit duration

Table 4-4: Uplink data coding

Logical '1'	Sequence D
Logical '0'	Sequence E
Start of communication	Sequence D
End of communication	Sequence F
No information	No subcarrier

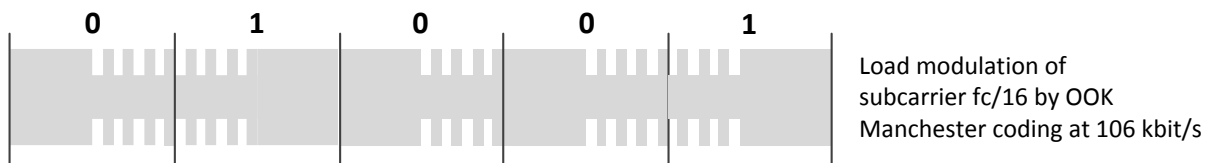


Figure 4-2: Example of uplink telegram

4.1.3 Frame pattern

The frame pattern for RF communication is based on the ISO14443 type-A protocol. There are three types of frame patterns illustrated in Figure 4-3. The frame types are as follows: short; standard; and bit-oriented anti-collision frames. The purposes of each frame type are summarized in Table 4-5. This frame format is applied for both downlink and uplink. Each frame begins with a start bit and ends with an end bit. Transmission starts with the LSB of the lowest byte of transmission data. Each byte is transmitted with an odd parity. For more information, please refer to ISO14443-3.

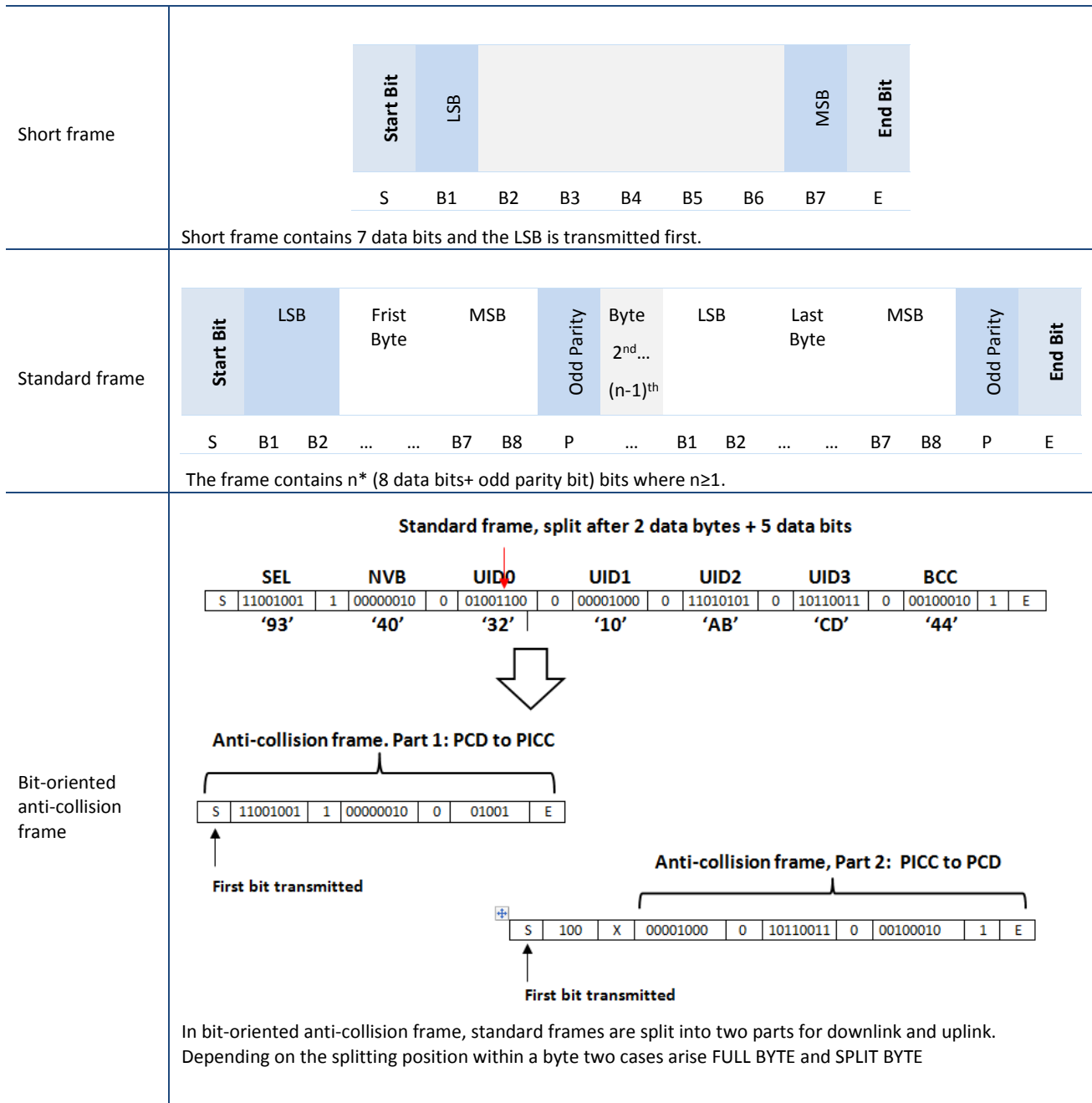


Figure 4-3: Frame format for RF communication

Table 4-5: Information to code with the uplink sequences

Frame type	Purpose	Command example
Short frame	Initiating	ISO14443A : <i>REQA, WUPA</i>
Standard frame	Transmitting regular command and data exchange between the transponder and NFC device.	ISO14443A : <i>SELECT1, SELECT2, HLTA, ReadE2, WriteE2, Compatible_WriteE2, PWD_AUTH, Read_Tamper</i>
Bit-oriented anti-collision frame	Transmitting and receiving data during anti-collision loops.	ISO14443A : <i>ANTI_COLLISION, ANTI_COLLISION2</i>

4.1.4 Timing

The commands and response timing of SIC43NT are according to the standard of frame delay time of the ISO 14443A. Based on the ISO14443A, there is frame guard time between downlink and uplink and vice versa. Downlink frame delay time is the guard time between end of the last pause transmitted by the NFC/RFID device and the first modulation edge of the start bit transmitted by the transponder. Depicted in Figure 4-4, the downlink frame delay time is $(n*128+84)/fc$ or $(n*128+20)/fc$ depending on end bit value ('0' or '1' respectively). The n value must be more than 9. The transponder response starts in a defined time slot. On the other hand, uplink frame delay is the guard time between the last modulation transmitted by the transponder and the first pause transmitted by the NFC/RFID, which is approximately at least $1172/fc$ or $87 \mu s$. The uplink frame delay is shown in Figure 4-5.

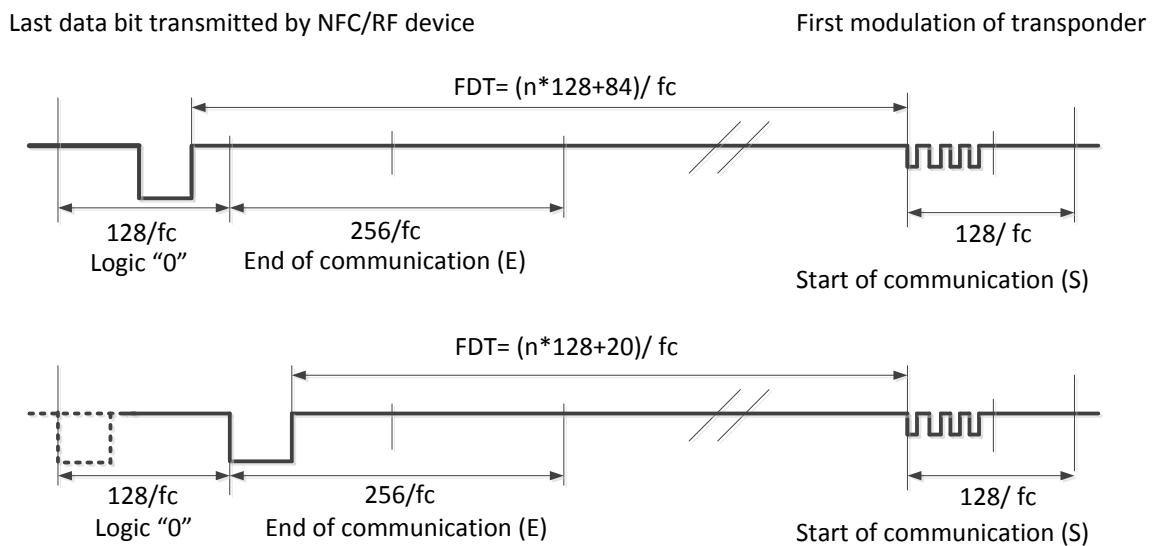


Figure 4-4: Downlink frame delay time

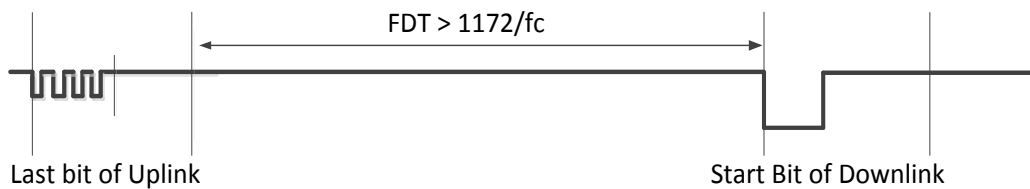


Figure 4-5: Uplink frame delay time

4.1.5 State of operation

When SIC43NT receives an operational command from the NFC/RFID device, the digital controller processes incoming commands and operates based on a current state. Figure 4-6 depicts the SIC43NT’s state diagram.

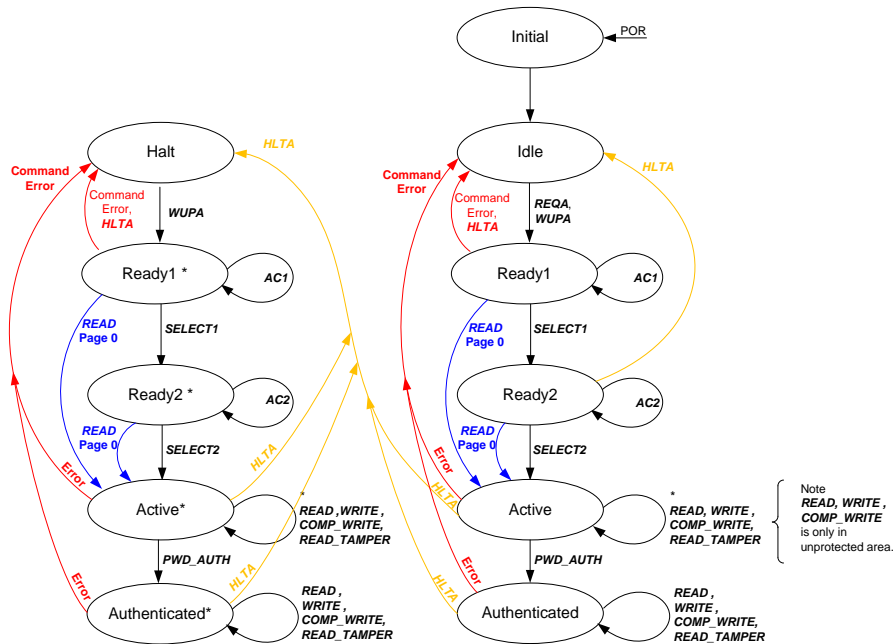


Figure 4-6: State of operation

Initial state: After powering up from the RF field, the state of SIC43NT enters the “Initial” state to initialize itself. In this state, the digital controller loads the pre-programmed configuration 0 and configuration 1 from the EEPROM to initialize pin RFD before entering “Idle”. Entering this state can also occur when the RF field is absent more than 10 us and the RF field reenergizes the power.

Halt & Idle state: After initialization, SIC43NT’s state stays in “Idle” waiting for WUPA or REQA to move the state to “Ready1”. Any other commands obtained in this state are considered as errors and the tag remains in the same state. Another equivalent state “Halt”, entered from the HLTA command is optionally for multiple-tag accessing in the same field. Only the WUPA command can make SIC43NT leave this state to “Ready1*”.

Ready1 & Ready1*: In this state, the digital controller expects a matched SELECT1 or ANTI-COLLISION1. For the ANTI-COLLISION1, SIC43NT responds the rest of UID. For the SELECT1, when a cascaded level1 UID matches, the digital controller responds SAK (0x04) and transits to “Ready2”. Except command Read accessing into page 0, any other commands obtained in this state are considered as errors and the digital controller returns to “Idle” or “Halt”. Reading page 0 in state “Ready1” or “Ready1*”, results in transition directly to “Active” or “Active*”.

Ready2 & Ready2*: In this state, the digital controller expects a matched SELECT2 or ANTI-COLLISION2. For the ANTI-COLLISION2, SIC43NT responds the rest of UID. For the SELECT2, when a cascaded level-2 UID matches, the digital controller responds SAK (0x00) and transits to the state “Active”. Except command Read accessing into page 0, any other commands obtained in this state are considered as errors and digital controller returns to “Idle” or “Halt”. Reading page 0 in state “Ready1” or “Ready1*”, results in transition directly to “Active” or “Active*”.

Active & Active*: In this state, the RFID-memory access commands ReadE2, WriteE2, Compatible WriteE2 can access the unprotected memory area, the page address having number lower than AUTH0 value. Also, command Read_Tamper can be applicable in this state.

Authenticated & Authenticated*: To access the protected memory areas, the reader shall send PWD_AUTH with a matched pre-defined password to enter this state. In this state, commands ReadE2, WriteE2, Compatible WriteE2 can access the entire memory as well as the protected area.

The digital state leaves “Active” or “Active*” or “Authenticated”/“Authenticated*” and switches to “Halt” by the HLTA command. If RF communication error or memory access error occurs in “Active”/“Active*” or “Authenticated”/“Authenticated*”, the digital controller replies a 4-bit NAK and returns to “Idle” or “Halt” depending on the previous state (State or State*).

5. Memory Configuration

5.1 EEPROM Organization

SIC43NT contains a 144 bytes of non-volatile EEPROM memory for user, and 48 bytes for UID and other user configurations. Figure 5-1 shows the EEPROM memory organization. The green section of the memory is the NFC static memory area and the rest of memory are the dynamic memory areas. The **UID**, the **Static Lock** value, and the **OTP** are stored in the NFC static memory area while the **Dynamic Lock** value (blue area) and the user **Configuration** (pink area) are stored in NFC dynamic memory area. The memory configuration is designed to conform the Tag Type 2 arrangement and the writeable Lock-control TLV block (TLV1) based on NFC NDEF standard.

Page (Hex)	Page (Dec)	Byte 0	Byte 1	Byte 2	Byte 3	Memory Type	Description	Note	
0x00	0	UID0	UID1	UID2	BCC0	R/O	UID / Lock	64-byte NFC Static Memory	
0x01	1	UID3	UID4	UID5	UID6	R/O			
0x02	2	BCC1		Lock0	Lock1	R/O, R/W-(OTP)			
0x03	3	OTP0	OTP1	OTP2	OTP3	R/W-(OTP)			
0x04	4	Data R/W	Data R/W	Data R/W	Data R/W	R/W	48-byte User Data		
...	...	Data R/W	Data R/W	Data R/W	Data R/W	R/W			
0x0F	15	Data R/W	Data R/W	Data R/W	Data R/W	R/W			
0x10	16	Data R/W	Data R/W	Data R/W	Data R/W	R/W	96-byte User Data		NFC Dynamic Memory
...	...	Data R/W	Data R/W	Data R/W	Data R/W	R/W			
0x27	39	Data R/W	Data R/W	Data R/W	Data R/W	R/W			
0x28	40	Lock2	Lock3	Lock4		R/W-(OTP)	Lock Byte		
0x29	41	FDP	Tdata0	DYN_PAGE_PTR	AUTH0	R/W	Configuration 0		
0x2A	42	AUTHL	Tdata1	RFD_CFG	DYN_DATA_CFG	R/W	Configuration 1		
0x2B	43	PWD	PWD	PWD	PWD	W/O	Password		
0x2C	44	PACK	PACK			W/O	Password ACK		
0x2D	45	KEY9	KEY8	KEY7	KEY6	W/O	KEY9-6		
0x2E	46	KEY5	KEY4	KEY3	KEY2	W/O	KEY5-2		
0x2F	47	KEY1	KEY0			W/O	KEY1-0		
0x30	48	IV3	IV2	IV1	IV0	R/W	Ini. Vector		

Figure 5-1: SIC43NT EEPROM memory map

Each data byte in the memory are described in details in the following sections.

5.2 UID

The **UID** value is a unique factory pre-programmed, write-protected, identification number that is composed of a 7-byte serial number along with its two check bytes (BCC0, BCC1). The **UID** value is stored in byte 0 of page 0 to byte 0 of page 3 of the EEPROM as depicted in Figure 5-1. When SIC43NT receives an **ANTI-COLLISION** command, it responds with the **UID** value or remaining part of the **UID** value. **BCC** is kept in the EEPROM during manufacturing to ensure that the **UID** value is uplinked correctly. Noted that UID0 is set to 0x39, and UID1 is set to 0x49.

Bytes 2 and 3 of page 2 of the EEPROM memory contain the static lock bytes named **Lock Byte0** and **Lock Byte1**. Each lock bit controls programmability of the specified page address or corresponding group of lock bits itself. When a certain lock bit in **Lock Byte0** or **Lock Byte1** is set to '1', the value in the addressed page cannot be changed. Bits of these lock bytes are one-time program (OTP). Therefore, once it is programmed to '1', such a bit cannot be cleared back to '0'.

Three LSB bits of **Lock Byte0** function as lock control bits of the lock-bits of the static user memory itself. When an individual bit in these three LSB bits is set, the corresponding page lock bit values cannot be altered and the addressed pages remain in locked or unlocked state based on the last individual lock bit value. Note that the new lock bit values take effect immediately after programming.

Byte in Page 2 (Page 0x02)		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 2	Lock Byte 0	Lock Page 7	Lock Page 6	Lock Page 5	Lock Page 4	Lock Page OTP	Lock of Lock Bit 15-10	Lock of Lock Bit 9-4	Lock of OTP Lock Bit
Byte 3	Lock Byte 1	Lock Page 15	Lock Page 14	Lock Page 13	Lock Page 12	Lock Page 11	Lock Page 10	Lock Page 9	Lock Page 8

Figure 5-2: Lock configuration in static memory

5.1 OTP

Page 3 of the EEPROM memory is the OTP page with four OTP bytes. All bits of these OTP bytes are set to '0' during manufacturing and can be programmed to '1' by the **WRITE** and **COMPATIBLE_WRITE** commands. Once any OTP bit are programmed to '1', these bits cannot be reprogrammed back to '0' by any write commands. The OTP programing behaviour is shown in Figure 5-3.

Byte in Page 3 (Page 0x03)	Byte 0	Byte 1	Byte 2	Byte3
Default value	0000 0000	0000 0000	0000 0000	0000 0000
Program with	1111 1111	0000 1100	0000 0101	0000 0000
Result in page 3	1111 1111	0000 1100	0000 0101	0000 0000
Program with	0000 0000	1111 1100	0000 0000	0000 0111
Result in page 3	1111 1111	1111 1100	0000 0101	0000 0111

Figure 5-3: OTP behavior in Page 3

5.2 User memory

If password protection is not enable, all memory address can be accessed by command **READ**, **WRITE** and **COMPATIBLE_WRITE**. In password protection mode, the authentication process with a matched password is required prior to accessing.

The organization of the EEPROM is designed to support the lock control TLV format. According to the NDEF standard, the location of CC in physical memory is located in page 3. The values in the OTP page and the user memory are all left as '0' as default values.

To make the tag ready for NFC deployment, example value of the CC and the blank NDEF value are shown in Figure 5-4, Figure 5-5 and Figure 5-6.

Page address	Byte number with in page			
	0	1	2	3
0x03	CC			
	Magic number 0xE1	Version (0x10)	Memory Size (0x12)	R/W access (0x00)
0x04	TLV-01-Lock			
	TLV header	TLV # byte	Lock location	# lock bit
0x05	TLV-01-Lock			TLV-03-empty
	#Byte/LockBit & #Byte/Page			Terminator

Figure 5-4: NDEF value in page 0x03 to 0x05 for NFC tag

Page address	Byte number with in page			
	0	1	2	3
0x03	0xE1	0x10	0x12	0x00
0x04	0x01	0x03	0xA0	0x0C
0x05	0x34	0x03	0x00	0xFE

Figure 5-5: Memory content in page 0x03 to 0x05 (Lock bit Style 1)

Page address	Byte number with in page			
	0	1	2	3
0x03	0xE1	0x10	0x12	0x00
0x04	0x01	0x03	0xA0	0x06
0x05	0x44	0x03	0x00	0xFE

Figure 5-6: Memory content in page 0x03 to 0x05 for 144 bytes (Lock bit Style 2)

5.3 Dynamic lock byte

Page 0x28 of the EEPROM contains the **Dynamic lock** bytes for the memory. Each bit of the **Dynamic lock** bytes sets an associated read/write memory area to be read-only. The lock configuration of the dynamic memory is shown in Figure 5-7 and 5-8. The new lock bit values take effect immediately after begin programmed. The lock bit format can be set in two different styles. As a result, there are two possible formats of CC and NDEF.

Byte in Page 40 (Page 0x28)		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 0	Lock Byte 2	Lock Page 30-31	Lock Page 28-29	Lock Page 26-27	Lock Page 24-25	Lock Page 22-23	Lock Page 20-21	Lock Page 18-19	Lock Page 16-17
Byte 1	Lock Byte 3	Lock Ini. IV	Lock Key	RFU (OTP)	RFU (OTP)	Lock Page 38-39	Lock Page 36-37	Lock Page 34-35	Lock Page 32-33
Byte 2	Lock Byte 4	RFU (OTP)	RFU (OTP)	Lock of Lock Page 36-39	Lock of Lock Page 32-35	Lock of Lock Page 28-31	Lock of Lock Page 24-27	Lock of Lock Page 20-23	Lock of Lock Page 16-19
Byte 3	Lock Byte 5	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)

Figure 5-7: Lock configuration of dynamic memory for 144-byte user memory configuration (Lock bit Style 1)

Byte in Page 40 (Page 0x28)		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 0	Lock Byte 2	Lock Page 36-39	Lock Page 32-35	Lock Page 28-31	lock of Locking Bit 5-7 (Page 28-39)	Lock Page 24-27	Lock Page 20-23	Lock Page 16-19	lock of Locking Bit 1-3 (Lock Page 16-27)
Byte 1	Lock Byte 3	Lock Ini. IV	Lock Key	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)
Byte 2	Lock Byte 4	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)
Byte 3	Lock Byte 5	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)	RFU (OTP)

Figure 5-8: Lock configuration of dynamic memory for 144-byte user memory configuration (Lock bit Style 2)

5.3.1 Lock_Key

Lock_Key is located at Byte1, Bit6 of the dynamic lock page. When **Lock_Key** is set to '1', the **Key9-0** of rolling code's configuration is no longer changeable.

5.3.2 Lock_IniIV

Lock_IniIV is located at Byte1, Bit7 of the dynamic lock page. When **Lock_IniIV** is set to '1', the **IV3-0** of rolling code's configuration becomes read-only, and cannot be reprogrammed anymore.

5.4 User Configuration

The last eight pages of memory store user configuration consisting of:

- **Configuration 0;**
- **Configuration 1;**
- **Password (PWD);**
- **Password acknowledge (PACK);**
- **Key of Rolling code (KEY); and**
- **Initial vector (IV) of the time stamp (TS) used for rolling code generation.**

These configurations allow user to set behavior of the SIC43NT for:

- (1) Behavior and function of the field detection pin;
- (2) Dynamic NDEF configuration;
- (3) Password protection;
- (4) Lock control for user configuration; and
- (5) Rolling code configuration.

When the **Configuration 0, Configuration 1, KEY** and **IV** are updated, the new values take effect after power on reset while the **PWD** and **PACK** take effect after programming immediately.

5.4.1 User Configuration 0

Figure 5-9 shows the byte arrangement of **Configuration 0** containing **FDP** in Byte 0, **Tdata0** in Byte 1, **DYN_PAGE_PTR** in Byte 2 and **AUTH0** in Byte 3.

Configuration 0 (0x29)	Byte 0	Byte 1	Byte 2	Byte 3
Name	FDP	Tdata0	DYN_PAGE_PTR	AUTH0
Default (Delivery format)	0x03	0x46	0x00	0xFF

Figure 5-9: Configuration 0

5.4.1.1 FDP

Figure 5-10 shows the Field Detect Pin configuration bits (**FDP**). It consists of the field detect trigger event (**FDT**), the sleep enable (**SleepEN**), and dynamic byte pointer (**DYN_BYTE_PTR**).

The **FDT** bits controls when the **RFD** in RF detection mode generates signal to wake up an MCU. Available options are after the first **SOF**, after the **SELECT** command, or when RF field is presented. **RFD** output can be disable by setting the value to 00b.

When **SleepEN** bit is set to '1', forcing logic low at the pin **RFD** during start up makes SIC43NT enters sleep state. In sleep state no RF communication can be operated.

DYN_BYTE_PTR bits are stored in FDP.[5:4]. These 2 bits specify the byte position within the starting page of dynamic NDEF data.

FDP Bit	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Name			DYN_BYTE_PTR		SleepEN		FDT	
Function			The 2 bits define the byte position within the start of dynamic NDEF data		0 : Sleep Disable 1 : Sleep Enable		Field Detect pin trigger event 00 – No Field Detect 01 – 1 st SOF 10 – Select 11 – Field Present	
Default (Delivery format)	0	0	00		0	0	11	

Figure 5-10: Field Detect Pin (**FDP**) configuration

5.4.1.2 Tdata0

The byte **Tdata0** is a user data configuration to represent tamper evidence detection status in dynamic NDEF data when the tampering state is detected. This value is recommended to be in readable ASCII format. The default value is configured to 0x46 that corresponds to alphabet "F" in ASCII format.

5.4.1.3 DYN_PAGE_PTR

DYN_PAGE_PTR byte defines the page that the beginning of dynamic NDEF data is located. See Section 7 for more information on dynamic NDEF data.

In order to enable the dynamic NDEF function. Users should set this byte to value that meet the following conditions. Otherwise, the dynamic data will not be mirrored into the NDEF message.

- **DYN_PAGE_PTR** is between page 0x04 and page 0x27
- The last byte of the dynamic data is located within the user memory area. The end of user memory area is byte 3 of page 0x27. The location of the last byte of dynamic data (**LAST_PAGE_PTR** and **LAST_BYTE_PTR**) can be calculated by the equation in Figure 7-2.
- If **LAST_PAGE_PTR** is located in the protected memory area, i.e. **LAST_PAGE_ADDRESS** >= **AUTH0**, dynamic NDEF mirror will be disabled until the tag receive a valid **PWD_AUTH** command.
- **DYN_PAGE_PTR** is by default set to 0x00, which means that dynamic NDEF function is disabled by default.

5.4.1.4 AUTH0

AUTH0 byte specifies the first page that password mechanism protects. Accessing address higher or equal than the value in **AUTH0** requires authentication with a matched password. The delivery value of **AUTH0** is 0xFF, which means the entire memory area is not protected.

5.4.2 User Configuration 1

Figure 5-11 shows byte arrangement of **Configuration 1** containing **Protection**, **Tdata1**, **RFDCFG** and **DYN_DATA_CFG**.

Configuration 1 (0x2A)	Byte 0	Byte 1	Byte 2	Byte 3
Name	Protection	Tdata1	RFDCFG	DYN_DATA_CFG
Default (Delivery format)	0x00	0x46	0x00	0xC0

Figure 5-11: Configuration 1

5.4.2.1 Protection

Figure 5-12 shows bit arrangement of **Protection** byte consisting of **PROT**, **CFGLOCK**, and **AUTHLIM**.

PROT bit defines protection method to be either write protection only or read/write protection for the in protected memory.

CFGLOCK bit is the lock bit for both **Configuration0** and **Configuration1**. If **CFGLOCK** is set to '1', the values in **Configuration0** and **Configuration1** cannot be changed. The lock is effective after power resets.

AUTHLIM bits defines the maximum number of incorrect authentication allowed. If **AUTHLIM** is set to a value other than 000b and an incorrect password occurs during authentication process, the tag counts the number of the incorrect attempt and records it in the EEPROM. If the number of failed authentication equals to the value of **AUTHLIM**, further authentication is rejected and the protected area is no longer accessible. If authentication with a valid password occurs before the internal counter reaches the limit, the internal counter is reset. Recording of incorrect counting is an anti-tearing process. If **AUTHLIM** is set to 000b, protection mechanism from incorrect authentication is disable.

Protection (Config1.Byte0)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Name	PROT	CFGLOCK				AUTHLIM		
Function	Accessing Protection 0 : Write Access is protected by password. 1 : Read and Write access is protected by password.	Lock bit of Configuration 0 and Configuration 1 0 : User configuration is open to write. 1 : User configuration is permanently locked for write access				Limitation of negative password verification attempt 000b : limiting of negative password verification attempted is disabled. 001b-111b : AUTHLIM value defines the maximum number of negative password verification attempt.		
Default (Delivery format)	0	0	0	0	0	000		

Figure 5-12: Protection configuration

5.4.2.2 Tdata1

The byte **Tdata1** has the same function as **Tdata0**. **Tdata1** is placed after **Tdata0** in tamper status field of the dynamic NDEF message.

The default value is configured to 0x46 that corresponds to alphabet "F" in ASCII format

5.4.2.3 RFDCFG

RFDCFG byte is used to control the **RFD** pin behavior as shown in Figure 5-13. **RFDCFG** consists of the control bits as follows **AutoDetEn**, **TamperConf**, **TamperMD**, **TamperST**, **OutputType**, and **AutoProgTamper**. Pin **RFD** can be configured to be an output to send trigger signal when RF signal is detected (**TamperMD** = '0'), or an input for tamper evidence detection mode (**TamperMD** = '1').

When the pin **RFD** operates in the RF detection mode, the related control bits are **OutputType** and **AutoDetEn**. **OutputType** defines output characteristic, which can be either open drain (**OutputType** = '0') or 1.8 V push-pull (**OutputType** = '1'). **AutoDetEn** enables automatic I/O sensing mechanism to define a proper I/O characteristic. Note that **OutputType** is only effective when **AutoDetEn** is set to '0'. If **AutoDetEn** is set to '1', the tag automatically senses the I/O logic level during power up. If the pin **RFD** is floating during start up, the output type is automatically set to push-pull mode. If the pin **RFD** is high during start up, the output type is automatically set to open drain mode to support external pull-up.

When the tamper detection mode is set (**TamperMD** = '1'), the pin **RFD** operates as an input with internal pull up. This **RFD** pin is normally tie to the tag's ground to indicate untampered state. If the conductor connecting the **RFD** pin and ground breaks, the logic level at the **RFD** pin will become '1' due to internal pull up. When the tag is powered up, it monitors the logic level of the **RFD** pin, if the tag is tampered, it will record the status in the EEPROM memory. Programming of the tamper status in the EEPROM is OTP.

TamperConf bits defines the biasing current for pulling up during tampering detection to mitigate noise interference. The higher the bias current is set, the lesser susceptibility to interference from environment the tag becomes. An example of interference is capacitive coupling from AC-power-line through human body to the torn conductor. The bias current is selectable from 0.8uA to 6.4uA. Typically, it is recommended to set **TamperConf** to "00b".

TamperST bit sets a scheme of tampering detection. The two available schemes are checking at power up only (**TamperST** is '1') or continuous checking (**TamperST** is '0').

To read tampering state, use command **Read_Tamper**. Please check section 8.2.5 for more information.

AutoProgTamper bit enables the auto-programing function for automatically updating tamper state into EEPROM memory. If **AutoProgTamper** is disable, any tamper event will not be recorded into the EEPROM.

RFDCFG (Config1.Byte2)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Name	AutoDetEn	TamperConf		TamperMD	TamperST	OutputType	AutoProgTamper	
Function	Automatic Pin Configuration Detection Enable 0 : Manual Configuration Pin behavior define from OutputType 1 : Auto Detect	Define Bias Current Strength for Tampering 00 – 6.4 uA 01 – 3.2 uA 10 – 1.6 uA 11 – 0.8 uA		Tampering Mode Enable 0 : RF detection Mode 1 : Tamper Mode	Tampering Checking Enable 0 : Check Tampering Continuously 1 : Check Tampering at Power up Only	Output of pin RFD in RF detection mode 0 : Open Drain 1 : Push-Pull (1.8V Output)	0: disabled 1: enabled	
Delivery format	0	0	0	0	0	0	0	0

Figure 5-13: RFDCFG byte configuration

Table 5-1: Effect of configuration on Pin RFD

Configuration Bit				Configuration Result		
TamperMD	SleepEN	AutoDetEn	OutputType	I/O	Type	Pin Behaviour
0	0	0	0	Output	Open Drain	Pull low when RF field is detected.
0	0	0	1	Output	Push Pull	Give logic high (1.8V) when RF field is detected
0	0	1	X	Output	Open Drain	If the pin is pulled high during start up. It will become open-drain. Pull low when RF field is detected
					Push Pull	If the pin is left floating during start up. It will become push-pull. Give logic high (1.8V) when RF field is detected
0	1	X	X	-	Float	Sleep mode is enable. If the pin is pull low during start up, the chip will enter sleep mode. It will not respond to any RF command.
1	X	X	X	Input	Input	Tamper detection mode

5.4.2.4 DYN_DATA_CFG

DYN_DATA_CFG consists of two groups of control configurations, which are 144_LockF and dynamic NDEF data control bits [TMP_CTRL_RLC, DYN_UID_EN, DYN_TMP_EN and DYN_RLC_EN].

144_LockF sets the style of the lock bits. Section 5.3, Figure 5-7, and Figure 5-8 describes lock bit arrangement for each style.

Dynamic NDEF data control bits consist of three following fields:

1. DYN_UID_EN enables presence of 14-byte, ASCII-formatted UID in dynamic NDEF data.
2. DYN_TMP_EN enables presence of Tdata0 and Tdata1 in the dynamic NDEF data in case the tag has been tampered. If the tag has not been tampered, Tdata0 and Tdata1 will be replaced by data 0x3030.
3. DYN_RLC_EN enables presence of 16-byte, ASCII-formatted Rolling Code (RLC) in dynamic NDEF data.

SIC43NT also provides 2 bits **TMP_CTRL_RLC** that control update of the rolling code according to the tamper status. This feature provides flexibility of starting/stopping the rolling code for various applications. The detail of its configuration is described in table below. When **TMP_CTRL_RLC** equals to 00b, **RLC** is a fixed value corresponding to the value of Time Stamp. This configuration is useful when the user wants a fixed unique rolling code for a specific tag.

MEMCFG (Config1.Byte3)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Name	TMP_CTRL_RLC		DYN_UID_EN	DYN_TMP_EN	DYN_RLC_EN	144_LockF		
Function	00: Rolling Code is always fixed. 01: Rolling Code runs when tamper evidence is detected 10: Rolling Code runs only when tamper evidence is not detected 11: Rolling Code will run regardless of the tamper status (default).		0: UID field in dynamic NDEF data disabled 1: UID field in dynamic NDEF data enabled	0: Tdata field in dynamic NDEF data disabled 1: Tdata field in dynamic NDEF data enabled	0: Tdata field in dynamic NDEF data disabled 1: Tdata field in dynamic NDEF data enabled	Lock Format for 144 Byte 0b: Lockbit Style 1 1b: Lockbit Style 2		
Delivery format	11		0	0	0	0	0	0

Figure 5-14: **DYN_DATA_CFG** byte configuration

5.4.3 Password (PWD) and Password Acknowledge (PACK)

The password protection is enabled by setting the **AUTH0** value to a page address within the user memory space. When SIC43NT receives a matched password, the digital state responses with two bytes **PACK**. **PWD** and **PACK** in the EEPROM memory are write-only bits. Reading these bits return zeros. To protect password from unauthorized modification, it is strongly recommended to set the **AUTH0** value to be less than or equal to the page 0x2B, where the **PWD** page is located.

5.4.4 KEY and Initial Vector (IV) of Rolling Code function

The rolling code generator uses 10 bytes of **KEY**. The MSB byte **KEY[9]** is stored into byte 0 of page 0x2D followed by **KEY[8]** in byte 1 of page 0x2D and continues to byte 1 of page 0x2F. **KEY** are write-only bits. Reading these bits returns zeros.

The 32 bits Initial Vector **IV** serves an initial value for the Time Stamp. A user can send **WriteE2** command at address 0x30 to initialize **IV** at any time. The data in this address will be automatically updated for generating next rolling code.

6. Rolling Code Generation

6.1 Time Stamp

Time Stamp (TS) is a 32-bit data stored in a dedicated section in the EEPROM memory. The TS is used by the Rolling Code Generator during *“Initial”* state to create the rolling code (RLC) section in the dynamic NDEF data.

During NDEF reading, if the last byte of the rolling code in the dynamic data is read and the update condition is met, the TS will be automatically updated for next rolling code generation. The configuration bits **TMP_CTRL_RLC** define TS update condition.

Table 6-1: Time Stamp Update Condition

TMP_CTRL_RLC	Time Stamp Update Condition
00	TS is never updated
01	TS is updated after tamper evidence is detected
10	TS is updated when tamper evidence is not detected. It will stop updating if the tamper evidence is detected.
11	TS is always updated regardless of tamper evidence.

TS is a monotonically-increasing number, i.e., the value of next TS will always be greater than the previous one. If the TS value reaches 0xFFFFFFFF, it will roll over to 0x00000000.

6.2 Rolling Code

Rolling Code Generator is a secure stream cipher operating as a pseudo-random generator. It uses 80 bits of KEY and 32 bit of Time Stamp (TS) stored in the EEPROM as inputs. Then, it generates 32 bits of rolling code (RND). The TS and RND are combined to create a 64-bit rolling code (RLC). Rolling code generation is enabled by setting **DYN_RLC_EN** bit to ‘1’.

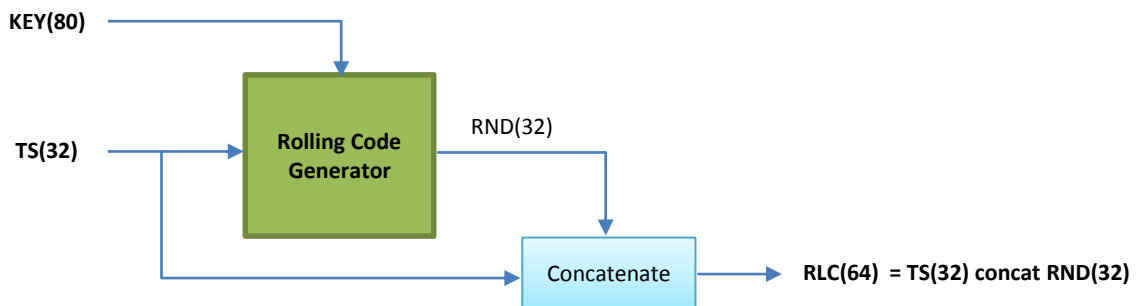


Figure 6-1: Rolling Code Generation Block Diagram

7. Dynamic NDEF Message

7.1 Dynamic NDEF Data Format

The dynamic NDEF data is formatted as shown in the following figure.

UID (ASCII format) 14 chars	Tdata 2 chars	Rolling Code RLC (ASCII format) 16 chars
--------------------------------	------------------	---

Figure 7-1 Dynamic NDEF Message Format

Note that the field UID and Rolling Code will be converted from hexadecimal data into ASCII-formatted character before being appended into the dynamic NDEF message. For example, the 7-byte UID of 0x E0 39 A1 B2 C3 D4 E5 read from the EEPROM memory will be converted to 14-byte ASCII-formatted data 0x 3339 4131 4232 4333 4434 4535.

Since there is no ASCII transformation of **Tdata**, the bytes **Tdata0** and **Tdata1** should be written in ASCII format.

The table below describes each data field in the NDEF message.

Table 7-1: NDEF Message Data Field

NDEF Message: www.sic.co.th/index.php?data=E039A1B2C3D4E5AA0000019BC5E4F7AC

Data Field	Number of characters	Description
www.sic.co.th/index.php?data=	Depends on user's URL	NDEF data defined by users in user memory area, the latter user-defined NDEF data will be replaced by the following Dynamic NDEF message.
E039A1B2C3D4E5	14	UID data that are mirrored into the NDEF message by properly defining DYN_PAGE_PTR byte and DYN_UID_EN bit. The chip automatically converts the hexadecimal UID data into ASCII-format data.
AA	2	Tamper evidence of the chip that is mirrored into the NDEF message by properly defining DYN_PAGE_PTR byte and DYN_TAMP_EN . If the chip is not tampered, these two characters will be "00". If the chip has been tampered, these characters will be defined by Tdata0 and Tdata1 bytes.
0000019BC5E4F7AC	16	Rolling code (RLC) that are mirrored into the NDEF message by properly defining DYN_PAGE_PTR byte and DYN_RLC_EN bit. The chip automatically converts the hexadecimal RLC data into ASCII-format data. RLC data are updated every time the tag enters "Initial" state after it is powered up.

7.2 Dynamic NDEF Data Configuration Bits

DYN_UID_EN, **DYN_TMP_EN** and **DYN_RLC_EN** are enabling bits for each field in dynamic NDEF data. These three bits could be independently set, resulting in different dynamic NDEF data format. The order of data fields inside the dynamic NDEF data is fixed by the order of **UID**, **Tamper Status (Tdata)**, and **Rolling Code (RLC)**. If any of these bits are disabled, the corresponding data field disappears from the NDEF message. When mirrored by **DYN_PAGE_PTR** byte these dynamic NDEF data will automatically replace original NDEF data programmed in the user memory.

The position within the memory where the dynamic NDEF shall start is defined by the **DYN_PAGE_PTR** and **DYN_BYTE_PTR**. The **DYN_PAGE_PTR** indicates the beginning page of dynamic NDEF data. The **DYN_BYTE_PTR** is used to point to the starting byte within **DYN_PAGE_PTR**.

The position of the last byte of the dynamic NDEF message can be calculated by the following equation.

$$nbBytePhy = (14 * DYN_UID_EN) + (2 * DYN_TMP_EN) + (16 * DYN_RLC_EN)$$

$$LAST_BYTE_PTR = (DYN_BYTE_PTR + nbBytePhy - 1) \text{ mod } 4$$

$$LAST_PAGE_PTR = DYN_PAGE_PTR + (DYN_BYTE_PTR + nbBytePhy - 1) / 4$$

Figure 7-2: Equation for calculating last location of dynamic NDEF message

The location of last byte of the user memory area is byte 0x03 of page 0x28. If the last byte of dynamic NDEF data is located outside of user memory area, dynamic NDEF message will not be mirrored into the NDEF message. In this case, physical data in the EEPROM will be read and uplink until the end of the NDEF message. Without correct **PWD_AUTH** command, dynamic NDEF function will be automatically disable when one part of dynamic NDEF data is inside the read-protected memory.

7.3 UID+RLC dynamic NDEF example

Table 7-2 shows the content of physical memory of SIC43NT. Without the dynamic NDEF function, the content would be:

sic43nt.co.th/?d=00000000000000000000000000000000

Table 7-2 UID+RLC dynamic NDEF data – Physical memory content

Page (Hex)	Page (Dec)	Byte 0	Byte 1	Byte 2	Byte 3	ASCII
0x00	0	0x39	0x49	0x0F	BCC0	
0x01	1	0x00	0x00	0x00	0x01	
0x02	2	BCC1		Lock0	Lock1	
0x03	3	0xE1	0x10	0x12	0x00	
0x04	4	0x01	0x03	0xA0	0x0C	
0x05	5	0x34	0x03	0x3A	0xD1	
0x06	6	0x01	0x36	0x55	0x03	
0x07	7	0x73	0x69	0x63	0x34	sic4
0x08	8	0x33	0x6E	0x74	0x2E	3nt.
0x09	9	0x73	0x69	0x63	0x2E	sic.
0x0A	10	0x63	0x6F	0x2E	0x74	co.t
0x0B	11	0x68	0x2F	0x3F	0x64	h/?d
0x0C	12	0x3D	0x30	0x30	0x30	=000
0x0D	13	0x30	0x30	0x30	0x30	0000
0x0E	14	0x30	0x30	0x30	0x30	0000
0x0F	15	0x30	0x30	0x30	0x30	0000
0x10	16	0x30	0x30	0x30	0x30	0000
0x11	17	0x30	0x30	0x30	0x30	0000
0x12	18	0x30	0x30	0x30	0x30	0000
0x13	19	0x30	0x30	0x30	0x30	0000
0x14	20	0x30	0xFE	0x00	0x00	0
...
0x27	39	0x00	0x00	0x00	0x00	
0x28	40	Lock2	Lock3	Lock4		
0x29	41	FDP 0x10	0x46	DYN_PAGE_PTR 0x0C	AUTH0	
0x2A	42	0x00	0x46	RFD_CFG	DYN_DATA_CFG 0xF8	
0x2B	43	PWD	PWD	PWD	PWD	
0x2C	44	PACK	PACK			
0x2D	45	KEY9	KEY8	KEY7	KEY6	
0x2E	46	KEY5	KEY4	KEY3	KEY2	
0x2F	47	KEY1	KEY0			
0x30	48	IV3	IV2	IV1	IV0	

The mirror function is able by setting bit **DYN_UID_EN** = 1b, **DYN_TMP_EN** = 1b, and **DYN_RLC_EN** = 1b in **DYN_DATA_CFG** byte. Also, the dynamic page and byte pointer must be properly set. From Table 7-2, setting **DYN_PAGE_PTR** = 0x0C, and **DYN_BYTE_PTR (FDP byte)** = 01b will result in the virtual memory map shown in Table 7-3.

The ASCII-formatted UID, tamper status, and ASCII-formatted RLC will be mapped into the memory address 0x0C byte 1. Users will see as if a part of the memory area is replaced by the dynamic NDEF data. However, actual physical data in the memory remain the same as shown in Table 7-2.

When reading the user memory area, the following data will be returned as an URL according to NDEF format.

sic43nt.co.th/?d=39490F00000001FF8899AABBCCDEEFF

Table 7-3 UID+RLC dynamic NDEF data – Virtual memory content

Page (Hex)	Page (Dec)	Byte 0	Byte 1	Byte 2	Byte 3	ASCII
0x00	0	0x39	0x49	0x0F	BCC0	
0x01	1	0x00	0x00	0x00	0x01	
0x02	2	BCC1		Lock0	Lock1	
0x03	3	0xE1	0x10	0x12	0x00	
0x04	4	0x01	0x03	0xA0	0x0C	
0x05	5	0x34	0x03	0x3A	0xD1	
0x06	6	0x01	0x36	0x55	0x03	
0x07	7	0x73	0x69	0x63	0x34	sic4
0x08	8	0x33	0x6E	0x74	0x2E	3nt.
0x09	9	0x73	0x69	0x63	0x2E	sic.
0x0A	10	0x63	0x6F	0x2E	0x74	co.t
0x0B	11	0x68	0x2F	0x3F	0x64	h/?d
0x0C	12	0x3D	0x33	0x39	0x34	=394
0x0D	13	0x39	0x30	0x46	0x30	90F0
0x0E	14	0x30	0x30	0x30	0x30	0000
0x0F	15	0x30	0x30	0x31	0x46	001F
0x10	16	0x46	0x38	0x38	0x39	F889
0x11	17	0x39	0x41	0x41	0x42	9AAB
0x12	18	0x42	0x43	0x43	0x44	BCCD
0x13	19	0x44	0x45	0x45	0x46	DEEF
0x14	20	0x46	0xFE	0x00	0x00	F
...
0x27	39	0x00	0x00	0x00	0x00	
0x28	40	Lock2	Lock3	Lock4		
0x29	41	FDP 0x10	0x46	DYN_PAGE_PTR 0x0C	AUTH0	
0x2A	42	0x00	0x46	RFD_CFG	DYN_DATA_CFG 0xF8	
0x2B	43	PWD	PWD	PWD	PWD	
0x2C	44	PACK	PACK			
0x2D	45	KEY9	KEY8	KEY7	KEY6	
0x2E	46	KEY5	KEY4	KEY3	KEY2	
0x2F	47	KEY1	KEY0			
0x30	48	IV3	IV2	IV1	IV0	

8. Commands

The SIC43NT supports two sets of commands: basic RFID commands, and data accessing commands.

8.1 Basic RFID commands

The basic RFID commands enable SIC43NT to communicate with NFC/RFID reader devices in both downlink and uplink mode. The commands are utilized for identifying the UID and accessing the EEPROM memory.

8.1.1 REQA

The **REQA** command changes SIC43NT in the “Idle” state into the “Ready1” state to prepare for further anti-collision and selection procedures. In response of **REQA**, the digital controller sends 2 bytes **ATQA** back to the NFC/RFID reader device. The ATQA of SIC43NT is to 0x0044. Note that the least significant byte (0x44) is transmitted first.

Table 8-1: **REQA** command format

CMD	REQA	
Format	0x26 (7 bits)	
Response	Successful operation	ATQA (0x0044)
	Error	No response
Operation	Change state from “Idle” state into “Ready1” state.	

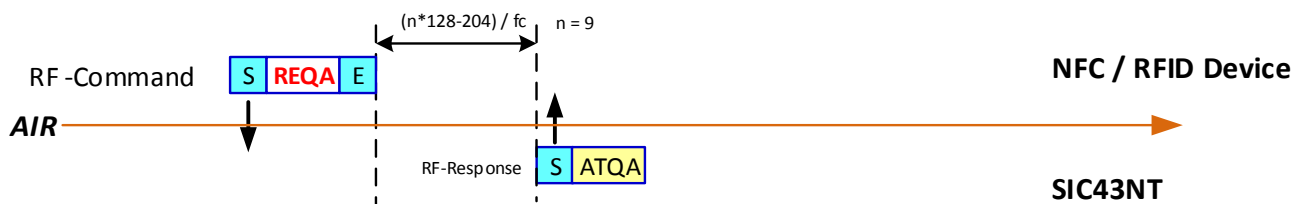


Figure 8-1: **REQA** command frame with a response

8.1.2 WUPA

The purpose of the **WUPA** command is the same as **REQA**. The only difference is that **WUPA** can be used in both “Idle” and “Halt” state.

Table 8-2: **WUPA** command format

CMD	WUPA	
Format	0x52 (7 bits)	
Response	Successful operation	ATQA (0x0044)
	Error	No response
Operation	Change state from “Idle” or “Halt” state into “Ready1” state.	

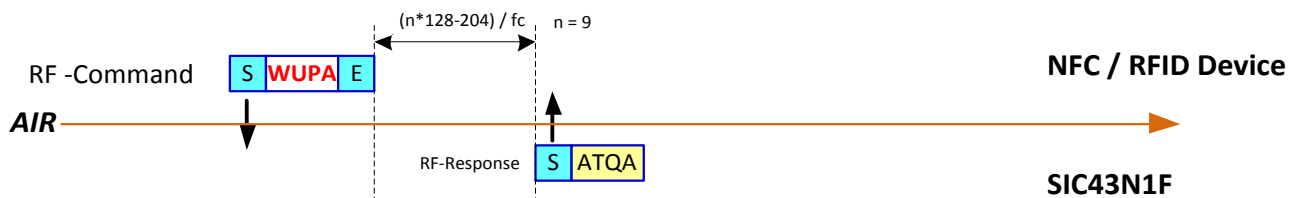


Figure 8-2: **WUPA** command frame with a response

8.1.3 ANTI-COLLISION

The **ANTI-COLLISION** command is used during the anti-collision procedure with bit oriented anti-collision frames. The purpose of **ANTI-COLLISION** command is to identify the target transponder and retrieve its UID. The **ANTI-COLLISION** command can be used in both cascade level 1, which states are “Ready1”, “Ready1*” and cascade level 2 which states are “Ready2” and “Ready2*” state. The **ANTI-COLLISION** command consists of the **SEL** code representing current cascaded level, the number of valid bits (**NVB**) and data. In the cascade level 1, the **SEL** code is 0x93 while the **SEL** code is 0x95 for the cascaded level 2. Transaction of the **ANTI-COLLISION** command and its response in both cascade level 1 and cascade level 2 are depicted in Figure 8-3 and Figure 8-4. For the cascade level 1, SIC43NT responds with the **CT** (cascade tag) code and the first 3-byte of UID. The **CT** code is 0x88.

Table 8-3: ANTI-COLLISION command format

CMD	ANTI-COLLISION	
Format	SEL + NVB + Data Cascade level1 : 0x93 + NVB + Data Cascade level2 : 0x95 + NVB + Data	
Response	Successful Operation	UID
	Error	No response
Operation	Response remaining part of UID and its BCC	

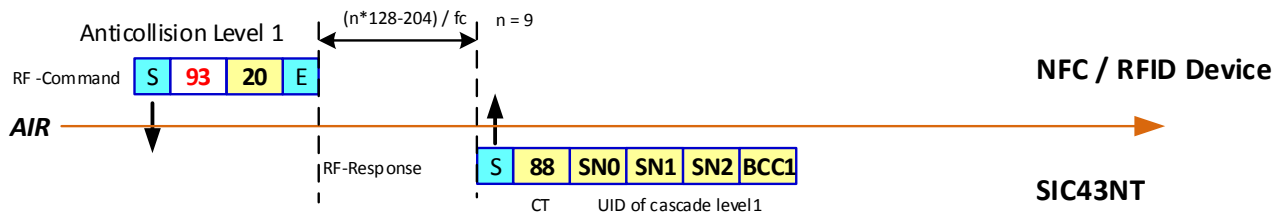


Figure 8-3 : ANTI-COLLISION in the cascade level 1 with a response

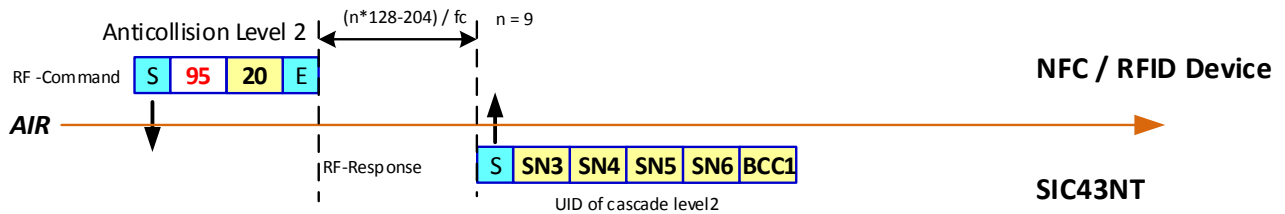


Figure 8-4 : ANTI-COLLISION in the cascade level 2 with a response

8.1.4 SELECT

The **SELECT** command format is based on the same structure as the **ANTI-COLLISION** command with 2-byte CRC appended at the end. SIC43NT responds to the NFC/RFID reader device with the **SAK** (select acknowledgement) code of 0x04 in **“Ready1”** and **“Ready1*”** state, indicating UID is not complete, and the **SAK** code of 0x00 in **“Ready2”** and **“Ready2*”**, indicating UID is complete. Then, the state changes to **“Active”** or **“Active*”**. Figure 8-5 and Figure 8-6 show the **SELECT** command for the cascade level 1 and cascade level 2, respectively.

Table 8-4: **SELECT** command format

CMD	SELECT	
Format	SEL + NVB + Data Cascade level1 : 0x93 + 0x70 + UID (4 bytes) + BCC + CRC Cascade level2 : 0x95 + 0x70 + UID (4 bytes) + BCC + CRC	
Response	Successful operation	SAK + CRC SAK = 0x04 for cascade level 1 SAK = 0x00 for cascade level 2
	Error	No response
Operation	Change state from “Ready1” or “Ready1*” to “Ready2” or “Ready2*” , or change state from “Ready2” or “Ready2*” to “Active” or “Active*” . Respond SAK (select acknowledgement).	

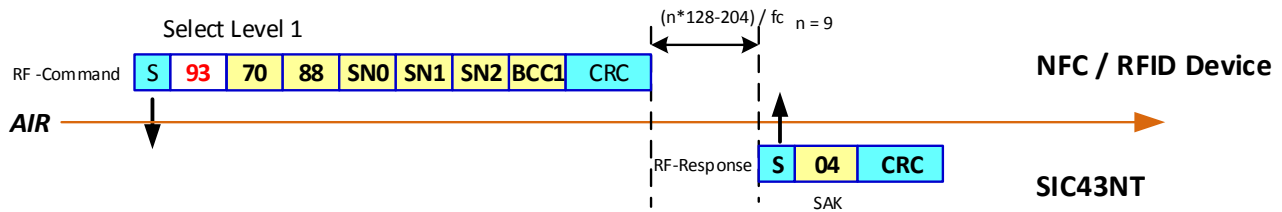


Figure 8-5: **SELECT** level1 command frame with a response

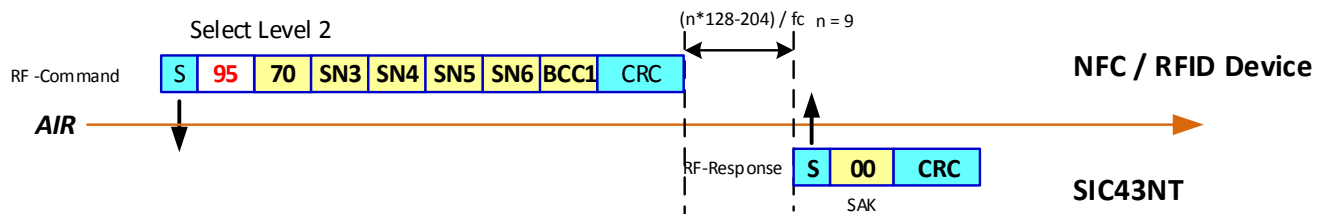


Figure 8-6: **SELECT** level2 command frame with a response

8.1.5 HLTA

The purpose of the **HLTA** command is to move transponder that is already processed into a waiting state. SIC43NT receiving **HLTA** in **“Active”** or **“Active*”** state changes its state to **“Halt”**. By using this command, the NFC/RFID reader device can identify the transponders that are already selected and those that have not yet been selected. The SIC43NT that receives **HLTA** in **“Ready1”** and **“Ready2”** changes to **“Idle”**. Receiving **HLTA** in other states changes the state to the **“Halt”** state. There is no response sent back to the NFC/RFID reader device for this command.

Table 8-5: **HLTA** command format

CMD	HLTA
Format	0x50 + 0x00 + CRC
Response	None
Operation	Change state from “Active” or “Active*” to “Halt” state



Figure 8-7: **HALT** command frame

8.2 Data accessing commands

8.2.1 ReadE2

The purpose of the **ReadE2** command is to read the EEPROM content. The **ReadE2** command contains a page address with a valid CRC. If the transponder gets a valid address in the command, it responds to the NFC/RFID reader by sending 16 bytes of data in 4 contiguous pages, starting from the addressed page. If the address is not valid, it sends a 4-bit NAK.

If AUTH0 is set within the user memory area, the memory area starting from the value of AUTH0 become protected. PWD_AUTH command is required prior to reading the protected address. Without PWD_AUTH, attempt to read the protected memory will result in NAK response.

For example, If AUTH0 is set to 0x0A and PWD_AUTH was not asserted, ReadE2 command at address 0x0A will return NAK. ReadE2 command at address 0x08 will return memory content of address 0x08, 0x09, 0x00, and 0x01.

Table 8-6: **ReadE2** command format

CMD	ReadE2	
Format	0x30 + Block + CRC (2 bytes)	
Response	Successful operation	BlockData (16 bytes) + CRC (2 bytes)
	Error	NAK (4 bits)
Operation	Read data from EEPROM at a specific address	

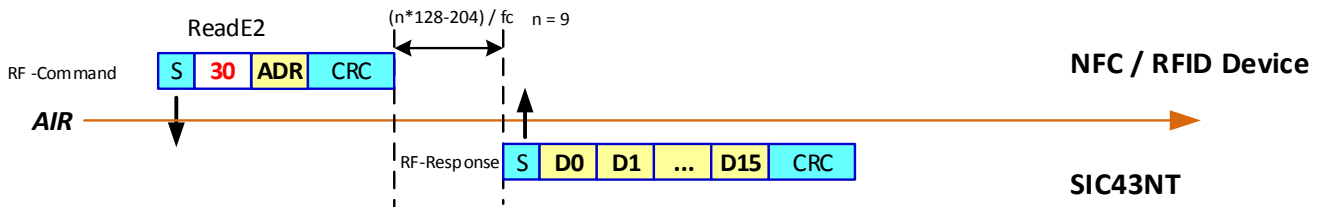


Figure 8-8: **ReadE2** command frame with response

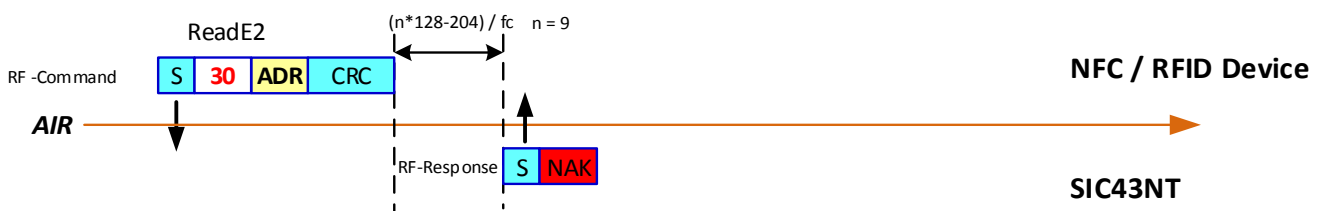


Figure 8-9: **ReadE2** command frame with a negative acknowledgement in response

8.2.2 WriteE2

The purpose of the **WriteE2** command is to write the EEPROM, program lock bits, OTP, and configuration. SIC43NT receiving the **WriteE2** command with a valid address in the "Active" or "Active*" state programs the received 4-byte data into the addressed page and sends an ACK to back the NFC/RFID reader device. If the address is not valid or the addressed page is already locked, SIC43NT responds with a NAK.

Table 8-7: **WriteE2** command format

CMD	WriteE2	
Format	0xA2 + ADR + D0 + D1 + D2 + D3 + CRC (2 bytes)	
Response	Successful operation	ACK (4 bits)
	Error	NAK (4 bits)
Operation	Check permission at the target address and write data to the EEPROM	

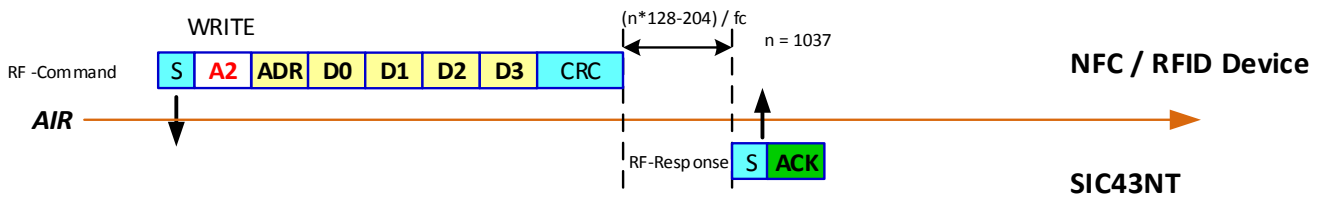


Figure 8-10: **WriteE2** command frame with an **ACK** response indicating successful operation

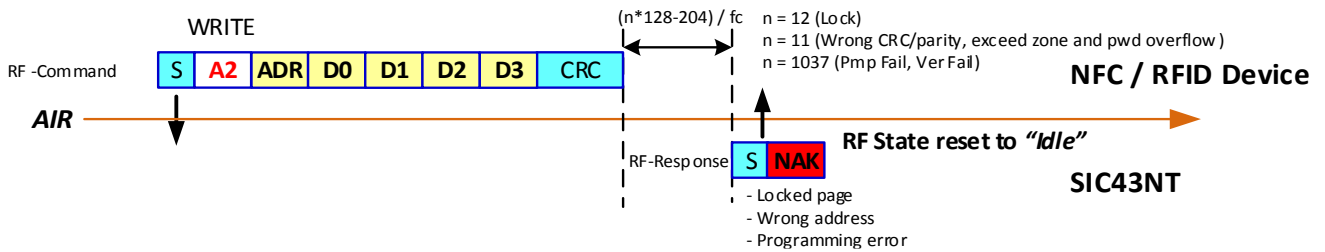


Figure 8-11: **WriteE2** command frame with a **NAK** response indicating unsuccessful operation

8.2.3 Compatible WriteE2

The purpose of the **Compatible WriteE2** command is to make programming process backward compatible with some reader system. The command contains a page address with a CRC. If SIC43NT gets a valid address, it responds with an **ACK**, else a **NAK**. The NFC/RFID reader device again sends 16-byte data but only the first 4 bytes are written into the memory. It is recommended to set the remaining bytes to '0's. Process of executing the **Compatible WriteE2** command is depicted in the Figure 8-12 and Figure 8-13.

Table 8-8: **Compatible WriteE2** command format

CMD	Compatible Write E2	
Format1	0xA0 + ADR + CRC (2 bytes)	
Response1	Successful operation	ACK (4 bits)
	Error	NAK (4 bits)
Format2	Block Data (16 bytes) + CRC (2 bytes)	
Response2	Successful operation	ACK (4 bits)
	Error	NAK (4 bits)
Operation	Check permission at target address and write data to EEPROM (only first 4 bytes are written)	

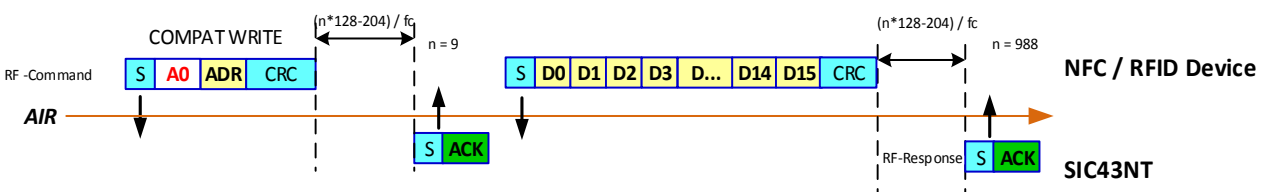


Figure 8-12: Two-step operation of **Compatible Write E2** with an **ACK** response

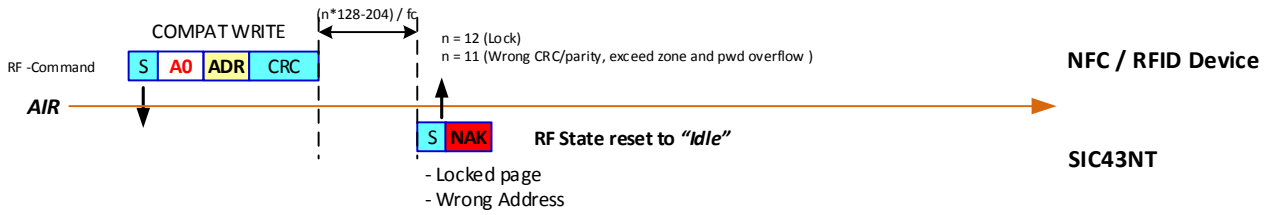


Figure 8-13: One-step operation of **Compatible Write E2** with a NAK response

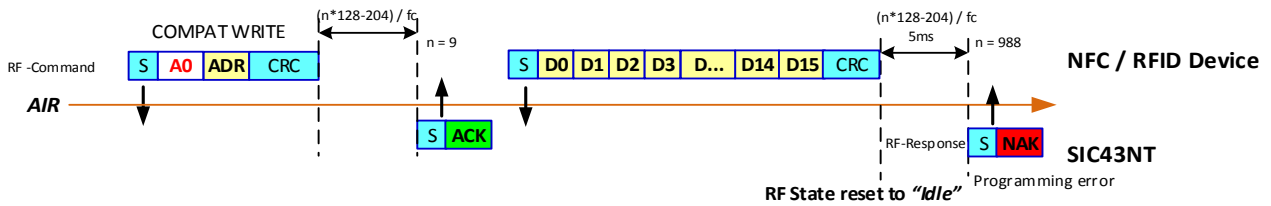


Figure 8-14: Two-step operation of **Compatible Write E2** with a NAK response

8.2.4 PWD_AUTH

The purpose of **PWD_AUTH** is for accessing to the protected memory. A memory address is protected if its address is higher than or equal to the **AUTH0** value. If the tag received a password that matches the stored password, authentication is successful. Then, SIC43NT responds with **PACK** and the state moves to **"Authenticated"** or **"Authenticated*"**. Then, the protected memory can be accessed by the read or write command. If the received password doesn't match, SIC43NT will not respond and the state goes back to **"Idle"**. If the number of incorrect authentication reaches the limit setting by **AUTHLIM**, SIC43NT responds with **NAK** and the protected memory area become locked and no longer be accessible.

Table 8-9: **PWD_AUTH** command format

CMD	Pass	
Format1	0x1B + PWD (4 bytes) + CRC (2 bytes)	
Response1	Successful operation	PACK (2 bytes) + CRC (2 bytes)
	Error	NAK (4 bits) (Authentication counter overflows) No Response (Incorrected password)
Operation	Grant permission to access the protected memory area. If operation is successful, state moves to "Authenticated" or "Authenticated*" .	

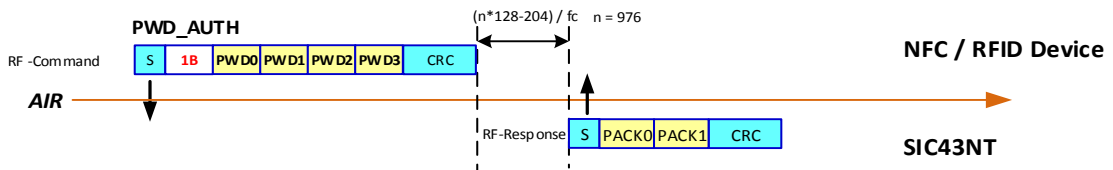


Figure 8-15: Successful authentication with matched password

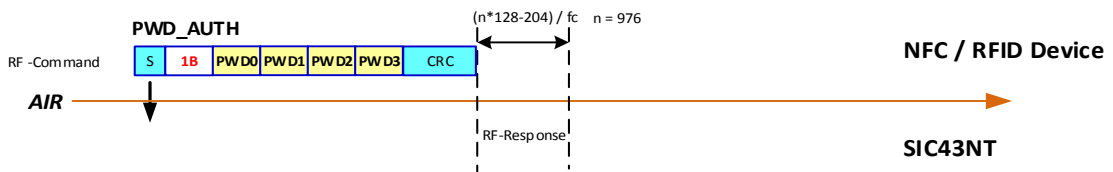


Figure 8-16: Fail authentication due to incorrect password

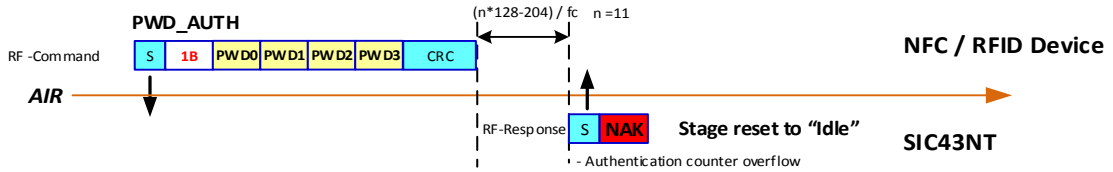


Figure 8-17: Fail authentication when authentication counter overflows

8.2.5 Read_Tamper

The **Read_Tamper** command is for reading the tamper evidence in the SIC43NT’s hidden memory. This command is applicable when the pin **RFD** is set in tampering detection mode. If there is no framing error, SIC43NT responds with two bytes indicating the tamper evidence. At delivery state, SIC43NT is set in untampered state. Reading the tamper evidence status gives all ‘0’s in the response. If the tag is already tampered, the response is all ‘1’.

Table 8-10: **Read_Tamper** command format

CMD	Read Tamper	
Format1	0xAF + 0x00 + CRC (2 bytes)	
Response1	Successful operation	0x00 + 0x00 + CRC (Tag is not tampered) 0xFF + 0xFF + CRC (Tag is tampered)
	Error	NAK (4 bits)
Operation	Read tampered status.	

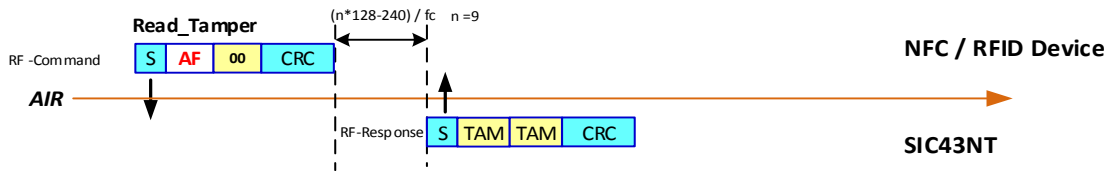


Figure 8-18: Successful Read_Tamper response

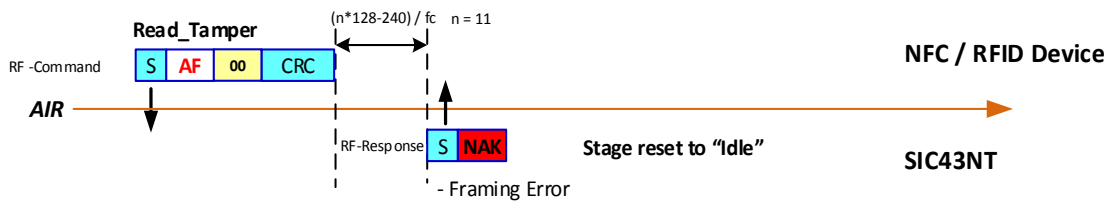


Figure 8-19: Fail Read_Tamper response due to framing error

8.3 Response Acknowledge

Apart from normal data response in **“Active”**, SIC43NT reports a 4-bit **ACK** (positive acknowledge) and a 4-bit **NAK** (negative-acknowledge), compliant to the NFC Tag Type 2 standard. SIC43NT responses the **NAK** (negative-acknowledge) for invalid downlink or operational errors. If SIC43NT answers with the 4-bit **NAK**, the RF state goes back to **“Idle”** or **“Halt”**. The response flag from operations are summarized in Table 8-11.

Table 8-11: 4-bits ACK/NAK

Response Flag	Code	Description
ACK	1010b	Positive acknowledge indicates operation is successful.
NAK	0000b	Negative acknowledge indicates <ul style="list-style-type: none"> - Accessing address is out of range, or - Programming a locked block, or - Accessing password protected area without authentication.
	0001b	Negative acknowledge indicates <ul style="list-style-type: none"> - Parity or CRC error.
	0100b	Negative acknowledge indicates <ul style="list-style-type: none"> - Authentication counter overflow.
	0101b	Negative acknowledge indicates <ul style="list-style-type: none"> - EEPROM programming error.

9. Packaging and Dimension

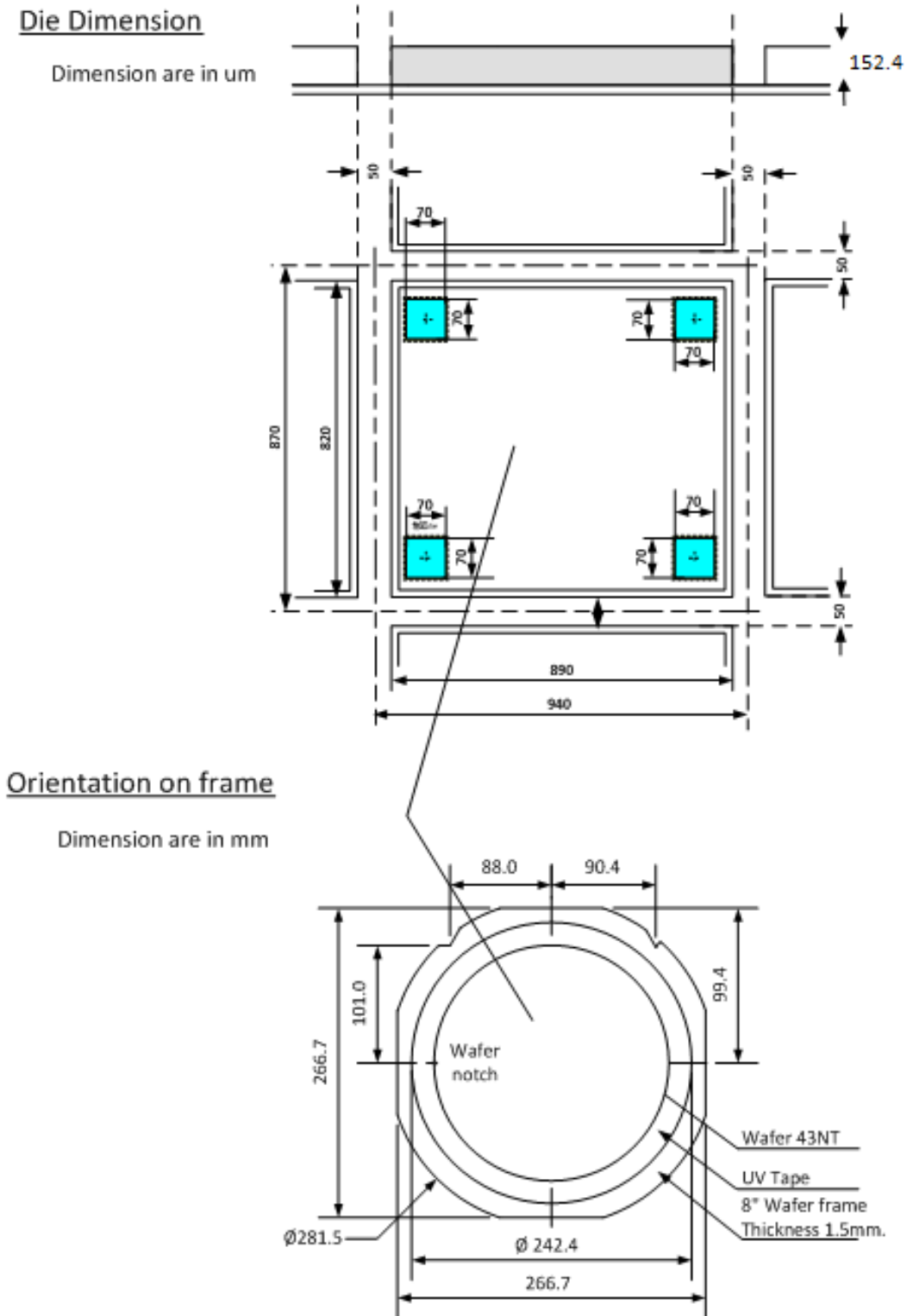


Figure 9-1: Die and Wafer Dimension

(All dimensions are in millimetre)

10. Disclaimer

- The information described herein is subject to change without notice.
- Although the IC contains a static electricity protection circuit, static electricity or voltage that exceeds the limit of the protection circuit should not be applied.
- Silicon Craft Technology assumes no responsibility for the way in which this IC is used in products created using this IC or for the specifications of that product, nor does Silicon Craft Technology assume any responsibility for any infringement of patents or copyrights by products that include this IC either in Thailand or in other countries.
- Silicon Craft Technology is not responsible for any problems caused by circuits or diagrams described herein whose related industrial properties, patents, or other rights belong to third parties. The application circuit examples explain typical applications of the products, and do not guarantee the success of any specific mass-production design.
- Use of the information described herein for other purposes and/or reproduction or copying without the express permission of Silicon Craft Technology is strictly prohibited.
- The products described herein cannot be used as part of any device or equipment affecting the human body, such as exercise equipment, medical equipment, security systems, gas equipment, or any apparatus installed in airplanes and other vehicles, without prior written permission of Silicon Craft Technology.
- Although Silicon Craft Technology exerts the greatest possible effort to ensure high quality and reliability, the failure or malfunction of semiconductor products may occur. The user of these products should therefore give thorough consideration to safety design, including redundancy, fire-prevention measures, and malfunction prevention, to prevent any accidents, fires, or community damage that may ensue.